THE PERCEPTION OF SECURITY IN SELECTED CONTEXTS

KAROLINE BUSSE

Dissertation zur Erlangung des Doktorgrades (Dr. rer. nat.)
der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt am: 20. Januar 2021

Karoline Busse (born in Neustadt am Rübenberge): *The Perception of Security in Selected Contexts*. Published in Bonn, 2021.
First examiner: Prof. Dr. Matthew Smith
Second examiner: Dr. Katharina Krombholz
The thesis was defended on July 1, 2021.

Any sufficiently advanced technology
is indistinguishable from magic.

— Clarke's third law

ABSTRACT

The perception of security has a strong impact on a person's choice of and interaction with security technology, especially within the context of Usable Security and Privacy research. This thesis sheds light on how people perceive security in their everyday lives through five studies embedded in selected contexts.

The individual narrative of security and its implications on work culture in IT security departments is examined and revealed that consciously shaping the narrative provides a powerful tool in the management of security workers. Mental models of encryption are investigated both in administrators and non-expert participants. Resulting meta models reveal the extent to which people can be confronted with technical details when dealing with secure systems. A replication of a study on security practices and advice is presented, highlighting fruitful improvements in Usable Security research and practice within the last years, and at the same time pointing to areas of action where secure technology still needs to improve before non-expert users can adopt it effortlessly. Security and privacy habits in payment and banking are investigated across four countries, revealing culturally-specific differences in security perception and credential management behavior. Last but not least, the effect of incentives on adopting secure technology and user perceptions of two-factor authentication are investigated to reveal the differentiation and evaluation process when selecting security measures.

Thus, this thesis contributes to a broader understanding of the human factor within the context of security by showing how mental models and personal influences shape the perception of security and influence the general awareness of relevant threats and corresponding measures. It furthermore highlights that mistrust and negative impressions are powerful inhibitors in the context of perception.

PUBLICATIONS

Some parts of this work have appeared previously in the following publications:

[1] Karoline Busse, Sabrina Amft, Daniel Hecker, and Emanuel von Zezschwitz. "Get a Free Item Pack with Every Activation!" In: *i-com* 18.3 (2019), pp. 217–236.

[2] Karoline Busse, Julia Schäfer, and Matthew Smith. "Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice." In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019. URL: https://www.usenix.org/conference/soups2019/presentation/busse.

[3] Karoline Busse, Jennifer Seifert, and Matthew Smith. "Exploring the security narrative in the work context." In: *Journal of Cybersecurity* 6.1 (Oct. 2020). ISSN: 2057-2085. URL: https://doi.org/10.1093/cybsec/tyaa011.

[4] Karoline Busse, Mohammad Tahaei, Katharina Krombholz, Emanuel von Zezschwitz, Matthew Smith, Jing Tian, and Wenyuan Xu. "Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries." In: *The 5th European Workshop on Usable Security*. Online: IEEE, 2020. URL: https://eusec20.cs.uchicago.edu/eusec20-Busse.pdf.

[5] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. ""If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS." In: *S&P 2019*. 2019. URL: https://publications.cispa.saarland/2788/.

Authorship agreements can be found in Appendix F.

ACKNOWLEDGMENT

This work would not have been possible without the help and assistance of others.

I would like to thank Matthew Smith and Katharina Krombholz for their support along my way, both professionally and personally. Additional thanks go out to my colleagues and collaborators, especially Yasemin, Jennifer, Maxi, Chris, Maria, Sabrina, Julia, and Mohammad. I am glad to have such a supporting and encouraging network.

Last but not least, I want to thank my family and especially Oliver for enabling me to start my academic journey at all and watching my back with strength and support through all that stressful and difficult time.

Thank you.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Most people[1] have a rather complicated relationship with security and privacy. When asked directly, they value it as an important factor in their digital lives and often claim to lay emphasis on security and privacy when browsing, selecting products or services, or conducing everyday businesses. On the other hand, we have evidence that people choose weak passwords and tend to recycle them [62, 163], do not pay attention to browser warnings [201], or develop software without security considerations in mind unless explicitly prompted [161].

These phenomena arise because usually, security is a so-called *secondary goal* [225]. When it clashes with the primary task, such as shopping, messaging or sending a tax report, users often try to work around the mechanisms which can expose them to various threats. When such clashes can be identified, they usually indicate areas of improvement in technical tools and processes.

An example for this is the process of authentication on mobile devices. A smartphone user usually unlocks their phone about 40 times per day on average [99]. For every unlock event, a pattern or code has the be entered on the device. It is only natural that users want to keep this code as simple as possible so both the overhead in time and cognitive effort, and the false-positive rate when authenticating throughout the day stay low. Many users even switch to biometric authentication instead of patterns, which is even faster but from a security standpoint very insecure, as biometric features such as fingerprints cannot be easily changed in case of a compromise and are easy to copy.

Through this secondary nature, security is often perceived differently depending on the situation. Decisions are rather made according to the primary goal, which makes it hard to predict security behavior without the context of the primary task.

This is also why it is so hard to pin security practices down to a universal formula. When having faced this issue through the course of my thesis, I opted for a series of studies to highlight individual situations and scenarios around the perception of security rater than trying to capture an all-encompassing picture. Each study can stand for itself, but is also used to create a larger picture which I will discuss in detail in Chapter 9.

1.1 RESEARCH QUESTION AND APPROACH

The main research question which I will investigate in this thesis is:

1 Myself included

How do people perceive security in their everyday lives?

Giving a universal, all-encompassing answer to this is impossible. Therefore, I picked selected studies to research the perception of security in smaller contexts that can shape a space for user studies. From these insights gained in these studies, I will formulate more general observations on user and expert perception of security.

The problem fields I am going to investigate in this thesis are:

THE WORKPLACE CONTEXT. Here, we focused especially on security workers and researched how their narrative of *security* is shaped by their individual backgrounds as well as by their work. We distilled common narratives for each company and connected these to identify higher-order conflicts within each company that shape the power dynamics between employees and their team leaders.

THE DAILY USE OF ENCRYPTED MESSAGING AND BROWSING. We investigated expert and non-expert mental models of encryption in these cases and showed that many misconceptions exist, particularly of what security *https* connections offer. Following from the interviews in the study, two meta-models were constructed, summarizing common correct and incorrect conceptions of security in internet communication.

SECURITY ADVICE AND PRACTICES By replicating a study on expert and non-expert security advice and practices by Ion et al. [115], we shed light on current problem fields in security, which are deemed very important by experts but not regarded as well usable by users and experts alike. Two of these problem fields were addressed in this thesis.

PAYMENT AND BANKING CULTURE. With a large-scale survey deployed in four culturally distinct countries, we investigated security perceptions and trade-offs in China, Germany, Iran, and the United States. We highlighted the differences in payment cultures and how this influences security decisions, for example when sharing payment credentials.

THE ADOPTION DECISION FOR TWO-FACTOR AUTHENTICATION. We investigated the popularity of incentive offers for activating Two-Factor Authentication (2FA) within the online gaming context, distilled user perceptions and transferred these to non-gaming contexts. A focus group study was conducted to evaluate these design proposals and yielded further insights in the perception of 2FA.

1.2 MAIN CONTRIBUTION

This thesis contributes to the greater understanding of human-centered security and privacy by looking at the user perception of security in different contexts.

Starting from conceptual work about narratives and mental models, the scope broadens by encompassing habits and practices, as well as advice from security experts. Then, the field is narrowed down to a selection of use cases, where the perception of security is investigated in close detail to gain in-depth insights that allow for answering the research question. Eventually, the insights from the case studies are taken into context again and generalized in an effort to sufficiently answer the research question posed above.

The findings distilled from connecting these studies with each other shed light on how mental models shape the perception of security, and how they are influenced by different factors such as education, profession, socio-cultural situation or news coverage of security technology. This allows for a greater understanding on how security is perceived and especially how these perceptions come to be and interact with other influencing factors in cases such as the choice of adapting a security mechanism.

1.3 THESIS STRUCTURE

The remainder of this work is structured as follows:

First, the *Theoretical Background* on Usable Security as a research discipline, prominent concepts for understanding the presented research, as well as the study methodology are laid out in Chapter 2.

The following part on the conducted studies presented above features one study per chapter. The *Security Narrative* is presented in Chapter 4, the study on *Mental Models of Encryption* can be found in Chapter 5. Research on *Security Advice* is featured in Chapter 6. The cross-cultural investigation into *Security Perceptions in Payment and Banking* is documented in Chapter 7, and the study on *Incentives For Adopting 2FA* is featured in Chapter 8.

The second part of this thesis connects the insights from the case studies in Chapter 9 and concludes with Chapter **??**.

All relevant study materials such as questionnaires, and the detailed agreements on authorship of the studies are collected in the Appendix.

1.4 LIMITATION

This thesis is not without limitations, especially when addressing such a broad topic as perception research. In the following, the main drawbacks of this work are outlined.

First of all, the researched populations were very different: Germans and Austrians in Chapters 4, 5, 7, 8, international security experts in Chapter 6, gaming-focused international participants in Chapter 8, and US-American, Chinese, Iranian participants in Chapter 7. This limits the extent to which the observation and connections presented in Chapter 9 hold, they should not be taken as strong connections or correlations without proper care.

Given the common research and publication cycle in the field of (usable) security, longitudinal studies and long-term observations are scarce, this also holds true for this work. While we can at least set the results from Chapter 6 in context to the original study that was replicated, all other studies in this thesis represent momentary snap shots that might yield misleading findings for generalization. Such short periods of observation are particularly prone to influences of current news or trend topics of the time they were conducted at (cf. Sections 5.4 and 6.4). These influencing effects might have further propagated into discussing and concluding the work without the author's notice.

2 THEORETICAL BACKGROUND

2.1 USABLE SECURITY

The first formal definition of USEC was made by Zurko and Simon at the 1996 Workshop on New Security Paradigms. They coined the term *User-Centered Security* as "security models, mechanisms, systems, and software that have usability as a primary motivation or goal" [238]. They furthermore mentioned the groups of administrators, developers, and end-users as relevant audiences within the problem field.

In 1999, two papers were published that shaped the field until today.

Whitten and Tygar conducted a user study about PGP-encrypted email with twelve participants. The participants had to fulfill several tasks around a given scenario of an election campaign. Only four participants were able to correctly execute all tasks within the given time limit, three of the participants even leaked the secret they were to protect. This work painfully highlighted how security technology is implemented within a professional vacuum, leading to software that requires too much domain knowledge to operate it properly [226].

In the same year, Adams and Sasse published a study on password practices and perception within organizations. They published a questionnaire and followed up with interviews which allowed the participants to introduce new issues that they encounter in the context of password management and handling. The results clearly showed that password policies and design are not considering the needs of users. The paper demands for password mechanisms that are "compatible with organizational and work procedures", and to make security decisions and procedures more transparent to users [6].

In 2003, the Computing Research Organization has compiled four Grand Challenges for Security and Privacy Research. In the fourth of these challenges, "Secure the Ubiquitous Computing Environments of the Future", the need for Usable Security was strongly demanded:

> The fourth and final grand challenge is to protect our future technological base. For the dynamic, pervasive computing environments of the future, we will give computer end-users security they can understand and privacy they can control. Technology can easily outrun comprehensibility, and a trustworthy computing base should not make this worse. By the same token, identity will be many-faceted and ubiquitous in a world of pervasive computing, and individuals should be able to maintain control of it. [55]

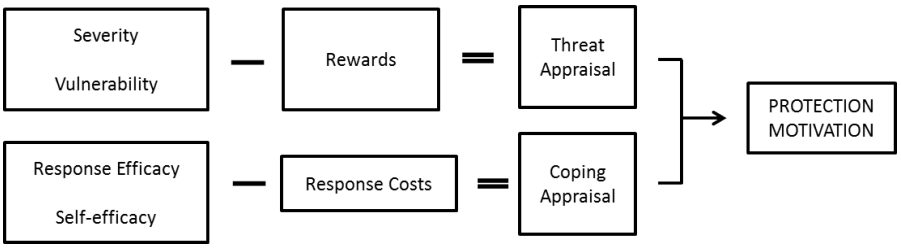


Figure 2.1: Key elements of the Protection Motivation Theory by Rogers [182]. Image CC BY-SA Suminshinoo/Wikimedia Commons.

As of today, USEC has become a prominent sub-discipline of security and privacy research with an active community and famed publications.

Perception research as a sub-topic of USEC has been present from the start, as the paper by Adams and Sasse already featured perception aspects [6]. Originally, security perception research roots in psychology, for example in the Protection Motivation Theory (PMT) formulated by Rogers [182].

PMT was developed to research the motivation of fear appeals, for example related to health risks and practice, but also applicable to security scenarios. As Figure 2.1 shows, the perceived severity of a threat as well as the personal assessment of vulnerability to said threat are related to the rewards stemming from potential protection. This relation is called the *Threat Appraisal*. On the other hand, the efficacy of the proposed response as well as the perceived self-efficacy are weighed against the predicted response costs. This forms the *Coping Appraisal* [182].

Within the PMT model, USEC aims to positively influence the Coping Appraisal by lowering response costs and increasing response efficacy through well-designed systems. Furthermore, USEC aims to positively influence self-efficacy through user empowerment and a general change of culture. Instead of seeing the cause for a security incident in the user, it is more likely the inadequate design and implementation of secure systems that lead to an incident [6].

2.2 VAGUENESS AND SYMBOLICAL MEANINGS OF SECURITY

Security is a socially constructed concept, as established by Luhmann [145] and further applied by Bonß [32].

According to Luhmann, security is a specific construction of structure[1] which serves the need to overcome a future that is per se insecure [145]. This construction allows for transforming unconquerable contingency into actionable security and thus overwhelming and uncontrollable insecurity into human-made and human-controllable *risk*. Some possibilities of risk are selected as actionable, while others are

1 *Erwartungssicherheit*

faded-out as irrelevant. Security can thus more or less be regarded as a *belief* rather than a fact, and this belief has strong influence on people's everyday lives and decisions [32, 121].

IT security as a contemporary facet of technical security obeys these rules all the same. Another aspect that comes into play when researching the perception of security is *vagueness* stemming from the inherent imprecision of human language [184, 228].

Language works by using symbols which convey different meanings, encompassing words, perceptions, thoughts, and similar. While certain meanings of a word are relatively common and constant, others are open to interpretation and personal association. For example, a "flower" is the seed-bearing part of a plant, consisting of the plant's reproductive organs, typically surrounded by bright petals. However, different people talking about flowers might have different colours or even species in mind: While one person might associate "flower" with a red rose, another might think of a yellow tulip, and a third one might think about the bigger entity with a stalk and leaves. Every symbol features a so-called *fringe* of uncertainty that is open to individual interpretation [184].

While the aforementioned flower example might not seem very impactful, the uncertainty of precision when talking about a concept can lead to conflicts and misunderstandings when it is integral to business.

While cryptographers for example might associate security with algorithms and encryption, a manager might rather relate to it as a process. Not only culture, society, and zeitgeist influence these meanings, but most importantly, context. By setting security in context, we can counter its vagueness to a degree. The clearer the context, the situation is, the better can we talk about security without creating misunderstandings.

2.2.1 *Vagueness and Power Dynamics*

Chapter 4 investigates the security narrative in the workplace context, as well as the influences on in-company power relations similar or diverging narratives among employees have. For the underlying theory of this research, we have to look not only at related work on perception, but also on Organizational Sociology [189] in order to understand the power dynamics within a company or department.

Since most work in the field of Sociology is closely focused on a specific society, we had to focus on literature suitable to our geographical region of research (i.e. Germany). Croizer and Friedberg published an important piece on Organizational Sociology in 1979 [58]. They focus on the organization's members and their relationship with the system and analyze the factors power, strategy, and play. For our work,

we draw from the part of power plays and how they emerge around organizational uncertainties.

The language imprecision around the security narrative create one so called *uncertainty zone*[2] in an IT security-focused department or company [58, p. 47]. Several actors try to utilize this uncertainty for their own incentives. This is how power relations emerge.

In addition, Croizer and Friedberg state that the so-called *common goals* within a company actually don't exist. Instead, every individual in a company has different priorities of the company's goals and derives their own action from them [190, p. 43-47].

Our assumption regarding the security narrative is as follows: The more this narrative diverges within a department – or the whole company, if it is centered around IT security – the more do each individual's priorities of the company goals diverge and the more diverge their actions within the department. We therefore derive that a department head – or the whole company – should aim to hire people with a similar mindset regarding security. This would keep the uncertainty zone small and limit the risk for the company from these resulting power relations (see [135, p. 40-42]).

Given that the primary theoretical literature in this case was first published in 1979, we will address the claim of "hiring people with a similar mindset" within the contemporary efforts of diverse recruiting. In reality, we see many efforts to diversify teams and their perspectives on the work matter such as security [22].

Chapter 4 investigates this idea through an interview study in two companies from the field of IT security.

2.3 SOCIAL FACTORS IN IT SECURITY WORK

Research around work conditions and employee issues in the field of IT security is a relatively new branch within the field of Usable Security.

First efforts in this domain were made by Hawkey et al. during the course of the HOT Admin project [102]. While the projects' goals centered on evaluating and improving tools for security practitioners, the researchers also conducted some groundwork about the organizational, technical, and human factors that challenge IT security management, such as different perceptions of risks, or the priority of security within the organization [102].

Chandran et al. have researched the phenomenon of burnout in Security Operation Centers [44]. Using methods from anthropological research, the authors sent a graduated student as an employee to a Security Operation Center, where they should observe the environment, the work and its effect on the people who are employed there. After six months, the observations were evaluated with a Grounded

2 *Organisatorische Ungewissheitszone* [58]

Theory approach. As a result, the researchers found a vicious cycle: Employees did not feel empowered by their workplace, which resulted in less creative and more repetitive tasks. These unpleasant tasks led to less personal growth which led to a decline in analytic and programming skills. Because the employees' skills lowered over time, their work motivation slowly fell and the cycle continued and eventually produced burnout-like symptoms. The authors concluded that breaking this vicious cycle by introducing more creative tasks and room for individual approaches to security analyst work would lead to motivated, empowered employees. This change may help combating security analyst burnout [44].

A follow-up from Chandran et al. presented in 2016 connected the work issues in Security Operation Centers to the Activity Theory model in order to analyze the working conditions with the overall goal to raise employee satisfaction. So-called "contradictions" were identified and set in connection to the problems found in the first study. Contradictions serve as potential foundations for innovation, so the authors then derived courses of action based on their findings, such as improved tools for reporting incidents that leave more room for creative tasks [200].

Work by Blythe et al. researched how employees engage in security actions [31]. Their research focuses around different factors that influence security behaviors within employees and what causes high or low levels of these factors. Another research question focused on the barriers that prevent more security-conscious behavior in employees.

Blythe et al. conducted a series of semi-structured interviews combined with the use of Vignettes. Evaluation of the interview data yielded that employee security behavior is influenced by individual knowledge and previous experiences as well as by individual perception of responsibility and the relation between work and personal life. Especially, the researchers found that employees apply different susceptibility levels to on- and offline threats, which prior theoretical research did not differentiate. Management behavior and positive reinforcement from the workplace can improve employees' security behavior [31].

Haney et al. investigated the development process of cryptographic software within the organizational context and the underlying security mindsets [98]. They conducted an interview study with security developers and found out that there exists a certain "security mindset" in companies that develop cryptographic products. Key aspects of this mindset are the strong commitment to security as a company's *core value* and the perpetuation of security, for example with mentoring programs for less experienced coworkers.

In a position paper, Alexander Serebrenik applies Hochschild's concept of emotional labor [108] to the profession of software engineer. Serebrenik theorizes that software engineers experience emotional

labor and presents examples such as Code of Conduct excerpts that define desired tone and discussion policies for community software projects. A methodological plan to further research the phenomenon by various means from neurological analysis to self-rating of previously expressed emotions is laid out [191].

Work by M'manga et al. researched how folk models coin security experts' perception of risk. They conducted an interview study with security analysts in three different organizations which was evaluated using Grounded Theory. Four groups of influencing factors were identified: Awareness, communication, tool capabilities, and individual capabilities. In addition, five constraints that restrict decision making were extracted: Business processes, data encryption, project management, lack of privileges, and third party dependencies [147].

2.4 MENTAL MODELS OF SECURITY

The study of people's mental models sheds light on their narratives and individual perceptions of security. Mental models can aid in the design of new technology and illustrate how much technical complexity the average user can cope with. Chapter 5 investigates expert and non-expert mental models of encryption in digital daily life.

2.4.1 *User Mental Models*

Users' mental models influence their behaviour and reactions in certain situations. Wash et al. [221] proposed a way to shape the mental models of non-experts to encourage security behavior irrespective of the users' technical understanding.

Bravo-Lillo et al. [34] studied how users perceive and respond to security alerts. Renaud et al. [180] found that incomplete threat models, misaligned incentives, and a general absence of understanding of the email architecture lead to non-adoption of end-to-end encryption for emails. Oates et al. [165] explored mental models of privacy, and Wu et al. [230] explored end user mental models of encryption. Abu Salma et al. [1] quantified mental models and misconceptions of a hypothetical encrypted communication tool and found a large percentage of users underestimate the security benefits of E2E encrypted tools.

Kang et al. [118] measured mental models about the Internet and its privacy and security challenges. Based on their findings, they proposed systems and policies which do not rely on the knowledge of users.

Gallagher et al. [84] conducted a study with experts and non-experts on their mental models of the Tor network and found severe gaps in their knowledge which could lead to deanonymization.

Zeng et al. [235] studied user understanding of smart-home technologies and revealed mismatches in users threat models compared

to reality. Related works on mental models revealed severe misconceptions with respect to message encryption or specific tools. We replicate and confirm some conceptual misunderstandings on message encryption and extend the state of the art by investigating mental models of transport layer security from the end users' and administrators' perspective. In comparison to message encryption, especially, the configuration of the protocol from an administrators' perspective is complex and has a severe impact on the security of the Internet ecosystem.

2.4.2 *Expert Mental Models*

Some previous work has explicitly focused on the mental models of security and privacy experts.

Theofanos et al. researched the gap between security experts and non-experts within the US Government [203]. In an interview study with 21 experts and 23 non-experts, they found out that expert participants have a very strong perception of risk and also base their security narrative on protecting from said risk. Experts further shared a general distrust in everything they encountered online. However, the strategizing around perceived risks helped them manage these risks, so they felt empowered rather than frightened.

In 2014, Posey et al. investigated the perception of risk in organizations using an interview study based on the Protection-Motivation Theory [170]. They interviewed security and non-security employees in various organizations and derived a model to identify gaps within risk and security perception between the groups. It turned out that non-technical employees tend to look towards the outside for threat and risk identification and were concerned about e.g. hackers or system vulnerabilities, while security workers were aware of inside risks like uneducated coworkers.

In addition to these explicit mental model studies, we can also learn from studies who looked at experts' handling of encryption when administrating or programming software.

Krombholz et al. [133] identified major challenges in HTTPS deployment from an administrator's perspective and showed that the procedure is too complex. They identified usability issues and protocol components that are difficult to understand even for knowledgeable users who managed to deploy valid configurations. The results from Krombholz et al. [133] also suggest that administrators rely heavily on online sources and that the quality of these resources often leads to faulty implementation. Acar et al. [4] showed that this is also the case for API documentations, which influence code performance and security. Their findings suggest simplifying interfaces, providing more support for a broad range of tasks, and giving code examples to pro-

mote effective security in applications. These API documentations are among the primary sources that construct mental models.

Fahl et al. [75] studied reasons for webmasters to misconfigure security-critical X.509 certificates which do not validate on their website. They found that one third accidentally misconfigured those certificates and two thirds explained why they deliberately used non-validating certificates. Oltrogge et al. [166] studied the applicability of pinning for non-browser software and implemented a web-application to support the deployment of pining-protected TLS implementations.

Manousis et al. [149] found that only 50% of the domains with Let's Encrypt certificates actually responded with a valid LE certificate on the standard HTTPS port which indicates that even automation does not obviate the need for administrators to deal with the complexity of the protocol, resulting in serious misconfigurations.

While these works [75, 133, 166] identified specific (protocol-related) tasks that are not sufficiently understood by knowledgeable users such as administrators and developers, they did not show *how* they are actually understood. This question will be addressed in Chapter 5, where expert and non-expert mental models of encryption are investigated.

2.5 HTTPS FROM THE USERS' PERSPECTIVE

To ensure a safe usage of the HTTPS infrastructure, SSL warnings and connection security indicators serve as primary interaction components for end users. Related work in our field has significantly contributed to improving these UI components; Sunshine et al. [201] conducted the first study on the effectiveness on browser warnings. Harbach et al. [101] studied how linguistic properties influence the perceived difficulty of warning messages. Akhawe et al. [9] focused on the (in)effectiveness of different security warnings in browsers, which are strongly correlated to user experiences. Weber et al. [222] used participatory design to improve security warnings. Felt et al. [82] studied differences of SSL warnings between Google Chrome and Mozilla Firefox along with click-through rates. As a follow-up, Felt et al. [79] introduced new SSL warnings, which helped 30% of the tested users to stay safe. Those opinionated design-based warnings were released by Google Chrome. To provide users with further visual feedback, they proposed a new set of browser security indicators for HTTPS security in Google Chrome [81] based on a user study with 1,329 participants.

Even though adherence rates have improved, they could still be much higher. Reeder et al. [178] explored reasons for low adherence rates and misconceptions about browser warnings. They identified contextual misunderstandings that influence users in clicking through warnings and found that users are inconsistent in their perceptions and security assessments.

Acer et al. [5] studied over 2,000 Google Chrome browsing errors and classified their root causes. They showed that the majority of errors were caused on the client-side or by network issues and proposed mitigation for spurious certificate warnings. Chothia et al. [51] presented a security analysis of TLS used in UK banking apps that emphasized the importance of security by revealing privacy and security flaws.

This thesis extends the state of the art by studying *how* connection indicators, warnings, and other UI cues contribute to the formation of valid mental models and perceptions of how to operate the system in the most secure manner. While related work has significantly improved security indicators and warnings and thus improved adherence rates, our results suggest that these UX components do not necessarily establish trust among end users.

2.6 MESSAGE ENCRYPTION

Already in 1999 Whitten and Tygar [226] had found that user interfaces for security applications need different usability standards to be effective. This led to a series of other studies, especially as messaging encryption became popular.

Fahl et al. [76] conducted a screening study on the usability of the message security of Facebook. Based on their findings that automatic key management and key recovery capabilities are important, they implemented a usable, service-based encryption mechanism. The effect of integration and transparency on users' trust was examined by Atwater et al. [16] and indicated that users have a stronger confidence in desktop applications and integrated encryption software than others. Different Instant Messaging applications were evaluated concerning their usability by Herzberg et al. [105], Schroder et al. [188], and Vaziripour et al. [213], concluding that the security mechanisms are impractical due to incorrect mental models, a lack of understanding, and usability problems.

Secure email exchange is desired by many users. However, as found by Ruoti et al. [183], the time component detains regular usage since simultaneous users are unsure at which point in time they use encrypted emails. Lerner et al. [141] introduced a prototype for encrypting emails with Keybase for automatic key management and showed that lawyers and journalists were able to efficiently send encrypted e-mails with few errors. However, the operational constraints differ, and there is no one-size-fits-all solution.

Abu-Salma et al. [2] studied users' perceptions of secure communication tools and reasons for not adopting them, and revealed misconceptions of encryption concepts in users' mental models.

2.7 ADVICE AND PRACTICES

In 2008, MacGeorge et al. proposed that for recipients to follow good advice, it should: be useful, comprehensible, and relevant; be effective at addressing the problem; be likely to be accomplished by the recipient; and not possess too many limitations and drawbacks. When giving advice, experts should make sure that the advice is solicited by the recipient, they only give advice if they are a qualified source on the topic; they consider the recipient's point of view; and they exercise sensitivity in phrasing and formulation [148].

Redmiles et al. researched which kinds of advice users adopted and which they rejected. They found that IT professionals, the workplace environment, and negative events, whether personally experienced or told by news media, are users' main sources of digital security advice [176]. As a result of being unable to evaluate the content of a piece of advice, users tend to wager the acceptance of advice based on the trustworthiness of the source. Rejection of advice is influenced by many factors, such as believing that the responsibility for security lies with someone else, perceiving that the advice contains too much marketing material, or believing that the advice might threaten the user's privacy.

In a follow-up US-representative survey on security advice and trusted sources in 2016, Redmiles et al. identified a digital security divide along lines of the socioeconomic status of participants. Wealthier people tended to have better skills and acquired advice from the workplace, while disadvantaged users relied on family and friends for advice [174].

A Pew Research study by Lenhart et al. investigated where teens between the ages of 12 and 17 get their privacy advice from [139]. A focus group study revealed that teens mainly research and iterate through privacy settings on their own, while a follow-up survey suggests that they also relied on personal advice from friends, parents, or siblings. In general, younger teens relied more on interpersonal advice, while older teens tried to figure things out for themselves.

Harbach et al. explicated in a 2014 survey that risk awareness is often the primary stage for the adoption of security mechanisms and their interactions [100]. While being an essential part of the study of human aspects of security research, it needs to be explored in detail in the context of users' daily lives. A fundamental part of devising usable IT security mechanisms is evaluating which risks and consequences are known to users and, therefore, are already accounted for in their mental budget of coping with security behaviors.

Wash researched so-called *folk models* of home computer users, conducting a series of interviews to identify common models about security threats, namely hackers and viruses. After identifying four virus and four hacker models, Wash set them in relation to popular security

advice and suggested which type of user would react in what fashion to each individual piece of advice. This gives a possible explanation for why users do not follow security advice given by experts [220].

Fagan and Khan further investigated why some users follow advice and others do not. They conducted a survey study where they asked participants about their motivations regarding (not) updating, using a password manager, using two-factor authentication, and changing passwords frequently. The authors determined that following security advice was mainly a trade-off decision between convenience and security, where users actively considered features such as set-up time and weighed that against the potential security benefits [74].

2.8 SECURITY AND PRIVACY PERCEPTIONS IN PAYMENT AND BANKING

Prior literature includes studies of payment systems adoption. Differences in countries is visible across numerous papers. For example, in the USA, decision-making factors are the amount of payment, education, and household income [164]. Whereas, in Europe, these factors are transaction size, type of good, and spending place were major factors for French participants [33]. Deciding factors for German users in particular are acceptance, convenience, speed, and security against financial loss [37]. Yet, there are similarities among cultures such as that cash usage is mostly adopted when people make low-valued transactions [18].

Besides financial factors, cultural nuances can play a key role in people's choices [11, 126, 194]. For example, in Denmark, *purchase* (context, time, amount), *personal* (control, cultural beliefs, risk), *payment instrument* (convenience, expenditure, spending), and *physical technology* (sensory perception, equipment) can affect how people interact and choose a payment instrument [103]. Ethnographic field works in the UK and India show the adoption of new payment methods is not easy and requires a decent understanding of the target population's background [136, 172]. Such behaviour is not unique to payment systems, culture is also a player in device sharing attitudes [185]. For women in countries like India, Pakistan, and Bangladesh, device sharing is common and they do not see it as a breach of their privacy [185].

Other cultural elements potentially influence choices; collective nations, e.g. China, are more accepting towards risky decisions because they feel supported by the group if anything bad happens [111]. A survey of 3500 people from seven countries shows that a global view to security research is not feasible because users' perceptions of security depend on their culture, nationality or location [186].

Several other studies focus on the understanding of trends in payment methods. A survey in the USA shows a slight increase in adoption rates of e-payments (1.2% points from 2013 to 2014) and virtual

currencies (0.4%), which suggests an increasing popularity of digital payments [93]. Differences between European countries have been another interesting topic for researchers [217, 231]. For example, Germans use cash in everyday life; 82% of German direct payments in 2008 were in cash (52% in terms of amount) [217]. Also, Austrian and German users prefer cash over other payment instruments regardless of transaction value. They perceive cash as a convenient and privacy-preserving offline payment method, that is cash transactions are not recorded anywhere [37, 134].

2.9 ADOPTION AND USABILITY OF TWO-FACTOR AUTHENTICATION

Chapter 8 investigates incentive mechanisms for Two-Factor Authentication. While there is not much research about the combination of 2FA with incentives to adopt it, there are several studies concerning adoption rates, effectiveness and usability.

In 2014, Gunson et al. conducted a study that compared single-factor authentication (1FA) to two-factor authentication (2FA) for automated banking purposes. The 1FA mechanism required users to recall secret knowledge, a few digit PIN, on the telephone. This is common procedure for telephone banking processes. The 2FA group however was additionally tasked to enter a code that was transmitted through a hardware token. The researchers found that while 2FA was perceived more secure, it was also reported to be less usable and convenient when compared to the 1FA mechanism as it took longer and required a bit more work [96].

Cristofaro et al. made a more general survey in 2015, trying to compare different approaches to 2FA in terms of usability. They conducted a survey that recruited 219 participants on Amazon MTurk and chose to compare three different kinds of 2FA: hardware security tokens, codes send via e-mail or SMS, and apps like Google Authenticator. While all 2FA mechanisms were overall perceived as usable, most users did only adopt it because they were forced to do so (37-44% depending on the 2FA solution), while 35-53 % were using it voluntarily. Only 9-19% responded that they use 2FA due to incentives [63].

In 2018, Colnago et al. released a paper on how the *Duo* 2FA system was distributed at their university in California. While students had the option to adopt the system, it was made mandatory for all of the universities employees. They conducted two surveys, one before and one after the mandatory enrollment of the service, finding that most users perceived the system to be a bit annoying, but still easy to use. It also became visible that after using Duo for a while, users became accustomed to 2FA and sometimes even started using it on other accounts as well [54].

From this work, we can learn that 2FA poses an increase in cognitive load during the authentication process. This disadvantage in perception can be offset in some cases by the increase in perceived security.

2.10 INCREASING USER MOTIVATION WITH INCENTIVES

It is possible to use virtual rewards such as badges to motivate users, as Anderson et al. showed in 2013. In their study they used a website similar to Stack Overflow, generated several tasks that included different kinds of participation with the community and awarded badges for users that took part in it. Their results show that not only did the badges increase the users' motivation and participation rates, they were also able to predict to a certain degree what an user would do [12].

Barata et al. conducted a study in 2013 where they added gamification elements to a master degree university course in engineering, including leaderboards, scores and levels. When compared to the same course in the previous year and other university courses, results showed that students and teachers seemed more content with the course and their achievements. Several other statistics such as attendance or preparation for courses also increased [19].

These studies show that incentives can be a powerful tool to motivate and steer users, even if they only exist meaningfully within a single platform. Based on the assumption that this could also be applied to incentives for 2FA that we find in videogames, Chapter 8 presents the first work to study the feasibility of using incentives for increasing 2FA adoption for non-gaming services.

3 METHODOLOGY

This thesis makes use of different methodologies which are typical for USEC. From a structural viewpoint, user research methodology can be categorized in *quantitative* and *qualitative* methods.

A new field of study is usually explored through qualitative research. Methods like interviews use a narrow sample of participants to get in-depth insight into participants' perspectives on a topic. Single-participant interviews allow for dense sampling of individual experiences, while group interviews are suitable to find opinions and pointers on potential behaviour in specific situations.

Quantitative research usually follows when a research theory has been extracted using qualitative methods. Large-scale instruments such as surveys allow easy research at scale to get larger and more diverse samples and thus more representative opinions on the underlying issue. Large and diverse enough samples even allow for careful estimation regarding the general populations' behavior.

3.1 SURVEYS

Questionnaires are an efficient method to reach a large number of diverse participants. Standardized questions allow for data evaluation at scale, however the question need to be formulated in the right way, as surveys often don't allow for capturing special experiences or thoughts about the topic of investigation. It is therefore important that the field of research has been thoroughly defined and understood from the survey recipients' perspective before deploying it. Otherwise, biasing effects might be introduced [160].

In Usable Security research, surveys a usually either deployed online through crowdworking services like Amazon Mechanical Turk, or handed out for design evaluation after an experiment. In some studies, surveys can also be used for screening a population and subsequent recruitment.

3.2 INTERVIEWS AND THEIR EVALUATION

Interviews are the classic method for in-depth sampling of participants' biographical experiences, attitudes, or associations with the subject of research. Interviews in USEC are usually semi-structured or completely open. This method can be employed in a one-on-one setting or as a group discussion method.

In the following, the methodology for evaluating interviews that was used in Chapter 4 of this thesis is explained in greater detail.

3.2.1 *Qualitative Content Analysis*

For our evaluation in Chapter 4, we applied Qualitative Content Analysis (QCA), as developed by Mayring [153] and refined by Gläser and Laudel for the application on domain expert interviews [89].

QCA is suited to evaluate qualitative data based on initial research questions and theoretical work (as opposed to Grounded Theory which wants the researchers to be as open minded as possible). However, relying heavily on theoretical pre-assumptions likely introduces informed bias into study design and evaluation [112]. Our solid theoretical foundation and the extracted a research question in Chapter 4 suggest a method that build on that, so we chose QCA as our evaluation approach.

In QCA, a theoretical model consisting of variables and their presumed relations is constructed from theory and initial assumptions based on the research questions. Each variable contains a definition, indicators from which an evaluation guideline is constructed, a time dimension, and a content dimension. Variables are set in relation to another, and a model about assumed causality relations is developed. This model is the basis for qualitative evaluation of the interview data.

After all interview data is gathered, the model is revisited and revised based on first impressions of the data. Concrete extraction rules for the interview material are finally derived from the model and documented for further repeatability.

While Mayring's original formalization of QCA demands a test run of the evaluation in which about 40% of the interview material is coded before developing the theoretical model, Gläser and Laudel's extension allows model alteration end extension during the evaluation process [89]. This caters to the usually low number of interviews that can be gathered in domain expert studies.

Information extraction from the text follows the constructed guideline which centers around variable indicators. Passages of the interview are coded and annotated with the extracted content and time dimensions, as well as a cause and an effect, if applicable. Further analysis focuses on these annotations, the source material is only considered as a reference and for documentation.

After extraction is complete, the information is cleaned, re-structured if needed and evaluated with respect to the original model. The goal of the final evaluation step is the extraction of cause-and-effect mechanisms that lead to answering the research question. For a study featuring only a small number of cases, the causal mechanisms for each case are extracted, discrepancies are explained, and the mechanisms are compared in order to eventually answer the research question.

3.3 MENTAL MODEL STUDIES

Mental models are a concept stemming from philosophy and psychology. Kenneth Craik formally defined the term in 1943 [56], but others like Wittgenstein [227] or Luquet [146] have discussed it long before. The key concept is that humans construct their reality through internal model representations. These representations might include filters or reduced complexity in comparison to the external systems they represent.

Staggers and Norico have introduced mental model research to human-computer interaction research in 1993 [195]. In Usable Security research, mental models can show the borders of how users understand systems and processes, and they can be used as a basis to improve software and tools.

Mental model research in USEC is usually conducted as an interview study which is centered around one or more drawing tasks in which the study participants are tasked to visualize their mental model. These drawings are then analyzed qualitatively and sometimes also quantitatively to find out about relevant shortcuts and misconceptions. One such mental model study is presented in Chapter 5.

3.4 FOCUS GROUPS

Focus groups are group interviews of 3-6 participants which foster group discussion and are often used for getting impressions on new concepts or ideas [20]. They are a special form of interview study and often not evaluated with a formal process like QCA or Grounded Theory, but instead more informally using thematic analysis or structured note-taking.

The social dynamics of focus group discussions can shed new light on a proposed system and allows for setting sentiments in context and discovering controversial elements in a design [20].

Part I

STUDIES ON THE PERCEPTION OF SECURITY

4

THE SECURITY NARRATIVE IN THE WORKPLACE CONTEXT

This chapter is based on joint work with Jennifer Seifert (University of Hannover) and Matthew Smith (University of Bonn) which has been published in the Journal of Cybersecurity [40]. I contributed the main part of the work, especially the design, execution, and evaluation of the interview study and the conception and writing of the text. See Appendix F for a detailed authorship agreement.

The authors would like to thank the following people for help and support during this project: Jens Bergmann, Julie M. Haney, Maximilian Häring, Yasemin Acar and Mary Theofanos, and all participants of our study.

It is a well known fact that the language of IT security experts differs from that of non-security related people, leading to a multitude of problems. However, very little work has examined the differences in perception between security experts within a single security department or company. The Sociological theory of power relations and organisational uncertainties by Croizer and Friedberg suggests that uncertainties about the narratives used in a department can lead to potentially harmful power relations, and dissatisfied employees.

We conducted a qualitative interview study within two distinct IT security companies in order to research the impact of diverging security narratives within security departments. Our results show that there is indeed an uncertainty about the term IT security. However, one company we interviewed regarded this uncertainty as highly beneficial for team creativity, communication and mutual education, while the other, more technical-focused company showed few diversions within the security staff, but a possibly uniting conflict with the company's IT department. Our results suggest that conscious shaping of a zone of uncertainty around the security narrative in the work context can be an important management skill for IT security practitioners. Furthermore, we show that the analysis of language uncertainties provides a powerful approach to studying the motivation of professional security groups.

4.1 INTRODUCTION

The term "security" in the context of Computer Science and Information Technology spans a broad field of associations and meanings. Starting with the spectrum from offensive attack-focused security to responsible and lawful defensive security, the single word is associated with lots of different nuances that coin an individual's view of IT security.

Formal definitions of information security include "preservation of confidentiality, integrity and availability of information" [196], "the process of protecting the intellectual property of an organization" [169], and "keep[ing] information in all its locations [...] free from threats" [48].

Over the course of their life, people align themselves on the topic, associate with certain facets and reject others, and granularly form their own personal narrative of IT security and thus their own personal

meaning of the word. Education is usually a big influencing factor in experts' narratives, but personal activism or public figures like Edward Snowden (cf. Section 4.3.2) can also play a significant role in a person's individual picture of security.

Regarding professional contexts, employers in the field of IT security may aim to find employees with a similar narrative to prevent internal conflicts resulting from people meaning different things when talking about the same word (cf. Section 2).

Previous research has shown that employee satisfaction in IT security departments is a newly emerging and perspective-widening field in security research [31, 44], extending the human factor in usable security from the individual level to organizational research. We want to further explore the understanding of employee relations and self-fulfillment with our research by looking at language projections of employees' narratives on security.

In this chapter, we look at similar and diverging security narratives within IT security companies. Corresponding theories from the field of Social Sciences suggest that the personal uncertainty about the definition of IT security leads to interpersonal uncertainties within a department, which can influence power relations and thus may have consequences on employee motivation and satisfaction (cf. Chapter 4).

Regarding the employees, we assume that a smaller zone of uncertainty may lead to fewer conflicts and a better work environment within a department and thus to a higher department effectiveness. In addition, the relationship between employees and the department head may improve when a similar security narrative shrinks the uncertainty zone and thus the potential for power games [21, p. 150f].

Originally, we formulated our research question around employee satisfaction in IT security departments in relation to security narratives of employees and department heads. During the course of the study however, the research focus shifted towards the effectiveness and work culture of security departments. Therefore we chose to reformulate our research question during the evaluation to better reflect our path throughout the project.

We thus summarize our main research question as:

> How do effectiveness and work culture in IT security departments change in relation to a similar or a different security narrative between employees and department head?

To investigate the effects of language uncertainties around the security narrative in the work context, we design a qualitative study centered around employee and department head interviews. The definition of IT security and the possible problems arising from it are most crucial within departments who actively work on IT security, but also between IT security departments and other parts of the company, such as management or development. This is why we conducted a focused study of two such departments. We focus on extracting employee and

department heads' perceptions of and associations with security in order to reconstruct individual narratives and, if possible, a set of shared facets of security that apply to the whole department. Additionally, we investigate actual or potential conflicts around diverging security narratives as perceived by the employees, as well as conflicts emerging from uncertainties around IT security in the respective companies.

We use the methodology of Qualitative Content Analysis [153] to develop a theoretical model and derive evaluation guidelines along this model (see Chapter 3).

This report presents findings from a series of interviews we conducted at two German companies: A company from the field of IT security and data protection consultancy, and the security branch of a large company for applied research.

Our results show that each company had its own prominent conflict around IT security and its meanings. We confirm that uncertainty around the term IT security exists in security companies and that it shapes company culture and employee satisfaction within the company. Both department heads were aware of diverging narratives. One department head was not only aware of the zone of uncertainty around the term IT security, but – contrary to our theoretical assumptions – viewed it as positive and actively used it to shape company culture and foster growth. This gives important hints that consciously shaping and cultivating a zone of uncertainty can be a powerful tool in managing IT security departments.

The rest of this chapter is structured as follows: Section 4.2 gives an overview on the methodology we used for conducting and evaluating our interview study and presents the evaluation model we extracted from theory and based our evaluation on. The collected results are presented in Section 4.3 and discussed in Section 4.4. Conclusions and future work are discussed in Section 4.5. Related work can be found in Chapter 2 at the beginning of this thesis, while more information on the evaluation method can be found in Section 3.2.1.

4.2 METHODOLOGY

In order to get as much insight about the motivations and each individual's narrative as possible, we opted for qualitative research. Qualitative studies are designed to be open and adaptive to the interview subject and allow for capturing complexity in habits, emotions, and experiences. Thus, they are well suited for exploring a new field [57], which is the case for our study.

Since we wanted to research power dynamics within security companies, getting a picture on internal relations and dynamics required to interview several security workers within a single organization. Thus, we needed to find companies that would participate by letting us interview several of their security-related employees.

We conducted a series of semi-structured interviews with two companies in the fields of IT security and data protection. In each company, we scheduled five interviews with technical employees and one with the corresponding department head. For further description, we will label the companies as *Consulting Company (CC)* and *Research Company (RC)*.

The *Consulting Company* is located in the field of corporate and public consultancy for IT security and data protection. The company was founded as a start-up in 2008 and now employs over 20 people, from which about half work on technical topics. Within the company, *CC* has always promoted democratic structures and flat hierarchies, so there is no dedicated department head. Instead, we interviewed one of the *Consulting Company*'s CEOs. Given the company's small size, this can be regarded as equivalent to a department head. We conducted the study in the *Consulting Company* in August and September 2016.

After an initial evaluation of the gathered data, we found that some conflicting results regarding the security narrative and the company culture emerged. We wondered if this was related to the small company size of the *Consulting Company*, and thus started the search for other, larger and more traditionally-structured IT security companies to diversify our sample and investigate if observed phenomena would also hold for larger company sizes. Sadly, finding a medium-sized to large company within the field of IT security that would allow us to conduct our research there turned out very hard, so it took some time to widen the sample.

The *Research Company* is the cybersecurity branch of a large semi-public company within the field of applied research. The company is structured in several independent sub-companies which operate individually. While the company as a whole employs several thousand people, the sub-company which also holds the cybersecurity departments has about 400 employees, further differentiating into several research teams who work more or less independently from each other. We interviewed five employees who work in different but closely related teams on applied research within the field of IT security, as well as the branch head. All interviews in the *Research Company* were conducted in December 2018.

In total, we have conducted and evaluated ten employee and two head interviews. The interviews were semi-structured and scheduled for one hour each. Participants were interviewed one-to-one in a separate room within the company facilities. Before the interview started, participants were informed about anonymity and confidentiality of their contribution as well as the recording of the interview. Participants were required to provide written consent prior to the interview. All participants received a compensation of 15 Euro. Employees and CEO roughly received the same questions. All interviews were conducted by the same interviewer. One interview was conducted in English, all

others were conducted in German. The interview guide document – English translations of the German questions used in the interview – can be found in Appendix A of this publication.

