



# USENIX

THE ADVANCED COMPUTING  
SYSTEMS ASSOCIATION

## Unpacking the Social and Emotional Dimensions of Security and Privacy User Engagement

*Nina Gerber, Technical University of Darmstadt; Verena Zimmermann, ETH Zurich; Alexandra von Preuschen, Justus-Liebig-University Gießen; Karen Renaud, University of Strathclyde, UK; University of South Africa, South Africa; and Rhodes University, South Africa*

<https://www.usenix.org/conference/soups2025/presentation/gerber>

This paper is included in the Proceedings of the  
Twenty-First Symposium on Usable Privacy and Security.

August 11–12, 2025 • Seattle, WA, USA

ISBN 978-1-939133-51-9

Open access to the Proceedings of the  
Twenty-First Symposium on Usable Privacy and Security  
is sponsored by USENIX.

# Unpacking the Social and Emotional Dimensions of Security and Privacy User Engagement

Nina Gerber\*  
Technical University of Darmstadt

Verena Zimmermann\*  
ETH Zurich

Alexandra von Preuschen  
Justus-Liebig-University Gießen

Karen Renaud  
University of Strathclyde, UK  
University of South Africa, South Africa  
Rhodes University, South Africa

## Abstract

Despite the acknowledged importance of security and privacy (S&P), user engagement with protective practices remains limited, influenced by complex social dynamics and emotional responses. In this study, we surveyed a representative sample of 496 U.S. participants to examine the interplay between social dynamics and emotional responses in shaping S&P behaviours. Our findings highlight that S&P conversations are infrequent, hindered by perceived social norms, complexity, and assumed disinterest from others. Participants associated S&P-savvy individuals with positive traits such as trustworthiness and intelligence, yet also challenge stereotypes of paranoia or social awkwardness. Normalizing discussions and fostering social interactions around S&P could drive greater user engagement. Emotionally, S&P practices evoke not only frustration, fear, and feelings of being overwhelmed, but also curiosity and a desire for empowerment. Participants cited simplification, enhanced self-efficacy, and tangible evidence of the impact of their actions as critical factors making S&P more approachable and engaging. These insights suggest opportunities to design socially supportive and emotionally resonant interventions to improve user adoption of S&P behaviours.

## 1 Introduction

In today's complex, digitised and interconnected world, security and privacy (S&P) are crucial [17, 59]. However, despite

\*Both authors contributed equally to this work.

their importance, many users struggle to adopt S&P protection measures. These challenges stem from various barriers, including a lack of awareness and skills, misconceptions about the efficacy of such measures, or simply a lack of motivation [21, 41, 42, 57, 71]. In recent years, the understanding of S&P as a social phenomenon [46, 52, 82] and the impact of emotional and psychological factors on users' engagement with S&P has gained attention. These factors were found to be closely intertwined [77] and suggest promising directions in predicting S&P behaviours [2, 29, 77].

Prior studies have shown that security is often associated with negative emotions such as fear, frustration, and uncertainty, which can hinder users' adoption of protective behaviours [42, 65, 77]. For instance, users frequently describe S&P measures as *overwhelming*, with the domain often perceived as *mystical, unknown, and fearful* to non-experts [19, p.1]. In contrast, positive emotional responses with high arousals, such as interest, were found to foster protective behaviours [77].

Despite extensive efforts to improve the usability of S&P measures, little attention has been given to fostering positive emotional engagement with S&P. Shifting from fear-driven narratives to a focus on enjoyment and empowerment could open new avenues for enhancing user engagement. This motivates our first research question:

**RQ1: How can S&P be made more enjoyable, and what positive attributes do users associate with S&P?** *This question seeks to uncover the factors driving both positive and negative emotional responses to S&P. We aim to identify strategies that make S&P more engaging and identify the positive and negative attributes users associate with S&P, aiming to uncover opportunities to enhance the broader perception of S&P.*

Social dynamics and emotions are found to be closely interconnected, with social dynamics causing emotional responses, and vice versa [77]. They have shown promise in addressing barriers to S&P adoption, such as raising awareness of S&P issues through informal storytelling [58, 61], or prompting actions like software updates and privacy settings

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025, August 10–12, 2025, Seattle, WA, United States.

adjustments [20]. Social cues also help users navigate S&P settings more effectively [23, 24, 28]