4.2.1 *Evaluation Method*

For our evaluation method, we applied Qualitative Content Analysis (QCA), as developed by Mayring [154] and refined by Gläser and Laudel for the application on domain expert interviews [89].

QCA is suited to evaluate qualitative data based on initial research questions and theoretical work (as opposed to Grounded Theory which wants the researchers to be as open minded as possible). For a detailed overview on the method, see Section 3.2.1.

4.2.2 *Variables and Assumed Relations*

Based on literature and initial assumptions, we construct the following model about power relations between security workers and their company, on which our evaluation is based on (cf. Figure 4.1). Please note that all hierarchies, tasks and the like all correspond to IT security work.

Our initial research question "How does the employee satisfaction in IT security departments change in relation to a similar or a different security narrative between employees and department head?" can be broken down in two variables: *Employee Satisfaction Within the Company* and *Power Struggles Around IT Security*. Power struggles are held between the company and its employees, so we added these two parties to the model and further investigated what tools each party has within this concrete struggle to shape their side.

The company usually sets the *Collective Goals Regarding IT Security*, and, to a large degree, shapes the *Company's Workplace Configuration*, for example by choosing open-plan offices or providing certain hardware to its employees. The *Flows of Communication* are an aspect over which both parties have power, so we modelled it as a shared variable.

An employee's narrative of security is shaped by their *Type of Work with IT security*, as well as their *Expertise* within the field. A person's *Own Precision of IT Security* shapes not only their *Satisfaction Within the Company*, but also their *Perceived Distance Towards the Employer*, as it is periodically compared against the company's collective goals. We theorize that *Compliance With Organizational Rules* might be connected to an individual's Degree of Activism, since a political mindset often influences behavior.

When thinking about the variable relations, we consciously opted not for directional influences, because we wanted to keep an open mind about two-way effects between variables. Connection lines in the model diagram thus only indicate suspected influences between

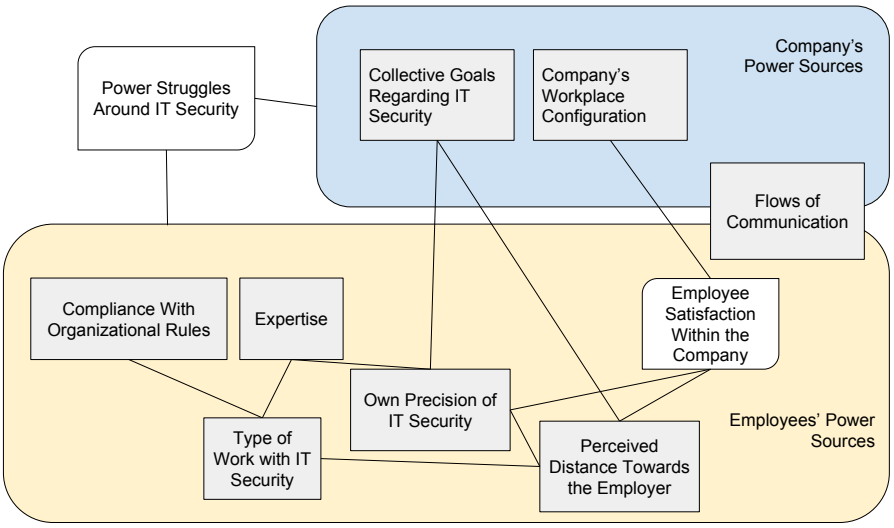


Figure 4.1: The evaluation model after conducting the interviews, depicting all variables used for evaluation. Variables corresponding to one party (company or employee) are grouped accordingly, and variables with two rounded corners are directly derived from the research question.

variables, which should aid in forming connections during the study evaluation.

In compliance with the QCA methodology, this model was constructed after surveying the theoretical foundations of our research questions and before conducting any interviews.

4.2.2.1 *Model Revisions*

During the data gathering and evaluation steps, we noticed that our research question was not well covered by the participants' data. Rather than talking about their personal satisfaction and happiness, the focus was on work culture and effectiveness. We therefore chose to adapt the reserach question as outlined in Section 4.1.

Furthermore, the model was not precisely fitting the reality we encountered. This is normal within QCA, especially when the theoretical and related work in a field is sufficiently sparse [89]. In the following, we list the revisions that were made during the course of the study and present the final theoretical model in Figure 4.2.

After the interviews were conducted, the variable *Activism* was added to the model to reflect the inspiration and motivation from political and activist actors such as Edward Snowden which emerged from the data. We encountered statements about these in a number of cases and theorized that security-centered activism shapes a person's view on the topic.

During the restructuring of the extracted information, it became clear that both the variables *Compliance With Organizational Rules* and

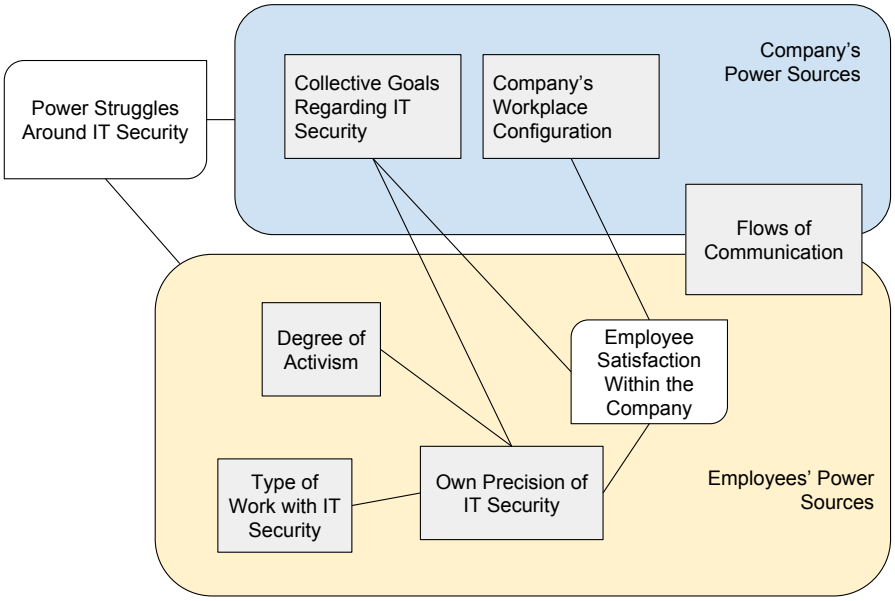


Figure 4.2: The final evaluation model. In comparison to our first model, the variable *Degree of Activism* was introduced, the variable *Expertise* was merged with *Type of Work with IT Security*, and the variables *Compliance With Organizational Rules* and *Perceived Distance Towards the Employer* were merged into *Power Struggles Around IT Security*.

Perceived Distance Towards the Employer were very closely related to *Power Struggles Around IT Security*, so we decided to merge them.

Furthermore, the variable *Expertise* became a part of *Type of Work With IT Security*, since they were very similar in content.

4.3 RESULTS

In this section, we present the findings from our interview study, support them with quotes, and extract the superior conflicts around IT security within both companies, according to our research method. We align the reporting of results by as follows: First, we present an overview on participants' fields of work and expertise, then we continue by expressed activism or association with activists around security, and follow up with portraying the security narratives we found. We conclude this section by listing the extracted conflicts for each employee and the overarching struggle within each company.

As mentioned in Section 4.2, our recruiting requirement was getting a sample of security workers from single companies that ideally stem from a single, security-related team within each company. We were able to sample two companies, each with five employees and one department head.

We thus interviewed twelve employees in total, out of which ten were male and two were female. This gender ratio is in line with the overall employment situation in tech in Germany [90]. Since both

companies have very few women among their security-related staff, we chose not to identify them in order to protect their privacy. All participants will be further addressed with the singular they pronoun.

While we did not specifically ask for personal backgrounds, it became clear that one participant was educated outside of Germany and that their native language was not German. We cannot say how representative this is, since we sadly did not find statistics on ethnic representation in the German tech sector. One participant reported during the course of the interview that they had studied Sociology for five years, which might have influenced their answers to our questions.

Participant	Contract	Employed for	Field of Work
C1	permanent	2 years	Security & Privacy Consulting
C2	permanent	1.5 years	Systems Administration
C3	permanent	2 years	Technical Privacy Consulting
C4	permanent	10 months	Administration, Security Auditing
C5	permanent	6 months	Security Auditing, Training
CD	permanent	8 years	CEO
R1	no answer	4 years	Malware Analysis
R2	limited	4 years	Risk Research & Assessment
R3	limited	2.5 years	Security Auditing
R4	limited	4 years	Reverse Engineering
R5	limited	2 years	Forensics, Database Reconstruction
RD	permanent	8 years	Company Branch Lead

Table 4.1: Participant overview. A C in participant pseudonym refers to the *Consulting Company*, an R refers to the *Research Company*. Employment time recorded at point of interview. Participants with a D alias are department or company heads.

All participants in the *Consulting Company* were on a permanent contract. This is a company-wide regulation and should not be considered special. In our sample from the *Research Company*, all participants but the head were on limited contracts. Employment time in the respective companies varied between 10 months and 8 years. For an overview on all participants, see Table 4.1.

All participants were asked for informed consent through a separate consent form that was also explained to them by the interviewer. At the time of the interviews, our department did not have a formalized IRB process. Instead, we aligned the consent statement and procedure along German data privacy law and EU-GDPR, which enforce strict handling of identifying information. Participant *R1* declined the recording of the interview, thus, we can only report paraphrased quotes. All other participants consented to a recording. The recordings were transcribed and deleted afterwards as communicated by the consent process. All but one interview were conducted in German (the other was conducted in English), the participant quotes in this report are thus translated from the original transcript.

4.3.1 *Fields of Work and Expertise*

The *Consulting Company* is operating in the field of data protection and privacy consulting, so four employees as well as CD reported that consulting, teaching, or auditing is part of their daily work. C2 and C4 reported systems administration as their only or as part of their tasks at work.

In the *Research Company*, employees were all working on technical topics like malware analysis, reverse engineering, or forensics. Several participants reported teaching or student coaching as part of their duties, since the company cooperates closely with nearby universities. All participants in the *Research Company* we interviewed were university educated. Some did not mention their study subject, but whenever they did, it was Computer Science[1].

Educational backgrounds in the *Consulting Company* were more diverse. C1 extensively reported about their studies and a lecture by a company's Chief Information Security Officer (CISO) on security management that greatly influenced them and their security narrative. C3 reported to have studied a non-security related field before, but didn't mention the exact topic. C5 reported to having studied Sociology for five years before switching to computer science. CD was a PhD student in Chip Design before founding the company.

For a summary of all participant's fields of work at the time of the interview, see Table 4.1.

4.3.2 *Degree of Activism*

Security is often a very political field, since it closely connects to privacy and thus to basic human rights.

Our participants mentioned Edward Snowden, the Free, Libre, and Open Source Software Movement (FLOSS), and the German *Chaos Computer Club* (CCC) [46], a grassroots political hacker association with large impact on national IT and security politics, as their influences. Several participants also mentioned the importance of citizen rights in the context of security, especially the German right of informational self-determination [125].

In the *Consulting Company*, all participants mentioned some degree of political or activist influence on their narrative. C1 and CD showed a strong consciousness for citizen rights, especially in regards to privacy and self-determination about their data.

> There is this nice civil right, the right of informational self-determination [...], and *I* believe that you can apply this

1 The German subject of *Informatik* might be slightly different than what an international audience understands as Computer Science, since it often is closer to Engineering than to Science.

> down to very concrete levels like requirements engineering within the software development process. (C1)

Participants C2 and C4 talked about hacker culture and hacker images. For C2, watching recorded talks of the annual CCC congresses [45] was a turning point in shaping their narrative about "hackers", and thus about security.

> That kind of opened my eyes back then, that even normal, or "normal", or good-willed people tear things apart to see how they work. And that exploits or other things that can be used to attack systems, are rather a byproduct from this curiosity about understanding things. (C2)

Edward Snowden was a prominent figure and source of inspiration for many participants (R2, R5, C2, C5). Participant C5 was so moved by Snowden's revelations about large-scale government spying that they decided to switch majors in their Computer Science Master, from computer graphics to security. C3 mentioned strong influence by the Echelon scandal in 2001 in the course of which was revealed that a group of governments eavesdropped on wireless communication, which is similar in nature.

4.3.3 *Security Narrative*

Traits and features our participants commonly associated with security are network security, encryption, data protection and privacy, malware, and a general consciousness about security. Table 4.2 differentiates these further into categories, namely core attributes of security (confidentiality, integrity, protection), management facets, technical facets, influences, and metaphors. While employees within the *Research Company* center their associations around technical facets, the associations among the *Consulting Company* employees are more heterogeneous. They often use metaphors such as security being a *toy* to illustrate their narrative. Furthermore, connections to *hacker culture* were only made among the participants from the *Consulting Company*, as was laid out in Section 4.3.2. On the other hand, the technical facet of *firmware and IoT* was only associated within the *Research Company*, which might reflect the daily work topics.

When asked about what coined their personal picture of security, most participants mentioned education in security or a related field. However, especially in the *Consulting Company*, some people reported being heavily influenced by data breach scandals, such as the Echelon scandal in 2001 or the Snowden revelations in 2013.

Some participants report a general frustration or a pessimist view on security in general. For example, R1 states that there is either *"bad, very bad, or okay-ish security"*.

	C1	C2	C3	C4	C5	CD	R1	R2	R3	R4	R5	RD
Confidentiality	•		•							•		•
Integrity	•		•						•			•
Protection	•	•	•	•	•		•		•	•	•	•
Risk (Management)	•		•					•	•		•	
Management/Processes/ Communication	•					•						•
Laws/Regulations	•		•		•							•
Human Factors				•		•				•	•	•
Securing Processes/ Apps/Communication	•		•		•	•	•	•	•	•		
Malware/Virus Protection		•					•		•	•	•	•
Cryptography	•		•		•		•	•	•			
Compromised Systems		•		•				•		•	•	
Firmware/IoT								•	•			
Tools		•										
News		•									•	
NSA/Snowden		•			•			•			•	
Hacker Culture		•	•									
Hacker Cliche		•	•									•
Toy	•		•	•	•							
Buzzwords		•	•			•					•	
Good vs. Evil		•			•					•		

Table 4.2: Study participants' individual associations with the term "IT Security", grouped into core attributes, management facets, technical facets, influences, and metaphors.

In the following, we portray the security narratives we found in each company.

4.3.3.1 *The Consulting Company*

Company head CD reports that their picture of security developed during their PhD studies in Electrical Engineering, when it became clear to them that security always needs to be considered, regardless of field of work. They see security as a process accompanying the whole product life cycle in IT.

Among the employees in the *Consulting Company*, we noticed that those employees who reported to mainly work in technical areas of security (namely C2 and C4, cf. Table 4.1), had a narrative that was very focused around the tools they mainly use. For example, C2 answered the following when asked about their associations with the term IT security:

> In the recent time [I think] mostly about cryptoviruses, and what has happened in the news. And yes, methods how you can counter them, good virus protection and so on, but also the NSA scandals, now that new parts of the software library have been leaked. That the Cisco routers are, again,

> still insecure. So yeah, the Heise[2] news connected to these examples. (C2)

C4 fell victim to a hacking attack on a self-hosted game server and subsequently started to become interested in securing their own as well as hacking other people's servers.

On the contrary, the *Consulting Company* employees that mainly worked in consultancy and training expressed a very differentiated narrative, distinguishing between terminology such as data protection, data security, and information security.

> And recently we had a discussion about data protection, and then there was another term, data security, that somehow competes with IT security and you have to consider, what is the difference? Or is it the same, yes? And then there is the term of information security where again the question is, is this different from IT security? (C1)

Following this statement, C1 proceeded to differentiate the terms they mentioned further.

Employee statements in the *Consulting Company* acknowledge that there is no unified narrative within the company:

> One could start with the fiction of a unified opinion in here regarding IT security, but there is none. And I think the only common thing we have here, is that it is something good, something we should have. (C3)

CD confirms this, further adding that there are frequent discussions about the concept of security which lead to frustration among the employees. They are aware of the tension and explicitly acknowledge the existence of a conflict around the security narrative, but consider it as a source of active knowledge exchange and eventually, fruitful discussion.

> And stemming from the fact that there are many different opinions around here, the discussion is never finished. Read: We wouldn't pose and say "We really know stuff about IT security and exactly *this* is how it works". This will never happen. It is inherent to the system, sometimes gets on your nerves and I even understand that, but I regard this as a very important part. It is part of the company and I think this is the way how security can work best, by constant questioning. (CD)

2 A major German tech news outlet, `https://heise.de`

4.3.3.2 *The Research Company*

Branch head RD's security narrative is closely aligned to the different levels of confidentiality that play a big part in the company's procedures. RD expresses strong consciousness about what type of information needs what level of protection and also applies this mental model to their daily life.

> For myself, I am very consequent on that matter. In contrast to many others, I regard it as noncritical to consciously send unencrypted emails, so I differentiate in my mind between what is deserving protection and what is not deserving protection. When we make an appointment, it is by my strongest belief not deserving much protection. But when we'd exchange on how I evaluate certain people [...], it would be a totally different thing. (RD)

In addition, CD mentioned Sun Tzu, the ancient Chinese military strategist as an inspiration for their security strategies. This is the only mention of an authoritarian figure across all interviews.

> The ancient strategist Sun Tzu has said on that: "Who defends equally in all areas, has no structured defense at all". And those who protect the canteen's menu the same level as they protect their most important technical design drawings where the company's competitive advantages are stored, they haven't properly set up their security. (CD)

Employees in the *Research Company* feel very close to their team leaders, but report struggles with the company's IT department.

> But then there are day where you file a request for an IP clearing, which is a port clearance on a firewall, and then it takes time until it's done, and then it has only been done for two or three parts but not in the other parts, because some person had the opinion that you wouldn't need that, but you actually needed that. But then nobody notifies you, and then you start debugging your own stuff until you eventually find out using *iptrace* or the like that you actually weren't the cause of the error, but the firewall rules were, and well, on such days you're really cursing it. (R5)

Two employees in the *Research Company* mention that some contracts the company acquires come from the military. While R3 sees the potential of a personal moral conflict for others, they report that they personally would have no problem with working on military projects. In contrast, R2 would not feel comfortable in such a situation, but they are sure that their team leader would respect their worries and would not assign them on such a project.

R3 assumes that the narrative varies significantly by team. R5 confirms this by stating that they have a very similar mindset with their team leader. RD assumes that the mindset within the company greatly diverges (*"We have 450 employees and likely 570 opinions on the topic"*), but assumes that most will have a similar narrative to them.

4.3.4 *Conflicts*

After extracting information according to our variables, the next step was to identify a high-level conflict around IT Security for each participant. Subsequently, these conflicts were grouped by company and then used to extract the company's conflict around the security narrative. An overview is provided by Tables 4.3 and 4.4.

C1	Own idealism and attention to detail clash with the necessity to offer realistic services. This leads to frustration.
C2	No conflict, self image as a "good hacker", narrative focuses around tools.
C3	Fun and intellectual challenge with security, but frustration with the business, also within the company.
C4	Administrator restricts the company-given flexibility by not offering certain tools.
C5	Inhibited communication culture within the company because of insecurities. Wishes for clarifying conflicts.
CD	Conscious insecurity around the narrative, therefore frequent discussions and fatigue among employees, but also education and advancement.

Table 4.3: Summary of conflicts within the *Consulting Company*.

Within the *Consulting Company*, two employees expressed internal conflicts about their own narrative of security. A strong personal interest in the topic contrasts with the realities that the participants face in their daily work life.

> I think the only potential conflict for me is that I work in a field in which I am personally interested. And you just can't do some things the way you personally regard them as right. And what *I* perceive as right for *myself*, does not necessarily have to be right for a company. (C3)

Participants from the *Consulting Company* also expressed awareness about diverging narratives within the company.

C1 refined this statement from C3 about the "fiction of a unified opinion" (cf. Section 4.3.3) further, explaining that:

> I think the dangerous thing is, that there is no explicit consensus. There is something implicit, that as developed

R1	No conflicts within the company. General frustration with quality of and consciousness about security.
R2	Security regulations imposed by the parent company hinder research work, active circumvention of these regulations with help of team lead.
R3	Only structural conflicts within the company. Personal conflict with consequently applying security knowledge in daily life.
R4	No conflicts within the company because of very similar narrative.
R5	Security regulations imposed by the parent company hinder research work, active circumvention of these regulations with help of team lead.
RD	Handling confidential information requires special considerations regarding security which are not well realized by employees and lead to conflicts. Active circumvention of the regulations is tolerated.

Table 4.4: Summary of conflicts within the *Research Company*.

> within people's minds from conversations and the like. But this doesn't sync, and at some point you have the feeling that you don't need to talk about it any more. (C1)

Participant C5 feels tension stemming from unresolved conflicts around the security narrative within the company.

> There is a lot of beating around the bush. Nobody speaks plain text. And this beating around the bush is such a hindrance, because nobody communicates their point of view clearly. Even when it should come to a conflict, we could resolve it. Even if it seems insurmountable, resolving conflicts os possible. (C5)

The *Consulting Company*'s head adds that the security narrative is frequent subject of discussions among the employees. CD consciously uses their power within the organization to keep this zone of uncertainty around the term security open.

> Within the *Consulting Company*, the differences at this point are somewhat embraced. That leads to frequent discussions, to frequent discrepancies, to disagreements. But this doesn't really harm the company, quite the contrary. (CD)

Discussions about the security narrative are frequent and lead to frustration and fatigue, but also to development and mutual education within the company (see also Section 4.3.3).

> Yes, there are frequent discussions, and my opinion [...] is of course questioned too, and discussed every now and then, sure. But as I said, I regard this as desirable. It might not be perceived this way by everyone, but I see this as a pleasant thing. (CD)

Participant C5 shares another view on the issue. Since they are relatively new in the company (6 months at time of interview, cf. Table 4.1), they welcome any coworkers who would share their opinion on security and privacy with them.

> Sure, first and foremost it is a conflict, but for *me*, as a relative newbie in the field, I really appreciate any input that I can get. I think about it, I process it somehow. And if I assume that someone wouldn't regard IT security as important as I do, but instead something else, then I am open to their point of view and accepting it. I don't think that my opinion is the non plus ultra. (C5)

The most prevalent conflict within the *Research Company* is the struggle around security guidelines. The company works with classified data and therefore, special considerations on infrastructure and protection need to be made. At one point in the interview, RD expressed that these rules often not align with employee mental models and thus lead to misunderstandings:

> We are in the process of advancing in the separation of networks I mentioned. This comes with a lot of uncertainty from the employees, and often it happens that the questions that are asked from the security point of view [...] are answered in a way that lead to a high level of security. For example, when someone says "Yes, I always work with classified data and always need to access it", that would lead to cutting off the access to Google because the page can not be made available within the high-security network. And that leads to frustration. (RD)

There are security guidelines for the whole company which also apply to the branch working on security. These guidelines regularly clash with active and experimental security research which is conducted in the *Research Company*.

> Many of my colleagues do reverse engineering of viruses for example, and conduct dynamic analyses of viruses. First, they can't do that on a Microsoft Windows. They can't work with a running antivirus, because of course there are viruses on their computers, that's the point of their work! Often, there are no company-level strategies for this, it only leads to friction on all levels. (R5)

There are conflicts both in complying with the security guidelines as well as applying the confidentiality rules. Team leaders support their employees in actively circumventing and working around these restrictions, so they can accomplish the tasks they are assigned to. RD knows about these rule breaks and tolerates them silently, but not without remorse.

> There are workarounds which touch critical areas and where I have to ask myself if I really want to know it. Usually, I don't. But of course, in a position of responsibility such as mine, I have to ask myself then, "How much control do we need, how many decisions do we really need to execute, and where can one sometimes look away?" (RD)

RD thus abstains from using their power within the zone of conflict.

4.4 DISCUSSION

We see frequent discussions about the *fringe* in the *Consulting Company*. CD regards them as fruitful because their employees already have a very defined mental model, but they acknowledge the emotional burden in form of frustration and fatigue (cf. Section 4.3.3). CD uses their power within the organization to keep the uncertainty zone around the company definition of security consciously open, as they believe that it would benefit the company, and eventually, its employees, too.

It was striking that individual security narratives were more precise among participants who worked in consulting, especially within the *Consulting Company* (cf. Section 4.3.3). The more technical participants C2 and C4 mainly aligned their narrative on technical terms and tools as well as activist motifs. The other employees expressed more layered narratives of security, encompassing (business) processes and different perspectives. This indicates that power struggles and dynamics might be more present in companies where security experts talk about security as part of their professions and poses a hypothesis for further investigation within the security consulting sector.

It was striking and even surprising based on our theoretical research (cf. Chapter 2) that CD was very aware of diverging security narratives within their company, the uncertainty zone they opened, and the effects of frequent discussions about this. Moreover, they regarded the power struggles as a benevolent effect, because they lead to mutual education and the exchange of knowledge and news around IT security. The sharing of resources and information in this scenario would be a suitable starting point for further research into the influence of news, scientific findings – CD explicitly mentioned being confronted with research papers – and stories, as it has already been researched that these different types are used to convey different types of information when shared [173]. On the other hand, the question about to what

degree language uncertainties are or can be used as a tool for staying up to date with security and privacy-related topics poses itself in this context.

The awareness of the narrative within a company and careful employee steering around the associated uncertainty zone could be an important *soft skill* for management positions. It remains open how targeted uncertainty zones can be cultivated by department or company heads. CD reports that there is no top-down definition of what security means for the company, and that they explicitly foster different opinions (cf. Section 4.3.4), but we do not yet know what other effects might play a role in cultivating uncertainty, so follow-up work in that direction is needed.

In comparison, we found employees in the *Consulting Company* to be idealistic people, in part motivated by activism, and to bring very defined models of security into the company. Why this was the case was sadly outside of our study scope.

Within the *Research Company*, the internal conflict of working on military projects was visible. One participant reported such a conflict for themselves, and another participant was not affected personally, but stated that their colleagues might have this conflict (cf. Section 4.3.3). It is important for department and company heads to carefully consider this conflict of interest among their employees, as such a strong, unresolved internal conflict can lead to employees leaving the company. However, the *Research Company* has developed a strategy for this potential of conflict, as it only tasks employees with military projects who explicitly want to (cf. Section 4.3.3).

The most prevalent conflict within the *Research Company* was the struggle around security guidelines. Participants from the *Research Company* have mentioned that they are supported by their team leaders in coping with this conflict, so allying against a "common enemy" within the company might boost an employee's bonding with their employer.

RD knows about the guideline circumventions and rule breaks and tolerates them silently, but not without remorse. They thus abstain from using their power within the zone of conflict, leaving it to the employees and the IT department. This might be because they do not want to lose their employees, since they mentioned that the biggest constraint for their branch is acquiring good personnel.

> The challenge is doing the most meaningful things with the available personnel. So there are only limits in acquiring new employees, content-wise, this is the land of opportunities. (RD)

To fully capture the conflict on security regulations in the *Research Company*, additional interviews with members of the company's IT department would be necessary.

4.4.1 *Limitations*

This work is not free from limitations which we will report in the following.

This study features a rather small sample size, which limits the generalization of our results. This stems from the recruiting difficulties we had, as it turned out to be very hard to get into companies for an interview study. Where other researchers could draw from their institutional background (e.g. Haney et al. [97]), we as university researchers had no such background and only few ties to local industry from which we could draw.

In addition, the participants we interviewed came from a very narrow socio-cultural window. All but one were white, there were only 17% non-males in our sample, and we consciously only chose one single socio-cultural area to recruit from, in order to not introduce additional effects because of culturally different work or interpersonal habits.

It was not our goal to get a large, representative overview on the security narrative, but instead go down deep into one special culture. Thus, follow-up work to extend our findings to other cultural contexts would be greatly appreciated and might be used to identify further, culture-specific influences on power struggles around the security narrative.

4.5 CONCLUSIONS AND FUTURE WORK

In this work, we investigated the narrative of the term IT Security within two companies working in or closely related to security. By looking at individual definitions of the term "security", we showed that different narratives exist within a company and that the level of detail might relate to an employee's task within the company. In our case, the people working in consulting and training had very precise narratives, technical employees such as systems administrators in comparison had a coarse narrative, centered around tools and protocols.

This provides new insights into the human factor and social dynamics between security workers, those who create or shape the creation of security and privacy practice. It is thus a contribution to deeper understanding social and power dynamics within the context of Usable Security and Privacy.

When addressing our initial research question, *How do effectiveness and work culture in IT security departments change in relation to a similar or a different security narrative between employees and department head?*, we can give an answer for each company we studied.

In the *Research Company*, the employees working on security research had narratives focused around the technology they work with and

reported no internal conflicts about the narrative, but struggled with the company's IT regulations. For example, malware research was jeopardized by mandatory antivirus software. Employees and whole teams have established workarounds and set up a second "shadow infrastructure" to arrange with this. The company head is aware of such workarounds but sees them with remorse.

In the *Consulting Company*, our theory of uncertainty zones around the definition of security was confirmed. The company has no top-down regulation of what security is, and employees often discuss and clash on that topic. However, in contrast to our initial assumption, the company's head was aware and actively fostered this culture by leaving the uncertainty zone around the security narrative consciously open. The diversity of narratives had a small negative impact on employee satisfaction, but profited the company as a whole. This indicates that uncertainty around IT security might not be inherently bad for company climate, although we see a clear trade-off with employee frustration and fatigue.

Shaping (or not shaping) the security narrative might thus be a new tool for managers in IT security to precisely foster their department's intellectual growth. A narrative can function as a bonding tool within the department and can create a clear distinction towards other departments. Cultivating collective uncertainty around it can lead to increased interpersonal exchange and mutual education around the topic.

Regarding research, this chapter shows – in its own, limited scope (cf. Section 4.4.1) – that the analysis of language uncertainties can be a powerful indicator on company climate and motivation within professional security departments. This opens up new possibilities for security perception research in professional communities as well as .

As for future work, one could continue the general direction which the results from the *Consulting Company* have outlined. The narratives among the consulting employees were very defined and the impacts of different narratives were prominent in their daily work life. Thinking the field of consulting further, the narratives of "opinion shapers" and communication multipliers such as blogs or news outlets could be investigated.

When considering the other direction outlined by our findings within the *Research Company*, a field of future research could be the uncertainty zone around IT security between security departments and other employees in non-technical companies with a high focus on security, such as banks.

5

MENTAL MODELS OF ENCRYPTION

This chapter is based on joint work with Katharina Krombholz (CISPA), Katharina Pfeffer (SBA Research), Matthew Smith (University of Bonn), Emanuel von Zezschwitz (University of Bonn) which has been published at IEEE S&P 2019 [131]. I contributed with administrator interview conduction, coding, evaluation and paper writing. See Appendix F for a detailed authorship agreement.

We would like to thank the reviewers and our contact point Rob Reeder for their constructive feedback, and the Leitstelle 511 e.V. for providing an interview location in Hannover.

The previous chapter focused on security perception in groups of people to highlight interpersonal influences to an individual's attitudes. This chapter concentrates on the individual. It presents research on mental models which shape interaction with technology and people on an elementary level.

HTTPS is one of the most important protocols used to secure communication and is, fortunately, becoming more pervasive. However, especially the long tail of websites is still not adequately secured. HTTPS involves different types of users, e.g., end users who are forced to make security decisions when faced with warnings or administrators who are required to deal with cryptographic fundamentals and complex decisions concerning compatibility.

In this work, we present the first qualitative study of both end user and administrator mental models of HTTPS. We interviewed 18 end users and 12 administrators; our findings reveal misconceptions about security benefits and threat models from both groups. We identify protocol components that interfere with secure configurations and usage behavior and reveal differences between administrator and end user mental models.

Our results suggest that end user mental models are more conceptual while administrator models are more protocol-based. We also found that end users often confuse encryption with authentication, significantly underestimating the security benefits of HTTPS. They also ignore and distrust security indicators. Administrators often do not understand the interplay of functional protocol components. Based on the different mental models, we discuss implications and provide actionable recommendations for future designs of user interfaces and protocols.

5.1 INTRODUCTION

In the context of information technologies, protecting communication content at large scale has become more important than ever before. Almost twenty years after Whitten and Tygar's usability evaluation of PGP [226], reliable encryption still cannot be taken for granted even though adoption rates are growing [80]. In today's Internet ecosystem, HTTPS is the fundamental cryptographic protocol to secure information in transit and to ensure data integrity and privacy between two communicating parties. However, HTTPS is still not the default for all websites, especially when it comes to the long tail of websites [5,

80]. As of March, 2020, Internet-wide scans from SSLPulse suggest that 36,3% of sites surveyed still have inadequate security[1]. Recent studies show that this is, among other reasons, due to the fact that the deployment of cryptographic protocols is a difficult task even for knowledgeable users [133]. Similar to message encryption, HTTPS confronts different types of users with cryptographic algorithms and protocols which they do not fully understand [5, 78, 92, 133, 166, 178]. In addition, users who are exposed to poorly configured sites are forced to make security-critical decisions and are often not aware of the respective consequences.

We argue that we still do not understand *why* these carefully designed protocols do not meet the needs of (knowledgeable) users to securely operate cryptographic applications. Therefore, this work employs an inductive approach to learn about the root causes for user misconceptions by formalizing mental models of end users and administrators. In particular, we focus on how users think that HTTPS works and against which types of attackers they think they are protected.We thereby contribute a qualitative study with 18 end users and 12 experienced administrators; our findings reveal interesting differences in the mental models of these two distinct user groups.

We found that many non-expert participants significantly underestimate the level of protection that HTTPS offers, whereas administrators generally have a good understanding of its benefits and limitations. We also discovered that most administrators have little conceptual knowledge of how the protocol works but are very familiar with the different steps of establishing a communication. Key elements are often considered as blackboxes and poorly understood. We further found that the distinction between authentication and encryption is unclear to many users – even to some experts. Based on our findings, we identified protocol components that diverge from user mental models and discuss implications and potential countermeasures.

The goal of this chapter is to derive and compare mental models in order to understand if and how they deviate from the underlying functionality of HTTPS and their impact on security. The main contributions of this chapter are as follows:

We conducted an in-depth qualitative study with $n = 30$ participants to formalize user mental models and threat models and to understand users' perceptions, attitudes and misconceptions of how HTTPS works. By focusing on different scenarios and studying two distinct groups of users, namely end users and system administrators, we were able to reveal group-specific differences.

1 `https://www.ssllabs.com/ssl-pulse/`, Accessed: 2020-03-11

5.2 METHODOLOGY

In the following, we describe our research questions and how we address them. Our goal is to understand why end users and administrators make mistakes when using or configuring HTTPS that result in security-critical situations. Our approach is to construct theories by means of identification of patterns in the data [104] (inductive approach), which is why we opted for a qualitative interview study with a diverse sample of participants. In particular, we sought to answer the following research questions:

- What are people's expectations and perceptions of encryption and visiting sites via HTTPS?
- How well do users understand the associated threat models?
- What are the differences between end users' and administrators' mental models of HTTPS?

5.2.1 *Study Design and Procedure*

Kearney et al. [122] showed that humans commonly possess superficial knowledge, of which they are not aware and which they cannot easily articulate. Nevertheless, this knowledge determines people's decisions and responses to new situations. Our study is designed in a way that it supports participants in exploring and reporting this knowledge by externalizing it. Based on related work on HTTPS usability [80, 81, 133] and recent mental model studies from usable security [84, 118, 180, 221, 235] we constructed an interview guideline for semi-structured interviews including a three-part drawing task and a short questionnaire with closed-ended questions covering demographics and questions on the participants' online communication behavior. The complete study material can be found in the Appendix, including the screening questionnaire in Section B.1 and the interview guideline in Section B.2. Twenty-seven interviews were conducted in person in three different cities in Austria and Germany, namely Vienna, Bonn, and Hannover. The participants were invited to a quiet room at one of our labs or at a local hackerspace. In addition, three interviews were conducted via Skype.

All participants were informed about the purpose of the study and then signed a consent form. Then, depending on whether a participant was classified as end user or administrator, they were presented a questionnaire. Afterwards, the main part of the study–namely the interview with the drawing tasks–was conducted. The drawing tasks were based on different scenarios and asked to verbalize their thought process as they drew, consistent with traditional think aloud protocols [73]. The scenarios were (1) a general scenario of

sending an encrypted message to a communication partner, (2) online shopping via HTTPS, and (3) online banking.

All but one interview were recorded after the participants gave their written consent. In addition to the audio recordings, the interviewers took notes.

Contrary to quantitative research, where the appropriate sample size can be determined by power calculations, the sample size in qualitative research is determined by the point at which no new themes or ideas emerge from the data. We conducted interviews until we reached this point of saturation [95]. As the sample of end users was more diverse in terms of demographics, education and technical experience (assessed in the screening questionnaire), a larger sample was required to reach saturation in comparison to the administrator sample. We validated our study design with pilot interviews and a post-hoc validity study.

5.2.2 *Expectations on User Mental Models*

While our scientific principles encourage us to evaluate results from a neutral, non-involved standpoint, researchers introduce their own individual biases and preconceptions. To make these personal influences more transparent, we discussed a series of expectations on mental models prior to analyzing the data. We argue that mental models of both types of users are constructed based on the protocols and UX with which they interact. We therefore expected these components to be essential parts of their mental models. Mental models are also influenced by media articles, education, experience, and other factors. As we cannot isolate these factors, we do not build our expectations on them.

Consequently, we assumed security indicators (e.g., the https prefix or the padlock icon) as part of end user mental models. We did not expect deep knowledge about encryption concepts and keys, e.g., we did not expect awareness for metadata from end users or an understanding about additional network nodes. While all researchers agreed that end users should not confuse encryption with authentication, we did not agree on whether the absence of a centralized encryption component can be expected from end users.

We expected more in-depth knowledge from administrators, e.g., knowledge about symmetric and asymmetric encryption. We also expected keys, certificates, and certificate authorities to be components of their mental models. We also assumed that their tacit knowledge on data transport routes would contain intermediary nodes in the network. We expected more sophisticated threat models and awareness of metadata.

5.2.3 *Recruitment and Participants*

Before the actual study, we conducted a series of pilot interviews, four in Vienna and two in Bonn. This pilot provided feedback on which we improved and extended the survey guideline.

In total, we recruited 45 participants. Since the first six and the last nine interviews were used for the pilot study and for the validation of the results, we excluded them from the final data set and thus had a final set of 30 participants, consisting of 18 end users and 12 administrators, respectively.

For the non-expert users, our goal was to recruit a diverse sample of participants. Hence, we used three separate recruiting mechanisms to build our sample: mailing lists, online forums, and personal contacts for recruitment. We especially limited the number of students in our sample and refrained from recruiting computer science students or IT professionals.

In contrast, the recruitment criteria for administrators was that they had to be in charge of administering systems and regularly-used services. We allowed both paid and voluntary work.

To recruit administrators, we contacted companies' IT departments directly or used personal contacts as entry points to larger organization. Five administrators were recruited over this channel. Additionally, we posted advertisements on social media and a hackerspace mailing list to recruit another seven administrators. Sadly, we were unable to recruit female or non-binary administrators. Table 5.1 lists information of our participants. Table 5.2 presents a summary of demographics.

Table 5.3 summarizes the administrators' previous work experience and security-specific education. Four of the 12 administrators reported that they never received any security-specific education. Four administrators were employed at IT service providers, two at national newspapers, and the remaining ones were administrating servers in the fields of data protection, social services, advertisement, mobility, radio and television, and education. Eleven administrators were full-time administrators at a company, and one was voluntarily administrating at a non-profit organization.

The recruitment text did not include information on the actual purpose of the study in order to prevent the participants from informing themselves about HTTPS before participation. All participants were compensated with 10 Euros for their time.

5.2.4 *Data Analysis*

We collected both qualitative and quantitative data. Our qualitative analysis is based on audio recordings, hand-written notes, and the drawings that emerged from the drawing tasks.

Table 5.1: Study participants (administrators, end users, pilot/validity study participants)

ID	Age	Gender	Education	Employment	IT Education
Administrators ($N_A = 12$)					
A01	29	m	high school	employed	no
A02	40	m	university	self-employed	no
A03	29	m	university	employed	yes
A04	34	m	high school	employed	no
A05	nA	m	university	employed	yes
A06	42	m	high school	employed	no
A07	31	m	university	employed	no
A08	35	m	high school	employed	yes
A09	31	m	university	employed	yes
A10	31	m	high school	employed	no
A11	37	m	university	employed	yes
A12	30	m	university	employed	yes
End users ($N_U = 18$)					
U01	56	f	junior high	self-employed	no
U02	24	m	high school	self-employed	no
U03	24	f	high school	employed/student	no
U04	41	m	university	employed	no
U05	26	f	university	employed	no
U06	35	f	university	employed/student	no
U07	43	f	university	employed	no
U08	28	f	university	employed	no
U09	60	m	university	employed	no
U10	27	m	university	student	no
U11	24	m	university	student	no
U12	56	f	university	employed	no
U13	28	f	university	employed	no
U14	32	f	university	student	no
U15	28	m	university	employed	yes
U16	24	f	high school	employed/student	no
U17	27	f	university	employed	no
U18	28	m	high school	employed	no
Pilot study participants ($N_P = 6$)					
P01	36	m	university	employed	no
P02	28	f	university	employed	no
P03	28	f	high school	employed	no
P04	21	m	high school	employed	no
P05	36	f	university	employed	yes
P06	29	m	junior high	employed	no
Validity study participants ($N_V = 9$)					
VA1	24	m	university	employed	no
VA2	36	m	university	employed	no
VA3	27	m	high school	employed	no
VA4	40	m	high school	self-employed	yes
VU1	52	f	university	employed	no
VU2	27	m	high school	employed	no
VU3	30	m	university	employed	yes
VU4	23	f	university	employed/student	no
VU5	24	f	university	employed/student	no

Table 5.2: Participant demographics. Total $N = 30$;

Demographic	**End users** $N_{End} = 18$	**Administrators** $N_{Admin} = 12$
Gender		
Male	7 (39%)	12 (100%)
Female	11 (61%)	0 (0%)
No Information	0 (0%)	0 (0%)
Age		
Min.	24	29
Max.	60	42
Median	28	34
Mean	34	34
Highest Completed Education		
Junior high	1	0
High school	4	5
University	13	7

Table 5.3: Administrators' Experience, as asked in the introductory questionnaire. Total $N_{Admins} = 12$;

	Number	**Percent**
Paid admin work	11	92%
Voluntary admin work	1	8%
Special IT-Sec Training	6	50%
Configured HTTPS Before	11	92%
Has written TLS-specific code	4	33%

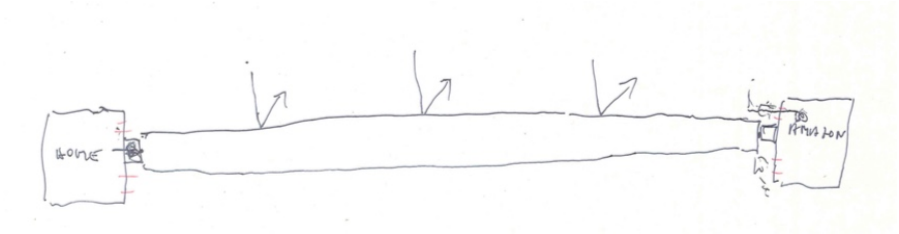


Figure 5.1: Example of a participant drawing (U09). Among other codes, this drawing was coded with F.5 scribbled line, G.4 local encryption component, J.5 not part of the model, N.5 model too sparse. [131]

For our analysis, we conducted inductive coding [47, 87, 88, 137, 155, 198] as commonly used to construct models and theories based on qualitative data in social sciences and usable security [133, 161].

We applied two rounds of open coding to detect observable patterns. We then performed Strauss and Corbin's descriptive axial coding [198] and selective coding to group our data into categories and models. We also used selective coding to relate the categories to our research questions. Throughout the coding process, we used analytic memos to keep track of thoughts about emerging themes. The final set of codes is listed in Appendix B.4.

As a first step, three researchers independently coded all questions and drawings of mental models. Subsequently, the resulting codes were discussed and refined to agree on a final code book. As a second step, two coders independently coded the data and again conflicts were resolved in discussions. To code drawings along with the think-aloud protocol, the coders looked at the drawings and read the audio transcript aloud. After each item, one or more codes were assigned. Our goal was to code contextual statements instead of singular entities of the drawings. Figure 5.1 shows an example of a drawing and selected assigned codes.

We calculated Krippendorff's Alpha [129] to measure the level of agreement among the coders. Our $\alpha = 0.98$ indicates a good level of coding agreement since the value is greater than 0.8 [129]. Most conflicts arose regarding the level of granularity of a drawing or representation. The conflicts were resolved based on discussions among all coders and additional consultation of the protocols and audio transcripts from the study.

Additionally, three researchers independently performed axial and selective coding to generate two models and two anti-models for HTTPS and message encryption. Then, the three coders met in person to reach agreement on these models and to resolve conflicts.

Our quantitative analysis is based on the closed questions from the questionnaire. We also evaluate quantitative aspects based on particular codes.

5.2.5 *Pilot and Post-hoc Validity Study*

During analysis, we observed that most participants naturally used the term encryption when articulating their understanding of HTTPS. Hence, it is natural to suspect a priming effect due to spatial task arrangement [158]. We conducted a post-hoc validity study with nine participants (four administrators [VA1-5] and five end users [VU1-5], demographics are shown in Figure 5.1) and a different set of warm-up questions and task ordering. The goal was to completely avoid the word "encryption" and let participants start with the HTTPS drawing tasks. The modified interview guideline is presented in Appendix B.3. The additional data was again coded, but no new codes emerged from these data, indicating that saturation was reached with the original study protocol.

5.2.6 *Ethical Considerations*

Both our institutions do not have a formal IRB process but a set of guidelines to follow for this kind of user study. A fundamental requirement of our universities' ethics guidelines is to preserve the participants' privacy and limit the collection of person-related data as much as possible. Therefore, every study participant was assigned an ID, which was used throughout the experiment and for the questionnaire. All participants signed consent forms prior to participating in our study. The consent form explained the goal of our research, what we expected from them, and how the collected data was to be used. The signed consent forms were stored separately and did not contain the assigned IDs to make them unlinkable to their real identities. The study complied with strict national privacy regulations and the EU's General Data Protection Regulation (GDPR).

5.3 RESULTS

In the following we present both quantitative and qualitative results along with selected direct participant quotes.

5.3.1 *Mental Models*

Our qualitative analysis yielded four different types of mental models representing the lower and upper bound of correspondence to the technical concepts of message encryption (as collected via drawing task 1 and shown in Figure 5.2, Figure 5.3) and HTTPS (as collected via drawing tasks 2 and 3, shown in Figure 5.4 and Figure 5.5). In the following, we provide qualitative descriptions and visualizations of the models and discuss the differences between administrators and end users. These differences are color-coded in the visualizations.

Section 5.3.2 discusses quantitative aspects of these models based on particular codes. The corresponding codebook can be found in Appendix B.4.

5.3.1.1 *Model of message encryption*

This model incorporates mental representations that correctly abstract the underlying technology and is shown in Figure 5.2. The main properties of this model are

- encryption and decryption are performed on the devices at the *communication end-points*,
- the *data in transit* is protected from attackers and eavesdroppers,
- the existence of *keys* is acknowledged, well-articulated models acknowledge the existence of two different keys (public and private), and
- that a vaguely defined *key exchange* process is required.

The model for both administrators and end users is conceptually correct but sparse when it comes to the purpose of these entities, especially regarding key exchange. Ten administrator participants mentioned that a key exchange via a key server or an in-person meeting needs to happen before sending encrypted messages, and 10 end users inferred during their think-aloud process that some kind of exchange needs to happen prior to communication. It is also notable that none of our participants actually incorporated key creation. Only one participant vaguely mentioned that the key should be created at some point without being able to further articulate how the process works. Our results indicate that administrators incorporated public and private keys more often than end users (as discussed in Section 5.3.2). Twenty-three participant drawings reflect properties of this model (thereof 12 by administrators and 11 by end users).

5.3.1.2 *Anti-model of message encryption*

Contrary to the (correct) model, the anti-model incorporates all mental representations that deviate from the actual components and workflow of message encryption. The model is shown in Figure 5.3, and its key characteristics are

- a centralized authority is a major component of this model and acts as *authentication service*, *message relay*, or *centralized encryption service*.
- while encryption is handled by the *centralized authority*, decryption is not part of the model.

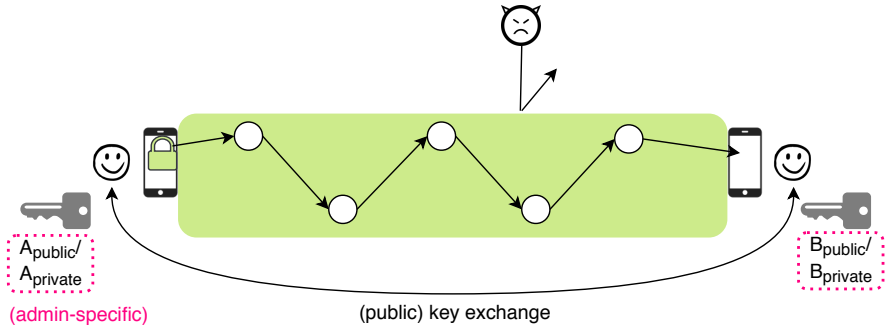


Figure 5.2: Model of message encryption. Entities that are solely reflecting administrator mental models are visually highlighted (dashed box in pink) [131].

- data in transit *is not protected from attacks*.
- keys are not articulated as components. However, a vaguely defined *code* is exchanged between the communication end-points and the centralized service.

Our results suggest that the misconception of a centralized authority is more common and specific to end user mental models. Six participant drawings (0 administrators, 6 end users) feature elements of this *anti-model of message encryption*.

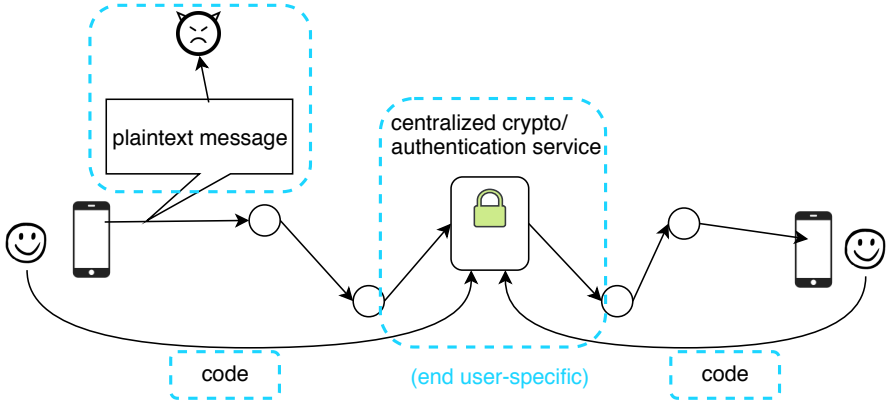


Figure 5.3: Anti-model of message encryption. Entities that are solely reflecting end user mental models are visually highlighted (dashed boxes in blue) [131].

5.3.1.3 *Model of HTTPS*

The best case model of HTTPS incorporates correct mental representations of the concept and components of HTTPS and is shown in Figure 5.4. Contrary to the correct model of message encryption, the correct model of HTTPS does not acknowledge the existence of keys (neither administrators nor end users mentioned them). This model is

based on the data gathered through drawing tasks 2 and 3. The main properties of this model are:

- *data in transit* is encrypted and protected from attacks,
- the existence of a *CA*, but no awareness of its role and context,
- the *browser* is perceived as relevant entity,
- best-case representations contain *security indicators* like the "https" prefix or a lock icon.
- (Mostly) administrators' mental representations contain *protocol-related tasks* such as certificate checks, TLS handshakes, or HTTP GET requests that are articulated as check lists without any further understanding of their purposes and the involved entities.

Similar to the correct model of message encryption, this model contains multiple nodes between sender and receiver. Administrators' mental models generally contained more entities (e.g., CA's, different devices) and protocol-related tasks. Nineteen participant drawings substantially overlap with the *correct model of HTTPS*; 12 were articulated by administrators and seven by end users.

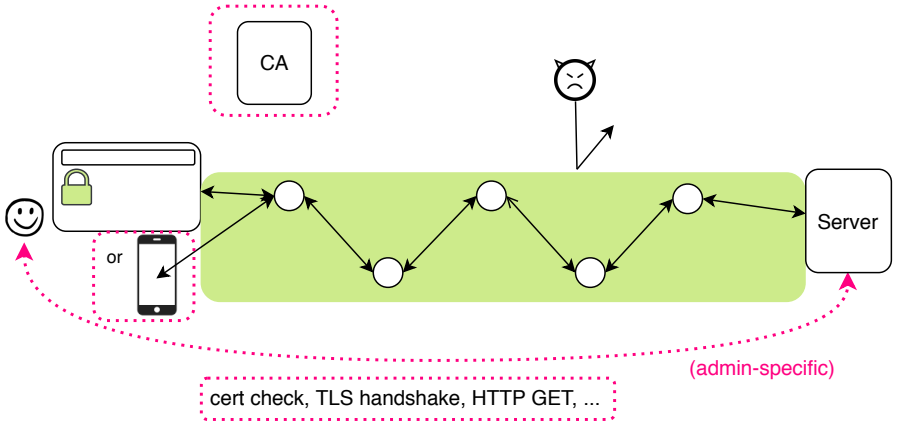


Figure 5.4: Model of HTTPS. Entities that are solely reflecting administrator mental models are visually highlighted (dashed boxed in pink) [131].

5.3.1.4 *Anti-model of HTTPS*

In contrast to the correct model of HTTPS but similar to the incorrect model of message encryption, the characteristics of this model are as follows:

- a *centralized blackbox HTTPS proxy* is responsible for authentication and/or encryption.

- the user's browser sends a *request/message along with a code* to the HTTPS proxy. The code is used to encrypt the data.
- if more security is required (e.g., in the case of online banking), the user sends an additional second factor to the HTTPS proxy, which then adds an *additional layer of encryption*.
- *decryption* is not part of the model. The server/website receives encrypted data, but it is unclear how it is then processed.
- *omnipotent attackers* such as intelligence agencies and surveillance programs, "hackers" but also ad trackers can attack the HTTPS proxy and eavesdrop information.
- *cookies* (represented by a gingerbread figure) may leak information via the browser.
- *smartphone* apps are generally perceived as insecure, regardless of whether HTTPS is used or not.

Especially end users (8 participants) thought that mobile devices and apps are not safe to be used in this context, as sensitive information may be leaked. Also, the idea of multiple layers of encryption using a code and an additional second factor was mostly part of end user mental models. Omnipotent attackers and a fairly negative security assessment are part of both groups' mental models. This model underestimates the security of HTTPS and does not contain keys, certificates, or security indicators. Interestingly, this is the only of the four meta-models that acknowledges the existence of metadata. Twelve participant drawings feature elements from this *incorrect model of HTTPS* (10 end user models and 2 administrator models also contained elements of this model).

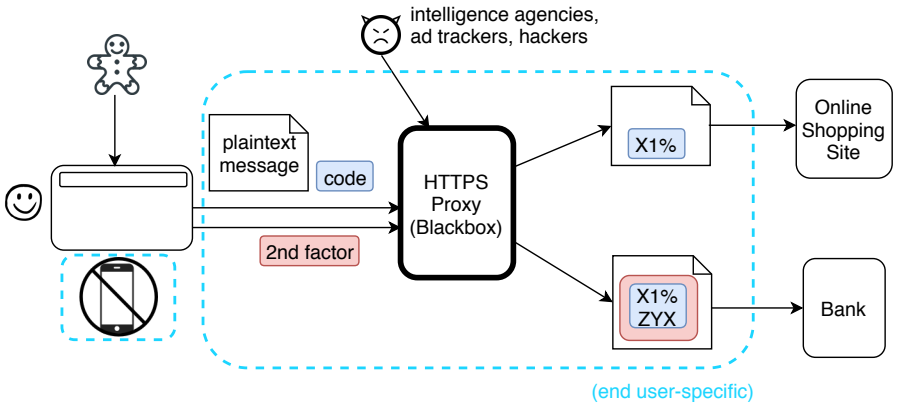


Figure 5.5: Anti-model of HTTPS. Entities that are solely reflecting end user mental models are visually highlighted [131].

5.3.2 *Mental Model Components and Emerging Themes*

We discuss themes and particular aspects that emerged during the drawing tasks and corresponding think-aloud protocol. Table 5.4 shows a selection of quantitative results per assigned codes where differences between groups are particularly interesting. The codes in parenthesis refer to the category codes (see Appendix B.5).

Table 5.4: Selection of mentioned concepts and identified codes. Percentages may not sum to 100 as some participants mentioned multiple aspects. p values are calculated with two-sided Fisher's exact tests comparing end users and admins, ϕ denotes the mean square contingency coefficient.

Code	End users	%	Admins	%	Total	%	ϕ (if $p < 0.05$)
Cryptographic concepts							
End-to-end (B.1)	11	61,1%	12	100,0%	23	76,7%	$\phi = 0.45$
Symmetric encryption (B.2)	3	16,7%	3	25,0%	6	20,0%	
Assymmetric encryption (B.3)	1	5,6%	8	66,7%	9	30,0%	$\phi = 0.1$
Blackbox (B.6)	2	11,1%	0	0,0%	2	6,7%	
Obfuscation or steganography (B.7)	2	11,1%	0	0,0%	2	6,7%	
Authentication (B.8)	1	5,6%	0	0,0%	1	3,3%	
Model too sparse (B.9)	5	27,8%	4	33,3%	9	30,0%	
Key generation and exchange							
Web of trust (D.2)	0	0,0%	1	8,3%	1	3,3%	
PSK: key server (D.3)	1	5,6%	1	8,3%	2	6,7%	
PSK: in-person key exchange (D.4)	2	11,1%	3	25,0%	5	16,7%	
PSK: undefined (D.6)	2	11,1%	6	50,0%	8	26,7%	
Shared knowledge (D.5)	3	16,7%	0	0,0%	3	10,0%	
Model too sparse (D.1)	11	61,1%	3	25,0%	14	46,7%	
Security indicators							
HTTPS (J.1)	4	22,2%	3	25,0%	7	23,3%	
Lock icon (J.2)	3	16,7%	5	41,7%	8	26,7%	
Checkmark (J.3)	0	0,0%	2	16,7%	2	6,7%	
Insecurity indicators (J.4)	0	0,0%	1	8,3%	1	3,3%	
No indicator (J.5)	13	72,2%	7	58,3%	20	66,7%	
Perceived security benefit of HTTPS							
Underestimated (K.1)	8	44,4%	1	8,3%	9	30,0%	$\phi = -0.39$
Realistic assessment (K.3)	6	33,3%	6	50,0%	12	40,0%	
Model too sparse (K.4)	3	16,7%	6	50,0%	9	30,0%	
No control (K.5)	1	5,6%	1	8,3%	2	6,7%	
Meta observations							
More buzzwords (T.1)	3	16.7%	7	58.3%	10	33.3%	$\phi = -0.43$
Conceptual model (V.2)	10	55.6%	3	25.0%	13	43.3%	
Protocol-based model (V.1)	1	5.6%	6	50.5%	7	23.3%	$\phi = -0.51$
Third Parties							
Centr. encryption/auth. service (M.1, M.9)	11	61.1%	0	0.0%	11	36.7%	$\phi = -0.62$

5.3.2.1 *User Expectations of Security Tools*

When asked of which *encrypted tools, apps or devices* they were aware, end users mostly referred to mobile apps (15 participants) and sensitive services such as banking services (14 participants) or phone calls (1 participant). Nine end users self-reported a lack of knowledge (see blue bars in Figure 5.6). In contrast, administrators (red bars) mentioned a broad spectrum of tools and applications, ranging from

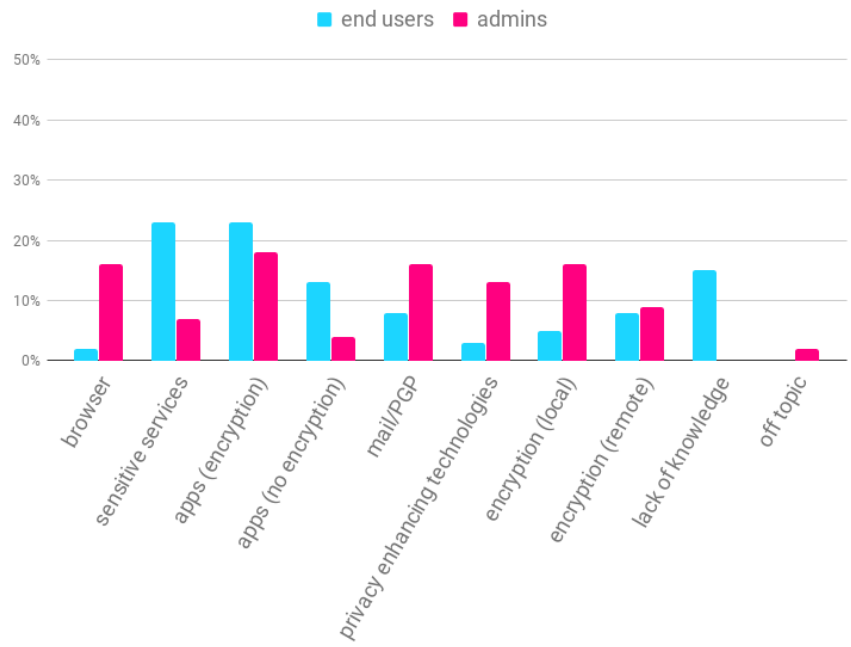


Figure 5.6: Reported knowledge of encrypted tools, apps or devices. Each bar indicates how often a certain category was named in relation to all namings. (Multiple mentions per participant) [131]

browsers (7 participants), email services (7 participants), and privacy preserving technologies such as VPN, SSH or Tor (6 participants) to local encryption such as disk encryption (1 participant) and remote encryption such as servers (4 participants). Interestingly, 8 end-users and 2 administrators explicitly stated that mobile apps are generally not encrypted and hence, untrustworthy. One end user (U04) reported to avoid mobile apps to handle sensitive data and that he accesses sensitive services, such as online banking, solely via the browser on his PC. This is in line with findings by Chin et al. [50] showing that users are commonly apprehensive about running sensitive tasks on their phones. Notably, eight non-experts and two administrators specifically brought up WhatsApp as a negative example of an application that is not or only partly encrypted. This implies that either the messaging app's initiative to offer end-to-end encryption did not yet reach all of its users or that users do not trust the service.

5.3.2.2 *Mistrust in HTTPS and Browser Security Indicators*

When it comes to *expectations of visiting a site with HTTPS*, nine end users reported a lack of knowledge, and some even claimed that they have never noticed the security indicator before (see Figure 5.7). One participant mixed up the HTTPS lock symbol with user authentication resp. authorization:

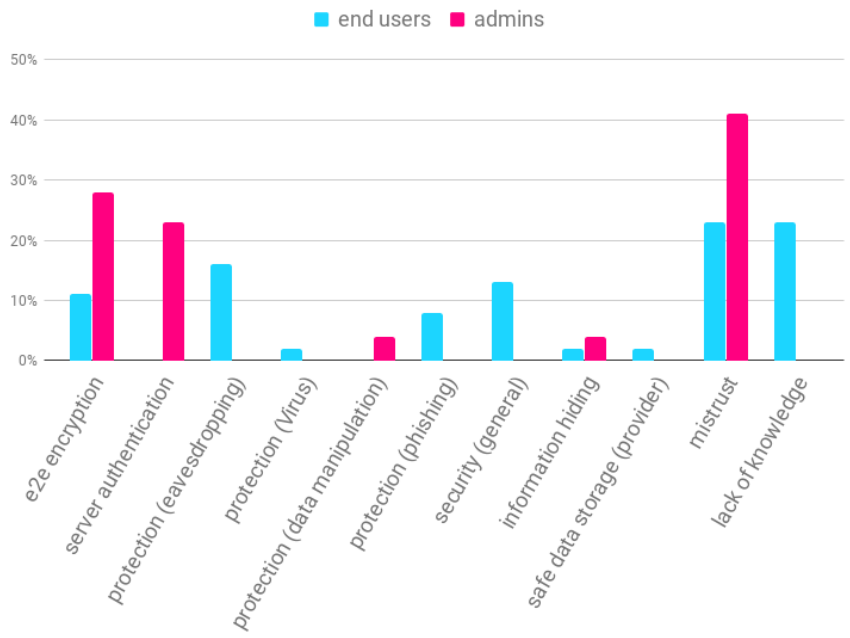


Figure 5.7: Reported expectations on HTTPS. Each bar indicates how often a certain category was named in relation to all namings. (Multiple mentions per participant) [131]

> "I think the lock symbol means that I have to authenticate myself. As I frequently forget my passwords, I usually try to click around to get rid of this symbol." (U12)

This shows that users still do not properly recognize the HTTPS security indicator, although much work has focused on improvements in this area. End users described their expectation of HTTPS on a superficial level, using general terms related to security and eavesdropping protection without further elaboration. Three participants wrongly assumed that HTTPS would protect against phishing, and one participant thought that HTTPS could ban viruses. Interestingly, one end user stated that

> "HTTPS prevents people from seeing what their partner did on the Internet or the employer from seeing whether employees were not working when they should have been." (U12)

None of the end users mentioned server authentication. In contrast, six administrators named end-to-end encryption and five server authentication. However, we observed that administrators described the two concepts decoupled from each other, which is in accordance with the finding from Fahl et al. [75] that administrators are not aware of the necessity of server authentication when establishing a secure encrypted channel.

Another emerging topic was mistrust in the security indicator and mistrust in HTTPS as a protocol. Generally, we were surprised about the high frequency of expressed mistrust against HTTPS and the security indicator coming from both end users (7 participants) and administrators (6 participants). One administrator stated that HTTPS does not offer eavesdropping protection, claiming

> "The lock symbol does not mean anything, it is pure marketing". (A06)

After this statement, we asked the participant a series of follow-up questions to allow him to clarify. As a result, the participant referred to powerful attackers and large (government) organizations and said that the arms race with powerful attackers is almost impossible to win for defenders.

Another dominant theme was the underestimation of the security benefits of HTTPS. For example, one end user articulated

> "The lock symbol puts security in people's mind with the purpose to build up trust. This does not mean that the website is secure." (P01)

Security indicators are a critical UI component of modern browsers [81]. The results from our study, however, suggest that security indicators are rarely part of user mental models. Twenty participants did not include security indicators in their drawings and the associated think-aloud protocol. One participant explicitly used an *insecurity* indicator in their drawing (note that the interviews were conducted shortly before Chrome started notifying users of unencrypted connections). The other participants referred to either the lock icon (5) and/or the HTTPS prefix (5) in their drawings.

5.3.2.3 *Perceived Security Benefits of HTTPS*

With respect to security perceptions, the elicited mental models were rather diverse. Eight out of the 18 end users from our study clearly underestimated the security benefit of HTTPS. Six end users had a realistic assessment of the security of HTTPS and understood that HTTPS encrypts the entire transport layer instead of just single data elements such as a username and a password, or a credit card number. U09 explicitly stated that he had no deeper understanding of keys, certificates, and other system components, but had a (correct) basic understanding of the underlying concept of transport layer encryption.

In the context of the two HTTPS-related drawing tasks, the participant said:

> "I expect the connection to the online shop to be secure (or insecure), irrespective of whether I want to buy a pen or a house." (U09)

A few participants also misunderstood the security benefits of HTTPS and assumed that it prevents any form of data leakage (2 non-experts) and can even prevent phishing attacks (3 non-experts). One participant imagined HTTPS to be a completely encapsulated system where all attempts to attack the sensitive information are bounced off.

> "HTTPS inhibits tracking, it is a completely encapsulated system that does not share the data." (U03)

Another participant (end user) perceived HTTPS as a tunnel between him and a server:

> "The connection between me and the server goes via a tunnel, and attempts to attack the data bounce off" (U09)

One administrator also described HTTPS and the attacker model as a tunnel:

> "SSL is like a tunnel, and data can be pushed through this tunnel." (A04)

Irrespective of security indicators, many participants expressed general distrust towards encrypted connections.

> "I always feel queasy, anyway. Nothing on the Internet is secure." (U01)

While for some types of attacks (e.g. phishing, malicious Javascript, or drive-by downloads) this is a true statement, this was not the type of attack to which the participants typically referred. Surprisingly, most participants questioned the protection mechanisms against attacks that HTTPS *can* protect them against (e.g., third parties stealing their passwords/credit card numbers when submitting a web form to an online shop).

Seven non-experts and six administrators expressed general doubts about whether cryptography can achieve what it promises. However, the participants considered cryptography necessary to protect various assets. Thirteen out of 18 end users mentioned sensitive data related to purchases or personal information as crucial to be protected by cryptography. Administrators again showcased a more diverse idea, referring to sensitive data (2 participants), protocol specific data (1 participant), as well as local data (1 participant) or data in transit (2 participants). Both end users and administrators had a similar picture of successful attackers, believing that the state, the police, or the secret

service (26 participants) as well as hackers (19 participants) and big companies such as Apple, Facebook, or Google (18 participants) are the most persistent attackers.

5.3.2.4 *Centralized Components and Authorities*

Another emerging theme was centralization vs. decentralization and powerful authorities. Eleven end users included a *centralized encryption entity* in their drawings, i.e., a remote service that is responsible for encryption and then forwards the encrypted data to the communication partner or to the online shop. In other models, the centralized component acted as a message release point that 1) checks the message for suspicious content and validity, 2) encrypts it, and then 3) forwards it to the receiver. Comparing our findings to related work, we observe that end users perceive other de-centralized cryptographic tools as centralized systems [84], or use centralized components since they are perceived as more trustworthy [132].

An interesting observation is that only one participant (U08) included key generation in their model. All other participants implicitly or explicitly assumed that the key was already there by default and did not include key generation in their models. Only a few participants discussed key exchange as part of their drawing and explanation as shown in Table 5.4.

5.3.2.5 *Authentication vs. Encryption*

Furthermore, misconceptions about the differences between encryption and authentication emerged as a theme for both groups of participants. Both end users and administrators from our sample confused encryption with authentication. In general, 13 users expressed concerns regarding the protocol's security promises. Especially when it comes to 2-Factor-Authentication (2FA), a common misconception of end users was that the secondary factor was used to add an additional layer of encryption. Participant U11 argued that 2FA is required for online banking to compensate the lack of security provided by HTTPS.

> "HTTPS is a bad protocol. If HTTPS were secure, I wouldn't need 2FA." (U11)

5.3.2.6 *Differences between Administrators and End Users*

For both groups of participants, mental models were diverse even among experienced administrators.

When asked about how they think *encryption works in theory*, 10 of 12 administrator drawings reflected concepts of end-to-end encryption. In comparison, fewer than 50% of the end user drawings clearly depicted

end-to-end encryption. Four end users incorporated symmetric keys in their drawings and two explicitly mentioned private and public keys without being able to further elaborate why two keys are necessary. In contrast, seven administrators explicitly referred to asymmetric encryption in their drawings and the think-aloud protocol. More than half of the end user mental models referred to a third party that acts as encryption entity or proxy, or, referred to encryption as a blackbox. One participant (U03) used ephemeral keys and anther one (U15) thought that encryption was the same thing as obfuscation and steganography. In contrast, none of the administrators' drawings reflected such misconceptions.

While comparing the differences between administrators and end users, a theme emerged. Our results suggest that expert mental models are mostly protocol-based instead of conceptual compared to non-experts. Most administrators were familiar with specific protocol characteristics, such as which messages are exchanged between server and client and how connections are established.

When asked to explain the underlying concepts, most administrators were unable to explain how HTTPS works and had sparse mental models of the underlying fundamentals and their interplay. This was often the case even for the first drawing task, which asked participants to depict how sending an encrypted message through any channel works in theory. Even in such a straight-forward scenario for knowledgeable users, some administrators showed and even admitted significant knowledge gaps. However, we also observed that administrators concealed these gaps more frequently and randomly dropped associated technical terms without being able to explain what they mean. Some participants, though (such as A09), explicitly admitted major knowledge gaps:

> "How HTTPS works... those are the things that I always forget. You should have asked me five years ago." (A09)

Another example of an administrator lacking conceptual knowledge but getting stuck on a configuration detail was participant A4, who said:

> "I am really not sure how Firefox validates certificates, but I know that Chrome uses the Windows Root CA." (A4)

In general, our results suggest that the administrators' level of expertise is rather diverse, much like that of end user participants. While some had sparse and incomplete mental models of encryption or HTTPS in particular (e.g., A09, A10, A11), some were confident and able to articulate how HTTPS works in a very detailed and accurate way.

5.3.2.7 *Mental Model Evolution*

Figure 5.8 shows the mental model refinement over time across the three drawing tasks. The refinement between the first and second drawing task was equally distributed across our participants. In contrast, 26 participants had a constant level of detail of their mental models across drawing tasks 2 and 3.

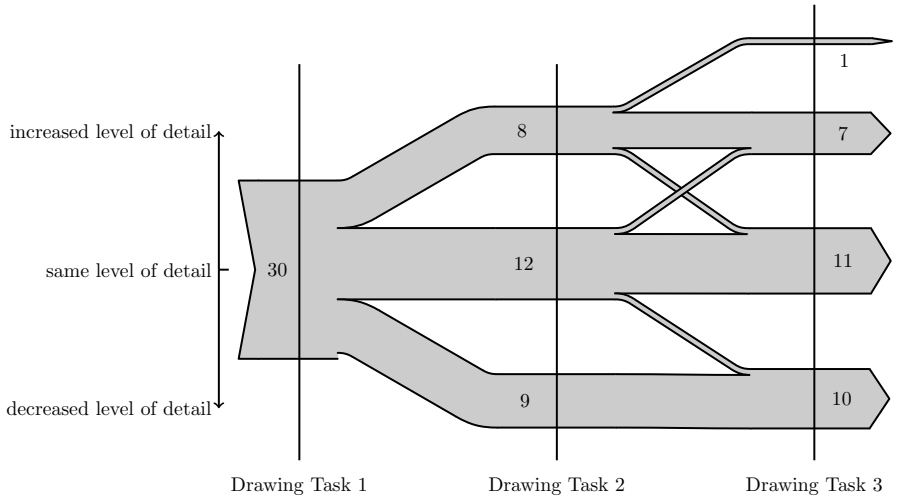


Figure 5.8: Development of user mental models across the 3 drawing tasks. [131]

5.3.2.8 *Terminology and Visualization Components*

While most administrators used *technical* terminology to elicit their mental models, end users sometimes created new terminology to compensate for missing technical terms in their vocabulary. The most frequently used technical term by the administrators was *cipher* followed by *session key* and *hash*. Twelve participants did not include a visualization of the encrypted message in their drawings. Five participants represented the encrypted message as scrambled text or numbers, four used a lock icon, three drew physical objects like an envelope or a treasure chest, and three marked the encrypted message with a different color. Others used scribbled lines, a different language, or chopped text.

For the first drawing task, 20 participants used an abstract example scenario. The remainder used an arbitrary messaging app or referred to apps and tools they knew from their everyday lives (Signal, WhatsApp, PGP/GPG).

Twenty-one participants clearly understood the connection between drawing tasks 2 (visiting an online shop) and 3 (visiting a bank's website).

Our results also suggest that only three participants were aware of the existence and associated risks of (unencrypted) metadata.

Regarding mental models of HTTPS, we classified 12 models as clearly conceptual, seven as protocol-based, and two with both conceptual and protocol-specific components. The remaining nine models were too sparse to classify them. Ten participants explicitly admitted their knowledge gaps and eight participants tried to cover them.

5.3.2.9 *Structure-Behavior-Function (SBF) Model*

The *Structure-Behavior-Function (SBF) framework* was proposed by Goel et al. [91] to describe complex systems based on three pillars: (1) *structure* (system components), (2) *behavior* (change of the system over time), and (3) *function* (effect of the system on the environment). It is often used by cognitive psychologists to describe mental models and compare them to actual system descriptions.

Hmelo-Silver et al. [106] applied the SBF framework in order to model novices and experts' understandings of complex systems. They found that the novices' system perceptions mostly focused on concrete aspects related to the structure of the system, often simplifying causality and assuming central control. In contrast, experts were more likely to discuss behavioral aspects.

Applying this model to HTTPS, we model an end user's computer or a server hosting a web page as structural components. We model behavioral aspects as perceivable browser indications. Functional aspects comprise authentication of end users and encryption of the communication path, resulting in a protection against various attack vectors such as eavesdropping or traffic injection.

The results from our study suggest similar trends to those presented by Hmelo-Silver et al. [106]. End users' representations frequently include structural aspects and assume a central entity pursuing encryption. Furthermore, the end users from our study rarely included descriptions of behavioral or functional aspects, showing neither that their perception of security indicators is particularly strong nor that they are aware of the actual purpose of HTTPS.

In contrast, the administrators largely focused on behavioral aspects and delivered abstract representations of state transitions (such as sequence diagrams of protocols). Nevertheless, the administrators' system descriptions are lacking functional aspects. The administrators furthermore described the protocol behavior mainly decoupled from its actual purpose. An interesting observation from our study is that none of our expert participants clearly pointed out at which point of the protocol execution the encryption starts. Hence, our results show that neither end users nor administrators are able to link the structural aspects of HTTPS and behavioral aspects to the actual function that the protocol achieves.

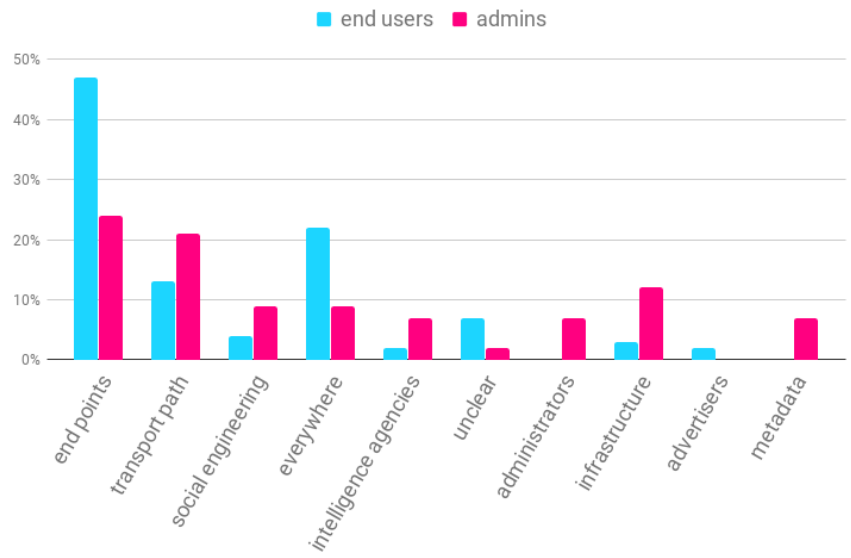


Figure 5.9: Attacker models in participant drawings. Each bar indicates how many percent of all drawings feature a certain attacker type. [131]

5.3.3 *Threat Models*

After the participants finished all three drawing tasks, we asked them a set of warm-up questions about attacker models followed by another drawing task asking a participant to mark where an attacker could eavesdrop. We coded these vulnerable components and present the results in Figure 5.9.

The most mentioned component believed to be vulnerable to attacks were the communication endpoints, which 26 of 54 end user drawings and 10 of 35 expert drawings featured. Besides the endpoints, many end users stated that attackers could eavesdrop everywhere within the communication process, while expert users tended to differentiate more and name concrete attackers or attack models.

Most participants visualized the attackers with arrows or circles indicating the vulnerable components of their drawings. Some participants chose to insert attackers with a drawn representation, e.g., a set of eyes (A08), exclamation marks (A11), or stick figures as actual shoulder surfers (A10). Especially regarding the endpoint attackers, not only were malware or infected devices given as the enablers of eavesdropping, but also shoulder surfing (A10) and actual violence against human users (A11).

5.4 DISCUSSION AND IMPLICATIONS

In this section, we discuss our findings and derive potential implications on correct, incorrect, and sparse models (where essential com-

ponents are missing for cases which put users directly at security or privacy risks).

Our analysis of mental models of HTTPS indicates differences between the two groups of participants. While administrator mental models were generally protocol-based and correct even if sparse, the mental models of end users were sometimes not only sparse but simply wrong or non-existent. Indeed, our user study was an opportunity for some end users to think about HTTPS and web encryption for the first time. However, we argue that fine-grained and fully correct mental models can and should not be expected from end users and partly not even from knowledgeable administrators. Thus, the following discussion places emphasis on misconceptions which crucially interfere with a secure and privacy preserving usage or configuration of HTTPS as well as actionable conclusions to mitigate these risks.

We also observed interesting corner cases which should not be ignored when discussing consolidated findings. Examples of such corner cases include contradictions, the confusion of authentication and encryption, or the assumption that publicly-available comments (i.e., consumer ratings) are not sent encrypted since this would prevent other consumers from reading them in plaintext. In contrast to the lower bounds of comprehension, we also found examples for the higher levels, e.g., an administrator who had a deep understanding of technical and operational details.

5.4.1 *Implications from Correct Mental Models*

The condensed representations of correct models show that participants of both user groups have a basic understanding of end-to-end encryption. In addition, the threat awareness was better than we initially expected. Many end users were aware that communication endpoints are often vulnerable (e.g. insecure devices like smartphones). This is a realistic assessment, since many smartphone vendors cease to ship security updates for their devices long before they reach their end of life. In contrast, administrators seem to focus on sophisticated but rare attacks, such as "man-in-the-middle." This may indicate an influence of tech news outlets and scientific publications which usually focus on more sophisticated attackers. Overall, we regard this as a benevolent effect since administrators should be aware of these attack types in order to deploy adequate countermeasures, and end users are currently held responsible for managing the security of their devices through, for example, regular OS and app updates.

Our results also indicate that mental models of end users may be influenced by media and marketing campaigns as the comprehension of message encryption (task 1) was often higher than the understanding of general HTTPS-encrypted traffic in web browsers. We hypothesize that one reason for this difference may be higher media coverage of

message encryption in comparison to HTTPS. In addition, several app manufactures (e.g., WhatsApp) specifically point out end-to-end encryption when users start a new conversation.

Finally, the pictorial representations of mental models indicate interesting differences between end users and administrators: while end users' correct models were rather conceptual, administrators' models were mostly protocol-related and often illustrated operational details. The protocol-based representations reminded us of flow charts common to academic lectures and online tutorials, suggesting that many administrators tried to recall previously-seen educational material.

However, there is still room for improvement, since even correct representations were often sparse. For example, only the best representations pointed out security indicators, and important aspects like key exchange and certification authorities (CA) were hardly mentioned. Overall, the correct mental models indicate that media coverage, marketing, and education can help in forming folk models, even for complex processes like HTTPS.

5.4.2 *Implications from Incorrect Mental Models*

While correct mental models emphasized the value of end-to-end encryption, participants with incorrect mental models tended to underestimate the security benefits of HTTPS and furthermore assume that omnipotent attackers can eavesdrop at multiple stages of online communication. We hypothesize that this might be the result of press attention on misuse of SSL/TLS in mobile apps created by the work of Fahl et al. [75] and Cothia et al, among others. [51]. Consequently, end users are incapable of making informed security decisions as they do not trust the protocol in even its best-case configuration. As a consequence, end users do not demand proper configurations. Even though WhatsApp was already mentioned as an example of an application which explicitly advertises end-to-end encryption, some users might not even recognize such notifications (or simply mistrust them) as WhatsApp was constantly mentioned as an example for an app being not or only partly encrypted. While this seems to not prevent users from using WhatsApp, it shows that the security benefits of end-to-end encryption are often not perceived as such.

Even more worrisome, we identified corner cases of incorrect mental models which may directly put users at risk. For example, one end user thought that HTTPS can protect against phishing web sites. Such assumptions may lead to an unjustified sense of security whenever HTTPS connections are indicated by the browser. We also found that end users were often not aware of security indicators or they were perceived as unimportant. Overall, the results show that the end users' interest in these indicators is mitigated by general mistrust in the protocol (i.e., the belief that cryptography/HTTPS cannot prevent

attacks and eavesdropping). Similarly, we found that many users are not impressed by warnings of insecure connections, since they do not trust the protocol in the first place. While administrators generally have more correct mental models, their representations frequently lacked important parts and meaningful interconnections. Also, the administrators' statements indicated a high level of mistrust. As an example, one administrator (A06) claimed that "The lock symbol does not mean anything, it is pure marketing". Additionally, administrators frequently expressed mistrust in the PKI system. These two facts might explain a diminished interest in configuring certificates correctly.

In summary, the incorrect mental models indicate that end users do not trust the security that HTTPS can offer if deployed in a best-case working scenario. We argue that recent news reports about intelligence activities influenced perceptions about omnipotent attackers and that users need to build up trust before concepts like security indicators and warnings can be effective. The multi-step approach of our user study indicates that education and brain teasers can be promising in that they helped many users adjust their mental models even if considering some aspects of HTTPS for the first time. For example, we observed that thinking about threat models caused participants to review and refine their mental model drawings in some cases. End user participant U12 stated, "Now I see that I didn't think logically" before revising her drawing for task 1. The same was true for administrators who became more aware of metadata leakage after being asked about potential attacks.

5.4.3 *Implications from Missing and Sparse Mental Models*

In addition to correct and incorrect mental models, interesting implications can be derived from sparse models, as well. We found that keys and certificates are not part of the correct conceptional representations of most mental models, which implies that users do not understand their purpose within the concept. We argue that not being aware of their purpose reduces the chance that users verify certificates manually. The same is true for keys in other application scenarios: it is no surprise that key verification in mobile messaging apps is rarely performed, as users are not aware of its necessity nor the underlying threat model that this measure protects them from. Helping users understand the functional perspective of keys and certificates in HTTPS and encrypted messaging is thus one of the main challenges for future research. While not all conceptual parts need to be understood by users, it is essential that users are motivated to engage measures demanded by the security concept.

Even though some administrators mentioned keys and certificates with respect to HTTPS, they tended to use them as buzzwords in their articulations and were often unable to explain how these components

contribute to a secure configuration. In addition, we found that most administrators were not aware that server authentication is a prerequisite for establishing a securely encrypted channel (which corresponds to the results from Fahl et al. [75]).

5.4.4 *Potential Countermeasures and Improvements*

While our data does not provide direct evidence for this, we hypothesize that education and online tutorials contribute to these mental models. This corresponds to the findings from Krombholz et al. [133], who showed that even administrators who successfully configure HTTPS strongly rely on online sources as they do not have a full understanding of the underlying concepts. For end users, our results have implications on security indicators, warnings and other UX cues that are designed to assist users in making informed security decisions.

5.4.4.1 *Suggested Workflow Changes for Tools and APIs*

We found that administrators often do not understand the interplay of functional protocol components (e.g. the CA, certificates for E2E, keys). In particular, our results suggest that the role of certificates and PKI as a whole for setting up an encrypted channel are poorly understood by administrators which indicates that administrators could benefit from a deployment process which more clearly illustrates the linkage between these components, resp. hides this complexity from them. Hence, as keys and certificates remain important functional components even in more user-friendly deployment concepts such as *Let's Encrypt*[2] and *Certbot*[3], it is necessary to provide tangible explanations to make their contribution to a secure configuration more intuitive. We acknowledge that Let's Encrypt and the ACME Protocol offer promising usability enhancements from the administrators' point of view, since they enable automatic issuance of certificates. However, these initiatives mainly simplify the process of obtaining a certificate, but do not completely obviate the need for its users to deal with certificates, keys and additional hardening measures. As our results show that the biggest challenge for administrators is to put these different components together in order to deploy a secure authenticated-encryption mechanism, we suggest that future protocol designs should aim at hiding this additional complexity from users.

Although we expected that server authentication was part of user mental models, our results suggest that this is rarely the case. Hence, the concept of server authentication along with its importance for communication security needs to be reflected in the user interface

2 `https://letsencrypt.org` – accessed: 2020-03-11.
3 `https://certbot.eff.org` – accessed: 2020-03-11.

in order to make server authentication part of user mental models. Such UI components should also motivate users to verify the server's authenticity.

An example for a promising starting point in this regard is the NaCl API presented by [26], which provides one simple function referred to as *crypto_box* that comprises several functionality for authenticating and encrypting a message.

5.4.4.2 *Trust Establishment*

Our results suggest that especially end users need UX cues that help to construct valid mental models, as these are important to establish trust in the protocol and its security properties. In order to deal with general mistrust towards HTTPS, we argue that the protocols in today's Internet ecosystem and the upcoming Internet of Things should provide state of the art encryption by default and that insecure protocols such as HTTP should be abandoned to establish a more user-friendly distinction between best-case security and vulnerable connections. Also, a security-by-default state would obviate the need for users to regularly check HTTPS-specific UI components. For end users, mistrust in the protocol and misconceptions about the role of certificates can lead to wrong decisions when warnings are displayed, putting users at danger of privacy and security violation. This is in-line with latest innovations enforced by Google[4], who at the time of writing began to roll out a new version of the web browser Chrome not showing any security indicators for HTTPS secured websites anymore. At the same time, websites still using HTTP are marked as insecure by displaying a red insecurity indicator in the address bar. Google argued that users should expect a secure Internet by default, which is in-line with our findings. Also, our results suggest that security indicators are often not part of end user mental models, which is why we agree with Google's less ubiquitous yet more precise risk communication with indicators.

5.5 LIMITATIONS

While we refrained from recruiting computer science students, our sampling method still has limitations. We aimed to recruit a diverse sample of users, however our sample is still skewed towards the more educated social class. Furthermore, our end user sample skewed female, but we did not manage to recruit a single non-male administrator. Sadly, female administrators are very rare in our region. Our sample was recruited in Central Europe which is generally privacy-aware, and HTTPS adoption rates are generally higher than e.g., in

4 https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

Japan [80]. Our results are therefore impacted by cultural effects. As research on perceptions of cryptographic tools and algorithms is still in its early stages, we followed an inductive approach and opted for a qualitative study to construct models and theory grounded in the data. Naturally, our methodology also has its limitations. The data is self-reported and qualitative in nature. While our sample is still sufficiently large to perform basic statistic tests, further investigations are necessary to determine large-scale effects and hence obtain significant results with larger effect sizes. We refrained from asking closed-ended knowledge questions. Also, the results from our pre-study showed that participants like to litter buzzwords which is why we designed our study to get a deeper context of their understanding. Our goal was to allow our participants to openly articulate how they think the protocol works. We decided to group our participants based on their role of being an administrator instead of their knowledge to avoid biasing effects by previously defined answer options.

5.6 CONCLUSION AND FUTURE WORK

In this chapter, we presented a qualitative study on user mental models of HTTPS. In examining 18 end users and 12 administrators, our approach revealed four types of user mental models of HTTPS and (abstract) message encryption. We furthermore revealed misconceptions about threat models and protocol components that lead to decisions that influence the security of the systems and, as a result, directly put users at risk.

Additionally, we shed light on differences between end users' and administrators' perceptions; while end user mental models were mostly conceptual, administrators' mental models frequently contained protocol components and technical terms without accompanying understanding of their functionality and purpose within the protocol configuration. Among other insights, our findings suggest that 1) many users confuse encryption with authentication, 2) end users assume the omnipotence of attackers and significantly underestimate the security benefits of HTTPS, and 3) many users of both types generally ignore or even distrust security indicators.

Our work reveals reasons for the usability challenges determined by Krombholz et al. [133] that are often responsible for vulnerable HTTPS configurations. Our results, furthermore, explain why users often fail to correctly assess the implications of clicking through warnings. And, finally, we provide foundations for future designs of cryptographic protocols that are easier for administrators and developers to deploy or implement related code in the most secure manner and therefore minimize the exposure of end users to security-critical decisions when communicating online.

As future work in this direction, it remains to show how our findings can be used to inform the design of future cryptographic protocols. We think that our results can inform a larger (quantitative) study which could make use of closed-ended questions. Such future work could also include questions on administrator qualifications and knowledge questions to measure large-scale effects and to perform multivariate analyses.

6

SECURITY ADVICE AND PRACTICES

This chapter is based on joint work with Julia Schäfer (University of Bonn), and Matthew Smith (University of Bonn) which has been published at SOUPS 2019 [39]. I conducted and evaluated the studies and wrote a majority of the paper. See Appendix F for a detailed authorship agreement.

We thank Iulia Ion, Rob Reeder, and Sunny Consolvo for their cooperation and support of our replication efforts. Furthermore, we thank all the people who helped in distributing and sharing the expert survey.

The previous chapter has shown that IT experts have somewhat different mental models when compared to end users. We continue this differentiated research of experts and non-experts in the following work on security practices and advice.

A 2015 study by Iulia Ion, Rob Reeder, and Sunny Consolvo examined the self-reported security behavior of security experts and non-experts. They also analyzed what kind of security advice experts gave to non-experts and how realistic and effective they think typical advice is.

Now, roughly four years later, we aimed to replicate and extend this study with a similar set of non-experts and a different set of experts. For the non-experts, we recruited 288 MTurk participants, just as Ion et al. did. We also recruited 75 mostly European security experts, in contrast to the mostly US sample from Ion et al. Our findings show that despite the different samples and the four years that have passed, the most common pieces of expert advice are mostly unchanged, with one notable exception. In addition, we did see a fair amount of fluctuation in the long tail of advice. Non-expert self-reported behavior, however, is unchanged, meaning that the gap between experts and non-experts seen in Ion et al.'s work is still just as prominent in our study. To extend the work, we also conducted an A/B study to get a better understanding of one of the key questions concerning experts' recommendations, and we identified types of advice where research by the usable security community is most sorely needed.

6.1 INTRODUCTION

Whenever the media picks up on the latest data breach, various sources seize the opportunity to give advice such as "Do not use the same passwords for all systems" [68] or "Antivirus software is crucial to protecting your computer." [162] Under this barrage of different advice, selecting and following "good" advice is a difficult task for users [74]. Factors such as socioeconomic status, consumer habits, or conveniences also play a role in the decision-making process [174, 176]. Even when advice is regarded as "good" by a user, it is not necessarily a given that they know how to apply it in their own individual context. We must not overlook the limits of users' capability taking into account the complexity of any advice we give [23].

In 2015, Ion, Reeder, and Consolvo explored the opinions and beliefs of expert and non-expert users in a survey study and found that

users neglect three vital security practices that experts strongly advise: installing software updates, using two-factor authentication, and using a password manager. On the other side, non-experts regarded antivirus software as a very important security practice, unlike the experts, who were not convinced by it. Almost four years have passed since that study, which is a long period of time in terms of technological innovation and security practices. Security and privacy continue to gain more widespread recognition, so we were interested to see what, if anything, had changed with respect to expert advice and non-expert self-reported behavior.

We thus conducted two online surveys, one for experts and one for non-experts, and compared the results to the previous study by Ion et al. Many of the past security topics and advice covered in the original work are still relevant today. We also discovered that some of the topics relevant to users in the past have been replaced by newer topics, for example, the spread of blocking extensions for web browsers, which are able to manage cookies. Where in the past, users were concerned with regularly deleting cookies, they now rely on blocking extensions.

Apart from seeing if and how our sample differed from the original, we wanted to explore a methodological issue in the original study. One of the central parts of the original study concerned how effective *and* realistic particular types of advice are. This information from experts was gathered using compound questions, and the advice was ranked and compared on that basis. Compound questions can be problematic because it is not clear how participants combine the separate components [17]. For example, when asked to rank advice on a five-point scale, a 3 could mean an expert thought that a piece of advice was extremely effective (5) but completely unrealistic (1), or vice versa, and the expert combined the two values into a simple average. However, a 3 could also be given because the expert thought the piece of advice was a 3 regarding realism and a 3 in effectiveness. To make matters worse, the same separate assessment from above (extremely effective (5) but completely unrealistic (1)) could also be combined by the expert into a 1 if the expert takes the view that if a piece of advice is unrealistic, then the combined effectiveness is also a 1 . So the same separate assessments can lead to very different combined scores and separate results from the same assessments can lead to very different combined scores.

While the combined score is useful because it reflects the personal assessment of an expert participant using whatever weighted combination they deem most appropriate, it potentially hides interesting discrepancies that could highlight which pieces of advice could be particularly important for researchers to improve and, more specifically, which areas need improvement. For example, a piece of advice that gets a 5 for effectiveness but a 1 for realism is probably a good candidate for researchers to improve the usability. On the other hand,

a 4 on realism and a 2 on effectiveness could indicate that systems research is needed to improve effectiveness or it might be best if the advice is discouraged, since it uses up valuable security budget without being particularly effective. To be able to compare our data directly with the original work by Ion et al., in addition to gaining the insights described above, we gave half our expert participants the original compound questions and half the experts got the questions broken down into their compound elements.

Based on our analysis, we suggest four fields where usable security research is needed to improve existing methods or invent new ways of handling the implied security issues. The areas are: password security, two-factor authentication, links and attachments, as well as application updates. Out of these four fields, three were already prominently discussed in the original work, suggesting that the research and engineering communities in usable security still have a lot of work to do.

The remainder of this chapter is structured as follows: Section 6.1.1 gives an in-depth look at the original study by Ion et al. Section 6.2 documents our survey methodology for both the expert and non-expert surveys and discusses the design changes we made. In Section 6.3, we present our replication results and compare them to the original work. The discussion of results, replication efforts, design changes, and fields of action follows in Section 6.4. We conclude by outlining the limitations of our study (Section 6.5) and summarizing our work's contributions in Section 6.6.

6.1.1 *The Original Study*

In 2015, Iulia Ion, Rob Reeder, and Sunny Consolvo presented their survey-based study on the differences and similarities in online security-related behavior of expert and non-expert users [115]. They developed a four-part survey asking about top security advice and the respondent's own security and privacy habits, as well as asking respondents to rate pre-formulated advice statements for their effectiveness and practicability.

The two surveys that make up the core of their study are based on data gathered by conducting semi-structured interviews with 40 security experts at the 2013 BlackHat, DefCon, and USENIX security conferences.

The expert survey, crafted from the information gathered in the preliminary interviews at security conferences, was conducted from February to April 2014. A minimum of 5 years of work experience in a security-related field was required to be counted as an "expert." Participants were recruited through a post on the Google Online Security Blog [179] and social media. The survey first asked participants to enter three pieces of advice for non tech-savvy users and the three

things the participants do themselves to protect their security online. The second part consisted of multiple-choice questions inquiring on certain security-related behaviors and practices. The main part asked the participants to rate pieces of advice directed at non-tech-savvy users. Experts were then asked to rate each piece of advice with regard to both the advice's effect on security and the probability that the user would follow the advice. The survey closed with demographic questions. 231 participants met the criteria for being an expert of working or studying in a security-related field for at least five years.

The non-expert survey was conducted with 294 US-based participants recruited via Amazon Mechanical Turk (MTurk).

The results showed that experts and non-experts followed different approaches to protecting their security online, with the practice of using strong passwords being the only commonality for both groups, ranking in the top 5 responses to the question about the respondents' personal top three security practices (cf. Figure 6.1). The security practices mentioned by experts were consistent with the experts' ratings of different pieces of advice. These pieces of advice were grouped into four categories: *software updates*, *antivirus software*, *password management*, and *mindfulness*. The security practices utilized by the non-experts received mixed ratings from the experts. Some non-expert practices were considered by the experts to be a good practice, like installing antivirus software and using strong passwords. However, the non-experts' failure to comply with some practices were considered bad habits by the experts, including failure to delete cookies and failure to visit only known websites, among others.

The authors found three security practices that experts followed and recommended that were not employed by the non-experts (see Figure 6.3), namely installing system updates, using a password manager, and using two-factor authentication, which were considered most important by a majority of the experts. Their results suggest that a combination of better communication and improvements in the systems and their usability were necessary to get non-experts to adhere to these three security practices.

6.2 METHODOLOGY

The authors of the original study shared their study materials with us so that we could recreate the surveys as precisely as possible. They also shared the data shown in Figure 6.1 from their original paper; however, the raw data could not be shared.

The questionnaire featured mostly closed questions that allowed participants to enter free-text data in an "other" answer option. The questions on the practicability of advice with featured the compound design in the original study were 5 point Likert-scale item batteries with optional free text comment fields in between. Our split-question

design thus increased the number of questions for participants who answered our modified survey.

The full questionnaires can be found in the appendix C.1. In total we had three different questionnaires: the expert and end-user questionnaires from the original study and our modified expert questionnaire which separated the compound questions. All questionnaires as well as the pre-study interviews started by getting informed consent. Audio recordings were made in the pre-study with participant consent and then stored on encrypted storage and deleted after evaluation. In compliance with the EU-GDPR, we did not store any personal identifying data such as IP addresses for any online survey.

The responses to the open-ended questions regarding the top three pieces of security advice and the top three personal security practices of experts were coded by two of the authors. First, both researchers coded the results independently and then codes were compared and differences were discussed. Since the coding was straight-forward, full agreement on the codes was reached.

6.2.1 *End User Survey*

We replicated the end user survey with the same MTurk recruitment criteria as the original authors used: Participants were required to be from the United States, have a task approval rate of 95% or better and have completed at least 500 tasks. For the sake of replication, we advertised the study with the original payment of 1$, but for fairness reasons we awarded an additional 2$ through MTurk's worker bonus system after the study was concluded. The study was conducted in May 2018.

6.2.2 *Expert Interviews and Survey*

Based on the expert survey from Ion et al., we conducted 40 interviews with IT security experts at the CeBIT international trade fair on information technology in 2018. Our goal was to evaluate the survey design and gather first impressions for the experts group.

During the course of the interviews, it became clear that the compound question regarding the evaluation of advice[1] led to confusion and insecurities in participants. They often misinterpreted or morphed the question's phrasing after rating a couple of items, leading to decreased comparability of results.

We discussed this finding and the problem of compound questions with the authors of the original study. They chose the compound

1 "For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online."

question due to time constraints. Their pre-testing suggested that the length of the survey had to be limited and thus this compromise was made. Also, they were mainly interested in what the experts' overall assessment of advice was and thus the separate components were not as relevant for their work.

Nonetheless, compound questions can be tricky to interpret and important nuances can be lost. In particular, we thought it would be valuable to see if there are any pieces of advice where effectiveness and realism diverge, since these could highlight areas of improvement.

To this end, we separated the compound rating tasks for advice effectiveness and realism. Since this is a divergence from the replication, we assigned half the participants to this survey and the other half completed the original survey with the compound questions. We chose a between-groups design over a within-groups one because we wanted to limit fatigue effects, as the survey was already rather long and repetitive. In addition, we randomized the order of appearance of individual advice items within the 5-piece rating blocks for both groups (see Appendix C.1) to minimize cross-influencing effects between advice items.

The original survey was advertised with a blog posting on the Google Online Security Blog [179]. Despite the support of the original authors, it was not possible to recruit developers the same way.

So instead we recruited experts through social media and mailing lists. We announced the survey link with a short advertising statement on Twitter[2], asked selected professional contacts (e.g., the original authors) to repost or share the advertising; and also announced the study, together with a link to the tweet, on a hacking and security community mailing list. All in all, the tweet was retweeted 28 times and received 5,540 impressions, according to Twitter's analytics tool. In addition, the survey link was shared in the following reddit communities: r/Defcon, r/cybersecurity, r/netsecstudents, r/netsec, r/sysadmin, r/SampleSize, r/computerscience, r/information_Security, r/privacy.

6.3 RESULTS

Of the 300 end user surveys that were completed, 12 participants got more than one of three quality assurance questions wrong and were, therefore, excluded from further analysis. This is the same procedure used in the original work. Our final sample thus consisted of 288 participants.

The collected demographic data is displayed in Table 6.1. The sample contained 48% female participants and was relatively young, with

2 "Dear #security experts, I'm conducting a study about security advice targeted at non-technical users and need your help. Please participate in this 10-Minute survey: https://studyportal-bonn.de I appreciate RTs and (cross-platform) shares. Questions? DM or busse@cs.uni-bonn.de" (`https://twitter.com/kb_usec/status/1047080662312898560`)

almost 80% of participants being younger than 45 years old. A little more than half have at least a bachelor's degree, and the majority, at 66%, reported an employment status of full-time employee. In comparison, the original study's sample had 40% female respondents, and 88% of the participants were younger than 45 years old. In the original study, 47% of the participants held a bachelor's degree or higher. In the original study, 47% of participants were from the US, data for EU-located participants was not given. In our sample, 70.4% of participants were from the EU and 26.8% were from the US.

The expert survey was conducted between June and November 2018. We recruited 75 expert participants online using our A/B testing design, 44 expert participants for survey form A (with compound questions), and 31 participants for survey form B (without compound questions). Participants were allowed one mistake regarding the three attention checks in the survey, as was done in the original study. We also excluded one participant who clearly gave nonsensical answers.

One prominent difference between our expert sample and the original expert sample is that our experts had less experience. The original study required experts to have at least five years of work or study experience in IT security or a related field. Only 59 participants fulfilled this requirement in our set, so we lowered this requirement to one year. We will discuss this in more detail in the limitations section.

The p values we report refer to chi-squared tests or, where not enough data in all categories was available, Fisher's exact test. Dependent on the original authors' approach, we applied the Holm–Bonferroni correction in R for all the tests conducted. To further illustrate our results, we utilized participants' comments provided by the optional clarification questions and "other, please specify" options of the survey.

6.3.1 *Differences between Experts and Non-Experts*

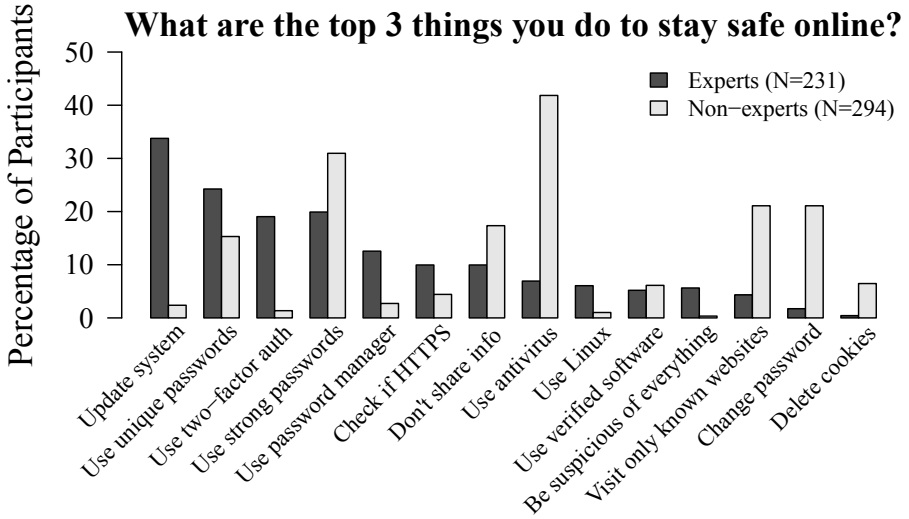
For this section, we focus on experts and non-experts to follow the approach of the original work. Experts A and B were combined in behavior-related questions since these questions were identical, but split when advice rating was considered.

The first question asked about the top three things participants do to protect their security online. The comparison of the answers is displayed in Figure 6.1. In accordance with the original work, we only considered items mentioned by at least 5% of the participants in each group.

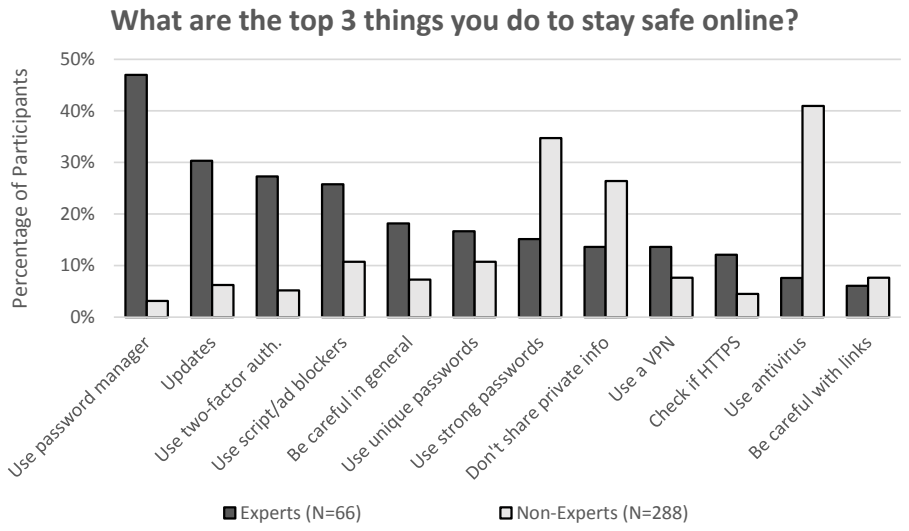
While most experts rely on a password manager (45%) and updates (31%) as well as two-factor authentication (29%) to stay safe, non-experts count on the usage of antivirus software (41%), strong passwords (35%), and not sharing personal information (26%).

Item	NE		E	
Female	137	47.6%	7	9.3%
Male	150	52.1%	59	78.7%
Transgender	1	0.4%	2	2.7%
No Answer	0	0%	7	9.3%
18 - 24	25	8.7%	3	4%
25 - 34	130	45.1%	30	40%
35 - 44	72	25%	26	34.7%
45 - 54	39	13.5%	9	12%
55 - 64	16	5.6%	2	2.7%
65 or older	6	2.1%	0	0%
No answer	0	0%	5	6.7%
Professional Doctorate	5	1.7%	3	4%
Doctoral Degree	3	1%	6	8%
Master	28	9.7%	29	38.7%
Bachelor	114	39.6%	18	24%
Associates Degree	38	13.2%	3	4%
Some college, no degree	45	15.6%	4	5.3%
Technical/Trade School	13	4.51%	2	2.7%
Regular HS Diploma	32	11.11%	0	0%
GED or alternative	5	1.74%	0	0%
Some high school	2	0.69%	0	0%
Other	0	0%	4	5.3%
No answer	3	1.04%	6	8%
Employed full-time	190	65.97%		
Employed part-time	26	28.26%		
Self-employed	36	12.50%		
Homemaker	16	5.56%		
Retired	6	2.08%		
Student - Undergrad	6	2.08%		
Student - Doctoral	2	0.69%		
Looking for work	9	3.13%		
Other	2	0.69%		
Industry			38	50.7%
University			16	21.3%
Corporate research lab			7	9.3%
Government			1	1.3%
Self-employed			2	2.7%
Other			9	2.7%
No answer			2	2.7%
1-5 years of security exp.			16	21.3%
5-10 years of sec. exp.			18	24.0%
10-15 years of sec. exp.			20	26.7%
15+ years of sec. exp.			21	28.0%

Table 6.1: Demographic information for expert (E, $n = 75$) and non-expert (NE, $n = 288$) survey participants.



(a) original study

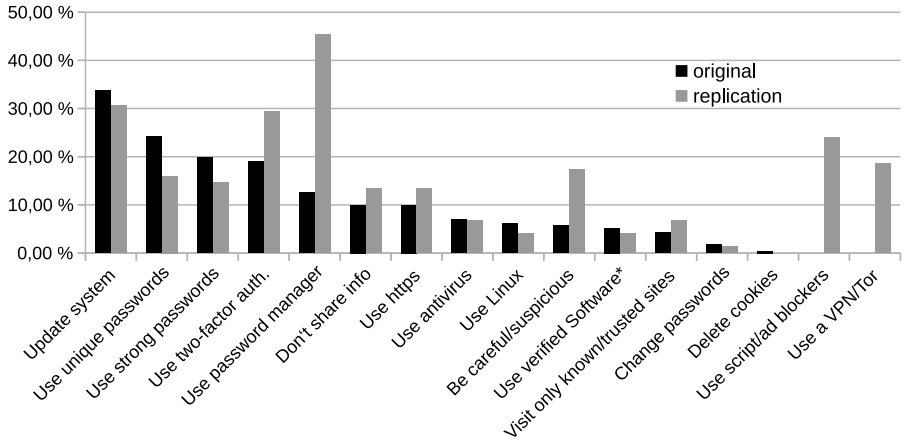


(b) replication study

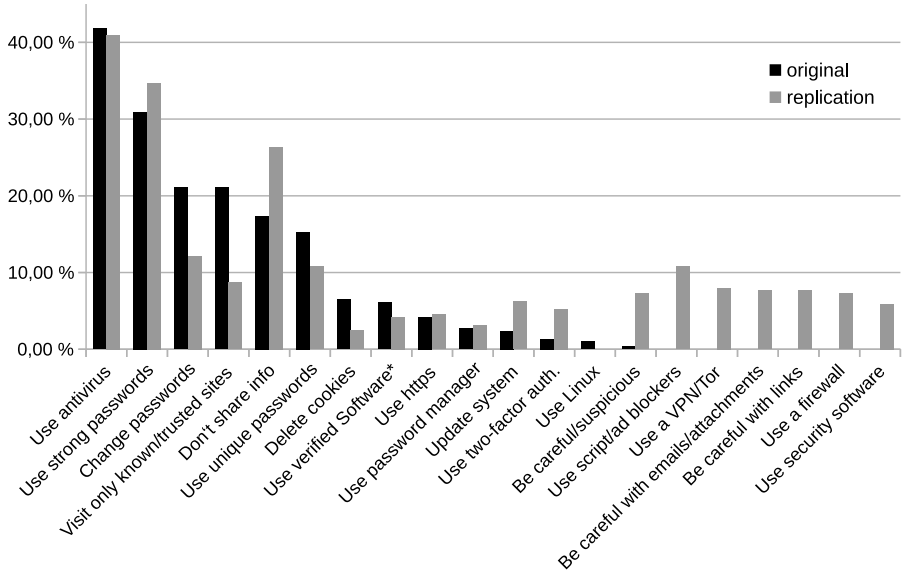
Figure 6.1: Security measures mentioned by at least 5% of each group

In comparison with the original study, the most common security practice mentioned by experts has shifted. Instead of updating regularly, the use of a password manager was now the most frequently mentioned habit among our experts. The use of unique passwords, which was the original study's second most common practice, ranked sixth in our sample. Since the use of password managers usually includes the use of unique passwords, these two are linked. The adoption of two-factor authentication was unchanged, in position three.

Overall, there were four new practices frequently mentioned: using ad and/or script blockers, being careful in general as well as when following links, and using VPNs. In contrast, the once common practices of using Linux, using verified software, changing passwords regularly, and manually deleting cookies were not present in our sample. The



(a) Expert Comparison

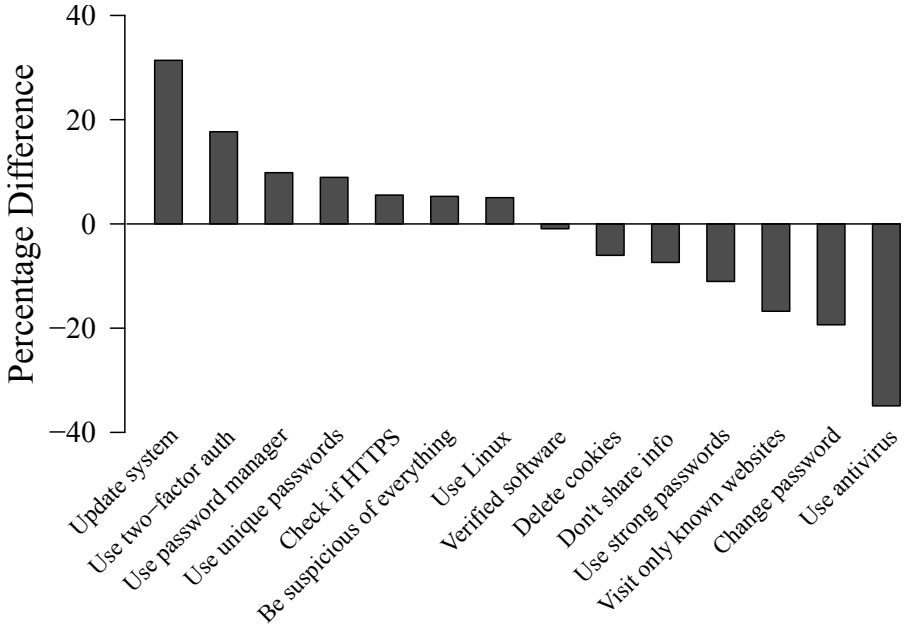


(b) Non-Expert Comparison

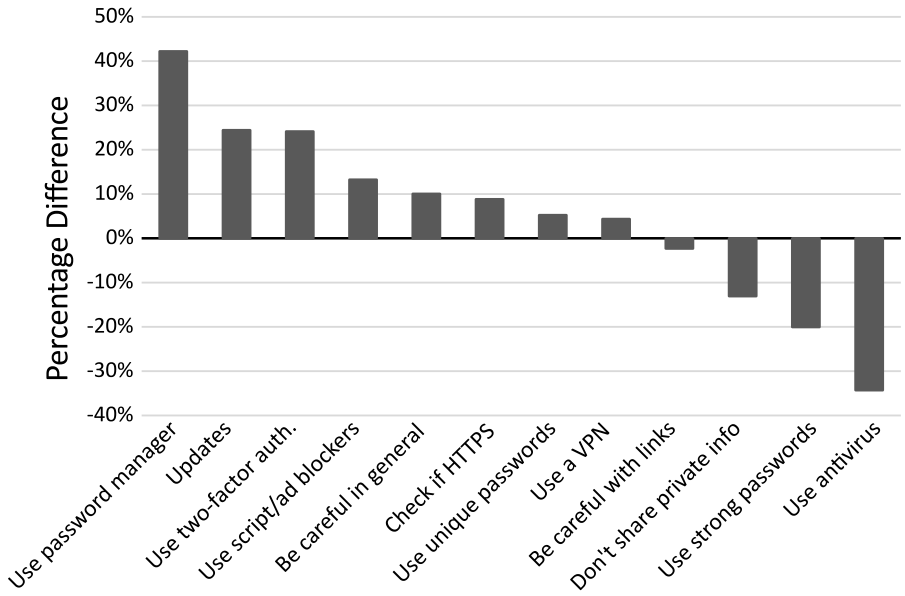
Figure 6.2: Answer comparison for the question "What are the top 3 things you do to stay safe online?" between the original study and our replication. Missing values for original data were mentioned by less than five percent of expert participants. (*) We aligned the original authors' code with our code "be careful with downloads".

replacement of "carefulness" with "practicing suspicion," however, might have been a product of different coding approaches.

The percentage differences between the groups of experts and non-experts are displayed in Figure 6.3. The practices mentioned least by non-experts relative to experts were: (1) use a password manager (42%), (2) keep your system up-to-date (24%), and (3) use two-factor authentication (24%). While the rankings of these three pieces of advice have shifted a bit (password managers climbed from difference position three to one), we still see the same overall trend as in 2014.



(a) original study



(b) replication study

Figure 6.3: Percentage difference of security practices mentioned by experts and non-experts as answer to the "things-you-do" question. Security measures with a positive percentage difference were mentioned more by experts than non-experts; a negative percentage difference indicates topics mentioned more by non-experts.

Reported Behavior	χ^2	p
How soon do you install updates?	7.95	< 0.001
Do you use antivirus software?	77.43	< 0.001
Do you use two-factor authentication?	23.41	< 0.001
Do you remember your passwords?	35.43	< 0.001
Do you write down your passwords?	20.03	< 0.001
Do you save your passwords in a file?	1.79	0.651
Do you use a password manager?	55.59	< 0.001
Do you reuse passwords?	21.43	< 0.001
Do you look at the URL bar?	22.28	0.001
Do you check if HTTPS?	5.48	< 0.001
Do you visit websites you haven't heard of?	48.16	< 0.001
Do you enter your PW on links in emails?	63.95	< 0.001
Do you open emails from unknown?	91.67	< 0.001
Do you click on links from unknown?	16.52	0.013

Table 6.2: Comparing expert and non-expert reports on their security behavior. $N_e = 74, N_n = 282$ for the first two questions, otherwise $N_e = 75, N_n = 288$. Degrees of Freedom: 4 for the first, 1 for the second and third question, 3 otherwise. Fisher's Exact test instead of Pearson's Chi-Squared was used to calculate p whenever not enough data was available in any category.

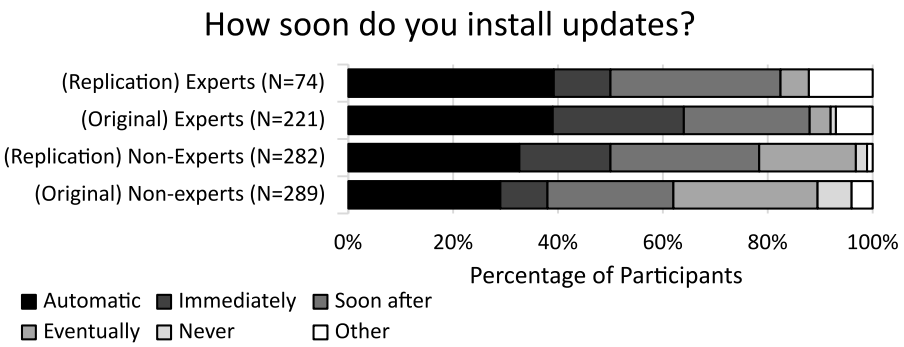


Figure 6.4: Answer distributions for the question "How soon after you discover that a new version of your operating system (OS) software is available do you (or somebody else managing your computer) install it? Examples of operating systems include Windows, Mac OS, and Linux.".

6.3.1.1 *Software and OS Updates*

As in the original study, we differentiated between operating system and application updates. In the question block about behavior with personal devices, we asked "How soon after you discover that a new version of your operating system (OS) software is available do you (or somebody else managing your computer) install it?" We saw that exactly half of all experts as well as non-experts reported installing their updates either *automatically* or *immediately* after they become available (cf. Figure 6.4). However, we can see that if compared to the findings of the original study, where 64% of experts and only 38% of non-experts installed their updates either automatically or immediately, fewer experts but more non-experts are reporting this behavior in our replication. While the numbers are closer together, the differences between the groups are still statistically significant ($\chi^2(4, N_e = 74, N_n = 282) = 7.95, p < 0.001$, cf. Table 6.2). This could be an artifact of widespread operating systems that employ automatic updates per default, as for example Windows 10 does.

Among the pieces of advice, we had the statements "turn on automatic updates," "install OS updates," and "update applications." In all three cases of update-related advice, less than 50% of non-experts rated the advice very effective, yet around 60% said they were very likely to follow it. Especially for the advice regarding application updates, we found a strong discrepancy within our A/B testing setup. More about this is reported in Section 6.3.2

6.3.1.2 *Antivirus and Protection Software*

Using antivirus software is still the security practice with the biggest difference in number of mentions between end users and experts (cf. Figure 6.3). As Figure 6.1 illustrates, 41% of non-experts and only 7% of experts stated that using antivirus software is one of the top three

things they do to protect their security online. This coincides with the findings of the multiple-choice questions on security-related behavior in the second part of the survey, where twice as many non-experts as experts ($E = 82\%$ vs. $NE = 41\%$) reported using antivirus software on their personal computers. As shown in Table 6.2, this difference is statistically significant ($\chi^2(1, N_e = 74, N_n = 282) = 77.43, p < 0.001$).

Several experts stated that the perceived usefulness of antivirus software might be higher than the actual usefulness. One expert stated, "*I think antivirus software creates more problems than it solves (including the feeling of being safe).*" Some experts strongly suggested caution when dealing with antivirus software. One expert participant commented, "*Anti-virus software often is snake-oil and detects only old viruses, but prevents users from these viruses. Also, they often implement suspicious features like breaking https without being clear to the end user about it.*"

Non-experts were asked to use a five-point Likert scale to rate how effective they see the security advice of using antivirus software: 63% rated it *very effective* and 19% rated it *effective*.

When asked how likely they would be to follow this advice if they heard that using antivirus software was effective, 73% of non-experts said they would be *very likely* to follow this advice, and 9% said they *likely* would. This strong acceptance of antivirus software is mirrored by the comments and feedback provided by non-experts.

A new type of security advice that emerged in the things-you-do question was the use of ad and/or script blockers. A proportion of 24% of experts and 11% of non-experts mentioned this security practice as one of their personal top three (cf. Figure 6.1).

6.3.1.3 *Password Management*

In many cases, both experts and non-experts cited password-related practices as an answer to the question "What are the top three things you do to protect your security online?" Using strong and unique passwords were frequently mentioned strategies by both groups. Where experts spoke more of having unique passwords than non-experts ($E = 16\%$ vs. $NE = 11\%$), using strong passwords was reported twice as often by non-experts than experts ($NE = 35\%$ vs. $E = 15\%$). While the practice of having unique passwords was mentioned less frequently than in the original data set (cf. Figure 6.2), having strong passwords was slightly less frequently mentioned by experts (then 20%, now 15%), but slightly more frequently mentioned by non-experts (then 31%, now 35%).

Similarly, experts named using a password manager substantially more often than non-experts ($E = 45\%$ vs. $NE = 3\%$), but almost did not mention changing passwords frequently (1% experts vs. 12% non-experts). Changing passwords is still not very prominent for experts (then 2%, now 1%), and has decreased in mentions by non-experts, as well (then 21%, now 15%; cf. Figure 6.2).

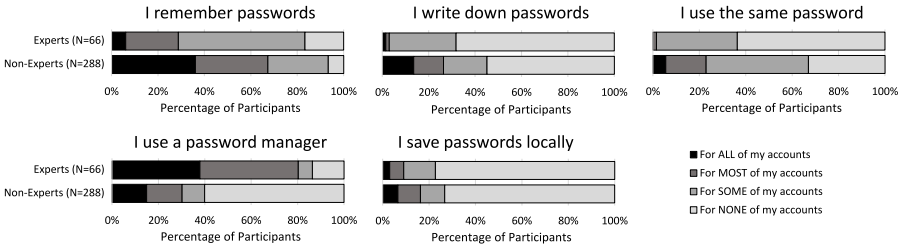


Figure 6.5: Non-expert habits regarding password management from out replication study.

Likewise, experts mentioned the use of two-factor authentication more than five times as much as non-experts ($E = 29\%$ vs. $NE = 5\%$). This practice has gained in prominence for both experts (then 19%, now 29%) and non-experts (then 1%, now 5%). This could be partially attributed to the fact that more services now offer two-factor authentication than in 2014.

The most common answer of experts to the things-you-do question was "using a password manager" ($E = 45\%$), in contrast to a very small group of non-experts ($NE = 3\%$). In comparison with the original study, the mention of password managers by experts had more than tripled, from 13% to 45%. This difference is in line with the fact that twice as many experts as non-experts reported using a password manager for at least some of their accounts ($E = 83\%$ vs. $NE = 40\%$, $\chi^2(3, N_e = 75, N_n = 288) = 55.60$, $p < 0.001$). One expert commented, *"Using a proper password manager is the best solution. In the end, it is about using different passwords for different accounts."*

Writing down passwords was seen by some experts as a user-friendly compromise to a password manager. One expert said, *"[The advice to use] different passwords is effective, but can be difficult for users if they don't use a password manager. Writing passwords down isn't really bad, as long as the paper is kept secure. This is basically just an offline password manager."*

While the advice to "write down passwords on paper" and "save passwords in a file" were rated poorly by non-experts for both effectiveness and the likelihood that they would follow the advice if they heard it was secure, especially the practice of writing down passwords on paper, was rather common among our participants. As can be seen in Figure 6.5, 45% of non-experts reported writing down passwords for at least some of their accounts (vs. 33% of experts, $\chi^2(3, N_e = 75, N_n = 288) = 20.02$, $p < 0.001$). Almost all experts commented on the importance of storing the paper securely.

Also shown in Figure 6.5, six times more non-experts than experts remember all of their passwords (36% non-experts vs. 5% experts, $\chi^2(3, N_e = 75, N_n = 288) = 35.42$, $p < 0.001$). These numbers have decreased in comparison to the original study, where 17% of experts

and 52% of non-experts cited being able to remember all of their passwords.

In addition, seven times more non-experts than experts stated that they reuse passwords for most or all of their accounts (23% of non-experts vs. 3% of experts, $\chi^2(3, N_e = 75, N_n = 288) = 21.43$, $p < 0.001$). While the proportion of end users who employ this practice rose slightly in comparison with the original study (19%), the rate among experts stayed about the same (3%).

6.3.1.4 *Mindfulness*

Among the remaining pieces of advice, the ones about checking the URL bar when browsing and looking for HTTPS connections are most interesting in comparison to the original study, since there have been major changes in the SSL/TLS certificate ecosystem within the last few years.

The rise of Let's Encrypt and automated certificate issuance and renewal have greatly increased the level of TLS-encrypted web traffic [8]. In consequence, HTTPS has become more widespread, but the indication about whether a site should be trusted because it features HTTPS has been weakened, since even phishing websites often come with security certificates [216].

When asked about the advice to check if the website they're visiting uses HTTPS, 54% of non-experts rated it very effective, and 61% considered themselves very likely to follow that advice. In comparison, the original data featured a proportion of 60% of non-experts rating this advice as *very effective*, and 50% saying they would likely follow it.

To put this in context, we asked all participants whether they practice checking for HTTPS while surfing. The portion of experts who *often* do so decreased from 82% in the original study to 73% in our replication. The portion of non-experts increased from 36% in the original study to 47% in our replication.

Regarding the more general question about checking the URL bar when visiting a website, 76% of experts and 60% of non-experts said they often look at the URL bar (original study: 86% and 59%). Some experts emphasized that it is not only important to look at the URL bar, but also to be aware of the specific information it displays. For example, one expert said, *"Watch out for correct URLs, valid SSL certificates, and enabled encryption (HTTPS) if sensitive information is requested."*

The question whether a participant enters their passwords on websites after they click on a link in an email is the only behavior question for which the chi-squared test for expert and non-expert answers yielded a different result than in the original study. While Ion et al. found no significant difference between the groups, our samples showed a large effect size ($\chi^2(3, N_e = 75, N_n = 288) = 63.95$, $p < 0.001$). This results from a large proportion of expert users choosing the *Other* option to further explain their behavior in that case.

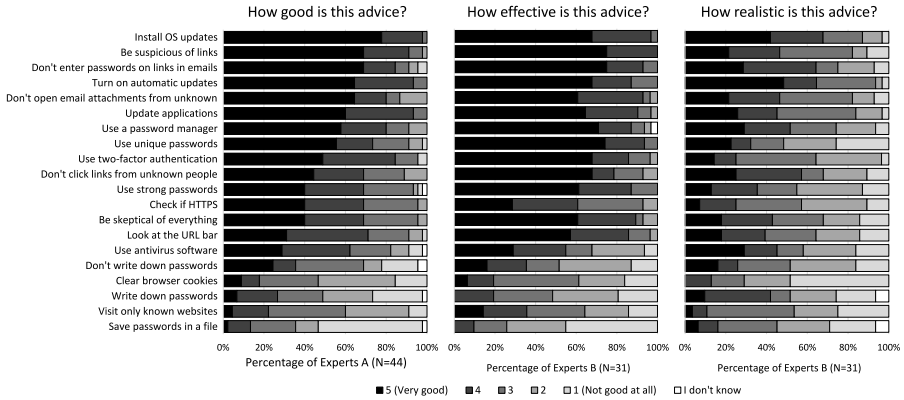


Figure 6.6: Side-by-side comparison of rating distributions in our replication study, showing from left to right: goodness ratings by experts A, efficiency ratings by experts B and realism ratings by experts B. The twenty pieces of advice are sorted by goodness ratings.

While some experts stated in the comments that they generally do not click on links in emails, another proportion of experts further differentiated, making comments such as, "*It depends. Am I expecting that email, is it from a reputable source, and does the URL match what I expect? Then yes; otherwise no.*" When excluding the *Other* option, the test results align again with the original study ($p = 0.63$ after correction).

6.3.2 *Compound Question Results*

As described in section 6.2.2, half the experts received the original survey with the compound questions (Group A) and for the other half we split up the goodness rating into effectiveness and realism (Group B). In the following, we compared the ratings of the split questions to those of the original compound questions.

In Figure 6.6, we look at the distribution of ratings given by experts A and B. Some pieces of advice, like installing OS updates, were rated very "effective" as well as very "realistic" by both expert groups. In the following, we will focus on the cases in which a piece of advice did not receive high scores in all cases, especially in terms of realism.

For example, not opening email attachments from unknown senders was rated positive in terms of goodness and effectiveness by experts A and experts B (64% *very good* and 16% *good* and 58% *very effective* and 35% *effective, respectively*). However, the *realistic* rating given by experts B peaks at a Likert score of 3, with 35%. Only 19% of experts B said this advice was very *realistic*, and 6% said it is *not realistic at all* (cf. Figure 6.7).

A piece of advice was classified as *good* and *effective* if a rating of 4 or better was present. We are most interested in those cases where this condition was met as well as having a realism rating of less than 4. As depicted in Table 6.3, this applies for eight pieces of advice.

Advice	δ_μ	μ_e	μ_r	σ_e	σ_r	δ_m	m_e	m_r
Use unique passwords	1.90	4.68	2.77	0.60	1.52	3	5	2
Use strong passwords	1.58	4.48	2.90	0.72	1.27	2	5	3
Use two-factor authentication	1.55	4.52	2.97	0.81	1.19	2	5	3
Be suspicious of links	1.35	4.71	3.35	0.46	1.28	2	5	3
Use a password manager	1.16	4.6	3.48	0.77	1.29	1	5	4
Don't open email attachments	1.16	4.48	3.32	0.72	1.17	2	5	3
Don't enter PW on links in emails	1.13	4.68	3.55	0.60	1.34	1	5	4
Update applications	1	4.51	3.52	0.77	1.12	2	5	3

Table 6.3: Pieces of advice that were received a mean effectiveness rating (μ_e) of at least 4, and a mean realism rating (μ_r) of less than 4, ordered by decreasing difference δ_μ. Also shown are standard deviations for effectiveness and realism ratings as well as medians and their difference.

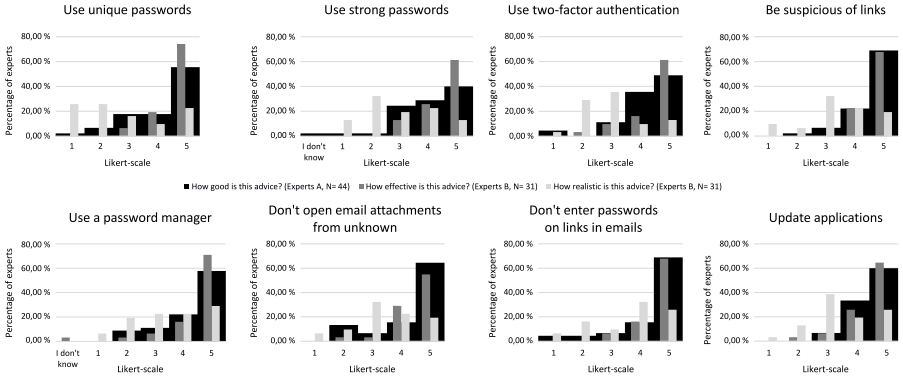


Figure 6.7: A/B comparison of advice rating from our replication study for pieces of advice identified as effective, but unrealistic. Descriptive statistics can be found in Table 6.3.

We can group these pieces of advice in four categories.

Using unique and strong passwords as well as using a password manager all relate to *Password Security*. The advice to adopt *Two-Factor Authentication* stands on its own. Being suspicious of links, not entering passwords after having clicked on a link in an email, and not opening attachments can be grouped as *Links and Attachments*. The last piece of (controversial) advice, *Updating Applications* regularly, again stands on its own.

6.4 DISCUSSION

In the following, we will discuss the popularity of selected findings and advice.

6.4.1 *Advice Rating*

While in the original study, the advice to regularly update showed the greatest difference between expert recommendations and non-expert usage, we found that using a password manager is now the piece of advice with the biggest gap between experts and end-users. Microsoft's shift toward mandatory automatic updates in Windows 10 might be the cause of this change. Because the operating system now takes care of keeping the system up to date, and thus secure, experts might not regard this advice to be as urgent as they did four years ago [159].

Password managers have the potential to solve the usability issue of passwords. Additionally, password managers might be a currently trending topic, which is reflected in the popularity of this practice as the single most frequently suggested piece of security behavior reported by experts (cf. Figure 6.1).

Installing and using antivirus software was the most frequently cited security measure by non-expert users in both the original study and our study. While antivirus software doesn't offer reliable protection against new and modified types of malware, the presence in advertising, as well as easy setup procedures, might have led to its unbroken popularity.

The advice to not share private information has become more important to both expert and non-expert users. However, one could argue that unconsciously shared information might, indeed, be more dangerous for users, whether it is conversation metadata [140, 193], tracking networks [3], or behavioral data like smartphone usage habits [142].

6.4.2 *New Advice*

When looking at the free text answers for personal top three security practices, we found four new items within the top 18 most frequently mentioned statements: using script and/or ad blockers, being careful when online, using a VPN, and being careful when interacting with links (cf. Figure 6.1). In addition, five additional practices made it just beyond the 5% threshold: only visiting known or trusted websites, using incognito browsing, employing virtual machines, compartmentalizing systems for different tasks or levels of security, using a firewall, and employing security software in general. For the sake of brevity, we excluded these five practices from our further discussion.

While the more general advice of being careful might have arisen from different coding approaches between the original study and our replication, the other two pieces of advice suggest new developments.

Internet advertising has become more aggressive, invasive, and risky over the last few years [24], and blocking extensions are a powerful tool to combat this. In addition to the rise of this security practice,

which 24% of the expert participants and 11% of the non-experts employ, the practice of manually deleting cookies was not included in the list anymore. This might be a replacement process, since many blocking tools also go after tracking cookies.

Using a VPN was a common response to the things-you-do question, but unfortunately, none of our participants elaborated on the meaning of this short statement. It is unclear exactly what kind of VPN participants were referring to. Just as Ferguson and Huston discovered two decades ago, "*VPN [has been and still is an almost] recklessly used*" [83] collective term to describe various technologies and applications. VPNs and onion routing services such as Tor are effective tools for circumventing regional (e.g., governmental) censorship or content restrictions. However, using a VPN entails placing trust in its provider, which is a thing that users often overlook [113, 199].

6.4.3 *Fields of Action*

The pieces of advice that experts rated as very effective, but not very realistic for a user to follow, highlight areas where more research or better technical solutions are needed (cf. Table 6.3 and Figure 6.7). We identified four key fields of action; namely, password security, two-factor authentication, links and attachments, and application updates.

It is striking that these areas of advice are very similar to the advice not followed by users in the original study (cf. Section 6.1.1): recommending frequent system updates has been replaced with regular application updates, while using a password manager and enabling two-factor authentication have stayed the same.

6.4.3.1 *Password Security*

The advice ratings on unique and strong passwords indicate strongly that passwords are still an issue. The fact that the advice about adopting password managers also has a large delta between average effectiveness and realism ratings suggests that password managers are not yet fit for general adoption. Password managers should be approachable, easy to set up, and well-integrated into the operating system, without causing new security risks [49, 77].

However, even among experts, the use of password managers is not without drawbacks. One expert acknowledged a potentially "steep learning curve for non-tech-savvy users," while an end user stated that *"Storing passwords digitally and/or trusting a company to protect your data seems counterproductive."*

6.4.3.2 *Two-Factor Authentication*

Aside from the use of password managers, the adoption of two-factor authentication (2FA) is another relatively easy way to greatly increase

account security. However, our expert group regarded this advice as not very realistic to be followed, while still acknowledging its effectiveness (cf. Table 6.3).

In general, more services need to support the setup of a second factor, since approximately 76% of websites do not offer users a full set of 2FA options [119]. Additionally, finding ways to increase user adoption of 2FA for accounts is a task for future research [10].

6.4.3.3 *Links and Attachments*

Three statements in our list of controversially rated advice related to links and attachments, specifically, being suspicious of links, not entering passwords on links received in emails, and not opening email attachments.

While the experts might have rated it as not very realistic, since opening attachments and following links is part of daily internet life, the risks arising from well-crafted phishing or malware emails should not to be neglected. A prominent example from recent years is the rise of ransomware, like wannacry [181].

Protecting against these types of threats purely from the technical side is rather difficult since they usually come with a measure of social engineering. Phishing URLs increasingly make use of invisible Unicode characters or identical-looking symbols from non-Latin alphabets [236].

One possible solution for preventing malware infection after opening an email or its attachments could be sandboxing technology. All attachments and links would be opened in an isolated, secure environment that doesn't harm the actual system.

6.4.3.4 *Application Updates*

Last but not least, our results suggest further research in the direction of update managers that not only reliably perform their task of keeping the system and its applications up to date, but also communicate clearly what updates include which features and fixes and that schedule their work intelligently without interrupting or hindering the user.

The need for a centralized, system-level update tool that takes care of application updates was already expressed by Ion, Reeder, and Consolvo in 2015 and recently confirmed by Mathur et al. [151]. Since then, some applications have started to implement their own more or less automatic update tools, while a centralized tool is not on the horizon. Microsoft tried establishing their own Windows Store as an app store-like entity with an integrated application updater, but adoption rates are still low.

6.5 LIMITATIONS

In the following, we will outline the limitations of our study to facilitate putting this work into context.

Because we could not recruit via the same channel as the original authors, our expert sample is drawn from a different population. Thus, there are two variables that are different, time and population from which our experts were recruited. For that reason, our results can be seen as extending the original results, but cannot be used to state that the effects are attributable to the intervening time or due to different populations.

In particular, we decided to include security experts with 1-5 years of experience in security or a related field, while the original study only considered participants with at least five years of experience as experts. Table 6.1 shows that participant distribution is almost equal between all age brackets. Since we saw no difference between experts with 1-5 years of experience and those with 5+ years of experience, we decided to include them to increase our overall sample size.

As for recruiting non-experts, we had to follow the same channel as the original work and thus suffer from the same limitations. While Amazon MTurk is heavily used for usable security and human–computer interaction studies, the population there tends to be younger, more female, and more tech-savvy than the general US population [36, 175, 192].

All data we collected were self-reported. It is known that people tend to put themselves in a better light in such situations; therefore, the adoption rates or likeliness of following a certain piece of advice are possibly skewed [177].

6.6 CONCLUSIONS

In this chapter, we replicated a 2015 study by Ion, Reeder, and Consolvo examining expert and non-expert security habits and corresponding advice. While our general findings relate with the original work, we could identify some new trends, like the use of script and ad blocking software.

In addition, we identified an issue in the original study design and improved upon it. Our results identify critical areas of effective but unrealistic practices that could be improved upon by the research and practitioner communities. Most of these practices (password security, 2FA, securely handling links and attachments from emails, and centralizing application updates) were already present as emerging topics in the 2015 study. This shows that the usable security community has not succeeded in solving these grave issues and clearly outlines the need for future action in researching and developing new or better security tools that non-experts can adopt and use.

7

SECURITY AND PRIVACY PERCEPTIONS IN PAYMENT AND BANKING

This chapter is based on joint work with Mohammad Tahaei (University of Bonn and University of Edinburgh), Katharina Krombholz (CISPA), Matthew Smith (University of Bonn), Emanuel von Zezschwitz (Google), Jing Tian (Zhejiang University), and Wenyuan Xu (Zhejiang University), which has been published at EuroUSEC 2020 [41]. I contributed with survey development and evaluation as well as a majority of the writing. See Appendix F for a detailed authorship agreement.

So far, we have looked at how security and privacy are perceived based on interpersonal context in the workplace, on individual mental models, and on security expertise. The scope is now broadened again to compare how security perception and habits – in this case in the payment context – are shaped by culture.

Payment cultures around the globe are diverse and have significant implications on security, privacy and trust. We study usable security aspects of payment cultures in four culturally distinct societies. Based on a qualitative study in Germany and Iran, we developed an online survey and deployed it in Germany, Iran, China, and the US. The results reveal significant differences between the studied countries. For example, we found that participants from Iran and China are more comfortable with credential sharing and German participants were most accepting towards cryptocurrencies. We suggest these kinds of differences in payment culture need to be considered in the context of HCI research when evaluating current payment mechanisms or designing new ones.

7.1 INTRODUCTION

Exchanging money for goods and services is the foundation of our capitalist world. Within the last century, a plethora of different electronic payment instruments has shaped our trading culture and partially even replaced traditional physical money. Examples of such electronic payment services are telephone or SMS-based models or sophisticated software coupled with biometric authentication. The current rise of cryptocurrencies such as Bitcoin, Etherium, or Litecoin marks the newest chapter of this evolution [117, 132].

The gradual change away from physical money in everyday trading situations poses challenges to individuals' management of financial assets. Instead of managing a single bank account and cash withdrawn from one account, users have the burden of choice to interact with different services. As electronic payment instruments often have complex and poorly understood information-sharing models and non-transparent networks of multinational service providers (e.g., German *girocard* debit cards in international contexts which are dependent on co-branding for international use, cf. Section 7.3), supporting users' trust is often difficult.

Trust is a multidimensional concept [152]. In traditional (non-financial) settings, perceived usefulness and ease of use are important factors for user trust [127], whereas in payment context, perceived security and privacy become increasingly important [43, 232]. Users desire security features such as secure connections, two-factor authentication, and other mechanisms to prevent fraud and "hacking", as well as privacy features such as data protection and responsible sharing of customer data [61, 86, 187]. Finally, concepts like cryptocurrencies also introduce new types of risks and attacks (e.g. loss of cryptographic keys and money) that may be hard to grasp could result in lower levels of trust.

Trust is shaped by cultural, societal, legal and economic factors. These factors also play a role in how people accept payment instruments [67, 171, 233], which is why studying trust in payment with a Western US-/Euro-centric lens is hardly generalizable to other populations. Previous work has already identified culture as an influential factor in payment choices [126] and security attitudes [185, 186]. As most related studies considered cultures in isolation and focused on either security factors or payment choices, a comparative analysis of payment cultures and holistic consideration of security and cultural factors alike is necessary.

While there is multiple research in the literature with cross-cultural viewpoints (cf. Chapter 2.8), this work focuses on four nations that have not yet been compared. We look into payment culture and study four societies with a distinct cultural background. We elicit an understanding of payment habits and trust of populations which are still underrepresented in our research community and compare identified behaviour and attitudes to users from Western societies.

We contribute a comparative user study on security, privacy, and trust across all modern payment methods from a usable security perspective. Our study places emphasis on user experiences with payment systems and their security and privacy features beyond traditional physical money with a focus on online payments, card-, mobile- and phone-based payments as well as cryptocurrencies. In particular, we sought to answer the following research questions:

- How do people perceive security and privacy in banking and payment instruments?
- What factors do people consider when selecting a payment instrument?
- What demographic, societal, and socioeconomic factors influence payment culture?

Following an inductive approach, we first conducted ten semi-structured interviews in Germany and Iran. Based on these findings, we generated a set of hypotheses and designed an online survey ($n = 1961$) which was deployed in different societies with regard to

banking and payment systems, i.e., Germany, Iran, China and the USA. This cross-cultural quantitative survey was used to collect evidence on payment habits, and perceptions and misconceptions of security mechanisms. We provide insights into the payment behaviour of four populations and show that social factors have a significant effect on the acceptance and perception of payment instruments. For example, we revealed great security risks in Iranian PIN entry practices in small shops, increased interest in cryptocurrencies among the German population which could indicate a wish to leverage privacy-preserving payments into the virtual world, and that participants from China and Iran often shared payment credentials with their romantic partners.

7.2 METHODOLOGY

We follow an inductive approach starting with an exploratory qualitative study.

We conducted semi-structured interviews in two different countries. Based on these results and related work, we designed a survey and gathered quantitative data across four countries. The survey was deployed on different (country-specific) online platforms. In all cases, we did not record any personal information and we complied with national privacy regulations and the General Data Protection Regulation (GDPR) for this type of research study.

We translated the interview script and the online survey to match the respective official languages of the target population. Each was drafted in English first and then translated by respective native speakers. To ensure translation quality and accuracy, additional native speakers were asked to proofread the translations and compare them to the original English version.

The chosen set of countries covers four geographical regions (Europe, Middle East, East Asia, North America), each with a different culture, language, economic and political system (for further information see Section 7.3).

7.3 COUNTRIES OF STUDY

In the following, we present a short overview on the four countries we studied, their economic context and eco-political features. We consciously refrained from including quantified data on culture such as the Hofstede scores [109] because they reproduce the essentialist view that all individuals of a country share the same values. These nation-level models implicate that no information about the individual people of a country can be derived from them, thus luring readers into false impressions [35, 60, 214]. We therefore abstain from reporting such quantitative metrics for our countries of study.

7.3.1 *China*

China, officially the People's Republic of China (PRC), is a unitary sovereign state in East Asia and the world's most populous country, with a population of around 1.4 billion [209] along with the second biggest economy in the world [229]. The renminbi (RMB) is the official currency of the People's Republic of China. As of 2016, renminbi banknotes are available in denominations from 0.1, 0.2, 0.5 yuan (1, 2, and 5 jiao), 1, 2, 5, 10, 20, 50 and 100 yuan. The denominations of coins are 1 yuan; 5, 2 and 1 jiao; and 5, 2 and 1 fen (10 fen = 1 jiao).

Internet access to resources outside of China has been regulated which resulted in the rise of successful national counterparts of international services [53]. However, many Chinese internet users use special methods like a VPN to unblock websites that are blocked. Recently, these regulations have been extended to Bitcoin mining and trade [30].

7.3.2 *Germany*

The Federal Republic of Germany is a central European, highly developed country with 83 million citizens as of 2020 [197]. Since 2001, the Euro is Germany's official currency, which comes in bills of 5, 10, 20, 50, 100, 200, and 500 Euro as well as coins of 2 Euro, 1 Euro, as well as 50, 20, 10, 5, 2, 1 Euro Cent. Apart from the three largest bills, all bills and coins are frequently used in daily life.

In contrast to other European countries, the use of debit cards within the national *girocard* ecosystem is very common and widely regarded as the default non-cash payment instrument [231]. For international use, girocards rely on co-branding with *Maestro* or *V-Pay* debit systems, but the more common practice for Germans is to acquire a separate credit card for travelling [65, 66].

7.3.3 *Iran*

The Islamic Republic of Iran is a developing middle eastern nation with 81.8 million cizitens as of 2018 [202]. After US sanctions in 2011 (which were lifted in 2015) [120], inflation rates in the country boomed (2009: 10.8%, 2014: 34.7% , 2016: 9%)[1]. At the same time, private transactions with other countries, buying and selling goods, internet shopping and international payment systems were blocked.

Internet censorship in Iran is a disputable issue. Aryan et al. discuss in depth and show that more than 50% of Alexa's top 500 websites are blocked in Iran [15]. Social networks such as Twitter, Facebook and Tinder are blocked (as of Feb 2018), although many Iranian politicians such as the President, Foreign Minister, ICT Minister and many others

1 `https://www.cbi.ir` – accessed: 2018-02-08.

use Twitter as a communication channel. With such barriers, many people rely on VPN and proxy applications to access blocked websites, however lots of these come from underground markets.

Official banknotes in Iran are 100, 200, 500, 1000, 2000, 5000, 10000, 20000, 50000 and 100000 Rials. The coins are 50, 100, 250, 500, 1000, 2000 and 5000 Rials. Although Rial is the official currency in Iran, it is more common to use the unofficial unit *Toman* (10 Rials) in daily routines.

7.3.4 *United States of America*

The United States of America are a federal republic in North America with about 327 million inhabitants (as of 2018 [210]). The country's economy is the largest in the world [229] and the US culture – including Music, Film, and Television – has had a large influence on most Western countries. The official currency is *US dollar*, which comes in bills of 1, 2, 5, 10, 20, 50, and 100 $ as well as in coins of 1, 1/2, 1/4 $ and 10, 5, and 1 cent. Revelations by Edward Snowden have uncovered that the US government is monitoring (but not actively censoring) large parts of national and international internet traffic [167].

7.4 INTERVIEW STUDY

The interview script contained questions about payment preferences, previous experiences with payment methods, and associated privacy and security concerns (See Appendix D.1). The procedure was tested with two pilot interviews which resulted in minor adjustments.

The interviews were conducted in Farsi (in Iran) and in German (in Germany) in a quiet room at the respective universities. The interviewers took notes and audio-recorded the interviews. The interviews lasted about an hour per participant. All participants were compensated with 10 Euro resp. 450,000 Rials. All participants signed an informed consent form.

We recruited ten participants (cf. Table 7.1) by posting flyers at universities and public libraries both in Bonn (Germany) and Teheran (Iran). We refrained from using security and privacy-related terms to prevent a sample bias.

As part of a thesis work, one author applied two rounds of Grounded Theory-like line-by-line open coding to detect observable patterns. Afterwards, descriptive and axial coding was used to thematically merge open codes into groups which resulted in 30 sub-categories. Consequently, the sub-categories were grouped into 7 main categories which describe our participants' attitudes and habits around payment (see Table 7.2).

Table 7.1: Interview study demographics and information whether a participant has a background in IT.

Participant	Gender	Age	Degree	Occupation	IT
IR1	F	26	MS	Student	No
IR2	M	23	BS	Student	No
IR3	M	25	BS	Student	Yes
IR4	F	22	BS	Course Coordinator	No
IR5	F	27	BS	Student	No
DE6	F	25	State Examination	Unemployed	No
DE7	M	23	Diploma	Student	No
DE8	F	23	Diploma	Student	No
DE9	F	19	Diploma	Student	No
DE10	M	57	MS	Freelancer	No

Table 7.2: Coding categories and sub-categories for interview study

Finance	Impression	Usability	Lever	Right to Know	Credentials	Physical Props
Amount	News	Ease of Use	Availability	Organisations	Physical vs. Virtual	Workstation & Internet
Change	Reputation	Accessibility	It's a Must	People	Need to do a Task	Location
Exact price	Knowledge	Time	Proxy & VPN		Patterns	
Discounts	Bad experiences		Travelling		Trust	
Fees	I'm an ordinary citizen				Point of Sale	
Keep track	Reliability					
	Powerful hackers					
	Security & Privacy					

HOW DO PEOPLE PERCEIVE SECURITY AND PRIVACY IN BANKING AND PAYMENT INSTRUMENTS? We found anecdotal evidence that risk perception with regard to different payment instruments and processes is different between countries.

According to our Iranian participants, it is a common practice among shopkeepers to ask for a customer's card and enter the amount and PIN for them. They may perform the operation in the back office or behind the counter, where the customer cannot observe what is going on with their card. However, this behaviour is not typical in banks and large chain stores. In contrary, Germans are privacy concerned as it is a common practice for German customers to enter their PIN themselves. Especially, covering the keypad with hand and/or plastic covers over the keypad is (as opposed to Iran) a common and socially accepted practice in Germany [215].

Regarding the *reputation* of payment instruments, Iranian and German respondents tend to trust international companies more. A German participant mentioned the role and negative association of large companies as a reason for starting to think about using cryptocurrencies. Related literature confirms the significant impact of reputation on consumers' emotions and risk perception [124].

We asked participants about their *bad experiences* with payment instruments and the impact on their behaviour. All Iranians mentioned at least one bad experience with a payment instrument. Two partici-

pants in Iran who had bad experiences with losing cash limited their cash usage as a result. In Germany, four participants mentioned bad experiences with a payment instrument.

> "My wallet was stolen twice, the same happened to my family and relatives too. I am stressed when using cash ... I do not carry large amounts in my pocket [anymore]. If I get some money, I deposit it immediately [to my bank account]" (IR3).

Proxies and VPNs are specifically important to Iranian users, all Iranian respondents reported to use proxy software or VPNs without being aware of their inner workings and distinctive features. On the other hand, selling and buying VPN and proxy servers which enable users to access restricted content is implicitly prohibited in Iran [114]. As a result, the providers of such services are commonly unknown and therefore difficult to verify. Four out of five Iranian respondents reported to use Psiphon[2]. When asked about using financial services via such services, most participants reported to do so and that they never thought about the associated risks and consequences.

WHAT FACTORS DO PEOPLE CONSIDER WHEN SELECTING A PAYMENT INSTRUMENT? We identified the *amount* of money spent per transaction as a relevant factor related to the use of specific payment mechanisms. In both countries, the findings about the payment amount are consistent with related literature [13, 110]: Two participants in Iran and one in Germany mentioned they prefer to use cash for small payments.

Two Germans additionally perceived cash as a suitable instrument for *keeping track* of their spendings. Another participant reported to use an app to track her expenses.

> "[I prefer] cash in daily use because it gives me the best overview of how much money I spend" (DE6).

In both countries, people are sometimes *forced* to use a specific payment instrument by a seller. A participant from Iran mentioned that charging campus cards required internet banking. Another participant from Iran mentioned that certain services (e.g., online shopping, app stores) require certain payment methods and thereby force their users into certain payment habits.

> "If there is no card reader, you must pay in cash like in a taxi, or when I do not have a card at the moment of payment." (IR4)

Some participants from Germany mentioned the need to use credit cards when *travelling*. International travelling and the international

2 `https://psiphon.ca` – accessed: 2019-09-23.

acceptance of payment instruments are more common concerns in Germany than in Iran, presumably due to practically open borders and the higher income among the population which facilitates travelling.

WHAT DEMOGRAPHIC, SOCIETAL, AND SOCIOECONOMIC FACTORS INFLUENCE PAYMENT CULTURE? It is a common practice in small Iranian shops to return sweets or gums instead of money, if the *change* is below a certain amount. Directly connected to the Iranian practice of substituting change with goods, the perceived problem of paying the exact amount has emerged from interviews conducted in Iran.

> "one of the main advantages [of cards] is that you can pay the exact cost, you do not need to get an extra good for your change" (IR2).

The possibility of *bargaining* and getting *discounts* at stores was also exclusively mentioned by Iranian participants. In contrast, however, the consideration of *transaction fees* when choosing a payment instrument was only mentioned by German participants.

The *news* aspect encompasses impressions people get from media, ads, news, newspapers, search engines, social networks, friends and word of mouth. Two Iranian participants mentioned Telegram channels as a source of information. Telegram is a widely used messaging application in Iran [212]. Two German participants mentioned their friends and family, among them computer scientists, as their source of information.

Respondents had diverse viewpoints towards trust in their family and friends. In Iran, all participants reported that they were sharing their financial credentials with at least one person from their social circle, potentially revealing their financial information. Some expressed discomfort with this situation. In contrast, only one participant from Germany explicitly reported that she shared her payment credentials with others. Two participants mentioned that they share some account credentials, such as Netflix or sports channels, but no financial accounts.

> "My fiancée knows all my passwords since we use multiple of them together. For instance, when my Instagram account has a problem, then I use his account. [I share my credentials] just with him and no one else."(IR4)

7.4.1 *Summary*

The interview results highlight important cultural differences for handling money and payments as well as for individual security and privacy behaviour. With regards to our research questions, we learned that Iran's inflated currency and common practices for card payment shape the people's perceptions of security. Besides, Germans are rather

opposed to sharing credentials and expressed the need for keeping track of their spendings. Also, participants from both countries shared a high trust in international companies.

7.5 ONLINE SURVEY

Based on the categories we extracted from our qualitative analysis, we constructed a questionnaire with fifty closed questions, covering payment habits and instruments, and opinions on security, privacy, usability and trust. The survey furthermore included questions on the influence of media advice, the usage of VPNs and proxies, bad experiences with payment methods and a set of questions on cryptocurrencies. We also added two attention check questions. All surveys were hosted on SurveyMonkey (See Appendix D.2). On average, participants spent about 20 minutes on the survey website.

For the design of the survey, we developed four key hypotheses based on our interview findings:

1. Digital payment methods (i.e. internet banking, mobile banking, cryptocurrencies) are on the rise in all countries with Western societies being the lead.
2. Cryptocurrencies are more attractive in Western societies (i.e. DE, US).
3. Credential sharing is more common in non-Western societies (i.e. CN, IRN).
4. Users are unaware of security and privacy risks when conducting payments over VPNs or Proxies.

As none of the interviewees from the qualitative study had reported using cryptocurrencies, we relied on previous work by Krombholz et al. [132] to study reasons for adoption and user attitudes towards these new payment methods.

7.5.1 *Recruitment and Participants*

Our survey covers four distinct countries across three continents. Hence we had to apply various recruitment techniques suited to the target population. We recruited participants in Germany and the US via Crowdflower[3]. Every participant on this platform received 1 USD as compensation. For Chinese participants, we used a Chinese crowdworking service specialised in surveys called Sojump[4]. These participants received 15 RMB (approx. 2.19 USD) as compensation.

3 `https://crowdflower.com` – accessed: 2018-08-02.
4 `https://sojump.com` – accessed: 2018-08-02.

Iranian users are not able to receive international payments, and services such as Crowdflower or Amazon MTurk do not support Iran. Therefore we opted for the distribution of flyers in several districts of Teheran, offering a raffle of 10 gift cards (each 1,000,000 Iranian Rials; approx. 23.75 USD) for an online shopping website roughly comparable with Amazon[5]. Flyers did not result in enough participants; therefore, we announced our study on a classified ad website[6]. Both methods resulted in 37 valid responses, three participants from these two group received gift cards. To recruit more participants, we performed a coffee house study as suggested in related work [218]. For this purpose, one of the authors spent about a week in various coffee shops in different neighbourhoods of Teheran, asking people to fill out the survey on a provided device (a tablet or a laptop), and compensated their time with a coffee or a tea. This process resulted in 65 additional valid responses.

After removing 76 (CN), 89 (DE), 15 (IRN) and 132 (US) participants who gave incomplete answers, and 536 (CN), 16 (DE), 10 (IRN) and 13 (US) participants who did not pass our attention check questions, we retained 1620, 138, 102 and 101 valid responses from China, Germany, Iran, and the US respectively. See Table 7.3 for demographic information of our participants.

For our quantitative evaluation, we used the χ^2 Test for testing proportions like technology adoption rates as well as the Mann-Whitney U Test for Likert questions. The significance levels were Bonferroni-Holm corrected for multiple comparisons where applicable.

7.5.2 *Findings*

DIGITAL PAYMENT METHODS ARE ON THE RISE IN ALL COUNTRIES WITH WESTERN SOCIETIES BEING THE LEAD Many interview participants indicated usage of digital payment methods, i.e. internet banking, mobile banking, and cryptocurrencies. Since Western societies, in our case Germany and the US, typically have an advantage in digital infrastructure and technology, we assumed that digital payment methods are even more common there.

When looking at the adoption rates of payment methods (cf. Figure 7.1), we found that internet banking is more common in China than in the US, with Germany having the lead in adoption rates (Germany 82.6%, US 78.2%, China 81.4%, Iran 38.2%). While there are is no significant difference between these three countries ($\chi^2 = 0.128$, $p = 0.938$), the adoption rate in Iran is significantly lower ($Chi^2_{all} = 19.479$, $p < 0.01$).

In comparison, 77.5% of Chinese participants reported to use mobile banking, compared to 15.2% in Germany, 34.6% in the US, and 47% in

5 https://digikala.com – accessed: 2019-09-23.

6 https://divar.ir – accessed: 2019-09-23.

Table 7.3: Participant demographics in the survey study.

Demographic	China	Iran	Germany	USA
Gender				
Male	47.7%	57.8%	67.4%	42.6%
Female	51.7%	41.1%	28.3%	57.4%
Other	0.5%	0.9%	4.3%	0%
Age distribution				
Under 18	0.24%	0.9%	0%	0%
18-24	12.3%	37.2%	12.3%	12.8%
25-35	47.9%	46.0%	27.5%	39.6%
35-44	24.3%	9.8%	17.3%	21.7%
45-54	9.3%	1.9%	22.4%	10.8%
55-64	2.4%	1.9%	17.3%	9.9%
$>$ 65	0.6%	1.9%	2.8%	4.9%
Education				
$<$ high school	0.49%	1.0%	2.1%	1.0%
High school	16.3%	23.5%	18.4%	23.7%
Associate degree	8.4%	10.7%	13.7%	12.9%
Bachelors' degree	70.0%	49.0%	50.0%	37.6%
Masters' degree	4.3%	10.7%	12.3%	20.8%
PhD	1.0%	5.0%	2.9%	4.0%
IT background				
Yes	18.5%	31.4%	24.6%	18.8%
No	81.4%	68.6%	75.3%	81.1%

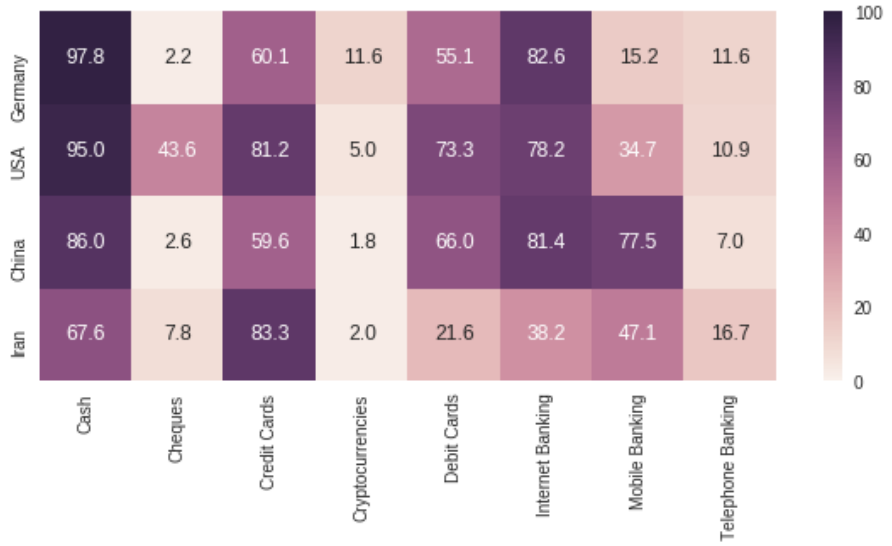


Figure 7.1: Payment method adoption rates across all studied countries, in percent.

Iran ($\chi^2_{all} = 46.98$, $p < 0.01$; $\chi^2_{IRN,US} = 1.88$, $p = 0.17$; $\chi^2_{US,DE} = 7.57$, $p = 0.06$; $\chi^2_{IRN,CN} = 7.45$, $p = 0.06$). Mobile banking is very popular in China for almost all aspects of daily life except paying rent, with 46.7% of mobile payment users reporting to pay for food using their smartphone (DE: 19%, US: 17.1%, IRN: 6.2%), and 56.4% reporting to pay this way for in-store purchases (DE: 33.3%, US: 31.4%, IRN: 6.2%).

Regarding cryptocurrencies, the results indicate that German participants were its biggest users: In general, 11.6% of German participants referred to themselves as cryptocurrency users (as opposed to 4.1% in the US, 1.8% in China, and 1.1% in Iran). Statistically speaking, the adoption rate in Germany is indeed significantly higher than in the other countries ($\chi^2_{all} = 12.417$, $p < 0.01$; $\chi^2_{CN,IRN,US} = 2.178$, $p = 0.34$).

In summary, the results were mixed: Online banking is only significantly less used in Iran, mobile payments are significantly more popular in China, and cryptocurrencies have a significantly higher adoption rate only in Germany. Thus, we reject the hypothesis that Western countries are generally leading in the adoption of digital payment methods.

CRYPTOCURRENCIES ARE MORE ATTRACTIVE IN WESTERN SOCIETIES We hypothesized that cryptocurrencies are a more frequently used tool in Western societies (i.e. Germany and the US), since international payments, which are often needed to exchange cryptocurrencies, are harder to perform in Iran and China whose governments restrict citizens' internet access.

The overall adoption of cryptocurrencies was presented in the former subsection, with Germany having significantly more active cryptocurrency users than the other populations (DE 11.6%, CN 1.8%, IRN

1.1%, US 4.1%). Because cryptocurrency adoption in the US is not significantly higher than in China and Iran, we reject the hypothesis.

When asked about detailed experiences with cryptocurrencies, 13% of German participants reported having used them before and 7.2% reported to use them regularly. In comparison, only 7.9% of US participants reported having used them and 3.1% use them regularly. 5.8% of Chinese participants reported to have used cryptocurrencies (2.7% use them regularly), and only 4.9% of Iranian participants have used them before (1.1% use regularly).

We also tested whether having a background in computer science correlates with the adoption of cryptocurrencies and found a significant correlation within our sample of participants from China ($\chi^2 = 8.669$, $p < 0.004$) and no significant correlation for the other countries. This might be a result of the larger sample size in China.

When asking "If X would endorse cryptocurrencies, I would use them (more often)", German participants reported that endorsement by online resources would have the biggest influence on their acceptance and usage of cryptocurrencies (28.3% agreement, highest value besides "None of the above would change my behaviour"), and radio and TV were reported as least influential to them (2.9% agreement). US-Americans reported to be moderately influenced by family and friends (29.7% agreement each), the government and newspapers were reported least influential (5.9% resp. 2.1% agreement). Chinese and Iranian participants reported their families as most influential factor (China: 46.6%, Iran: 46.1%), followed by the government (IRN: 35.3%, CN: 31.7%), and tech companies (CN: 29.6%, IRN 29.4%). Iranian participants expressed interest in the adoption of cryptocurrencies if they would be pushed more by the general public.

CREDENTIAL SARING IS MORE COMMON IN NON-WESTERN SOCIETIES We asked participants to check in a multiple-choice matrix "I'm comfortable with the following people knowing about my..." to find out which parties they trust to see their bank card details, bank transactions, shopping details in online shops, emails, social network activities, and cellphone activities. In all categories besides email, the Chinese participants had the highest rates of comfort with their spouses/significant others knowing all these information, ranging from 47.9% agreement concerning cellphone activities to 66.5% agreement about online shopping details.

When asked if they ever shared a bank credential, 38.1% of Chinese participants and 30.4% of Iranian stated they mutually share credentials with a person they trust (US: 25.7%, DE: 19.6%). Since we found no significant difference between the populations ($\chi^2 = 6.43$, $p = 0.09$), we reject the hypothesis. In contrast, 71.74% of German participants stated that they have never shared a credential (US: 48.5%, IRN: 48%, CN: 42.7%). Statistical testing yields a significant differ-

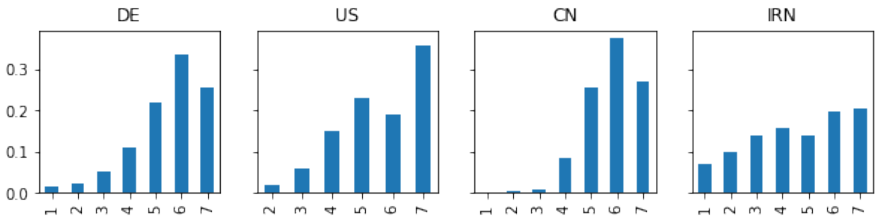


Figure 7.2: Relative answer distribution in percent for the question "I am very cautious of my surroundings while conducting payment transactions.", with 1 representing "not at all" and 7 representing "very much".

ence when comparing all countries ($\chi^2 = 9.5$, $p = 0.02$), but the rates between China, Iran, and the US showed no difference ($\chi^2 = 0.45$, $p = 0.8$).

We further investigated security and privacy awareness of participants by asking them to rate "I am very cautious of my surroundings while conducting payment transactions." Only Iran shows a significant difference (fewer precautions) with other countries ($\text{MWU}_{IRN,US} = 6638$, $p = 0.0002$; $\text{MWU}_{IRN,DE} = 8884.5$, $p = 0.0003$; $\text{MWU}_{IRN,CN} = 111250$, $p < 0.0001$) which is in line with our interview findings (cf. Figure 7.2).

We also asked our participants two questions about third parties observing their financial transactions. Two-thirds of Iranian participants think that their government can see their financial transactions, though only 13.7% think that it is okay. Among Chinese participants, 37.5% of participants think that the government can see their transactions (compared to US: 53.5%, DE: 33.3%). However, only 11.9% of US participants think that this should be the case, as opposed to 26.5% of Chinese participants (DE: 9.4%). Across all observed countries, we saw a consensus in disagreement to the statement that advertising companies should be allowed to observe financial transactions (US: 4.9%, DE: 2.9%, CN: 1.4%, IRN: 0%).

USERS ARE UNAWARE OF SECURITY AND PRIVACY RISKS WHEN CONDUCTING PAYMENTS OVER VPNS OR PROXIES In a number of countries, access to the internet is restricted by repressive governments. In those cases, software like VPNs or proxies help users overcome those restrictions. Therefore, we need to take VPN and proxy usage into account when looking at such countries like Iran and China [107], especially in the payment context, since their usage does come with additional risks like unsolicited data collection and analysis.

Between one quarter and two thirds of participants stated that they use VPNs at least once a month (IRN 63.7%, CN 47.8%, DE 29%, US 25.7%). The differences between all countries are statistically significant ($\chi^2 = 22.56$, $p < 0.01$). When comparing pairwise, the usage rates in China and Iran ($\chi^2 = 2.28$, $p = 0.13$) resp. Germany

and the US ($\chi^2 = 0.19$, $p = 0.66$) are not significantly different. Proxies are overall less popular, between 18.8% (US) and 45.1% (Iran) of our participants use them at least once a month (China 35.1%, DE 27.5%). Again, the rates differ significantly between countries ($\chi^2 = 11.83$, $p < 0.01$).

Germans and Iranians seem to be aware of security risks [52] when conducting financial transactions over VPNs or proxies, 64.7% of Iranians and 44.2% of Germans reported they do *not* conduct financial transactions over VPNs or proxies (CN 28.9%, US 25.7%; $\chi^2 = 0.23$, $p = 0.97$). Note that participants also had the option to answer "I don't use Proxy/VPN" besides the yes and no options. Across all countries, VPNs and proxies were considered not safe in general, with proxies being perceived as more unsafe throughout the field (VPN is safe: CN 29.1%, DE 24.6%, US 23.8%, IRN 21.6%; $\chi^2 = 1.2$, $p = 0.75$; Proxy is safe: DE 17.4%, CN 12.3%, US 11.9%, IRN 11.8%; $\chi^2 = 1.64$, $p = 0.65$). This finding leads us to reject the hypothesis, because our users were apparently aware about the associated risks. For all countries, a majority of users does not know their VPN or proxy providers (US: 75.6%, IRN: 72.6%, DE: 69.8%, CN: 65.1%).

Based on the results, we can reject the hypothesis, because people regard proxies and VPNs as not safe. however only a small portion of Chinese and US American participants reports to not use them for financial transactions.

7.6 DISCUSSION AND IMPLICATIONS

Of our four hypotheses, none could be fully accepted. We found that among our studied countries, Chinese payment culture is leading in the adoption of mobile payment which led us to reject our first hypothesis. Cryptocurrencies are significantly more adopted in Germany, rejecting a similar assumption about the US population. The popularity of credential sharing could furthermore not be divided along the Western/non-Western axis with high sharing behaviour in the US that we observed. Regarding security and privacy perception of VPNs and proxies, they were not considered safe across the board, which rejects our fourth hypothesis that users are unaware of risks when paying over VPNs or Proxies.

Therefore, we chose not to structure the following discussion along the hypotheses, but instead along our study's general topics.

7.6.1 *Perceptions of Security and Privacy*

Our study reveals differences regarding perceived threats to private data and credential sharing. While German interviewees reported discomfort when their PIN entries were observed in public, Iranian interviewees reported the common practice of passing their cards and

PINs along to shop assistants. This finding indicates that commonly assumed threat models (e.g. shoulder surfing) might not universally apply in all cultures.

Except for Iranians, our participants claimed that they are very cautious of their surroundings while making transactions. This outcome contradicts conclusions from previous work [64, 215] which found that most people from the UK, Sweden, Netherlands, and Germany do not take sufficient security measures while entering their PINs at ATMs. However, in contrast to related observational studies [64, 215], our findings are based on self-reported data.

At the same time, we found that card-based payments are common in Iran. In this regard, our results indicate that Iranian and Chinese participants were more comfortable than German and US participants sharing their credentials with close acquaintances like family members and spouses.

As discussed, internet censorship is a concern in China and Iran [53, 107]. Our data indicates that people in these countries actively circumvent such barriers using e.g., VPN services and proxies without knowing their operators. In comparison, the popularity of these tools was less prevalent in the US and Germany. Even though the awareness of associated security risks was high among German and Iranian users, the use of cryptographic technologies was higher in Iran as more than half of Iranian survey respondents reported to conduct financial transactions over VPN services or proxies. This shows the use of payment instruments and the protection of privacy may require advanced technical knowledge, especially when using international services in restricted areas.

7.6.2 *Adoption of a Payment Instrument*

The findings from both our studies confirm that cash is still popular in Germany compared to Iran, China and the US, with the main reason being the ease of keeping track of spendings. Even though German participants reported negative experiences with cash, the perceived benefits still seem to outweigh the negatives.

One of the negative aspects of using cash in Germany was the risk of receiving an incorrect amount of change. While this indicates a human error or bad intentions, people in Iran reported avoiding cash payments due to technical problems. As getting the right amount of change is often not possible, change is commonly substituted by (undesired) sweets. This aspect increases the acceptance for cashless payments. Another explanation for this behaviour could be the effects of a bad experience. Iranian and Chinese people had more bad experiences with cash compared to other payment instruments.

Focusing on cashless payments, mobile concepts were particularly popular in China compared to other countries. This could result from

popular apps which are specifically tailored towards the Chinese culture and lifestyle [204] and big companies like Alibaba pushing users toward their cashless payment systems [144].

The data from our survey suggests that German participants are far more accepting towards cryptocurrencies in comparison to participants from other countries. One of the reasons that Germans like cash is its privacy benefit [37, 134]. Therefore, a possible reason for higher cryptocurrency adoption in Germany could be rooted in the idea of cryptocurrencies and their privacy-preserving nature. Also, the use of this relatively new payment instrument seems to be more common in wealthy Western nations which could result from available infrastructure and more options to spend such currencies.

We also found that news and media articles have a considerable impact on how secure and reliable a payment instrument is perceived. Media seems to influence the adoption of payment instruments indirectly. For example, US participants reported that online resources have a high impact on their usage behaviour and acceptance. Likewise, many Iranian participants reported that the low proliferation dissuades them from using cryptocurrencies, even though they expressed high interest in this payment instrument.

7.6.3 *Payment Culture*

We identified cultural norms regarding payment which are specific to the respective societies. The use of candy or gums to substitute small amounts of change in Iran clearly represents such a habit. This directly affects the use of payment instruments as many Iranian consumers rely on other payment methods than cash, such as cards, as they disagree with the substitution and prefer exact payments, thus avoiding change.

The habits reported by German study participants confirmed that German consumers are concerned about their privacy and like to be in control of their own credentials. In contrast, credential sharing with close family members was commonly accepted among our Iranian and Chinese participants. This once again illustrates the importance of considering cultural differences in usable privacy and security research.

7.7 LIMITATIONS

Recruiting comparable samples in the four countries was a major challenge as the respective countries are diverse in terms of educational background, cultural and political factors. In order to get a truly global view, a larger and more representative sample per country and a comparison of more countries per geographic region is needed.

Internet access is not equally available to citizens in the surveyed countries which also biases our sample towards the population with

access to modern communication technology. Due to the recruiting method in our quantitative study, our sample of participants is potentially biased and not representative of the entire population from the studied countries. In our qualitative study, interview participants were mostly students, and we distributed our interview flyers in two universities which introduces bias toward younger and more educated participants. Such participants tend to make active use of several payment instruments and thus might have skewed the results towards the population of early-adopters.

Moreover, translations to other languages may not convey the same meanings and participants may have had different understandings from our text. For example, Iranians are shown as users of debit and credit cards. However, credit cards in Iran are not common, and there is a high probability that some participants could not distinguish the difference between credit and debit cards. We initially planned to recruit participants online. Due to the challenges we faced in Iran, we changed our recruitment strategy and used the coffee shop method.

7.8 CONCLUSIONS AND FUTURE WORK

In this chapter, we explored payment cultures and user perceptions of payment instruments with respect to security, privacy, and trust across four countries: China, Germany, Iran, and the United States.

We found that unique societal features such as Iranian shopkeepers entering their customers' card PINs, clearly shaped security and privacy perceptions. Also, both Chinese and Iranian participants expressed comfort regarding credential sharing with close acquaintances in contrast to participants from Germany who were less comfortable with that. We furthermore found that proxy software and VPN services are popular in Iran and China, presumably due to mistrust in the government and censorship. While participants generally regarded these tools as unsafe, many of them nonetheless conduct payments over them. In addition, German participants were most willing to accept cryptocurrencies.

Our results suggest that the preference for a particular payment instrument is influenced by local payment culture as well as media. Therefore, we argue that tools to perform sensitive financial transactions should respect these cultural factors and consider them already in the design phase for large-scale adoption.

This work forms a basis for further cross-nation studies on usable security aspects of payment systems. We consider the following paths for future research:

- to study the impact of bad experiences and possible solutions to encourage future interactions,

- to measure the influence of proxy tools on privacy and security with respect to financial transactions,
- to show if credential sharing behaviour induces particular vulnerabilities,
- if external factors influence choices for payment instruments (e.g., social norms), and last but not the least,
- a study on the impact of media on adoption rates of payment instruments with an emphasis on cryptocurrencies.

8

INCENTIVIZING SECURITY – A STUDY ON TWO-FACTOR AUTHENTICATION

This chapter is based on joint work with Sabrina Amft (Leibniz University Hannover), Daniel Hecker (University of Bonn) and Emanuel von Zezschwitz (Google), which has been published in the i-com Journal of Interactive Media [38]. I contributed with the conception, project management, and a majority of the paper writing. See Appendix F for a detailed authorship agreement.

We thank all our survey and focus group participants. Thanks to Matthew Smith for valuable feedback and supervision during the early conception of this work.

The work presented so far concentrated on researching the status quo with the goal of highlighting internal and external factors that shape the perception of security and privacy. The following chapter leverages this knowledge to research and present designs for applying the insights to the case of two-factor authentication.

Account security is an ongoing issue in practice. Two-Factor Authentication (2FA) is a mechanism which could help mitigate this problem, however adoption is not very high in most domains. Online gaming has adopted an interesting approach to drive adoption: Games offer small rewards such as visual modifications to the player's avatar's appearance, if players utilize 2FA. In this chapter, we evaluate the effectiveness of these incentives and investigate how they can be applied to non-gaming contexts. We conducted two surveys, one recruiting gamers and one recruiting from a general population. In addition, we conducted three focus group interviews to evaluate various incentive designs for both, the gaming context and the non-gaming context. We found that visual modifications, which are the most popular type of gaming-related incentives, are not as popular in non-gaming contexts. However, our design explorations indicate that well-chosen incentives have the potential to lead to more users adopting 2FA, even outside of the gaming context.

8.1 INTRODUCTION

The most widespread way to authenticate users is to require them to input a combination of an identifier such as a e-mail-address or a username as well as a password. Often, these passwords are either very easy to guess [7, 123] or can be disclosed through several other means, e.g. phishing, data leaks or insecure storage [156, 219]. Two-factor authentication (2FA) is a security mechanism that was designed to help increase security [116] by adding a second factor to the authentication instead of relying on secret knowledge, such as a passwords, as a single factor. Common manifestations of this second factor include SMS and e-mail notifications, dedicated smartphone applications, or hardware tokens.

When research looks into the process of adopting 2FA, usually the transition process and usability issues within larger organizations are accompanied, with a focus how users react and adopt to the change [54, 143, 223]. From these papers we know that 2FA is perceived

(a) (b)

Figure 8.1: Examples of incentives for adopting 2FA. (a) shows an exclusive dance emote for player characters in *Fortnite* [71], while (b) shows a promoting message for a small gameplay advantage, namely more item space in *World of Warcraft* [28]. Images used with permission, see Acknowledgement for full copyright statements.

as secure but annoying, and that forced 2FA adoption in the workplace sometimes leads to increase usage rates for personal accounts [54]. Less research has been done for individuals who choose whether to adopt 2FA in their private life [130].

In the past there have been attempts to increase the 2FA adoption rates by offering rewards to users who choose to do so. This is especially widespread in the gaming sector and only very rarely found with other companies. Possible incentives include e.g. visual benefits such as virtual pets or gameplay advantages such as premium currency or access to special ingame vendors (see Figure 8.1 for examples). For most of these incentives, two rules apply: 1) They can only be received by complying and adopting 2FA, and 2) if the player chooses to deactivate 2FA again, the rewards are withdrawn from their access. We argue that there are no obvious reasons why other sectors did not yet adopt incentives in the same way the gaming business did. One hypothesis might be that users who play video games might tend to be more interested in IT and security mechanisms and are therefore faster to comply and activate 2FA. Another reason could be that the accounts in this sector often do not only contain monetary value as players bought games, premium currency, or items; but also that players might have spent hundreds of hours to establish a rank or a well-working game status that is often very desired by criminals. In fact, there is a huge market for valuable accounts as just buying a high-leveled status saves other users much time. Due to this, video game accounts are often targeted by malicious actors [150, 206].

Typical incentives in video games are cosmetic modifications like redesigns for characters or items [28, 71, 208], cosmetic companions [14, 28], gameplay advantages like larger inventories [28], in-game pre-

mium currencies [27], multipliers on certain factors such as experience gains [42], or access to special items or in-game vendors [27] (cf. Figure 8.1). One notable exception is Valve's store and community platform Steam. Without the use of 2FA, item trades or sales between players are on hold for up to fifteen days before a trade is concluded [211]. Similarly, Electronic Arts requires users to enable 2FA for their accounts before granting access to the online or mobile versions of FIFA Ultimate Team since 2015 [70].

Since these kinds of incentive mechanics are almost exclusively found in the gaming sector, we assume that we can learn from their presumed success. Therefore, we chose to investigate this topic further and posed the research question:

> How can we transfer (successful) incentives for adopting two-factor authentication from gaming to non-gaming contexts?

During the course of this study, we reached out to developer studios and publishers of video games that employ incentives for 2FA adoption. Our goal was to get data on adoption rates before and after the introduction of an incentive. In addition, we planned a short interview on 2FA and their experiences with it. Sadly, no studio answered our request, and personal acquisition at the Gamescom 2018 convention did also not lead to any responses.

In response to this lack of data from the service provider side, we put strong emphasis on user research. We conducted two survey studies with a gaming-focused ($N = 462$) as well as a general population sample ($N = 288$) about 2FA and incentives for adopting it. From these surveys, we extracted design proposals for transferring incentive models from gaming to non-gaming contexts and tested these in a focus group study with three groups and a total of 15 participants.

We found that incentives increase the adoption rates for 2FA for services that employ them, but users rather self-report that they activated 2FA for security reasons and not for the incentives. The most often encountered type of incentive in gaming contexts, namely cosmetic modifications or items, was perceived least attractive in our focus group study, suggesting that such approaches are not directly applicable to non-gaming contexts. In contrast, small monetary or service-focused incentives were considered most attractive in a non-gaming scenario. Through discussion and comments, we identified a security-privacy trade-off in users' mental models when it comes to adapting 2FA, suggesting that offering users a selection of 2FA methods along with basic educational material would lead to higher adoption rates.

8.2 ONLINE SURVEYS

In order to get a better overview on users' attitudes towards incentives for adopting 2FA in gaming, we developed an online survey that was deployed in various online gaming communities in January and February 2018. Afterwards, this survey was modified and deployed again on Amazon MTurk to recruit a more general sample in January and February 2019.

8.2.1 *Methodology*

Based on our research question, we created a 14-question online survey consisting mostly of multiple choice and Likert-scale questions. We asked participants what services from a pre-selected list they use, whether they have 2FA enabled for these services, and some general perception and usability questions regarding various 2FA methods. Afterwards, we asked about different types of incentives and how they would influence adoption as well as deactivation of 2FA.

We distributed the survey via social media and through posts in the following subreddits: r/SampleSize, r/Blizzard, r/Steam, r/WoW and r/GuildWars2. As this survey was conducted as part of a student project of one of our authors, we weren't able to compensate the participants of this study. After the survey was evaluated, a follow-up post with summarized results was posted in the respective communities as a token of appreciation.

For the general audience, some modifications were made to the survey. First, a question about the term *valve* was included with different possible meanings provided to test whether or not the person would recognize it as the company behind the game marketplace Steam, followed by a second question that directly asked if the user enjoys playing video games. These were added in order to be able to better differentiate between users that were similar to the participants of the first study, e.g., having an affinity for video games and maybe already familiar with incentives, or if they were part of a more general population. We specifically asked about Valve and Steam, which might be best known to PC gamers, but less likely to console or mobile gamers. This was a conscious decision because most of the games who employ 2FA mechanics are PC-centered or even exclusive, such as World of Warcraft. In addition, questions and answer options regarding incentives were modified to include not only gaming-related options. To counter-balance our participant's mental load of this extended survey, we chose to change our Likert-scale questions from 7-point to 5-point, trading a finer resolution with (hopefully) more accurate answers. The full question set of both surveys can be found in the Appendix.

After a pre-test with 20 personal contacts which led to minor improvements in the survey design, we hosted the modified survey on

Service	Overall	2FA
Blizzard	56.7%	43.1%
Discord	71.4%	26.0%
Facebook	50.9%	24.5%
GOG	25.0%	6.9%
Guild Wars 2	65.6%	55.0%
Nintendo	23.4%	3.9%
Origin	33.5%	11.0%
PSN	17.3%	5.2%
Reddit	87.7%	11.5%
Slack	16.0%	4.3%
Steam	88.1%	62.6%
Telegram	13.2%	5.4%
Twitter	43.3%	16.9%
Wargaming	1.3%	0.6%
WhatsApp	36.8%	6.1%
Xbox Live	11.0%	4.1%

Table 8.1: Usage and adoption rates for various gaming-related surveys within a gaming-centered population. Both percentages in relation to all participants, $N = 462$.

Amazon Mechanical Turk (MTurk) with the following participant requirements: Participants had to have a HIT approval rate of at least 90% and needed to be based either in Canada, Germany, the USA, or the United Kingdom. We chose the geographic locations for potential participants in accordance with our demographic sample from the gaming-focused survey. All MTurk participants were compensated with USD 2.00 for their work.

8.2.2 *Results*

8.2.2.1 *Gaming Community*

For our gaming-related sample, we could collect 594 data sets, from which 462 were valid. The participants were on average 27 years old ($\sigma = 7.2$). Of all participants, 76% self-identified as male, 19% as female, and 4% as non-binary. Most people were living in the United States of America (36%), 14% were from Germany, 7% from Canada, and 7% from the United Kingdom. Other countries were represented by less than 5% of participants and are omitted here.

At the beginning of the survey, we asked participants to check which services (from a pre-compiled list of 2FA-enabled services) they

use and for which of them they have 2FA enabled. The results are presented in Table 8.1. Only 21 participants stated that they do not use 2FA for any of their accounts. Overall, gaming-related accounts have a higher adoption rate for 2FA than non-gaming accounts, with those that prominently offer an incentive (Blizzard, Guild Wars 2, Steam) having even higher rates. The participants had the opportunity to add other services for which they use 2FA. Twenty-three people named Google services like Google Mail, five mentioned online banking and one person claimed they would use 2FA on all their accounts if the service would support it. Other online platforms mentioned were Dropbox, GitHub, GitLab, Microsoft services, e-mail provider and games like Star Wars: The Old Republic, Wildstar, EVE Online, and Final Fantasy XIV.

Regarding different 2FA methods, SMS is the most widespread method of 2FA with 311 reported users (67.3% of all participants). Google Authenticator is used by 54% of the participants, while service specific apps are used by 50%. A portion of 44.8% is using e-mail as a way of getting the second factor. Hardware tokens are way less widespread with only 6.5% of participants using them.

Afterwards, participants were asked to rate the different presented 2FA methods regarding their perception of how convenient the usage of those methods is and how secure they regard a method, both on a 7-point Likert scale.

SMS was rated very convenient with an average score of 5.14 ($\sigma = 1.88$, median=6), but received only an average rating of 4.85 ($\sigma = 1.79$, median=5) in perceived security. Receiving access codes via mail received an average convenience score of 4.55 ($\sigma = 1.78$, median=5) and an average security rating of 4.11 ($\sigma = 1.55$, median=4). The Google Authenticator received both a slightly higher convenience rating ($\mu = 5.32$, $\sigma = 1.70$, median=6) as well as a slightly higher security rating ($\mu = 5.72$, $\sigma = 1.28$, median=6) on average compared to SMS. Service specific applications were rated on average 4.79 in convenience ($\sigma = 1.99$, median=5) and 5.77 in security ($\sigma = 1.39$, median=6). The lowest convenience score ($\mu = 3.38$, $\sigma = 1.97$, median=3), but the highest perceived security ($\mu = 6.17$, $\sigma = 1.40$, median=7) was given to hardware tokens.

In the next part of the survey, participants were asked about what motivates them to enable 2FA on their accounts. The enhancement of the account security was a motivational aspect for 88.1% of participants. The second most indicated motivation for using 2FA is a high monetary value attached to the corresponding account for a total of 50.9%. The possibility of circumventing restrictions motivates 27.3% of participants, whereas visual bonuses are only able to attract 21.9% of participants. Just 5% of participants stated that they have activated 2FA to gain gameplay advantages. Afterwards, we presented hypothetical scenarios that might influence the adoption of 2FA and asked

	Gaming Sample	General Sample
Total Participants	462	288
From the USA	36.0%	50.7%
From Germany	14.0%	49.3%
From Canada	7.0%	0.0%
From the UK	7.0%	0.0%
Male	76.0%	68.8%
Female	19.0%	30.9%
Non-binary	2.0%	0.0%
No gender data	2.0%	0.0%
Avg. Age	26.5	32.3
Standard Deviation	7.2	9.5

Table 8.2: Demographic data from both surveys, reported after cleaning the data.

participants how likely they would enable it in the given situation. In the first scenario the user would lose a functionality if 2FA would not be activated, as it has happened on Steam with their trade and market hold. 228 of the 462 participants (49.4%) stated that they would very likely activate 2FA ($\mu = 5.6$, $\sigma = 1.87$, median=6). The next scenario was the introduction of gameplay advantages, if the user activates 2FA. Of all participants, 237 (51.3%) stated that they would use 2FA in this case ($\mu = 5.61$, $\sigma = 1.93$, median=7). In the last scenario the users were offered an exclusive visual in-game modification for using 2FA. Only 181 of the asked people (39.2%) indicated they would very likely start using 2FA to gain said modification ($\mu = 5.01$, $\sigma = 2.09$). This stands in contrast to the self-reported reasons for activating 2FA in practice, as reported above.

8.2.3 *General Population Sample*

While we opened the recruitment to people from Canada and the UK, nobody from these countries participated in our survey. Therefore, we got 313 participants in total, with 155 from the US and 158 from Germany. After cleaning the data and removing participants who failed the attention check, we retained a total of 288 participants, with 146 being from the US and 142 from Germany. The complete demographic data can be found in Table 8.2.

While 92.7% of participants (95.2% from US, 90.1% from Germany) stated that they enjoy playing video games, only 62.5% (US: 62.3%, DE: 62.7%) associated the term *valve* with video games. For further

Service	Overall	2FA	GSS	2FA
Online Banking	94.8%	65.3%	96.1%	67.6%
Backup & Cloud	73.3%	14.6%	76.5%	17.9%
E-Mail	96.2%	40.3%	97.8%	41.3%
Social Media	88.5%	23.6%	88.3%	23.5%
Messaging	85.1%	11.8%	86.6%	12.8%
Online Games	73.6%	30.6%	88.3%	44.1%
Retail	89.9%	22.9%	91.6%	25.7%
Productivity	63.2%	8.0%	68.7%	9.5%
Hosting	23.6%	6.3%	27.9%	9.5%

Table 8.3: Usage and adoption rates for various gaming-related services from the general population sample ($N = 288$), and its gaming sub-sample (GSS, $N = 179$).

analysis, we considered the sub-sample who recognized the company Valve as well as enjoyed gaming as our *gaming sub-sample* ($N = 179$). The average age for the gaming sub-sample is at 30 years, while the non-gaming sample average at 35 years. While the gender ratio is equally divided on all mentioned genders for non-gamers (53.2% female compared to 46.8% male), there is a much larger imbalance within the gaming sub-sample where 82.1% identified as male and only 17.3% as female.

When asked whether participants use 2FA for at least one of their accounts, 85.7% agreed to do so (US: 85.6%, DE: 85.9%). The adoption rate for people from the gaming sub-sample was 87.7%. A detailed overview of account types and 2FA usage rates can be found in Table 8.3.

Overall, we can see that the gaming sub-sample has higher 2FA adoption rates throughout all categories. Online games have the third highest 2FA adoption rate (after banking and e-mail) for the overall sample, while in the gaming sub-sample, they are placed second highest.

After asking again about selected services, the participants were asked about what 2FA instruments they use. Again, e-mail and SMS were the most common instruments, with 35.8% of participants using e-mail and 34.4% using SMS at least once a week (gaming sub-sample: 38.0% e-mail, 40.8% SMS).

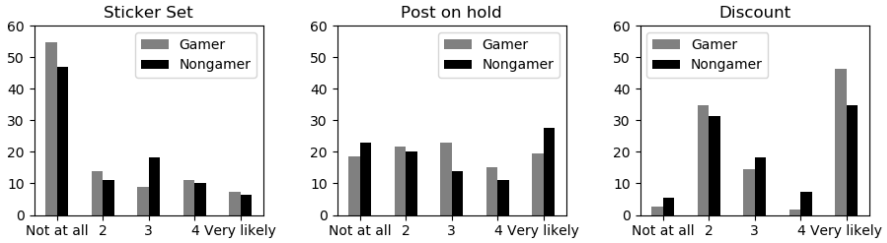
As for convenience and perceived security, SMS was ranked most convenient ($\mu_{all} = 3.22$, $\sigma_{all} = 1.78$, $\mu_{GSS} = 3.38$, $\sigma_{GSS} = 1.70$) and most secure ($\mu_{all} = 2.98$, $\sigma_{all} = 1.66$, $\mu_{GSS} = 2.98$, $\sigma_{GSS} = 1.59$). These ratings are a change from our first survey with a gaming population where Google Authenticator was ranked most convenient, and hardware tokens were ranked most secure (cf. Section 8.2.2.1).

For each Likert scale question we conducted a Mann-Whitney-U test and compared the ratings of the gaming sample with those of the non-gaming sample. The results were corrected using the Bonferroni-Holm method which shows that there are almost no significant differences concerning how both groups rate different 2FA methods. A notable exception to this is the convenience of service specific 2FA apps (such as the Blizzard Authenticator), which was rated significantly higher by gamers ($U = 7544$, $p < 0.001$). This implies that gamers are more comfortable or familiar using them.

Regarding reasons for using 2FA, the large majority of 76.0% stated that their primary reason for using 2FA is account security. This is again in line with the previous study where security was also the major concern for users.

To test which kind of incentive might be interesting for a general population we decided to phrase several ideas for incentives that were inspired by existing incentives, but modified to lose the direct gaming context and used a 5-point Likert scale to ask how likely participants would activate 2FA in this scenario. While most of these examples were closely connected to the categories we find in gaming-related incentives, i.e. cosmetic enhancements, gameplay advantages, and sanctions, we also added incentives such as one-time payments, discounts, or physical gifts to complement the selection. Results show that monetary incentives like one-time payments would be most interesting for our participants with an average score of 3.75 ($\sigma = 1.39$, median=4). When differentiating between the gaming and non-gaming sub-samples, we see that gamers are more interested in gaming-related incentives like gameplay advantages with an average Likert score of 3.38 ($\sigma = 1.48$, median=3) in comparison to 2.67 ($\sigma = 1.47$, median=2) for non-gamers. This is supported by a Mann-Whitney-U test that shows a significant difference between the gaming and non-gaming sub-sample ($U = 6568.5$, $p < 0.001$). There are no other outstanding differences in the ratings for other incentives. In our first study, participants rated only three gaming-related incentives on a 7-point Likert scale. The results suggested that all were well received by users, although loss of function ($\sigma = 5.60$) and gameplay advantages ($\sigma = 5.61$) attracted more users than visual modifications ($\sigma = 5.01$).

A graphical overview on the attractiveness of various incentives is presented in Figure 8.2. We can see a bimodal distribution for the permanent discount scenario with most participants of both groups finding it *very likely* that this kind of incentive would lead them to activate 2FA for an account. Participants from both groups found sticker sets, which we thought would correspond closely to visual incentives found in online games, very unattractive as an incentive in general. For the restriction scenario of keeping social media posts on hold for moderation unless a user has activated 2FA, we received very mixed answers.



(a) (b) (c)

Figure 8.2: Answer distributions for the question *How likely is it that you would activate 2FA in the following scenarios?*. Only selected incentives are presented.

To see whether incentives increase the adoption rate for 2FA, we looked again at adoption rates by service. Although most gaming-related accounts we listed in the first survey were replaced by general services, we still asked about Steam and Blizzard accounts regarding 2FA. While both have mediocre usage rates over the whole population with 54.9% for Steam and only 33.0% for Blizzard, both have high 2FA adoption rates when compared to other services. Between the gaming and non-gaming sub-samples, we see again that Steam and Blizzard have comparably very high 2FA adoption rates for all specific accounts we asked within the gaming sub-sample, i.e. 22.9% of our gaming participants use 2FA for their Blizzard accounts and 35.2% for Steam while these values in the non-gaming sub-sample are between 3.7% and 5.5%.

The 2FA adoption rates for both in the gaming sub-sample are also larger than the respective ones for all participants, where 16.3% stated to have 2FA activated for their Blizzard accounts and 23.3% use 2FA for Steam. For both the whole population as well as the gaming sub-sample these values are only topped by online banking, where 45.1% of all participants employ 2FA, and 49.2% of participants within the gaming sub-sample. Services such as Paypal, Amazon and Google Mail also have 2FA adoption rates between 28.8% and 36.3% for both groups. The other 23 specific services in the list we provided achieved lower adoption rates of at most 16.2%.

Overall we performed Fisher's exact tests to compare the general usage rates to the 2FA adoption rates between the gaming and non-gaming samples. While we find no significant differences for specific websites, we find that participants from the gaming group are more likely to adopt 2FA for online game accounts in general (0.342, $p = 0.004$, Bonferroni-Holm corrected for multiple testing).

8.3 DESIGN SPACE AND CONCEPTS FOR NON-GAMING INCENTIVES

From the surveys, we learned that account security and account value are seen as large motivators to adopt 2FA. When it comes to incentive types, we see that both restrictive measures for non-adopters as well as financial or gameplay advantages are rated as convincing for the adoption of 2FA. This was why we decided to pursue these incentive types further and draft non-gaming examples of these types. In addition, we also decided to adopt an example for visual modifications, since these were the most common type of incentive seen in the gaming landscape.

The first step in transferring popular incentive types from gaming to non-gaming contexts was reflecting how the design space would change.

Online games have a closed economy and a fixed number of distinct items to acquire. This nudges players to complete collections of items such as companion pets, and a 2FA incentive can easily hook into this mechanic. When trying to transfer the incentive of visual modifications or companions, we searched for a similar mechanic that is of only cosmetic (i.e. not functional) value and that comes with a collection or completionist nudge. We found that stickers in instant messaging are an increasingly popular cosmetic gimmick, and that some people exhibit a similar collection behaviour [237]. Therefore, we chose to select exclusive messenger stickers as a non-gaming incentive for adopting 2FA. We thus created a mock-up of a WhatsApp conversation which features two users discussing and presenting an exclusive sticker that was obtained by activating 2FA.

Economic advantages were generally well-accepted by the survey participants (see also Figure 8.2); most participants stated that it would be very likely that they activated 2FA if they were either offered a discount in e.g. an online shop or if they received a one-time payment for activation. In gaming, economic advantages as incentives for activating 2FA in gaming are less frequent and come in different implementations, such as more inventory space (cf. Figure 8.1). As we found it hard to model an equivalently "powerful" incentive in a non-gaming context, we chose a discount for an online shop, which is also an economic advantage. This keeps the design generally applicable as opposed to service-specific economic advantages like extra storage space for a file sharing service. Therefore, we designed a mock-up of a popular German clothing shop website offering a 5% discount while 2FA using e-mail as the second factor was activated.

We were also very interested in restriction mechanisms such as those of Steam, so we additionally included a scenario which inhibited platform use without 2FA activated. While other scenarios were possible, we chose post moderation and restrictions in a social network as an ex-

ample. Again, this was so that as many participants as possible would relate to the scenario. We created two case mock-ups using Facebook as a template. In the first, the user attempted to post a status update that included another user. Since the second person had 2FA activated, but the first user did not, the mock-up does not allow the status to be posted. In the second example, the user tried to post something in a public group but was once again stopped and made aware of the fact that before their post was published, a moderator needed to confirm it. Both inhibitions could be circumvented by activating 2FA.

To summarize, we chose the following incentive types to design artifacts: Economic advantages, inhibited social media, and exclusive sticker sets. All mock-ups can be found in Figure 8.3.

8.4 FOCUS GROUP STUDY

In order to get deeper insights into users' attitudes towards 2FA in general and the various incentives we designed, we decided to conduct a focus group study. Since our goal was to explicitly evaluate new concepts for 2FA incentives in non-gaming contexts, we chose this method for our evaluation.

8.4.1 *Methodology*

We tested the mock-up designs (cf. Figure 8.3) in a focus group study with 15 participants, who received EUR 10 as compensation for their participation.

The group interview contained discussion of general knowledge and usage experience of various 2FA methods, associated group rating exercises regarding simplicity, ease of use, security and likeliness of adoption. Afterwards, real 2FA incentives as well as our mock-ups were presented and discussed.

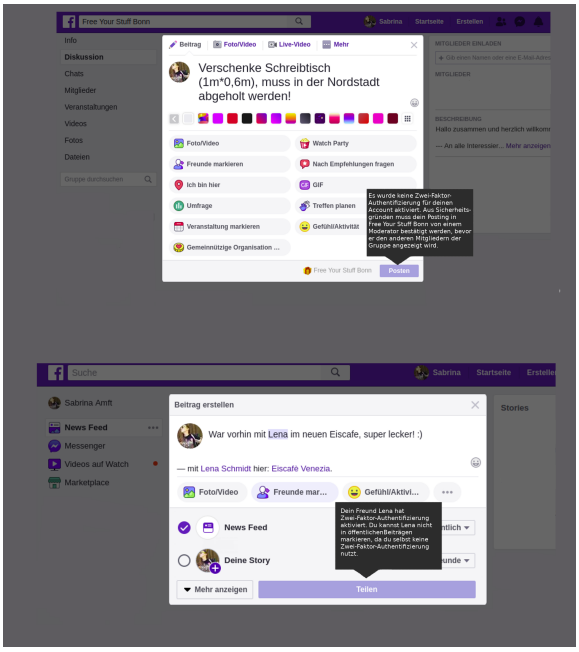
Three groups of participants were recruited through personal contacts and advertisements placed around the university campus. All participants were between 18 and 29 years old and from Germany. While the first group was an all-male assembly of five computer science students, the second group consisted of three women and two men, who also all studied computer science. The third group featured three women and two men, all participants were not enrolled into a computer science program.

In the following, we present the most important arguments and findings from our different group sessions.

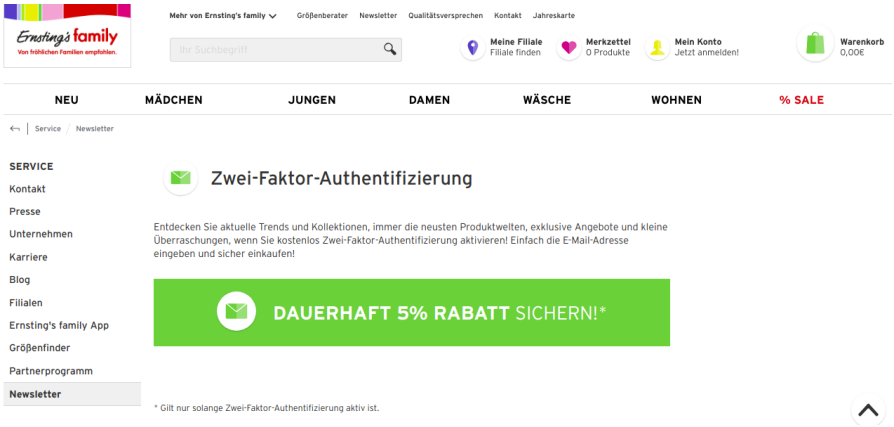
8.4.2 *Results*

At the start of each session we asked participants to tell us what they knew about 2FA. While both computer science groups were able to

(a) Exclusive stickers for a messaging app.



(b) Two social network scenarios: Posts to a group need to be moderated without 2FA (top), tagging a person who uses 2FA is disabled unless the poster themselves enables 2FA, too (bottom).



(c) Permanent shop discount while having 2FA activated.

Figure 8.3: 2FA incentive mock-ups for various services which were designed for the focus group evaluation.

name different methods, the third group only knew about SMS and e-mail as well as some examples from banking contexts. During the session, they seemed to have different misconceptions about what 2FA was and when it was used as they confused it with e-mails about suspicious account activities or SMS that included account activation codes.

> Isn't that sufficient? I mean, you have registered with [your phone number], so it's a kind of two-factor authentication when they send you the confirmation code via SMS and the phone processes this code. (A participant from group 3)

When asked about the properties of different methods, there were major misconceptions about the security of SMS. The method was perceived as very secure in all three groups with arguments such as *"since they only arrive on my phone and operate on the SIM card"*, or that *"you cannot read the code on the lock screen, and without my fingerprint nobody can access it"*. All three groups also voiced concerns about e-mail being not secure enough as they either thought hacking an e-mail inbox was incredibly easy or that it was purely depending on their password strength. This shows a lack of understanding even in the computer science groups that were otherwise able to explain not only the basic concepts of 2FA methods but in some cases also the underlying algorithms. Interestingly, although SMS was perceived as more secure than e-mail, most participants seemed to prefer the usage of an e-mail-address for 2FA and did not want to disclose their number. Authenticator apps like the Google Authenticator were mostly unknown by our focus group participants. Some people who identified as gamers reported to use them, for example for their Blizzard accounts. Hardware tokens were on the other hand very common, as many German banks require token-generated TANs for online banking transactions. An example of such a token can be seen in Figure 8.4. User sentiment about these generators was often negative, as our participants have experienced delays and hindrances in acquiring such a generator from their bank in the past. In addition, they report problems in generating the TANs by holding the token in front of a flickering code on their computer screen that contains the transaction information. For example, a participant from group 2 reported *"it's a fifty-fifty chance"* if the device would actually work as intended. Another participant stated

> It depends on what kind of token you have. If I think about my TAN generator, it's horrible. (A participant from group 2)

While most participants had no previous experience with hardware token, they were perceived as secure. However, participants expressed

Figure 8.4: A *SmartTAN Optic* TAN generator from a German bank. The customer's card is inserted into the device, transaction data is transmitted through optical sensors by holding the token in front of a flickering code on screen. As a fallback mechanism, the data can also be entered through the device's keypad. After the relevant transaction data is displayed on the screen and acknowledged by the user, the device eventually displays the TAN.

concerns about this method as the token needs to be carried in person and could easily get lost. Therefore they were rated as less convenient than other methods such as SMS.

In addition, there were often different views on which methods participants would use in different cases. We saw a clear differentiation between accounts where payment data was attached or shopping history was collected, for these accounts our participants would accept 2FA rather than for "unimportant" accounts such as credentials for online forums. A de-facto consensus was the wish for a selection of 2FA methods, as then every user could cherry-pick the method they liked best.

In general, all groups seemed to agree that while rewards were an interesting approach, especially the sticker set was perceived as not good enough to weigh out the negative sides of 2FA usage, i.e. as the extra effort required and the potential disclosure of contact data. They also rejected incentives that were "too good": Group 2 and 3 voiced concerns that a company offering rewards for i.e. a phone number required for 2FA might have malicious intents such as selling the number or abusing it for unwanted advertisements.

> I would be a little skeptic whether they would sell my [phone number] later on, especially when I get something in return for [enabling 2FA]. (A participant from group 2)

Participants found the shop discount scenario very appealing, especially since it used e-mail as the second factor instead of SMS or a

custom solution. Participants in group 1 and 2 explained that the shop would have their e-mail address anyway, so enabling 2FA in this case would not come with additional exposure of personal information. One participant in group 2 argued that this might abuse the situation of lower income households, basically forcing them to adopt 2FA as they would be dependant on the discount.

The inhibition of social media in the Facebook example was partially accepted as a good incentive, although some participants in groups 2 and 3 were unsure about the benefit for the users and stated that they might not use the service at all in this case as they found the inhibition to be annoying.

All three groups stated that websites that either directly handled monetary purposes such as online banking or those that indirectly handled their bank data or valuable items such as Amazon or Steam were likely candidates for 2FA adoption. Other personal information was also named, although participants deemed them not as important as websites that dealt with money. A participant from group one even explicitly stated that he would not use 2FA for dating apps, although these might hold very intimate information about a user.

Another often mentioned aspect was that participants seemed to weigh the usefulness of 2FA against the potential benefits. If a website did not hold important enough information or if a login with 2FA was required too often, they rejected 2FA usage in general. However, for i.e. a bank account, users would even use their phone number as this was deemed important enough.

Finally, participants argued that often there would be no need to lure users with rewards, but one for more explanations and educations on what 2FA is and why they should adopt it.

8.5 DISCUSSION

In the following, we will discuss selected topics that emerged from the focus group interview and put them in context with our research question.

8.5.1 *General Privacy and Security Perception of 2FA*

We found grave misconceptions about the security of SMS. SMS messages are sent in plain text and can be easily attacked with low equipment costs [205], which is why NIST declared them insecure as a second factor in 2016, but reverted the statement in a later update [69]. Despite these security flaws, the participants in our survey as well as the focus group interviews tended to regard SMS as very secure and placed a lot of trust in the medium.

Some participant statements in the survey and the focus groups suggest that there might be a differentiation between primitive mobile

phone features that use a SIM card (i.e. calling, SMS), and smartphone features that resemble typical computer applications and behaviour (i.e. apps, messaging, and web browsing) within users' mental models. While the phone features might be regarded as more secure, the smartphone features come with similar risk perceptions as general internet and PC applications [131]. News coverage and vulnerability disclosures could have worked toward this narrative, because it is usually the phone operating system or selected apps that are portrayed as insecure, while there is no such coverage about primitive phone features.

Participants also had clear differentiation between which accounts were worth protecting with 2FA. A common pattern in our focus groups was that when monetary value or sensitive payment data (e.g. SEPA account details) is connected to an account, it becomes worthy of securing it with 2FA. In contrast, accounts which are rich with personal and intimate data but not associated with money are not deemed worthy of additional protection by our participants. This confirms prior research on the monetary value of personal data [25, 59]

This conception about data being not as worthy as actual money has been discussed before [94], and it remains open if we as a professional community should see this as a need for better concepts and communication of those, or as a field where strict consumer protection is necessary to soften the impact of these user mental models.

When it comes to handing over phone numbers, we saw some mix-up between account validation purposes and actual 2FA setup. While companies usually employ account validation via SMS to restrict automated account creation and increase the advertising value of their users' data, 2FA via SMS has the only purpose of making the account more secure. We regard this tendency as very alarming, since we hypothesize that the practices for user data harvesting have the potential to negatively influence users' mental models of 2FA's security benefits.

8.5.2 *Incentives in Gaming*

While the adoption rate for 2FA in gaming services that offer incentives are rather high (cf. Table 8.1), we see only very small approval when asking directly about the influence of an incentive on adopting 2FA.

It could be that these gaming accounts in question are first and foremost seen as valuable accounts by our participants, since especially Massively Multiplayer Online game (MMO) accounts often contain hundreds of hours of playtime and an assortment of valuable items. The side-economy of buying and selling actual accounts for often several hundred Dollars on marketplaces like eBay or special platforms like g2g [85] gives this perception additional weight. This might make

the value of gaming accounts more visible than for example, social media accounts [168].

Another approach to explain this discrepancy could be increased advertising of 2FA through the measure of incentives. Usually, gaming publishers release accompanying news and social media posts when introducing an incentive for 2FA adoption [29, 72, 207], this generates publicity and might introduce players to the concept of 2FA who haven't been in contact with this security measure before, thus raising awareness for account security in general. These news are often further distributed by major gaming news websites such as Kotaku [157, 234]. Our findings from the focus group interviews where participants generally wished for more and better education on the subject of 2FA resound with this observation.

Besides social media posts and press releases, visual incentives in an online game are also advertising in itself. Players see new items, skins, or companions in-game and might start asking around or researching how to acquire them. This way, they also eventually reach the information about account security and might become aware of the security benefits of adopting 2FA. However, our focus group interviews have clearly shown that this mechanism only works in closed economies with a focus on collecting rare and different items. In the general online world, the attractiveness of a sticker set incentive was made highly dependant on the target group, e.g. teenagers.

8.5.3 *Influence of Incentives on Security*

When an incentive allows for reliable distinction between users who have activated 2FA and those who have not, the service provider might endanger their users who have 2FA not enabled. A well-designed incentive thus must not allow to filter users by 2FA activation.

Visual incentives in games like skins, emotes, or mini pets can be disabled, switched out, or simply not used by players. Access to restricted vendors is not visible to outsiders, the same goes for inventory space and in-game wallet.

Steam's trading hold time for 2FA-disabled accounts is visible to trading partners, but initiating a trade needs confirmation from both participating users.

When designing incentives for non-gaming contexts, designers have to keep this security constraint in mind, especially for social features such as moderated posting.

8.5.4 *Transferability between Gaming and Non-Gaming Contexts*

Video games and especially MMOs have fixed and clear rules of *value* [138]. Collecting a wide variety of items, especially rare items, is deemed an important meta-goal in online multiplayer games. This

pressure to collect is not as prominent in daily life in Western societies as it is in gaming communities, which has to be taken into account when discussing the transferability of incentives for 2FA.

Our focus group results have shown that especially visual incentives work better in closed-economy contexts than in the daily online world, as sticker sets were dismissed as rather special or only suitable for a narrow audience like teenagers. The general controversy about incentive types we saw in the group discussions suggests that maybe offering a range of incentives from which participants could pick the one they like best would be a golden way for non-gaming contexts. However, this would come with increased setup costs for service providers.

Our focus group results also indicate that there is a certain sweet spot about the power of an incentive. Participants acknowledged the increased pressure on low-income customers in the context of discount incentives. While all participants agreed that 2FA was a good thing in general, they were rather torn on incentives that de-facto pressured users into enabling 2FA because of powerful advantages. In addition, we observed concerns about unfair advantages or even incentives as bait for data abuse. When an incentive looked too good to be true, our participants turned skeptical and suspected a bait offer to gather phone numbers or the like. Regarding the transfer of 2FA incentives into non-gaming contexts, incentives that offer discounts or in-ecosystem advantages such as more space in the cloud might work best.

8.5.5 *Suggested Incentives for the non-gaming Context*

Gamers have an overall higher adoption rate throughout all categories of services we asked about. This could indicate that successfully adopting 2FA in at least one field lowers the bar for adoption in other fields.

In regard to our proposed examples for incentives mechanisms in non-gaming contexts (cf. Figure 8.3), we found that the shop discount was the most attractive example for our focus group participants. The monetary discount is a strong pull, and e-mail as a second factor is perceived as non-intrusive. No additional user data disclosure is needed for setting up 2FA in this case, which was an aspect that our participants highlighted as positive.

In contrast, the other scenarios we proposed were dismissed as not very attractive (sticker set), and too restrictive (Facebook posting restrictions). We were curious about the attractiveness of cosmetic incentives and thought the sticker feature of many modern messengers would be a good equivalent to gaming contexts, but it turned out that stickers have no such collection effect as weapon skins or mini pets in the gaming context might have.

Drawing from these results, we propose the following design recommendations:

- The industry should consider monetary benefits as we found that 2FA incentives for non-gaming contexts to be attached with monetary value where applicable and effective.
- Services should offer a set of alternatives as second factors to suit users' needs and their willingness to accept privacy trade-offs for enhanced account security.
- Also, as we saw the wish for more education regarding 2FA, we strongly propose some educative text or media to accompany a 2FA campaign in non-gaming contexts, as users are usually not as tech-savvy as gaming populations.

Suitable education is orthogonally important as it could help with clarifying and correcting divergent mental models about how 2FA works and what privacy risks are associated with it.

8.6 LIMITATIONS

As every scientific work, this one is not without its limitations.

First and foremost, all data we collected through our surveys and focus group study was self-reported. It is known that people try to put themselves in a better light in such cases, especially when reporting about security and privacy practices and motivations. This phenomenon could have skewed our results, so field study work is needed to confirm (or reject) our findings. In addition, some users might not know that they already use some kind of 2FA in their daily lives, which would result in a skew in the other direction.

While both surveys we conducted were similar, there were some modifications to the second run. Furthermore, both samples were conducted on different platforms, several months apart and with different motivations as the gaming sample received no compensation whereas the general sample was rewarded with USD 2.00. All of these differences might have had an influence on the answers our participants gave.

Our focus groups only portray a very narrow cultural and demographic sample, since all participants were rather young and from Germany. Students are known to be more tech-savvy and innovation-friendly in general, and German cultural and societal values like an emphasis on privacy [128] might have influenced our results. Further research with more diverse sets of participants is clearly needed and much appreciated.

8.7 CONCLUSION AND FUTURE WORK

In this chapter, we presented the design, evaluation, and interpretation of three user studies about incentives for adopting two-factor authentication (2FA). We conducted two surveys with multi-national samples, within a gaming-focused population and a general population sourced by crowdworking. Based on the results of these surveys, we designed three novel concepts for incentive mechanisms in non-gaming contexts, namely a sticker set reward for a messenger application, the revocation of posting restrictions in certain areas of a social network, and a permanent discount for an online shop as long as the customer has 2FA enabled.

We found that there is no "one fits all" solution. This confirms previous work on authentication [224]. Participants expressed needs to minimize the risk of losing access to a second factor as well as portability of said factor. They were concerned about disclosing private information like phone numbers for SMS 2FA and favoured a selection of 2FA instruments to choose from, based on their needs and the perceived importance of the respective account they want to protect.

From the three designs we proposed, the online shop discount incentive was considered most attractive, while the sticker set turned out uninteresting for most participants. This suggests that the apparent effectiveness of cosmetic incentives which can be found in gaming contexts is not applicable per se to non-gaming contexts. Furthermore, participants favoured a selection of different 2FA mechanisms instead of one "golden way". From these experiences, we formulated three actionable recommendations for deploying incentivized 2FA: Use monetary incentives where applicable, as they have the strongest pull. Offer alternatives to suit users' individual needs. Educate about 2FA and its benefits in general.

Future research could attach here and evaluate different combinations of 2FA mechanisms that cover a wide range of audience. In addition, field studies about the actual adoption likeliness and user behaviour in the wild are needed.

8.8 ACKNOWLEDGEMENT

Portions of the materials used are trademarks and/or copyrighted works of Epic Games, Inc. All rights reserved by Epic. This material is not official and is not endorsed by Epic.

World of Warcraft ©2004 Blizzard Entertainment, Inc. All rights reserved. World of Warcraft, Warcraft and Blizzard Entertainment are trademarks or registered trademarks of Blizzard Entertainment, Inc. in the U.S. and/or other countries.

Part II

INSIGHTS FOR RESEARCH AND PRACTICE

9 CONCLUSION

In the previous chapters of this thesis, the perception of security was portrayed for different contexts. In the following, these separate insights are connected and brought in context to reach a higher-level understanding of the underlying research question:

> How do people perceive security in their everyday lives?

9.1 STUDY FINDINGS IN CONTEXT

In Chapter 4, it was shown that personal narratives of security diverge between people and that they are shaped by personal context, as the study participants who worked in consulting had clearly different narrative from those who had a more technical relation to security. Furthermore, the narrative showed to be a powerful tool for shaping interpersonal relations in the professional context. Both department heads we interviewed were aware of different narratives and both used the uncertainty around a common narrative for shaping and managing team culture.

Chapter 5 explored a similar direction, namely the mental models of experts and non-experts in security. It was striking that administrators features more elaborate and differentiated mental models than end users, which is in line with the findings from Chapter 4 that work position and context shape a narrative, which can be seen as a central basis of a mental model. Furthermore, we can see fragments of external influence on mental models, for example protocol and flowchart components that are often found in educational material about security. In addition, threat models were different depending on personal context. While administrators often featured sophisticated attackers on a network-level, non-experts generally had a focus on their personal devices and their security.

Chapter 6 showed that the perception of security practices strongly shapes human interaction on that topic, and that researching perception is a key method for finding out fields of action for security technology. Practices that were deemed very effective but not easy to follow or adopt indicate areas where system and UX design need to improve before a measure can be unconditionally recommended and adopted.

When seen in context of each other, Chapters 5 and 6 provide an impression of how mental models and advice are connected. Personal context and the degree of involvement in the topic of security, for example through professional work or close friends, shape a person's

mental model of security. Based on the complexity and level of detail of the mental model, threats are identified and assigned priorities. These threats and their mitigation form the basis of security advice and are externally shaped by the available systems and their usability.

In Chapters 7 and 8, use cases for secure technology are explored and researched in relation to perception. From both contexts, payment and 2FA, we learned how security practices are woven into daily lives and what trade-offs are made regarding protection.

Studying security practices in payment across four countries allowed us a glance at how culture shapes security habits. While some habits such as sharing credentials with a partner are shaped intrinsically and influenced by cultural factors such as the value of family bonds, others like handing over the PIN to a cashier are externally pressured, in that case by shopkeepers' general preference for immovable payment terminals.

The study on incentives illustrated how security mechanisms are evaluated as a trade-off. The focus group participants provided very differentiated reasoning behind the decision whether to adopt 2FA for a given category of user account and what kinds of incentives would offset the additional effort for handling a second factor during login. In addition, the influence of badly designed security mechanisms became very clear during the study. Participants had made negative experiences with specific 2FA tokens for banking which made them reluctant about trying out 2FA for other accounts or using other methods as a second factor.

9.2 WHAT FACTORS SHAPE THE PERCEPTION OF SECURITY?

Throughout the studies presented in this thesis, we unconvered a lot of mistrust in security, both on the community level as well as regarding technical premises such as HTTPS.

Some participants in the study about security narratives reported a disillusioned view on the security business and its way of marketing and selling security products and services.

Chapter 5 uncovered some additional areas of mistrust directed at the security of WhatsApp and HTTPS. Although Whatsapp's rollout of end-to-end encryption was well before the time of the interviews, many participants still reported it as an example of an unencrypted messaging app. We could also identify a general mistrust in the perceived security of HTTPS, as the results of the mental model study presented outline. The findings features both over- and underestimations of the security benefits provided by HTTPS, as for example one participant stated that it could protect from phishing attacks. Other participants mistrusted warnings about certificates and misconfigured connections, peaking in one administrator claiming that HTTPS security indicators are "pure marketing" (cf. Section 5.4).

The survey study on security advice also uncovered an interesting case of multi-faceted perception. Password managers were a controversial topic which was rated high in effectiveness as a security measure, but not realistic for users to adopt. The interesting case with password managers is that they contradict a long-standing paradigm of password management: When resorting to writing a password down, it should never happen digitally, as all data on a computer or phone is prone to virtual attacks that can happen unnoticed to the user. The use of password managers therefore presents a paradigm shift in credential management. One expert added a comment in the survey that storing passwords digitally can be compared to writing down passwords on paper and storing said paper securely, while a non-expert commented on the same advice that "storing passwords digitally [...] seems counterproductive" (cf. Section 6.4). While the expert approached the shift with an analogy between the physical and virtual world to reason the advice, the non-expert relied on the previously learned practice that virtual storage is vulnerable to outside attacks and thus should be avoided as a credential store. The important feature of password managers, namely the cryptographically secure storage of data, is neither part of the expert nor the non-expert perception. Based on the findings from Chapter 5 on the complexity of public key infrastructure, it can be assumed that this technical facet is not included in typical mental models about password managers.

The study about payment culture in Chapter 7 shed light on a closely related concept to security, namely *trust*. In their daily lives, our study participants were confronted with a series of decision based on trust when conducting payments. This could be the use of ATMs and the associated risks of a skimmed device or a shoulder surfing passerby, or the need to hand over payment credentials to cashiers as was reported by Iranian participants, or the decision whether to share account credentials with family or intimate partners. Regarding credential sharing, German participants were significantly less likely to share payment credentials with a partner or family in comparison to Chinese, Iranian, and US-American participants. Together with related findings regarding German participants' preference for privacy-preserving payment instruments such as cash and – to an extent – cryptocurrencies, this indicates a different foundation for perceiving trust and security that makes the German population stand out in comparison.

The study on two-factor authentication presented in Chapter 8 also uncovers new aspects about the perception of security and the area of conflict between effectiveness of a security measure and the effort for adopting it. Although the survey participants generally reported to activate 2FA for security reasons and not because of the attached incentive, the services that employed such incentives were more frequently mentioned as being 2FA-enabled. As discussed, this could result either

from an unconscious influence of the nudge posed by the attached incentive, or a side-effect of increased publicity and information about 2FA in general. Accordingly, the focus group participants confirmed the latter possibility by expressing a general desire for more information about what 2FA is and how it protects accounts when being confronted with the possibility to adopt it. Furthermore, an incentive for adopting 2FA was not always seen as positive. Some offers raised the concern that additional purposes might be served when adopting 2FA. The harvesting of phone numbers was the most common of these concerns, where participants feared to also receive advertising when providing their phone number to receive login confirmation SMS. When money or payment information is attached to an account, the additional effort for logging in with 2FA is generally deemed worth it, as money was the key asset that emerged during the focus group interviews. This indicates a strong tie to the perception of security and underlying threat models.

In summary, these individual findings illuminate the research question of this thesis in the following ways:

- Mental models shape the perception of security, and are themselves partially influenced by personal context, socio-cultural situation, education, and profession.
- Mistrust and negative impressions on security stemming from personal experience, education, or news coverage present powerful inhibitors in the perception, adoption, and endorsement of secure technology and practices.
- Users are generally aware of relevant threats and some corresponding security measures, but scarce or misleading mental models can inhibit or skew this assessment.

9.3 IDEAS FOR FUTURE WORK

The need for longitudinal research and more diverse study populations has already been mentioned in the previous section, so these are obvious points of attachment for future work.

Another powerful factor that effects the perception of security is the impact of news and media coverage, especially the effect of bad publicity such as reports of security breaches or wide-reaching security problems. An example case is the coverage of the SSL/TLS ecosystem in relation to the mental models and perception of HTTPS security.

In general, the perception of security is an ongoing topic for research as one thesis such as this one can never answer in its entirety. Any future work on security perception is therefore highly encouraged.

Part III

APPENDIX

A

ADDITIONAL MATERIAL FOR "THE SECURITY NARRATIVE IN THE WORKPLACE CONTEXT"

A.1 CONSENT FORM

Ziel dieses Interviews ist, neue Einsichten und Erkenntnisse über Mitarbeiter*innenzufriedenheit und -unzufriedenheit sowie Beziehungsdynamiken in IT-Sicherheitabteilungen zu erlangen. Es gibt kein "richtig" oder "falsch" in diesem Interview, wir messen keine Leistungen und teilen keine persönlichen Daten von dem, was im Rahmen des Interviews gesagt oder angedeutet wird, an Andere (insb. Vorgesetzte) weiter. Die erhobenen Daten sollen anonymisiert in einer wissenschaftlichen Studie genutzt werden.

Das komplette Interview wird von uns aufgezeichnet (nur Ton, kein Video), Ihre Aussagen werden anschließend von einer studentischen Hilfskraft transkribiert und von uns wissenschaftlich analysiert. Bei der weiteren Verwendung des Interviews werden wir Ihre Aussagen komplett anonymisieren, sodass zu keinem Zeitpunkt ein Rückschluss auf Ihre Identität möglich ist.

Es steht Ihnen jederzeit frei, das Interview zu pausieren oder abzubrechen. Wir möchten nicht, dass Sie sich unwohl fühlen und werden entsprechenden Aufforderungen ohne weitere Nachfrage nachgehen.

Vielen Dank, dass Sie diese Hinweise zur Kenntnis genommen haben. Mit Ihrer Unterschrift bestätigen Sie Ihr Einverständnis mit oben genannten Regelungen.

A.2 INTERVIEW SCRIPT GERMAN

1. Wie lange arbeiten Sie schon in dieser Abteilung?
2. Sind Sie befristet oder unbefristet angestellt?
3. Wie sehen Ihre Aufgaben dort aus?
4. Es gab ja einige Umstrukturierungen, wie haben Sie diese wahrgenommen? Sind Sie zufrieden mit Ihrer aktuellen Arbeitssituation?
5. Vielen Dank. Wir möchten nun mit Ihnen über das Thema IT-Secutity im Allgemeinen sprechen. Woran denken Sie, wenn Sie den Begriff hören?
6. Was verbinden Sie persönlich mit dem Begriff "IT-Security"?
7. Hatte der Begriff für Sie schon immer diese Bedeutung?

8. Wie fasst Ihrer Meinung nach Ihr Arbeitgeber den Begriff "IT-Security" auf?
9. Sehen Sie ein Konfliktpotenzial zwischen diesen Auffassungen?
10. Wenn Sie eine Sache an Ihrer aktuellen Arbeitssituation verbessern könnten, was wäre das?

A.3 INTERVIEW SCRIPT TRANSLATED TO ENGLISH

In this section, the English translation of the German interview script is provided. Please note that the interview was semi-structured, thus the structure might have varied a bit between participants.

1. First, we'd like to know some general information about you. For how long have you been working in this company resp. this department?
2. Are you on a temporary or a permanent contract?
3. What are your tasks here?
4. There have been some restructuring measurements within the company. How did you experience these? Are you content with your labour situation?
5. Thank you. Now, we would like to talk to you about the topic of IT Security in general. What are you thinking of when you hear the term?
6. What do you personally connect to the term IT Security?
7. Did the term always have this meaning to you?
8. How do you think your employer regards the term IT Security?
9. Do you see any potential of conflicts between these two notions?
10. If you could change one thing about your current work situation, what would it be?

B

ADDITIONAL MATERIAL FOR "MENTAL MODELS OF ENCRYPTION"

B.1 SCREENING QUESTIONNAIRE

Demographics

- Age/ Gender/ Profession/ Highest completed level of education/ Recent professional status
- Do you have an IT-security background? If yes, please specify: ...
- Are you a software developer? If yes, since:...
- Are you a system administrator? If yes, since: ...
- Technical Score: I have a good understanding of Computers and the Internet: Likert Scale from 1 (agree) - 7 (disagree)
- I often ask other people for help when I am having problems with my computer: Likert Scale from 1 (agree) - 7 (disagree)
- I am often asked for help when other people have problems with their computer. Likert Scale from 1 (agree) - 7 (disagree)

Technology use

- Which of the following technologies and services below have you used in the past year? (Check all that apply.)
  - Social Networks (Facebook, Twitter, Instagram, LinkedIn, etc)
  - Online Audio and Video Conferencing (Skype, FaceTime, Google Hangout, etc.)
  - Office Software (Word, Excel, PowerPoint, etc.)
  - Mobile Messaging (Signal, Threema, Whatsapp, etc.)
  - Online Banking
  - Online Shopping (Amazon, Zalando, etc.)

Expert-specific questions

- Have you ever written non-browser TLS code? (e.g. for TLS certificate validation?)

- Have you ever configured HTTPS?
- How long have you been working as admin/developer?
- How big is the company that you are working for?
- What is your company's scope?
- Security plays an important role in my everday work. (7-point-Likert, strongly agree - strongly disagree)
- When you are confronted with security-critical decision, do you make them mostly alone or mostly with a team?

B.2 INTERVIEW PROTOCOL

General

- In your daily life, are you aware of any tools, apps or devices where cryptography is used?
- why do you choose to use them?
- Was cryptography part of your education?
- If yes, where did you learn about it? If possible, briefly outline the basic content and topics that you heard of.
- What are your expectations when you visit a site with HTTPS and you see the green lock next to the URL in your browser?
- What is encryption?

B.2.1 *Mental Models*

In the following, I'm going to ask you to explain your perceptions and ideas about how encryption on the Internet works. The purpose of this interview is to understand your views, opinions, and understanding regarding how encryption works with respect to the technology you use in your everyday life. Please keep in mind that there is no correct answer to these questions - please just answer these questions based on your knowledge and experiences. Also, please think aloud and explain your thought process while drawing.

- *Phase 1: encryption in theory.* Please draw a picture of how you think encryption works, when you send an encrypted message to your friend. Remember to include all relevant persons and components into the drawing.

- *Phase 2:* Visiting a site with HTTPS. Imagine you are visiting a website with the HTTPS prefix (e.g. your favorite online shop). Please make a drawing of what makes such a site different to a site with the HTTP prefix.
- *Phase 3: Online Banking.* Imagine you log into your online banking. Usually, those sites are encrypted and you see a green lock next to the URL in your browser. Can you please make a drawing of what happens when you log into your bank account. Focus on what happens between you and your bank's website.

B.2.2 *Attacker Models*

- Why is cryptography used on the Internet?
- What information does cryptography protect?
- Who is the attacker that encryption protects you against? [Images of NSA, person in the same WiFi, Teenage hacker in the basement, Google, Apple, Facebook]
- Please take your drawings (from before). Can you maybe mark where an attacker could eavesdrop?

B.3 POST-HOC VALIDITY STUDY SCRIPT

General

- In your daily life, which security practices do you apply to stay secure online?
- Do you sometimes pay attention to the green lock icon in the browser?
- Have you ever thought about what the green lock next to the URL means?
- What are your security expectations when you visit a site with HTTPS and you see the green lock next to the URL in your browser?

Mental Models

In the following, I'm going to ask you to explain your perceptions and ideas about how security on the Internet works. [...]

- *Phase 1*: Visiting a site with HTTPS.*
- *Phase 2*: Online banking.*
- *Phase 3*: encryption in theory.*

Attacker Models

[See previous section]

B.4 FINAL SET OF CODES FOR GENERAL QUESTIONS AND ATTACKER MODELS

A. tools	**C. expectations on HTTPS**	**E. administration responsibility**	**G. info to protect**
A.1 browser	C.1 e2e encryption	E.1 academic	G.1 data: sensitive/personal/purchase
A.2 app	C.2 server authentication	E.2 service/industry IT	G.2 data: protocol specific
A.3 service: mail/PGP	C.3 safe data storage at provider	E.3 service/industry other	G.3 data: governmental/business
A.4 service: sensitive calls	C.4 information hiding/targeted advertisements	**F. crypto motivation**	G.4 data: in transfer
A.5 privacy enhancing technologies	C.5 security: general	F.1 authenticity communication partner	G.5 data: local
A.6 encryption: local	C.6 protection: data manipulation	F.2 integrity	G.6 data: remote
A.7 encryption: remote	C.7 protection: phishing	F.3 protection: privacy/anonymity	G.7 data: general
A.8 negative: mobile apps have no encryption	C.8 protection: virus	F.4 protection: third party	G.8 data: no protection
A.9 lack of knowledge	C.9 protection: eavesdropper	F.5 protection: malware	G.9 metadata: no protection
A.10 off topic	C.10 mistrust: no eavesdropping protection	F.6 protection: eavesdropper	G.10 lack of knowledge
B. education content	C.11 mistrust: meta data leakage	F.7 protection: sensitive data	G.11 off topic
B.1 work experience	C.12 mistrust: general	F.8 protection: general	**H. successful attacker**
B.2 lecture/academic	C.13 lack of knowledge	F.9 mistrust	H.1 state/police/secret service
B.3 aspect: encryption applied	**D. definition crypto**	F.10 no comment	H.2 hacker
B.4 aspect: cryptography theoretical	D.1 data obfuscation		H.3 big player
B.5 self education: books/videos/internet	D.2 data modification		H.4 insider
B.6 self education: programming	D.3 data tunnel		H.5 provider
B.7 non technical	D.4 en-/decryption keys		H.6 attacker omnipresent
B.8 no education	D.5 symbolic explanation		H.7 no attacker
B.9 cannot remember	D.6 mathematical concept		
	D.7 protection from eavesdroppers		
	D.8 lack of knowledge		

B.5 FINAL SET OF CODES FOR MENTAL MODELS

A. communication path	**F. visualization of encrypted message**	**K. perceived security benefit of HTTPS**	**P. connection between 1 and 2?**
A.1 direct path	F.1 not part of the model	K.1 underestimated	P.1 yes
A.2 additional nodes as system components	F.2 scrambled text/numbers	K.2 overestimated	P.2 no
A.3 additional nodes as relays	F.3 color	K.3 realistic assesment	P.3 unclear
A.4 model too sparse	F.4 physical object (envelope, treasure chest)	K.4 model too sparse	**Q. certificates are introduced in 2**
B. cryptographic concepts	F.5 scribbled line	K.5 no control	Q.1 yes
B.1 end-to-end	F.6 encoded text/digits	**L. communication partner leaks data**	Q.2 implicitely (reference to 2nd drawing)
B.2 symmetric encryption	F.7 lock	L.1 no data leakage	Q.3 no
B.3 assymetric encryption	F.8 different language	L.2 leaks credit card data	Q.4 "stronger" certificates
B.4 ephemeral keys	F.9 chopped text	L.3 undefined data leakage	Q.5 yes, but they are misinterpreted
B.5 transport encryption	**G. provider role**	L.4 general distrust	**R. encryption point in 2**
B.6 blackbox	G.1 not part of the model	L.5 model too sparse	R.1 directly (local machine)
B.7 obfuscation or steganography	G.2 keyserver	**M. third parties**	R.2 crypto proxy
B.8 authentication	G.3 remote encryption component	M.1 centralized encryption service/proxy	R.3 after remote validation at remote service
B.9 model too sparse	G.4 local encryption component	M.2 PKI/CA	R.4 undefined
C. definiton quality	G.5 message release point	M.3 (ad) tracker	R.5 model too sparse
C.1 accurate model	G.6 in-software encryption	M.4 credit card provider/bank	**T. More technical buzzwords**
C.2 model too sparse	G.7 omnipotent observer	M.5 metadata leakage	T.1 yes
C.3 passphrase exchange	**H. confusion of concepts**	M.6 insiders	T.2 no
C.4 authentication	H.1 encryption equals authentication	M.7 successful intruders	T.3 conceptual representation
C.5 message is recognizable	H.2 encryption is a distinct service	M.8 unsuccesful intruders	**U. Distraction from knowledge gaps**
D. key generation and exchange	H.3 encryption is well-defined	M.9 authentication proxy	U.1 yes
D.1 model too sparse	H.4 model too sparse	M.10 model too sparse	U.2 no
D.2 Web of Trust	**I. model refinement (1-2)**	**N. HTTPS specific components**	U.3 knowledge gaps are explicitely admitted
D.3 PSK_keyserver	I.1 increased level of detail	N.1 certificates	**V. Representation**
D.4 PSK_in-person key exchange	I.2 decreased level of detail	N.2 keys	V.1 protocol-based
D.5 shared knowledge	I.3 constant level of detail	N.3 codebook (PKI)	V.2 conceptual
D.6 PSK_Undefined	**J. security indicators**	N.4 not part of the model	V.3 both
E. example scenario	J.1 https	N.5 model too sparse	V.4 model too sparse
E.1 abstract	J.2 lock icon	**O. model refinement (2-3)**	W. **Awareness of metadata**
E.2 arbitrary messaging app	J.3 check mark	O.1 increased level of detail	W.1 yes
E.3 WhatsApp	J.4 insecurity indicator	O.2 decreased level of detail	W.2 no
E.4 Signal	J.5 not part of the model	O.3 constant level of detail	
E.5 PGP/GPG			
E.6 not part of the model			

C

ADDITIONAL MATERIAL FOR "SECURITY ADVICE AND PRACTICES"

C.1 SURVEYS

All multiple-choice questions were single answer only. The questions were identical for the Expert A, Expert B, and Non-expert survey, unless otherwise stated. The questions marked "(Experts A only)", "(Experts B only)" or "(Non-experts only)" were asked in only one of the surveys.

- *(Experts A&B only)* What are the top 3 pieces of advice you would give to a non-tech-savvy user to protect their security online? *(open-ended)*
- What are the 3 most important things you do to protect your security online? *(open-ended)*
- How did you learn about the things you listed above? *(open-ended)*
- Do you use a laptop or desktop computer that you or your family owns (i.e., not provided by school or work)? *(multiple-choice)*
  - Yes
  - No
- When did you get that computer? *(multiple-choice)*
  - Less than 1 year ago
  - At least 1 but less than 2 years ago
  - At least 2 but less than 3 years ago
  - At least 3 but less than 5 years ago
  - 5 or more years ago
  - I don't know
- How soon after you discover that a new version of your operating system (OS) software is available do you (or somebody else managing your computer) install it? *(multiple-choice)*
  - OS updates are installed automatically
  - Immediately
  - Soon after
  - Eventually

  - OS updates are never installed
  - Other *(open-ended)*

- Do you use anti-virus software on that computer? *(multiple-choice)*
  - Yes
  - No
  - I don't know
  - Other *(open-ended)*

- Which anti-virus software do you use? *(open-ended)*

- How do you keep track of your passwords for your online accounts? *(grid question)*
  Answer options: For ALL of my accounts, For MOST of my accounts, For SOME of my accounts, For NONE of my accounts
  - Remember them
  - Write them down on paper
  - Save them in a local file on my computer
  - Have my password manager (e.g., 1Password, LastPass) remember them
  - Use the same password on multiple accounts

- If you use a password manager, which one do you use? *(open-ended)*

- (optional) What other things, if any, do you do to keep track of your passwords? *(open-ended)*

- Do you use two-factor authentication (e.g., 2-Step Verification) for at least one of your online accounts? *(multiple-choice)*
  - Yes
  - No
  - I don't know
  - Other *(open-ended)*

- Do you look at the URL bar to verify that you are visiting the website you intended to? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know

  - Other *(open-ended)*

- Google began in January 1996 as a research project. Its initial public offering took place on August 19, 2004. Did the initial public offering of Google take place in 1996? *(multiple-choice)*
  - Yes
  - No
  - Other *(open-ended)*

- Do you check if the website you're visiting uses HTTPS? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other *(open-ended)*

- Do you visit websites you have not heard of before? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other *(open-ended)*

- When you click on a link in an email and that link takes you to a website that asks for your password, do you enter it? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other *(open-ended)*

  Do you open emails you receive from people or companies you don't know? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely

  - No
  - I don't know
  - Other *(open-ended)*

- Do you click on links that people or companies you don't know send you? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other *(open-ended)*

- *(Experts A only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software

  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies

- *(Non-experts & Experts A only)*(optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how REALISTIC (that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies

- *(Non-experts & Experts B only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts A only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer

  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper

- *(Non-experts & Experts A only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how REALISTIC (that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper
- *(Non-experts & Experts B only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts A only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts
- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know

  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts

- *(Non-experts & Experts A only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how REALISTIC (that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts

- *(Non-experts & Experts B only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you

  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to

  - Don't open email attachments from people or companies you don't know

- *(Non-experts & Experts A only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how REALISTIC (that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know

- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know

- *(Non-experts & Experts B only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- What is your gender? *(multiple-choice)*

  - Female
  - Male
  - Transgender
  - I prefer not to answer
  - Other *(open-ended)*

- What is your age? *(multiple-choice)*
  - 18-24 years old
  - 25-34
  - 35-44
  - 45-54
  - 55-64
  - 65 or older
  - I prefer not to answer

- What is the highest degree or level of school that you have completed? *(multiple-choice)*
  - Professional doctorate (for example, MD, JD, DDS, DVM, LLB)
  - Doctoral degree (for example, PhD, EdD)
  - Masters degree (for example, MS, MBA, MEng, MA, MEd, MSW)
  - Bachelor (for example, BS, BA; also German Berufsausbildung)
  - Associates Degree (or German Abitur)
  - Some college, no degree
  - Technical/Trade school
  - Regular High School Diploma (or German Realschulabschluss)
  - GED or alternative credential
  - Some High School (or German Hauptschulabschluss)
  - I prefer not to answer
  - Other *(open-ended)*

- *(Experts A&B only)* How many total years of experience do you have in computer security?
  'Experience' includes years at work or studying in a security-related field. *(multiple-choice)*
  - At least 1 but less than 5 years
  - At least 5 but less than 10 years

  - At least 10 but less than 15 years
  - 15 years or more
  - None

- *(Experts A&B only)* What is your current job role?
  For example, Network Security Engineer, Penetration Tester *(open-ended)*
  - Researcher
  - Principal Architect
  - IT Strategist
  - CEO
  - Manager
  - Security Engineer
  - Engineer
  - Other *(open-ended)*

- *(Experts A&B only)* Which of the following best characterizes your workplace? *(multiple-choice)*
  - University
  - Corporate research lab
  - Industry
  - Government
  - Self-employed
  - Other *(open-ended)*

- *(Experts A&B only)* In what country do you work? *(multiple-choice)*
  - Australia
  - Canada
  - Germany
  - India
  - United Kingdom
  - United States
  - Other *(open-ended)*

- *(Experts A&B only)* In what state do you work? (open-choice)

- *(Non-experts only)* Which describes your current employment status? *(multiple-choice)*
  - Employed full-time
  - Employed part-time
  - Self-employed

  - Care-provider
  - Homemaker
  - Retired
  - Student - Undergraduate
  - Student - Masters
  - Student - Doctoral
  - Looking for work / Unemployed
  - Other *(open-ended)*

- *(Non-experts only)* What is your occupation? *(open-ended)*
- *(Non-experts only)* What is your Mechanical Turk Worker ID? *(open-ended)*
- *(Experts A&B only)* Do you remember taking a survey with similar questions in the past (ca. 2014)?
  - Yes
  - No
- (Optional) Is there anything else you'd like to add or clarify? *(open-ended)*

D

ADDITIONAL MATERIAL FOR "SECURITY AND PRIVACY PERCEPTION IN PAYMENT AND BANKING"

D.1 INTERVIEW

1. What kind of payment systems do you use?
   - Cash • Debit Cards • Credit Cards • Cheques • Telephone banking/payments • Internet banking/payments • Mobile banking/payments • Cryptocurrencies
2. What types of payment do you use them for? (asked for each item in Q.1)
   - Shopping • Food/Beverages • Rent • Bills • Money transfer • Balance checking • Tickets • etc.
3. For each payment method, please indicate a typical range you spend & the maximum you spend with that method (asked average and max amount for each item in Q.1)
4. How often do you use each payment method per week?
5. Can you tell me why you choose a payment method?
   - My family uses the same method, so do I
   - It's because of my job
   - I've always used it
   - Comfort & ease of use
   - Security & privacy
   - Popularity of the method
6. Can you tell me why you avoid a payment method?
   - Not thought about it • Unknown • Too complex • Too dangerous • Security & privacy • Few people use this payment method
7. What I spend money on can be seen by:
   - None • Service provider company • Ad companies • Governments • Banks • Family • Friends • Hackers • etc.
8. How much do you mind that X can see your transactions? (X refers to items in Q.7)

9. Please rank the following list based on how secure the methods are (from 1 to 7, 1 is the least secure, and 7 is the most secure) (list refers to items in Q.1)
10. Please rank the following list based on how easy to use they are (from 1 to 7, 1 is the least easy to use, and 7 is the most easy to use)
11. Please rank the following list based on how much you trust them (from 1 to 7, 1 is the least you trust, and 7 is the most you trust)
12. Have you had a bad experience with it?
13. How many userIDs and passwords do you have (approx.)?
    - How many unique passwords do you have?
    - Do you have different policies for your bank/finance account vs. other accounts?
14. Do you have different security considerations for your accounts and devices?
    - Email • Social networks (Facebook, Twitter, Instagram, ...) • Bank account • Mobile phone • Laptop/PC
15. Have you ever shared your pins/passwords with someone else? If yes, with whom & why?
    - Email • Social networks • Laptop • Mobile phone • Bank accounts
16. How often do you receive a request to share your personal info, e.g., pins and passwords in payment systems?
    - What is/was your answer for that?
17. Have you ever been a victim of fraud/identity theft? Any kind, social media, ...?
    - Have you lost any amount of money during your lifetime because of fraud? If yes, how did it affect your behavior toward that specific system.
    - Do you have a very close person who was a victim of fraud/identity theft?
18. Where do you get your security/privacy advice from?
    - TV • Internet, googling • Magazines • Work • Friends • Family
19. What security measure do you undertake while using ...?
    - Do you check the URL of the page while you are doing the payment?

- Do you know what is HTTPS/SSL? If yes, do you check it during your payment process?
- Any specific environment you prefer?
- Do you have different cards for different purposes?
- Do you use any kind of VPN or proxy applications (like Tor)?
  - If yes, do you use banking services over VPN/proxy?
  - Smartphone, laptop

20. If you are a user of mobile banking (apps), what kind of apps & services do you use?
    - Give me some names, examples.
    - How did you choose this app to do the payment?
    - Why do you trust to do payments in this app?
    - Do you have any additional financial management/brokerage apps in your phone? If yes, how often do you use them?
21. How did you hear about payment method X?
    - Family • Friends • TV • Ads • Banks • etc.
22. Which wallet do you use for managing your cryptocurrencies?
    - Is it password protected?
    - is it encrypted?
    - is it backed up?
23. If she/he is not a user but knows what cryptocurrencies are: would you start using a cryptocurrency if it was endorsed by the government/ or an organization? Who/what should support this currency to make you use/trust it?
24. What is the typical payment method you choose in online shopping?
    - Cash • Cards (debit, credit) • Online Payments (Paypal, . . .) • Direct debit • Others: ....
25. What are the typical products that you buy online?
    - Electronics • Food • Books • Apparels • etc.
26. Do you buy products, services, ... from international companies, websites? How do you handle the payment?
27. Do you have any relatives, friends abroad?
28. Do you have any financial transaction with them?

- If yes, how often?
- Approximate amount?

29. How do you usually send & receive money? Which one do you think is better?
    - Did you have a bad experience with this process?
30. What do you think about security and privacy protocols in banks?
31. Do you think banks are sharing your data with someone else? If yes, who?
32. What is your gender?
33. How old are you?
34. What is your highest level of education?
35. What is your profession?
36. Do you have any work experience or degree in IT/computer related fields?
37. How many hours per day do you spend on internet?
38. How do you define a secure and private payment system?

D.2 ONLINE SURVEY

For our research on computer interfaces, we would like to ask you a few questions about your use of bank accounts. Please read all instructions carefully. We will be checking all of your answers for consistency, and may reject your task if you provide inconsistent answers. This project is conducted by researchers at the Computer Science Institute, UNI REDACTED. Your responses are confidential and you can withdraw at any time. Any questions? Contact us here.

1. I have read and understood the information about the study, as provided above and consent to take part.
    - I consent • I do not consent
2. What kind of payment systems do you use?
    - Cash • Debit cards • Credit cards • Cheques • Telephone banking/payments (e.g. Hotline, SMS) • Internet banking/-payments (e.g. Paypal, Online Banking) • Mobile banking/-payments (on your smartphone) • Cryptocurrencies (e.g. Bitcoin, Litecoin)
3. How often you use each payment method?

- Daily • Weekly • Monthly • Less than once a month • Never

4. What types of payment do you use for the following expenses?
   - Online Shopping • In-store Shopping • Food/Beverages • Tickets • Rent • Bills • Money transfer • Balance checking
5. Why do you use the following payment types?
   - Convenience • I have control over what I buy • I can track what I spent money on • Ease of use • I trust it • Security • Privacy • Low cost • My family/friends use it
6. Please rate how much you agree with the following statements. (Likert scale 1-7)
   - I like shopping online because of discounts.
   - I like shopping online because of the diversity of available products.
   - I like shopping in-store because I can touch the product.
   - I like shopping in-store because I can bargain.
7. Please rate how much you agree with the following statements. (Likert scale 1-7)
   - I trust international websites more than local, national websites.
   - I am more willing to use international banks and payment services, rather than local, national banks and payment services.
   - I prefer to use internationally accepted payment methods, even when I'm not abroad.
8. Please rate how much you agree with the following statements. (Likert scale 1-7)
   - I like to use cashless payment methods because I do not like to handle change.
   - I'm eager to try out new payment methods.
   - Having an overview of my payments is important to me.
   - I do not use card payment in stores I don't know.
   - I feel in control when using mobile/internet banking.
   - I don't trust online shops to keep my financial information secure.
   - Please answer "Very much" on this question to confirm that you read carefully.
   - It is important to me that I know how my personal information will be used.

- I think my transactions are private and secure.
- I check for security indicators before entering my data on banking websites (e.g. "https://", a lock icon).

9. Please rate how much you agree with the following statements. (Likert scale 1-7)
   - I think bad things on the internet happen only to famous people and companies.
   - I'm not an interesting subject for hackers.
   - I don't do anything interesting, so I don't care who can see my transactions.
   - No matter how much banks secure their systems, hackers can hack them if they want to.
   - I believe my financial data has been leaked at least once.
10. Please rate how much you agree with the following statements. (Likert scale 1-7)
    - I do not change my bank passwords (PINs and passwords), unless I have to.
    - I use a PIN, passcode or pattern to unlock my mobile phone.
    - I use a password/passcode to lock my laptop or tablet.
    - I am very cautious of my surroundings while conducting payment transactions.
11. Where do you get your security/privacy advice?
    - TV/Radio • Online media, Internet, Googling • Print magazines/Newspapers • Work • Friends • Family • Social networks (Facebook, Twitter, Instagram, ...) • Messaging apps (Telegram, WhatsApp, Viber, ...) • Outdoor ads, billboards, posters, ... • None of above • Other (please specify)
12. How much does the advice from the following sources influence your choice of payment method? (Likert scale 1-7)
    - TV/Radio • Online media, Internet, Googling • Print magazines/Newspapers • Work • Friends • Family • Social networks (Facebook, Twitter, Instagram, ...) • Messaging apps (Telegram, WhatsApp, Viber, ...) • Outdoor ads, billboards, posters, ...
13. Have you had a bad experience with
    - I never had a bad experience in payment • Cash • Debit cards • Credit cards • Cheques • Telephone banking/payments (e.g. Hotline, SMS) • Internet banking/payments (e.g. Paypal, Online Banking) • Mobile banking/payments (on your smartphone) • Cryptocurrencies (e.g. Bitcoin, Litecoin)

14. How did the bad experience change your behaviour? (Please only answer this if you had a bad experience with a payment method)
    - I decreased my use of that instrument
    - I stopped using it for a while
    - It did not have an influence on me
    - I kept using it, but I was stressed
15. Who do you think can see your financial transactions?
    - My Government • My bank • Advertising companies • The company that I'm transacting with • No one
16. Who has the right to see your financial transactions?
    - My Government • My bank • Advertising companies • The company that I'm transacting with • No one
17. I'm comfortable with the following people knowing about my... (matrix, rows and columns)
    - my parents • my siblings • my spouse (or significant other) • my friends • my secretary • my flatmates
    - Bank card details • Bank transactions • Shopping details in online shops • Emails • Social network activities • Cell-phone activities
18. Sometimes I must pay with a certain payment instrument, even though I do not have it. In that case:
    - I use a friend's payment account
    - I search for a different shop
    - I acquire that instrument
    - Other (please specify)
19. At least once I have shared my bank credentials with someone, because:
    - I needed to accomplish a task
    - Someone asked me
    - We trust each other, so we share our credentials
    - I was forced to do it
    - I never shared my bank credentials
20. After I have shared my credential with someone,
    - I did not change it after sharing
    - Changed it after sharing
    - Planned to change it, but didn't change it in the end

- I never shared my bank credential

21. If you have more than one payment card which requires a PIN, do you use the same PIN for several cards?
    - Yes • No • I don't own more than one card
22. When choosing your bank/payment PIN, what did you have in mind?
    - My PIN represents a date and/or year.
    - My PIN represents a pattern on the keypad when I enter it.
    - My PIN is some other number which I chose.
    - I didn't choose my own PIN.
23. What devices do you use for banking?
    - Smartphone • Tablet • Laptop • PC
24. I use ... for online banking.
    - My own device • A shared device • A public device
25. I do my financial transactions in:
    - Public spaces (e.g. Events, Airport, Public transport) • Semi-Public Spaces (e.g. Gym, Work, School, Restaurant) • Banks • Private spaces (e.g. Home, Car)
26. How familiar are you with cryptocurrencies such as Bitcoin?
    - Not at all • I have heard about them • I have used a cryptocurrency before • I frequently use cryptocurrencies
27. If ... would endorse cryptocurrencies, I would use them (more often)
    - Friends • Family • Co-workers • The internet, online resource • A Tech company like Google, Facebook, Amazon • Print magazines/newspapers • My government • Radio/TV • Celebrities • None of the above would change my behaviour
28. What are your main reasons for using cryptocurrencies?
    - The opportunity of financial gain
    - Curiosity
    - Their anonymous nature
    - Their decentralized nature
    - A friend/colleague suggested to me to start using them
    - The possibility to internationally transfer money with relatively low fee

- The possibility to accept cryptocurrencies for my services or for my products
- I do not use cryptocurrencies

29. What services or products you pay for with cryptocurrencies?
    - Bars • Restaurants • Bitcoin gift cards • Donations • Tipping • Drugs • Gambling sites • Travel • Online marketplaces and auctions • Online shopping (Newegg, ...) • Altcoin (e.g. Litecoin, ...) • Physical stores that accept bitcoins • Underground marketplaces • Virtual goods (webhosting, online newspapers, ...) • Medium for currency exchange • I do not use cryptocurrencies
30. Please rate how much you agree with the following statements. (Likert scale 1-7)
    - I use cryptocurrencies on a regular basis.
    - My experience with cryptocurrencies has been positive.
    - Please answer "Not at all" on this question to confirm that you read carefully.
    - I would like to know more about cryptocurrencies.
31. How secure do you regard each method when it comes to verifying your identity for a financial transaction? (Likert scale 1-7)
    - PINs • Passwords • Two-Factor authentication (e.g. TAN, mobile Authenticator) • Signature • Fingerprints • Iris scans • Cryptographic signatures
32. How reliable do you think the following payment systems are? (Likert scale 1-7)
33. How much do you trust the following payment systems? (Likert scale 1-7)
34. How secure do you think the following payment systems are? (Likert scale 1-7)
35. How easy to use do you think the following payment systems are? (Likert scale 1-7)
36. How useful do you think the following payment systems are? (Likert scale 1-7)
37. How often you use following tools? (matrix, rows and columns)
    - VPN • Proxy
    - At least daily • At least once in a week • At least once in a month • Less than once in a month • Never

38. Do you do your financial transactions over VPN or a proxy software/app?
    - Yes • No • I don't use proxies & VPNs
39. If you use a VPN or proxy, do you know its provider?
    - Yes • No
40. Which one do you think is safe?
    - VPN • Proxy • WiFi • None • Don't know
41. Please rate how much you agree with the following statements. (Likert scale 1-7)
    - My internet connection is fast.
    - My internet connection is reliable.
42. Approximately how many hours do you spend on the Internet each day? (0-24 hours scale)
43. Overall, how many unique internet passwords do you have? (0-20 scale)
44. What is your age?
45. What is your gender?
46. Please select your highest completed level of education:
    - Did Not Complete High School • High School • Associate degree (2 years)/College • Bachelor's Degree • Master's Degree • Advanced Graduate work or Ph.D.
47. Do you work or study in a computer science related field?
    - Yes • No
48. Please select your employment status.
    - Employed full-time • Employed part-time • Retired • Not employed for pay • Self-employed • Student • Other
49. What is your approximate average household income?
    - $0-$24,999 • $25,000-$49,999 • $50,000-$74,999 • $75,000-$99,999 • $100,000-$124,999 • $125,000-$149,999 • $150,000-$174,999 • $175,000-$199,999 • $200,000 and up
50. Please enter your Worker ID here, so we can reward you for taking this survey.
51. If you have any comments or feedback you would like to share with us, please enter it in the box below.

E

ADDITIONAL MATERIAL FOR "INCENTIVIZING SECURITY"

E.1 GAMING SURVEY

Here we present the questionnaire for the first survey that was distributed in online gaming communities. This survey was designed and conducted as part of a student project.

The usage of services in the internet is rising. Historically the user accounts of such services are secured by using a password. To increase the security, two factor authentication (2FA) is used. When 2FA is used, the user needs another information to login. As an example, this could be a code provided via a mobile app or a SMS sent to a specified phone number. In many online games or game services it is feature-wise beneficial for the user to activate 2FA. The goal of this survey is to gather statistical data how the incentives or restrictions have influenced the 2FA adoption rate within the user base. This survey should only take you a few minutes. Thanks in advance for participating!

1. DEMOGRAPHICS Please fill in your age, gender and your current country of residence. *free text entry*

2. WHICH SERVICES DO YOU USE?

- Blizzard Battle.net
- Discord
- Facebook
- GOG.com
- Guild Wars 2
- Nintendo Account
- Origin
- Playstation Network
- Reddit
- Slack
- Steam

- Telegram
- Twitter
- Wargaming
- WhatsApp
- XBox Live
- I don't use any services on this list

3. FOR WHICH SERVICES DO YOU HAVE 2FA ACTIVATED? Please mark the services you are actively using 2FA for.

- Blizzard Battle.net
- Discord
- Facebook
- GOG.com
- Guild Wars 2
- Nintendo Account
- Origin
- Playstation Network
- Reddit
- Slack
- Steam
- Telegram
- Twitter
- Wargaming
- WhatsApp
- XBox Live
- Other (free text entry)
- I do not have 2FA activated

4. WHICH METHODS OF 2FA DO YOU USE?

- SMS
- Email
- Google Authenticator
- Specific app solution, e.g. Blizzard Authenticator
- Hardware-Token
- Other
- I don't use any 2FA methods

5. HOW WOULD YOU RATE THE FOLLOWING METHODS OF 2FA REGARDING THEIR CONVENIENCE? (7-point Likert scale from *not convenient* to *very conventient* with *don't know* option)

- SMS
- Email
- Google Authenticator
- Specific app solutions, e.g. Blizzard Authenticator
- Hardware-Token

6. HOW WOULD YOU RATE THE FOLLOWING METHODS OF 2FA REGARDING THEIR SECURITY? (7-point Likert scale from *not secure* to *very secure* with *don't know* option)

- SMS
- Email
- Google Authenticator
- Specific app solutions, e.g. Blizzard Authenticator
- Hardware-Token

7. WHY DID YOU ACTIVATE 2FA? Please mark your primary reasons why you have activated 2FA.

- Account security
- High monetary value is attached to the account
- Gameplay advantage, e.g. an exclusive in-game shop
- Visual bonus, e.g. an exclusive in-game pet

- To circumvent a restriction, e.g. Steams Community Market Trading hold
- Other (free text entry)
- I do not have 2FA activated

8. IF AN INCENTIVE CONVINCED YOU TO ACTIVATE 2FA, ... how easy was the activation of 2FA? (7-point Likert scale from *very hard* to *very easy* with *I wasn't convinced* option)

9. IF AN INCENTIVE CONVINCED YOU TO ACTIVATE 2FA, ... how convenient is the usage of 2FA? (7-point Likert scale from *not convenient* to *very convenient* with *I wasn't convinced* option)

10. HOW LIKELY IS IT THAT YOU WOULD ACTIVATE 2FA IN THE FOLLOWING SCENARIOS? (7-point Likert scale from *not likely* to *very likely*)

- You would lose a previously available feature for not activating 2FA (e.g. When Steams Community Market Trading hold was introduced)
- You could gain a gameplay advantage for using 2FA (e.g. additional inventory slots, exclusive shop)
- You could gain an exclusive visual modification for using 2FA (e.g. companion, special skin)

11. WHAT IS THE PROBABILITY OF YOU DEACTIVATING 2FA, IF YOU COULD KEEP THE GAINED BENEFIT(S)? (7-point Likert scale from *not likely* to *very likely*) Probability of you deactivating 2FA

12. WHY WOULD YOU DEACTIVATE 2FA? Please mark all applicable answers

- I don't like the additional steps required to login
- I don't care about the additional security layer
- I think the account is safe enough without 2FA
- Other (free text entry)
- I would not deactivate it

E.1.1 *General Population Survey*

Here we present the questionnaire for the second survey that was distributed on Amazon MTurk. This survey was designed and conducted as part of a Master's thesis.

This survey will ask you questions about your online behavior and different security mechanisms as part of a research project at University of Bonn. The results will be used to research and improve existing security mechanisms. Please read the questions carefully and answer honestly. We estimate this will take you 10-15 minutes.
By completing this survey you consent to the collection and evaluation of your answers. This will only be shared as part of our project and only with researchers of University of Bonn. The published results will be anonymized. Leaving the survey without finishing it equals withdrawing your consent, although you can return to finish it as long as the project is not completed.
If you have any questions or feedback regarding this survey please feel free to contact Sabrina Amft, Karoline Busse or Emanuel von Zezschwitz.
Thank you for participating!

1. AGE Please fill in your age. *natural number entry*

2. DEMOGRAPHICS Please fill in your gender and your current country of residence. *free text entry*

3. WHAT DO UNDERSTAND UNDER THE TERM 'VALVE'?

- A metal piece used to block or release a pipe
- The company behind a well-known game shop and different video games
- A TV Show about metal works
- A brand for summer clothing
- None of the above

4. DO YOU ENJOY PLAYING VIDEO GAMES? *single selection*

- Yes
- No

5. WHICH KINDS OF ONLINE SERVICES DO YOU MAKE USE OF?

- Online-Banking
- Backups and Clouds (e.g. Dropbox, Google Drive)
- E-Mail (e.g. Gmail)
- Social Media (e.g. Facebook, Twitter)
- Messaging (e.g. Skype, Whatsapp)

- Games (e.g. Battle.net)
- Retail (e.g. Amazon, eBay)
- Productivity (e.g. Google Docs)
- Hosting-Services (e.g. Amazon Web Services)
- Other (please specify)

6. PLEASE MARK THE SERVICES YOU ACTIVELY USE.

- Amazon
- Blizzard Battle.net
- Discord
- Dropbox
- eBay
- Facebook
- Google Drive
- Google Mail
- Instagram
- Kickstarter
- LinkedIn
- Nintendo Account
- OneDrive
- Online-Banking
- Origin
- Patreon
- Paypal
- Playstation Network
- Reddit
- Signal
- Skype
- Steam
- Telegram

- Twitch
- Twitter
- WhatsApp
- XBox Live
- Yahoo Mail
- Youtube
- I don't use any services on this list
- Other (please specify)

TWO-FACTOR AUTHENTICATION (2FA) is a security mechanism that requires a second piece of information (a second factor) if someone tries to log into an account. This is used to increase confidence that the person requesting access is really you. Such information is often a single-use code that is communicated via e.g. SMS, e-mail or apps such as Google Authenticator.

7. DO YOU USE TWO-FACTOR AUTHENTICATION FOR ANY OF YOUR ONLINE ACCOUNTS? *single selection, participants who answered with No were forwarded to question 15.*

- Yes
- No
- I don't know

8. DO YOU USE TWO FACTOR AUTHENTICATION (2FA) FOR THE FOLLOWING?

- Online-Banking
- Backups and Clouds (e.g. Dropbox, Google Drive)
- E-Mail (e.g. Gmail)
- Social Media (e.g. Facebook, Twitter)
- Messaging (e.g. Skype, Whatsapp)
- Games (e.g. Battle.net)
- Retail (e.g. Amazon, eBay)
- Productivity (e.g. Google Docs)
- Hosting-Services (e.g. Amazon Web Services)
- Other (free text answers from question 5)
- Other (please specify)

9. PLEASE MARK THE SERVICES YOU ARE ACTIVELY USING 2FA FOR *Answers are carried over from question 6.*

- Amazon
- Blizzard Battle.net
- Discord
- Dropbox
- eBay
- Facebook
- Google Drive
- Google Mail
- Instagram
- Kickstarter
- LinkedIn
- Nintendo Account
- OneDrive
- Online-Banking
- Origin
- Patreon
- Paypal
- Playstation Network
- Reddit
- Signal
- Skype
- Steam
- Telegram
- Twitch
- Twitter
- WhatsApp
- XBox Live

- Yahoo Mail
- Youtube
- I don't use any services on this list
- Other (free text answers from question 6)
- Other (please specify)

10. HOW OFTEN DO YOU USE THE FOLLOWING 2FA METHODS? (5-point Likert scale with the options *Daily*, *Weekly*, *Monthly*, *Sometimes*, *I don't use any 2FA mechanisms*)

- SMS
- E-Mail
- Google Authenticator
- Specific app solutions, e.g. Blizzard Authenticator
- Hardware token e.g. a SmartCard or Yubikey

11. HOW WOULD YOU RATE THE FOLLOWING METHODS OF 2FA REGARDING THEIR CONVENIENCE? (5-point Likert scale from *very convenient* to *not convenient* with *I don't know* option)

- SMS
- E-Mail
- Google Authenticator
- Specific app solutions, e.g. Blizzard Authenticator
- Hardware token e.g. a SmartCard or Yubikey

12. IF YOU PERCEIVED THE CONVENIENCE OF ONE OR MORE METHODS TO BE LOW, PLEASE TELL US WHY. *free text entry*

13. HOW WOULD YOU RATE THE FOLLOWING METHODS OF 2FA REGARDING THEIR SECURITY? (5-point Likert scale from *very secure* to *not secure* with *I don't know* option)

- SMS
- E-Mail
- Google Authenticator
- Specific app solutions, e.g. Blizzard Authenticator
- Hardware token e.g. a SmartCard or Yubikey

14. IF YOU PERCEIVED THE SECURITY OF ONE OR MORE METHODS TO BE LOW, PLEASE TELL US WHY. *free text entry*

15. WHAT IS THE PRIMARY REASON WHY YOU WOULD ACTIVATE 2FA? *single selection*

- Account security
- High monetary value is attached to the account
- Functional advantage, e.g. new or enhanced features
- Visual bonus, e.g. a sticker set or an exclusive in-game pet
- To circumvent a restriction
- I don't use 2FA
- Other (please specify)

16. IF AN INCENTIVE CONVINCED YOU TO ACTIVATE 2FA, ... how easy was the activation of 2FA? (5-point Likert scale from *very* to *not at all* with *I don't know* option)

... how convenient is the usage of 2FA? (5-point Likert scale from *very* to *not at all* with *I don't know* option)

17. HOW LIKELY IS IT THAT YOU WOULD ACTIVATE 2FA IN THE FOLLOWING SCENARIOS? (5-point Likert scale from *very likely* to *not likely* with *I don't know* option)*first part of the question, item order was randomized*

- You could gain a functional advantage for using 2FA (e.g. new features, exclusive shop)
- You are offered a sticker set for your favorite social media/messenger
- Posts including media (e.g. pictures) are kept on hold until reviewed by a moderator if 2FA is not activated
- You receive a small physical gift as a thank-you (e.g. keychain of your choice)
- You would lose a previously available feature (e.g. posting status updates, exclusive sales)
- You could gain a gameplay advantage for video games such as World of Warcraft (e.g. additional inventory slots, exclusive shop)

18. HOW LIKELY IS IT THAT YOU WOULD ACTIVATE 2FA IN THE FOLLOWING SCENARIOS? (5-point Likert scale from *very likely* to *not likely* with *I don't know* option) *second part of the question, item order was randomized*

- Please choose "very likely" for this question to let us know you're still paying attention.
- You could gain an exclusive visual modification for using 2FA (e.g. a pet or costume for video game characters)
- You are offered a special offer (e.g. small permanent discount)
- It is not possible to access or interact with certain profiles if you do not activate 2FA
- You receive a one time bonus payment for using 2FA.

19. WHAT IS THE PROBABILITY OF YOU DEACTIVATING 2FA, IF YOU COULD KEEP THE GAINED BENEFIT(S) FROM ACTIVATING IT? (5-point Likert scale from *very high* to *very low*)

20. WHAT IS THE PROBABILITY OF YOU KEEPING 2FA ACTIVE IF OTHERWISE YOU WOULD LOOSE THE GAINED BENEFIT(S) FROM ACTIVATING IT? (5-point Likert scale from *very high* to *very low*)

21. WHY WOULD YOU DEACTIVATE 2FA?

- I don't like the additional steps required to login
- I don't think that 2FA will help increase the security of my account
- I don't need additional security mechanisms
- I would not deactivate it
- It's not working properly for me (e.g. delays with code delivery)
- Other (please specify)

22. DO YOU HAVE ANY FURTHER REMARKS ABOUT THIS STUDY OR ITS TOPIC? *free text entry*

23. PLEASE ENTER THE FOLLOWING CODE IN AMAZON MTURK TO HELP US VERIFY THAT YOU COMPLETED THE SURVEY *a code was shown* Yes, I copied the code to MTurk.

Thank you for completing this survey! Your answers were transmitted, you may close the browser window or tab now.

F

DOCUMENTATION OF AUTHORSHIP

The majority of this thesis was made through collaborative work with other researchers. In the following, collaboration statements and documentation for all publications are presented for the sake of transparency.

F.1 EXPLORING THE SECURITY NARRATIVE IN THE WORK CONTEXT

The study presented in Chapter 4 was collaborative work between Jennifer Seifert (JS), Matthew Smith (MS), and myself (KB) [40]. The individual contributions on the paper are listed in Table F.1.

F.2 MENTAL MODELS OF ENCRYPTION

The work on mental models of encryption presented in Chapter 5 is based on a study conducted by Katharina Krombholz (KK), Katharina Pfeffer (KP), Matthew Smith (MS), Emanuel von Zezschwitz (EZ), and myself (KB) [131]. The individual contributions on the paper are listed in Table F.2.

F.3 SECURITY ADVICE AND PRACTICES

The study presented in Chapter 6 is based on a publication by Julia Schäfer (JS), Matthew Smith (MS), and myself (KB) [39]. The individual contributions are listed in Table F.3

F.4 SECURITY AND PRIVACY PERCEPTIONS IN PAYMENT AND BANKING

The work presented in Chapter 7 is based on joint research between Mohammad Tahaei (MT), Katharina Krombholz (KK), Emanuel von Zezschwitz (EZ), Mathew Smith (MS), Jing Tian (JT), Wenyuan Xu (WX), and myself (KB) [41]. The individual contributions are listed in Table F.4.

F.5 INCENTIVIZING SECURITY

The study presented in Chapter 8 is based on a publication by Sabrina Amft (SA), Daniel Hecker (DH), Emanuel von Zezschwitz (EZ), and

Task	Contributors
Conception	JS and KB developed the concept together
Concept Discussion	Consulting with Jens Bergmann regarding the underlying theoretical framework
Related Work	Jens Bergmann provided the theoretical work by Croizer and Friedberg, KB researched the rest of the related work.
Study Design	KB drafted the interviews, JS reviewed and revised it
Study Execution	KB conducted the interviews
Study Helpers	Transcription for the Consulting Company interviews was done by Saskia Gehrke, a student assistant. KB transcribed the other interviews.
Data Analysis	KB conducted the analysis
Writing	KB wrote the paper
Proofreading and Feedback	JS provided feedback for the whole paper, especially for the theoretical foundation. MS also reviewed the finished paper.
Revisions	KB implemented all revisions
Support	MS provided funding for interview participant compensation, student work for transcription, and a professional proof-reading service.
Initial Idea	KB confronted JS with the initial idea, they developed it further together

Table F.1: Individual contributions for Chapter 4.

Task	Contributors
Conception	KK lead the conception of the study
Related Work	KK, KP, KB conducted an extensive research for related work.
Study Design	KK designed the study, EZ took part in the study design.
Study Execution	KK and EZ conducted the pre-study. KB conducted five interviews for the main study and recruited another three participants which EZ interviewed. KK and KP conducted the rest of the interviews. For the validity study, KK adjusted the guideline, KB, KK, and KP conducted the interviews.
Data Analysis	KK, KB, and EZ constructed the codebook. KK and KB coded the attacker models. KK, KB, and KP coded the mental models. KP and EZ constructed the codebook for the general questions and coded the general questions. KK, KB, KP, EZ refined the codebook and conducted the final coding. KB calculated Krippendorff Alpha value. KP counted the codes. KK conducted the Fisher's exact test. KB analyzed the data from the questionnaire. MS advised the construction of the meta models. KK, KB, and EZ constructed the meta models. KP constructed the structure-behaviour-function model.
Writing	KK wrote the majority of the paper. KK constructed the mental model graphics, the demographics table, and the code table. KB and KP constructed the bar charts. KB collected the expectations and wrote the section on expectations on user mental models. KB wrote the section on Attacker Models. KP wrote the section on Structure-Behavior-Function. KB und KP constructed the codebook tables.
Revisions	All authors contributed to the revision. KB organized the proof-reading and integrated the results.
Support	MS funded the proof-reading service. KK and MS organized the funding of the study.
Initial Idea	KK designed the concept of the study and led the work on the project.

Table F.2: Individual contributions for Chapter 5.

Task	Contributors
Conception	JS and MS screened candidates for replication, all authors decided together for No One Can Hack My Mind
Related Work	JS with support from KB
Study Design	A/B testing idea from MS, discussion with KB, implementation by JS
Study Execution	KB conducted pre-study interviews, JS created the surveys, KB conducted the studies on Mturk. Expert recruitment through JS (reddit) and KB (Twitter, email).
Data Analysis	Conducted by KB after preparation by JS
Statistics	Conducted by KB after preparation by JS
Writing	Draft by JS (her Master's thesis), writing by KB, feedback from MS
Proofreading and Feedback	Maximilian Häring, Emanuel von Zezschwitz, and Christian Tiefenau
Support	MS provided funding
Initial Idea	Rob Reeder, Iulia Ion, Sunny Consolvo

Table F.3: Individual contributions for Chapter 6.

Task	Contributors
Conception	MT had the first idea, MS assigned KB and KB and MT fleshed it out into a full research design
Concept Discussion	KB and MT with support from MS
Related Work	MT contributed related work from his thesis, KB, KK and MT added additional works
Interview Study Design	MT designed it as part of his thesis, KB supervised
Interview Study Execution	MT (Teheran), KB (Bonn)
Interview Study Evaluation	MT evaluated as part of his thesis, KB supervised and gave feedback
Survey Study Design	KB and MT designed the survey together based on MT's first draft from his thesis
Survey Implementation	MT for English and Farsi, KB for German, JT and WX for Chinese
Survey Execution	KB for German and English versions (crowdworking), JT and WX for Chinese version (crowdworking), MT for Farsi version (classified ads, flyers, coffee house recruiting)
Data Analysis	KB with some help from MT
Statistics	KB
Writing:	
Abstract, Intro, Conclusion	KB and KK with some help from MT
Related Work	KB and MT with help from EZ
Methodology, Countries	KB with help from MT and JT
Interview Study	MT with help from KB
Online Survey	KB with help form MT
Discussion	KB with help from MT, EZ (esp. CHI version) and KK
Proofreading and Feedback	MS and EZ
Revisions	KB and KK with some help from MT
Support	MS provided funding, WX paid for Chinese survey
Initial Idea	MT, KB, and MS

Table F.4: Individual contributions for Chapter 7.

myself (KB) [38]. This individual contributions on the paper are listed in Table F.5.

Task	Contributors
Conception	General idea came from KB, further developed together with DH, then with SA and EZ
Concept Discussion	Some input from Matthew Smith and Blase Ur
Related Work	SA with some help from KB
Gamer Study	Designed, conducted, and evaluated by DH under supervision by KB
General Survey Design	SA designed study based on DH's prior work, input/help from KB and EZ
General Survey Execution, Evaluation	SA
Focus Group Design and Execution	SA with input from KB and EZ
Study Helpers	KB and EZ helped with note taking
Focus Group Evaluation	SA
Writing:	
Abstract, Conclusion	KB
Introduction	SA and KB
Related Work	Main contribution by SA with help from KB
Design, Evaluation	Originally by SA, modified and adapted by KB
Discussion	KB
Proofreading and Feedback	EZ
Revisions	KB
Support	Matthew Smith provided funding
Initial Idea	KB

Table F.5: Individual contributions for Chapter 8.

G

THESIS SUMMARY

This thesis presents novel research and insight on the topic of how people perceive security and privacy. It employs both quantitative and qualitative methods from the field of usable security and privacy research, such as descriptively and inferentially evaluated survey studies, or interview and mental model studies that are evaluated using systemic associative induction and deduction. The five studies presented in this thesis have been published independently at different scientific venues and stand for themselves, but also form the body upon which the research question is investigated.

Through an interview study with ten participants, the influence on converging or aligning narratives on the term of "IT security" is researched among two teams of information security professionals at different companies. The results procured though qualitative content analysis show that in one of the companies, conscious shaping and not shaping of a common narrative provides a management tool for the company head to foster mutual education and discussion around the topic of IT security. In the other company, a common narrative unites the information security workers against the company's IT department in a conflict centered on infrastructure control and company security.

Another interview study investigated expert and non-expert mental models of encryption in three scenarios: end-to-end encrypted messaging, online shopping, and online banking. The replies and drawings of non-expert participants and administrators were evaluated qualitatively to extract correct and incorrect depictions of encryption procedures. The models and anti-models clearly showed that some details such as exchange and management of public and private keys were only mentioned by expert participants. Furthermore, administrators tended to cover their knowledge gaps up with jargon and often structured their drawings along educational formats such as protocol charts. The findings explain - to a degree - why people struggle to use online encryption and why services are sometimes misconfigured by administrators.

A second study among security experts and non-experts investigated security practices and advice through a quantitative survey study. This work is a replication effort of a 2015 paper by Ion, Consolvo, and Reeder. Expert and non-expert participants were asked about personal security practices, personal advice and rating of pre-formulated pieces of advice. Through an improvement in survey design, a number of areas in which the advice is rated as very effective, but not realistic to follow were identified as fields of action for research and design.

Those areas centered around password management, application updates, and being careful with links and attachments.

The perception of security and privacy in payment and banking was investigated in a cross-cultural survey study with participants from China, Germany, Iran, and the United States. Habits and attitudes such as the use of different payment instruments or banking credential sharing behavior was investigated. The main study insights were that Germans least likely share payment credentials, that well-tailored mobile payment instruments might have a great influence on adoption, and that German participants show the greatest interest in cryptocurrencies, presumably because of the high value of privacy that is reflected in the country's laws and payment usage habits.

The last study researched how security and privacy are perceived as opposed to ease of use when considering to activate two-factor authentication (2FA) for online accounts. Specifically, the use of small incentives for activating 2FA was investigated. For online gaming accounts, a small incentive such as a player emote or a cosmetic item are often offered to advertise 2FA. Through two survey studies, user sentiments toward this mechanic and a potential design space for non-gaming incentives are explored. In a subsequent focus group study, three design ideas for such incentives outside of gaming services were discussed along general sentiments towards 2FA. The results show that monetary incentives such as a small discount work best for increasing attractiveness of 2FA, along with good educational material on the security benefits. Additionally, having the choice from different second factors was also perceived as beneficial.

With respect to the thesis's research question on how security and privacy are perceived in selected contexts, the studies show that there is a lot of mistrust in security, both on the community level and regarding technical aspects. To further research this issue, the influence of opinion shapers such as media outlets should be investigated further.

BIBLIOGRAPHY

[1] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. "Exploring User Mental Models of End-to-End Encrypted Communication Tools." In: *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*. 2018.

[2] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. "Obstacles to the Adoption of Secure Communication Tools." In: *Security and Privacy (SP), 2017 IEEE Symposium on (SP'17). IEEE Computer Society*. 2017.

[3] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. "The web never forgets: Persistent tracking mechanisms in the wild." In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2014, pp. 674–689.

[4] Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim, Michelle L Mazurek, and Christian Stransky. "Comparing the Usability of Cryptographic APIs." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2017.

[5] Mustafa Emre Acer, Emily Stark, Adrienne Porter Felt, Sascha Fahl, Radhika Bhargava, Bhanu Dev, Matt Braithwaite, Ryan Sleevi, and Parisa Tabriz. "Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors." In: *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017.

[6] Anne Adams and Martina Angela Sasse. "Users are not the enemy." In: *Communications of the ACM* 42.12 (1999), pp. 41–46.

[7] Anne Adams, Martina Angela Sasse, and Peter Lunt. "Making passwords secure and usable." In: *People and Computers XII*. Springer, 1997, pp. 1–19.

[8] Maarten Aertsen, Maciej Korczyński, Giovane Moura, Samaneh Tajalizadehkhoob, and Jan van den Berg. "No domain left behind: is Let's Encrypt democratizing encryption?" In: *Proceedings of the Applied Networking Research Workshop*. ACM. 2017, pp. 48–54.

[9] Devdatta Akhawe and Adrienne Porter Felt. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness." In: *USENIX Security Symposium*. 2013.

[10] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. "A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA)." In: *International Journal of Human–Computer Interaction* 33.11 (2017), pp. 927–942. DOI: 10.1080/10447318.2017.1306765.

[11] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. "Security practices for households bank customers in the Kingdom of Saudi Arabia." In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 2015, pp. 297–308.

[12] Ashton Anderson, Daniel Huttenlocher, Jon Kleinberg, and Jure Leskovec. "Steering user behavior with badges." In: *Proceedings of the 22nd international conference on World Wide Web*. ACM. 2013, pp. 95–106.

[13] Carlos Arango, Dylan Hogg, and Alyssa Lee. *Why is cash (still) so entrenched? Insights from the Bank of Canada's 2009 methods-of-Payment survey*. Tech. rep. Bank of Canada Discussion Paper, 2012.

[14] ArenaNet. Guild Wars 2. Game [PC]. Aug. 2012.

[15] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. "Internet Censorship in Iran: A First Look." In: *Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet*. Washington, D.C.: USENIX, 2013. URL: https://www.usenix.org/conference/foci13/internet-censorship-iran-first-look.

[16] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. "Leading Johnny to Water: Designing for Usability and Trust." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2015.

[17] Earl R Babbie and Lucia Benaquisto. *Fundamentals of social research*. Cengage Learning, 2009.

[18] John Bagnall, David Bounie, Kim P Huynh, Anneke Kosse, Tobias Schmidt, Scott D Schuh, and Helmut Stix. "Consumer cash usage: A cross-country comparison with payment diary survey data." In: (2014).

[19] Gabriel Barata, Sandra Gama, Joaquim Jorge, and Daniel Gonçalves. "Engaging engineering students with gamification." In: *Games and Virtual Worlds for Serious Applications (VS-GAMES), 2013 5th International Conference on*. IEEE. 2013, pp. 1–8.

[20] Kathy Baxter, Catherine Courage, and Kelly Caine. *Understanding your Users (Second Edition)*. Second Edition. Interactive Technologies. Boston: Morgan Kaufmann, 2015. ISBN: 978-0-12-800232-2. DOI: https://doi.org/10.1016/B978-0-12-800232-2.09988-0.

[21] Guido Becke. "Die Entdeckung des Informellen im Organisationswandel. Zum Potenzial kommunikativer Forschungsmethoden." In: *Formalität und Informalität in Organisationen*. Springer VS, 2015. ISBN: 978-3-658-00603-7.

[22] R Meredith Belbin. *Management Teams, Third*. 3rd ed. Routledge, 2010.

[23] Zinaida Benenson, Gabriele Lenzini, Daniela Oliveira, Simon Parkin, and Sven Uebelacker. "Maybe poor Johnny really cannot encrypt: The case for a complexity theory for usable security." In: *Proceedings of the 2015 New Security Paradigms Workshop*. ACM. 2015, pp. 85–99.

[24] Ross Benes. *Five Charts: Why Users Are Fed Up with Digital Ads*. `https://www.emarketer.com/content/five-charts-users-are-fed-up-with-digital-ads`. last accessed on 2019-02-20. 2018.

[25] Alastair R Beresford, Dorothea Kübler, and Sören Preibusch. "Unwillingness to pay for privacy: A field experiment." In: *Economics Letters* 117.1 (2012), pp. 25–27.

[26] Daniel J. Bernstein, Tanja Lange, and Peter Schwabe. "The Security Impact of a New Cryptographic Library." In: *Proceedings of the 2Nd International Conference on Cryptology and Information Security in Latin America*. LATINCRYPT'12. Santiago, Chile, 2012, pp. 159–176. ISBN: 978-3-642-33480-1.

[27] BioWare Austin. Star Wars: The Old Republic. Game [PC]. Dec. 2011.

[28] Blizzard Entertainment. World of Warcraft. Game [PC]. Nov. 2004.

[29] Blizzard Entertainment. *Upgrade Your Account Security and Gain a Backpack Upgrade*. `https://worldofwarcraft.com/en-gb/news/21366969/upgrade-your-account-security-and-gain-a-backpack-upgrade`, last accessed 2019-04-08. Jan. 2018.

[30] Bloomberg. *This Is How China Is Stifling Bitcoin and Cryptocurrencies*. lasta accessed February 28, 2020. URL: `http://fortune.com/2018/01/17/china-bitcoin-cryptocurrency-crackdown/`.

[31] John M Blythe, Lynne Coventry, and Linda Little. "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors." In: *Symposium on Usable Privacy and Security*. USENIX Association, 2015, pp. 103–122.

[32] Wolfgang Bonß. "Die gesellschaftliche Konstruktion von Sicherheit." In: *Sicherheit in der unsicheren Gesellschaft*. Ed. by Ekkehard Lippert, Andreas Prüfert, and Günther Wachtler. Wiesbaden: VS Verlag für Sozialwissenschaften, 1997, pp. 21–41. ISBN: 978-3-322-90744-8. DOI: `10.1007/978-3-322-90744-8_2`.

[33] David Bounie and Abel François. "Cash, check or bank card? The effects of transaction characteristics on the use of payment instruments." In: *Telecom Paris Economics and Social Sciences Working Paper No. ESS-06-05* (2006).

[34] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. "Bridging the gap in computer security warnings: A mental model approach." In: *IEEE Security & Privacy*. Vol. 9. 2. IEEE, 2011, pp. 18–26.

[35] Paul Brewer and Sunil Venaik. "On the misuse of national culture dimensions." In: *International Marketing Review* (2012).

[36] Michael Buhrmester, Tracy Kwang, and Samuel D. Gosling. "Amazon's Mechanical Turk." In: *Perspectives on Psychological Science* 6.1 (2011), pp. 3–5. DOI: 10.1177/1745691610393980.

[37] Deutsche Bundesbank. *Payment behaviour in Germany in 2014: Third study of the utilisation of cash and cashless payment instruments*. Deutsche Bundesbank, 2015.

[38] Karoline Busse, Sabrina Amft, Daniel Hecker, and Emanuel von Zezschwitz. "Get a Free Item Pack with Every Activation!" In: *i-com* 18.3 (2019), pp. 217–236.

[39] Karoline Busse, Julia Schäfer, and Matthew Smith. "Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice." In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019. URL: https://www.usenix.org/conference/soups2019/presentation/busse.

[40] Karoline Busse, Jennifer Seifert, and Matthew Smith. "Exploring the security narrative in the work context." In: *Journal of Cybersecurity* 6.1 (Oct. 2020). ISSN: 2057-2085. URL: https://doi.org/10.1093/cybsec/tyaa011.

[41] Karoline Busse, Mohammad Tahaei, Katharina Krombholz, Emanuel von Zezschwitz, Matthew Smith, Jing Tian, and Wenyuan Xu. "Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries." In: *The 5th European Workshop on Usable Security*. Online: IEEE, 2020. URL: https://eusec20.cs.uchicago.edu/eusec20-Busse.pdf.

[42] Carbine Studios. WildStar. Game [PC]. June 2014.

[43] Juan Carlos Roca, Juan José Garcıa, and Juan José de la Vega. "The importance of perceived trust, security and privacy in online trading systems." In: *Information Management & Computer Security* 17.2 (2009), pp. 96–113.

[44] Sathya Chandran, Xinming Ou, Alexandru G Bardas, Jacob Case, Michael Wesch, John Mchugh, and S Raj Rajagopalan. "A Human Capital Model for Mitigating Security Analyst Burnout." In: *Symposium on Usable Privacy and Security*. Ottawa, Canada: USENIX Association, 2015, pp. 347–359.

[45] Chaos Computer Club e.V. *Browse Videos by Category: Congress*. last accessed 2019-01-29. URL: `https://media.ccc.de/b/congress`.

[46] Chaos Computer Club e.V. *Chaos Computer Club*. last accessed 2019-01-29. URL: `%7Bhttps://www.ccc.de/en/home%7D`.

[47] Kathy Charmaz. *Constructing Grounded Theory: A Practical Guide through Qualitative Research*. SagePublications Ltd, London, 2006.

[48] Yulia Cherdantseva and Jeremy Hilton. "Information Security and Information Assurance: Discussion about the Meaning." In: *Organizational, Legal, and Technological Dimensions of Information System Administration* (2013), p. 167.

[49] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. "A Usability Study and Critique of Two Password Managers." In: *USENIX Security Symposium*. 2006, pp. 1–16.

[50] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. "Measuring User Confidence in Smartphone Security and Privacy." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2012.

[51] Tom Chothia, Flavio D Garcia, Chris Heppel, and Chris McMahon Stone. "Why Banker Bob (still) Can't Get TLS Right: A Security Analysis of TLS in Leading UK Banking Apps." In: *International Conference on Financial Cryptography and Data Security*. Springer. 2017.

[52] Cisco. *SSL VPN Security*. 2019. URL: `https://www.cisco.com/c/en/us/about/security-center/ssl-vpn-security.html`.

[53] Justin D Clark, Robert M Faris, Ryan J Morrison-Westphal, Helmi Noman, Casey B Tilton, and Jonathan L Zittrain. "The shifting landscape of global internet censorship." In: (2017).

[54] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. ""It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University." In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM. 2018, p. 456.

[55] Computing Research Association. *Four Grand Challenges in Trustworthy Computing*. Tech. rep. Computing Research Association, 2003, p. 32. URL: `http://archive.cra.org/reports/trustworthy.computing.pdf`.

[56] Kenneth James Williams Craik. *The nature of explanation*. Vol. 445. CUP Archive, 1952.

[57] John W Creswell and Cheryl N Poth. *Qualitative inquiry and research design: Choosing among five approaches*. 4th ed. Sage publications, 2017.

[58] Michel Croizer and Erhard Friedberg. *Die Zwänge kollektiven Handelns.Über Macht und Organisation*. 1979.

[59] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. "A Study on the Value of Location Privacy." In: *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*. WPES '06. Alexandria, Virginia, USA, 2006, pp. 109–118. ISBN: 1-59593-556-8. DOI: 10.1145/1179601.1179621.

[60] Philippe d'Iribarne. "National cultures and organisations in search of a theory: an interpretative approach." In: *International Journal of Cross Cultural Management* 9.3 (2009), pp. 309–321.

[61] Tomi Dahlberg, Niina Mallat, and Anssi Öörni. "Trust enhanced technology acceptance modelconsumer acceptance of mobile payment solutions: Tentative evidence." In: *Stockholm Mobility Roundtable* 22 (2003), p. 23.

[62] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. "The Tangled Web of Password Reuse." In: *NDSS*. Vol. 14. 2014, pp. 23–26.

[63] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. "A comparative usability study of two-factor authentication." In: *arXiv preprint arXiv:1309.5344* (2013).

[64] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. "Towards understanding ATM security: a field study of real world ATM use." In: *Proceedings of the sixth symposium on usable privacy and security*. ACM. 2010, p. 16.

[65] Deutsche Bundesbank. "Zahlungsverhalten in Deutschland – Eine empirische Studie über die Auswahl und Verwendung von Zahlungsinstrumenten in der Bundesrepublik Deutschland." In: (2009).

[66] Deutsche Bundesbank. "Zahlungsverhalten in Deutschland 2014 – Dritte Studie über die Verwendung von Bargeldund unbaren Zahlungsinstrumenten." In: (2014).

[67] Patricia M. Doney, Joseph P. Cannon, and Michael R. Mullen. "Understanding the Influence of National Culture on the Development of Trust." In: *The Academy of Management Review* 23.3 (1998), pp. 601–620. ISSN: 03637425. URL: http://www.jstor.org/stable/259297.

[68] Samuetta Hill Drew. *Drew: Tips on creating passwords to protect your privacy*. https://www.birminghamtimes.com/2018/11/drew-tips-on-creating-passwords-to-protect-your-privacy/. last accessed 2018-12-09. Nov. 2018.

[69] William Dudley. *Rollback! The United States NIST NO LONGER recommends "Deprecating SMS for 2FA"*. https://blogs.sap.com/2017/07/06/rollback-the-united-states-nist-no-longer-recommends-deprecating-sms-for-2fa/, last accessed 2019-03-27. July 2017.

[70] EA Sports. *FIFA 16 Ultimate Team - Login Verification*. https://www.easports.com/uk/fifa/ultimate-team/news/2015/login-verification, last accessed 2019-03-12. Oct. 2015.

[71] Epic Games. Fortnite. Game [PC, Switch, Playstation 4, Xbox One, iOS, Android]. July 2017.

[72] Epic Games. *PROTECT YOUR ACCOUNT! ENABLE 2FA*. https://www.epicgames.com/fortnite/en-US/news/2fa, last accessed 2019-04-08. Apr. 2018.

[73] K Anders Ericsson and Herbert A Simon. "Verbal reports as data." In: *Psychological review*. Vol. 87. 3. American Psychological Association, 1980, p. 215.

[74] Michael Fagan and Mohammad Maifi Hasan Khan. "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice." In: *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 2016, pp. 59–75.

[75] Sascha Fahl, Yasemin Acar, Henning Perl, and Matthew Smith. "Why eve and mallory (also) love webmasters: a study on the root causes of SSL misconfigurations." In: *Proceedings of the 9th ACM symposium on Information, Computer and Communications Security*. ACM. 2014.

[76] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. "Helping Johnny 2.0 to encrypt his Facebook conversations." In: *Symposium on Usable Privacy and Security (SOUPS)*. ACM. 2012.

[77] Sascha Fahl, Marian Harbach, Marten Oltrogge, Thomas Muders, and Matthew Smith. "Hey, you, get off of my clipboard." In: *International Conference on Financial Cryptography and Data Security*. Springer. 2013, pp. 144–161.

[78] Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, and Matthew Smith. "Rethinking SSL development in an appified world." In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM. 2013, pp. 49–60.

[79] Adrienne Porter Felt, Alex Ainslie, Robert W Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. "Improving SSL warnings: Comprehension and adherence." In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM. 2015.

[80] Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, and Chris Bentzel. "Measuring HTTPS Adoption on the Web." In: *USENIX Security Symposium*. 2017.

[81] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. "Rethinking Connection Security Indicators." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2016.

[82] Adrienne Porter Felt, Robert W Reeder, Hazim Almuhimedi, and Sunny Consolvo. "Experimenting at scale with google chrome's SSL warning." In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM. 2014.

[83] Paul Ferguson and Geoff Huston. "What is a VPN? - Part I." In: *The Internet Protocol Journal* 1.1 (1998).

[84] Kevin Gallagher, Sameer Patil, and Nasir Memon. "New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2017.

[85] Gamer2Gamer Corp. *g2g.com – About Us*. `http://corp.g2g.com/about-us-in-general/`, last accessed 2019-04-10. 2019.

[86] Xianyi Gao, Gradeigh D Clark, and Janne Lindqvist. "Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users." In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 2016, pp. 1656–1668.

[87] Barney G Glaser. *Emergence vs forcing: Basics of grounded theory analysis*. Sociology Press, 1992.

[88] Barney G Glaser and Anselm L Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction publishers, 1967.

[89] Jochen Gläser and Grit Laudel. *Experteninterviews und qualitative Inhaltsanalyse*. VS Verlag für Sozialwissenschaften, 2010.

[90] Honeypot GmbH. *Frauen in der IT-Branche 2018*. last accessed 2019-07-01. 2018. URL: `https://www.honeypot.io/de/women-in-tech-2018/`.

[91] Ashok K. Goel, Spencer Rugaber, and Swaroop Vattam. "Structure, Behavior, and Function of Complex Systems: The Structure, Behavior, and Function Modeling Language." In: *Artif. Intell. Eng. Des. Anal. Manuf.* Vol. 23. 1. New York, NY, USA: Cambridge University Press, Feb. 2009, pp. 23–35.

[92] Matthew Green and Matthew Smith. "Developers are Not the Enemy!: The Need for Usable Security APIs." In: *IEEE Security & Privacy* 14.5 (2016), pp. 40–46.

[93] Claire Greene, Scott D Schuh, and Joanna Stavins. *The 2014 survey of consumer payment choice: summary results*. Tech. rep. Federal Reserve Bank of Boston, 2016.

[94] Jens Grossklags and Alessandro Acquisti. "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information." In: *WEIS*. 2007.

[95] Greg Guest, Arwen Bunce, and Laura Johnson. "How many interviews are enough? An experiment with data saturation and variability." In: *Field Methods*. Vol. 18. 1. 2006, pp. 59–82.

[96] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking." In: *Computers & Security* 30.4 (2011), pp. 208–220.

[97] J. M. Haney, S. L. Garfinkel, and M. F. Theofanos. "Organizational practices in cryptographic development and testing." In: *2017 IEEE Conference on Communications and Network Security (CNS)*. Oct. 2017, pp. 1–9. DOI: 10.1109/CNS.2017.8228643.

[98] Julie M. Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. ""We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products." In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, 2018, pp. 357–373. ISBN: 978-1-931971-45-4. URL: https://www.usenix.org/conference/soups2018/presentation/haney-mindsets.

[99] Marian Harbach, Alexander De Luca, and Serge Egelman. "The anatomy of smartphone unlocking: A field study of android lock screens." In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 2016, pp. 4806–4817.

[100] Marian Harbach, Sascha Fahl, and Matthew Smith. "Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness." In: *Computer Security Foundations Symposium (CSF), 2014 IEEE 27th*. IEEE. 2014, pp. 97–110.

[101] Marian Harbach, Sascha Fahl, Polina Yakovleva, and Matthew Smith. "Sorry, I don't get it: An analysis of warning message texts." In: *International Conference on Financial Cryptography and Data Security*. Springer. 2013.

[102] Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. "Human, Organizational, and Technological Factors of IT Security." In: *CHI '08 Extended Abstracts on Human Factors in Computing Systems*. CHI EA '08. Florence, Italy: ACM, 2008, pp. 3639–3644. ISBN: 978-1-60558-012-8. DOI: 10.1145/1358628.1358905. URL: http://doi.acm.org/10.1145/1358628.1358905.

[103] Jonas Hedman, Felix B Tan, Jacques Holst, and Martin Kjeldsen. "Taxonomy of payments: a repertory grid analysis." In: *International Journal of Bank Marketing* 35.1 (2017), pp. 75–96.

[104] Cormac Herley and PC van Oorschot. "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit." In: *IEEE Symposium on Security and Privacy (SP)*. IEEE. 2017.

[105] Amir Herzberg and Hemi Leibowitz. "Can Johnny Finally Encrypt? Evaluating E2E Encryption in Popular IM Applications." In: *ACM Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. 2016.

[106] Cindy Hmelo-Silver and Merav Green Pfeffer. "Comparing Expert and Novice Understanding of a Complex System From the Perspective of Structures, Behaviors, and Functions." In: *Cognitive Science*. Vol. 28. Feb. 2004, pp. 127–138.

[107] William R Hobbs and Margaret E Roberts. "How sudden censorship can increase access to information." In: *American Political Science Review* (2018), pp. 1–16.

[108] Arlie Russell Hochschild. *The managed heart: Commercialization of human feeling*. 1991.

[109] G. Hofstede, G.J. Hofstede, and M. Minkov. *Cultures and Organizations: Software of the Mind, Third Edition*. McGraw-Hill Education, 2010. ISBN: 9780071770156.

[110] Jacques Holst, Martin Kjeldsen, Jonas Hedman, and Felix B Tan. "Payment instrument characteristics: a repertory grid analysis." In: (2015).

[111] Christopher K Hsee and Elke U Weber. "Cross-national differences in risk preference and lay predictions." In: (1999).

[112] Hsiu-Fang Hsieh and Sarah E. Shannon. "Three Approaches to Qualitative Content Analysis." In: *Qualitative Health Research* 15.9 (2005), pp. 1277–1288. DOI: 10.1177/1049732305276687.

[113] Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps." In: *Proceedings of the 2016 Internet Measurement Conference*. IMC '16. Santa Monica, California, USA: ACM, 2016, pp. 349–364. ISBN: 978-1-4503-4526-2. DOI: 10.1145/2987443.2987471.

[114] Internet.ir. *Cyber crime law, Iran*. 2017. URL: http://internet.ir/law.html.

[115] Iulia Ion, Rob Reeder, and Sunny Consolvo. ""...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices." In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, 2015, pp. 327–346. ISBN: 978-1-931971-249. URL: https://www.usenix.org/conference/soups2015/proceedings/presentation/ion.

[116] Sharwan Kumar Joram, Grzegorz Pelechaty, Pawan Kumar Chauhan, and Srikanth Vittal. *Multiple factor user authentication system*. US Patent App. 11/846,965. Mar. 2009.

[117] Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl. "Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms." In: *Synthesis Lectures on Information Security, Privacy, & Trust* 9.1 (2017), pp. 1–123.

[118] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. ""My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security." In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, 2015, pp. 39–52. ISBN: 978-1-931971-249. URL: https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[119] Eitan Katz. *Dashlane Research Finds Majority of Two-Factor Authentication Offerings Fall Short*. https://blog.dashlane.com/2fa-rankings/. last accessed 2018-12-19. 2018.

[120] Kenneth Katzman. *Iran sanctions*. Tech. rep. Congressional Research Service Washington United States, 2016.

[121] Franz-Xaver Kaufmann. *Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*. Vol. 31. 1973.

[122] Anne R. Kearney and Stephen Kaplan. "Toward a Methodology for the Measurement of Knowledge Structures of Ordinary People: The Conceptual Content Cognitive Map (3CM)." In: *Environment and Behavior*. Vol. 29. 5. 1997, pp. 579–617.

[123] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms." In: *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE. 2012, pp. 523–537.

[124] Jiyoung Kim and Sharron J Lennon. "Effects of reputation and website quality on online consumers' emotion, perceived risk and purchase intention: Based on the stimulus-organism-response model." In: *Journal of Research in Interactive Marketing* 7.1 (2013), pp. 33–56.

[125] Claudia Kodde. "Germany's "Right to be forgotten" – between the freedom of expression and the right to informational self-determination." In: *International Review of Law, Computers & Technology* 30.1-2 (2016), pp. 17–31. DOI: 10.1080/13600869.2015.1125154.

[126] Anneke Kosse and David-Jan Jansen. "Choosing how to pay: The influence of foreign backgrounds." In: *Journal of Banking & Finance* 37.3 (2013), pp. 989–998.

[127] Marios Koufaris and William Hampton-Sosa. "The development of initial trust in an online company by new customers." In: *Information & management* 41.3 (2004), pp. 377–397.

[128] Hanna Krasnova, Natasha F Veltri, and Oliver Günther. "Self-disclosure and privacy calculus on social networking sites: The role of culture." In: *Business & Information Systems Engineering* 4.3 (2012), pp. 127–135.

[129] Klaus Krippendorff. *Content Analysis: An Introduction to Its Methodology*. SAGE Publications, 2004, pp. 241–243.

[130] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M Angela Sasse. ""They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking." In: *arXiv preprint arXiv:1501.04434* (2015).

[131] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. ""If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS." In: *S&P 2019*. 2019. URL: https://publications.cispa.saarland/2788/.

[132] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. "The Other Side of the Coin: User Experiences With Bitcoin Security and Privacy." In: *International Conference on Financial Cryptography and Data Security*. 2016.

[133] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar R. Weippl. ""I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS." In: *USENIX Security Symposium*. 2017.

[134] Malte Krueger and Franz Seitz. "Cost and Benefits of Cash and Cashless Payment Instruments." In: *Overview and initial estimates. Study commissioned by the Deutsche Bundesbank, Frankfurt* (2014).

[135] Stefan Kühl. *Organisation - Eine sehr kurze Einführung*. VS Verlag für Sozialwissenschaften, 2011. ISBN: 978-3-531-17978-0.

[136] Deepti Kumar, David Martin, and Jacki O'Neill. "The times they are a-changin': mobile payments in india." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2011, pp. 1413–1422.

[137] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

[138] Vili Lehdonvirta, Terhi-Anna Wilska, and Mikael Johnson. "Virtual consumerism: case habbo hotel." In: *Information, communication & society* 12.7 (2009), pp. 1059–1079.

[139] Amanda Lenhart, Mary Madden, Sandra Cortesi, Urs Gasser, and Aaron Smith. "Where teens seek online privacy advice." In: *Pew Research Center, Internet & Technology* (2013).

[140] Peter Leonard. *Mandatory Internet Data Retention in Australia – Looking the horse in the mouth after it has bolted*. 2015.

[141] Ada Lerner, Eric Zeng, and Franziska Roesner. "Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists." In: *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE. 2017.

[142] Yibin Li, Wenyun Dai, Zhong Ming, and Meikang Qiu. "Privacy protection for preventing data over-collection in smart city." In: *IEEE Transactions on Computers* 65.5 (2016), pp. 1339–1350.

[143] Martin C. Libicki, Edward Balkovich, Brian A. Jackson, Rena Rudavsky, and Katharine Watkins Webb. "Influences on the Adoption of Multifactor Authentication." In: (2011).

[144] Lerong Lu. "Decoding Alipay: Mobile Payments, a Cashless Society and Regulatory Challenges." In: (2018).

[145] Niklas Luhmann. *Soziale systeme*. Suhrkamp, 1985.

[146] Georges-Henri Luquet. "Le dessin enfantin.(Bibliothèque de psychologie de l'enfant et de pédagogie.)." In: (1927).

[147] Andrew M'manga, Shamal Faily, John McAlaney, and Christopher Williams. "Folk risk analysis: Factors influencing security analysts' interpretation of risk." In: *Proc. of the 13th Symposium on Usable Privacy and Security, ser. SOUPS*. Vol. 17. 2017.

[148] Erina L MacGeorge, Bo Feng, and Elizabeth R Thompson. ""Good" and "bad" advice." In: *Studies in applied interpersonal communication* 145 (2008).

[149] Antonis Manousis, Roy Ragsdale, Ben Draffin, Adwiteeya Agrawal, and Vyas Sekar. "Shedding light on the adoption of let's encrypt." In: *arXiv preprint arXiv:1611.00469*. 2016.

[150] Angela Marrujo. *Fraud is taking the fun out of video games: scams, spam & account takeovers*. https://venturebeat.com/2018/06/07/fraud-is-taking-the-fun-out-of-video-games-scams-spam-account-takeovers/, last accessed 2019-01-04. June 2018.

[151] Arunesh Mathur, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. "Quantifying Users' Beliefs about Software Updates." In: *Proceedings 2018 Workshop on Usable Security* (2018). DOI: 10.14722/usec.2018.23036.

[152] Roger C. Mayer, James H. Davis, and F. David Schoorman. "An Integrative Model of Organizational Trust." In: *The Academy of Management Review* 20.3 (1995), pp. 709–734. ISSN: 03637425. URL: http://www.jstor.org/stable/258792.

[153] Philipp Mayring. *Qualitative Inhaltsanalyse. Grundlagen und Techniken*. 12th ed. Beltz, 2012.

[154] Philipp Mayring. *Qualitative content analysis: theoretical foundation, basic procedures and software solution*. Social Science Open Access Repository (SSOAR), 2014, p. 143.

[155] Sharan B Merriam and Elizabeth J Tisdell. *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons, 2015.

[156] Dennis Mirante and Justin Cappos. "Understanding password database compromises." In: *Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02* (2013).

[157] MMO Games. *Guild Wars 2: Free Mini Mystical Dragon Now Available*. https://www.mmogames.com/gamenews/guild-wars-2-free-mini-mystical-dragon-now-available/, last accessed 2019-04-08. July 2015.

[158] Sergio Moreno-Ríos and Juan A García-Madruga. "Priming in Deduction: A Spatial Arrangement Task." In: *Memory & Cognition*. Vol. 30. 7. Springer, 2002, pp. 1118–1127.

[159] Jason Morris, Ingolf Becker, and Simon Parkin. "In Control with no Control: Perceptions and Reality of Windows 10 Home Edition Update Features." In: *Workshop on Usable Security and Privacy (USEC)*. 2019.

[160] Claus Adolf Moser and Graham Kalton. *Survey methods in social investigation*. Routledge, 1971.

[161] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. "Why do developers get password storage wrong?: A qualitative usability study." In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2017, pp. 311–328.

[162] NCSA. *The Stay Safe Online Blog*. last accessed on 2018-12-09. July 2018. URL: https://staysafeonline.org/blog_category/privacy/.

[163] NCSC. *Most hacked passwords revealed as UK cyber survey exposes gaps in online security*. last accessed 2019-04-26. Apr. 2019. URL: https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security.

[164] Shaun O'Brien. *Consumer Preferences and the Use of Cash: Evidence from the Diary of Consumer Payments Choice*. Tech. rep. Federal Reserve Bank of San Francisco, 2014.

[165] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Cranor. "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration." In: *Proceedings on Privacy Enhancing Technologies*. Vol. 2018. 4. De Gruyter Open, 2018.

[166] Marten Oltrogge, Yasemin Acar, Sergej Dechand, Matthew Smith, and Sascha Fahl. "To Pin or Not to Pin-Helping App Developers Bullet Proof Their TLS Connections." In: *USENIX Security Symposium*. 2015.

[167] Oslo Univeristy Library. *Global surveillance*. last accessed February 28, 2020. 2016. URL: https://www.ub.uio.no/fag/naturvitenskap-teknologi/informatikk/faglig/bibliografier/no21984.html.

[168] Reza M Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, Mohammad Hammoudeh, and Gregory Epiphaniou. "Security in online games: Current implementations and challenges." In: *Handbook of Big Data and IoT Security*. Springer, 2019, pp. 367–384.

[169] Donald L Pipkin. *Information security: protecting the global enterprise*. Prentice Hall PTR, 2000.

[170] Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, and Ross T. Hightower. "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders." In: *Information & Management* 51.5 (2014), pp. 551–567. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2014.03.009.

[171] Rasmus Prentow, Rasmus Steiniche, Simone D Johansen, Jeni Paay, Ivan Aaen, and Jesper Kjeldskov. "When value is greater than money: a micropayment system in Uganda." In: *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. ACM. 2015, pp. 765–772.

[172] Gary Pritchard, John Vines, and Patrick Olivier. "Your money's no good here: The elimination of cash payment on London buses." In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM. 2015, pp. 907–916.

[173] Emilee Rader and Rick Wash. "Identifying patterns in informal sources of security information." In: *Journal of Cybersecurity* 1.1 (Dec. 2015), pp. 121–144. ISSN: 2057-2085. DOI: 10.1093/cybsec/tyv008.

[174] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. "How i learned to be secure: a census-representative survey of security advice sources and behavior." In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2016, pp. 666–677.

[175] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. "How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples." In: *How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples*. IEEE. 2019.

[176] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security." In: *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE. 2016, pp. 272–288.

[177] Elissa M Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L Mazurek. "Asking for a Friend: Evaluating Response Biases in Security User Studies." In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2018, pp. 1238–1255.

[178] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. "An Experience Sampling Study of User Reactions to Browser Warnings in the Field." In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 2018.

[179] Robert W. Reeder. *If you cold tell a user three things to do to stay safe online, what would they be?* https://security.googleblog.com/2014/03/if-you-could-tell-user-three-things-to.html. last accessed on 2019-02-20. Mar. 2014.

[180] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. "Why doesn't Jane Protect Her Privacy?" In: *International Symposium on Privacy Enhancing Technologies*. 2014.

[181] Jean-Loup Richet. "Extortion on the internet: the rise of crypto-ransomware." In: *Harvard* (2016).

[182] Ronald W. Rogers. "A Protection Motivation Theory of Fear Appeals and Attitude Change." In: *The Journal of Psychology* 91.1 (1975), pp. 93–114. DOI: 10.1080/00223980.1975.9915803.

[183] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. "We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users." In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM. 2016.

[184] Bertrand Russell. *Vagueness*. 1923.

[185] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. ""Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia." In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, 2018, pp. 127–142. ISBN: 978-1-931971-45-4. URL: https://www.usenix.org/conference/soups2018/presentation/sambasivan.

[186] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior." In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM. 2017, pp. 2202–2214.

[187] Paul Gerhardt Schierz, Oliver Schilke, and Bernd W Wirtz. "Understanding consumer acceptance of mobile payment services: An empirical analysis." In: *Electronic commerce research and applications* 9.3 (2010), pp. 209–216.

[188] Svenja Schröder, Markus Huber, David Wind, and Christoph Rottermanner. "When SIGNAL hits the fan: On the usability and security of state-of-the-art secure mobile messaging." In: *roceedings of the 1st European Workshop on Usable Security*. EuroUSEC '16. Internet Society, 2016.

[189] W Richard Scott. *Institutions and organizations: Ideas and interests*. Sage, 2008.

[190] Christoph Seidel. "Ungewissheit, Vielfalt, Mehrdeutigkeit – Eine Heuristik unsicherer Umwelten." In: *Organisation und Unsicherheit*. Springer VS, 2015. ISBN: 978-3-531-19237-6.

[191] A. Serebrenik. "Emotional labor of software engineers." English. In: *BENEVOL 2017 : BElgian-NEtherlands Software eVOLution Symposium, 4-5 December 2017, Antwerp, Belgium*. Ed. by Serge Demeyer, Ali Parsai, Gulsher Laghari, and Brent van Bladel. CEUR-WS.org. CEUR-WS.org, Dec. 2017, pp. 1–6.

[192] D. J. Simons and C. F. Chabris. "Common (mis)beliefs about memory: A replication and comparison of telephone and Mechanical Turk survey methods"." In: *PLOS ONE* 7.12 (2012).

[193] Christopher Simpson. *Data Mining of Telecom Metadata is "More Dangerous than Intercepting Conversations"*. https://newsmonitors.blog/2018/04/19/data-mining-of-telecom-metadata-is-more-dangerous-than-intercepting-conversations/. last accessed on 2019-02-14. 2018.

[194] Supriya Singh, Anuja Cabraal, and Gabriele Hermansson. "What is your husband's name?: sociological dimensions of internet banking authentication." In: *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments*. ACM. 2006, pp. 237–244.

[195] Nancy Staggers and A. F. Norico. "Mental models: Concepts for human-computer interaction research." In: *International Journal of Man-Machine Studies* 38 (1993), pp. 587–605.

[196] International Organization for Standardization. *Information Technology; Security Techniques; Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002*. International Organization for Standardization, 2009.

[197] Statistisches Bundesamt. *Bevölkerungsstand*. last accessed 2020-02-28. 2020. URL: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/Tabellen/zensus-geschlecht-staatsangehoerigkeit-2019.html.

[198] Anselm Strauss, Juliet Corbin, et al. *Basics of qualitative research*. Vol. 15. Newbury Park, CA: Sage, 1990.

[199] W.Timothy Strayer. "Privacy issues in virtual private networks." In: *Computer Communications* 27.6 (2004). Internet Performance and Control of Network Systems, pp. 517–521. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2003.08.016.

[200] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. "Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations." In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver,

CO: USENIX Association, 2016, pp. 237–251. ISBN: 978-1-931971-31-7. URL: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy.

[201] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. "Crying Wolf: An Empirical Study of SSL Warning Effectiveness." In: *USENIX security symposium*. Montreal, Canada. 2009, pp. 399–416.

[202] The World Bank. *Population, total - Iran, Islamic Rep.* 2020. URL: https://data.worldbank.org/indicator/SP.POP.TOTL?locations=IR.

[203] Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman, and Simson Garfinkel. "Be Prepared: How US Government Experts Think About Cybersecurity." In: *USEC Workshop*. 2017.

[204] Thomas Guillemaud. *Why are mobile payments so popular in China*. 2017. URL: https://it-consultis.com/blog/why-are-mobile-payments-so-popular-china.

[205] M. Toorani and A. Beheshti. "Solutions to the GSM Security Weaknesses." In: *2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies*. Sept. 2008, pp. 576–581. DOI: 10.1109/NGMAST.2008.88.

[206] Trend Micro. *Data Privacy and Online Gaming: Why Gamers Make for Ideal Targets*. https://www.trendmicro.com/vinfo/us/security/news/online-privacy/data-privacy-and-online-gaming-why-gamers-make-for-ideal-targets, last accessed 2019-01-04. Jan. 2015.

[207] Ubisoft. *2 STEP VERIFICATION RANKED LOCK UPDATE FOR PC*. https://rainbow6.ubisoft.com/siege/en-gb/news/detail.aspx?c=tcm:154-340676-16&ct=tcm:154-76770-32, last accessed 2019-04-08. Nov. 2018.

[208] Ubisoft Montreal, Ubisoft Kiev, Ubisoft Toronto, and Ubisoft Barcelona. Tom Clancy's Rainbow Six Siege. Game [PC, Playstation 4, Xbox One]. Dec. 2015.

[209] *UN country profiles*. last accessed 2019-09-23. 2016. URL: http://data.un.org/.

[210] United States Census Bureau. *Annual Estimates of the Resident Population: April 1, 2010 to July 1, 2018*. last accessed 2020-02-28. 2020. URL: https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk.

[211] Valve. *Steam Trade and Market Holds*. https://support.steampowered.com/kb_article.php?ref=8078-TPHC-6195, last accessed 2019-04-09. Oct. 2017.

[212] Elham Vaziripour, Reza Farahbakhsh, Mark O'Neill, Justin Wu, Kent Seamons, and Daniel Zappala. "A Survey Of the Privacy Preferences and Practices of Iranian Users of Telegram." In: *Workshop on Usable Security (USEC)*. Jan. 2018.

[213] Elham Vaziripour, Justin Wu, Mark O'Neill, Ray Clinton, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. "Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2017.

[214] Sunil Venaik and Paul Brewer. "Critical issues in the Hofstede and GLOBE national culture models." In: *International Marketing Review* 30.5 (2013), pp. 469–482.

[215] Melanie Volkamer, Andreas Gutmann, Karen Renaud, Paul Gerber, and Peter Mayer. "Replication Study: A Cross-Country Field Observation Study of Real World {PIN} Usage at ATMs and in Various Electronic Payment Scenarios." In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association. 2018.

[216] Elliot Volkman. *49 Percent of Phishing Sites Now Use HTTPS*. `https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https`. last accessed on 2019-02-13. 2018.

[217] Ulf Von Kalckreuth, Tobias Schmidt, and Helmut Stix. "Choosing and using payment instruments: evidence from German microdata." In: *Empirical Economics* 46.3 (2014), pp. 1019–1055.

[218] Emanuel Von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. "Survival of the shortest: A retrospective analysis of influencing factors on password composition." In: *IFIP Conference on Human-Computer Interaction*. Springer. 2013, pp. 460–467. ISBN: 978-3-642-40477-1.

[219] Riley Walters. "Cyber attacks on US companies in 2014." In: *The Heritage Foundation* 4289 (2014), pp. 1–5.

[220] Rick Wash. "Folk models of home computer security." In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM. 2010, p. 11.

[221] Rick Wash and Emilee Rader. "Influencing mental models of security: a research agenda." In: *Proceedings of the 2011 Workshop on New Security Paradigms*. ACM. 2011.

[222] Susanne Weber, Marian Harbach, and Matthew Smith. "Participatory design for security-related user interfaces." In: *Workshop on Usable Security (USEC)*. 2015.

[223] Jake Weidman and Jens Grossklags. "I like it, but i hate it: Employee perceptions towards an institutional transition to BYOD second-factor authentication." In: *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM. 2017, pp. 212–224.

[224] Catherine S. Weir, Gary Douglas, Mervyn Jack, and Tim Richardson. "Usable security: User preferences for authentication methods in eBanking and the effects of experience." In: *Interacting with Computers* 22.3 (Oct. 2009), pp. 153–164. ISSN: 0953-5438. DOI: 10.1016/j.intcom.2009.10.001.

[225] A Whitten. "Making Security Usable." PhD thesis. Carnegie Mellon University, 2004.

[226] Alma Whitten and J. D. Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In: *Proceedings of the 8th USENIX Security Symposium*. 1999.

[227] Ludwig Wittenstein. *Tractatus Logico Philosophicus*. Simon and Schuster, 2012.

[228] Ludwig Wittgenstein. *Philosophische Untersuchungen Kritisch-genetische Edition*. Ed. by Ludwig Schulte, Heikki Nyman, Eike von Savigny, and Georg Henrik von Wright. Suhrkamp, 2001.

[229] World Economic Forum. *The world's 10 biggest economies in 2017*. last accessed 2020-02-28. 2017. URL: https://www.weforum.org/agenda/2017/03/worlds-biggest-economies-in-2017/.

[230] Justin Wu and Daniel Zappala. "When is a Tree Really a Truck? Exploring Mental Models of Encryption." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2018.

[231] Maximilian Yang. "Card Payments and Consumer Protection in Germany." In: *Anglo-German Law Journal* 2 (2016), p. 6.

[232] Shumaila Y Yousafzai, John G Pallister, and Gordon R Foxall. "A proposed model of e-trust for electronic banking." In: *Technovation* 23.11 (2003), pp. 847–860.

[233] Masaki Yuki, William W. Maddux, Marilynn B. Brewer, and Kosuke Takemura. "Cross-Cultural Differences in Relationship- and Group-Based Trust." In: *Personality and Social Psychology Bulletin* 31.1 (2005), pp. 48–62. DOI: 10.1177/0146167204271305.

[234] Zack Zwiezen. *Earn Free Money And Gold In GTA Online and Red Dead Online By Activating Two-Step Verification*. https://kotaku.com/earn-free-money-and-gold-in-gta-online-and-red-dead-onl-1833178166, last accessed 2019-04-08. Mar. 2019.

[235] Eric Zeng, Shrirang Mare, and Franziska Roesner. "End User Security & Privacy Concerns with Smart Homes." In: *Symposium on Usable Privacy and Security (SOUPS)*. 2017.

[236] Xuding Zheng. *Phishing with Unicode Domains*. https://www.xudongz.com/blog/2017/idn-phishing/. last accessed 2019-02-14. 2017.

[237] Rui Zhou, Jasmine Hentschel, and Neha Kumar. "Goodbye text, hello emoji: mobile communication on wechat in China." In: *Proceedings of the 2017 CHI conference on human factors in computing systems*. New York, NY, USA: ACM, 2017, pp. 748–759. DOI: 10.1145/3025453.3025800.

[238] Mary Ellen Zurko and Richard T. Simon. "User-centered security." In: *ACM New Security Paradigms Workshop*. 2004, pp. 27–33. DOI: 10.1145/304851.304859.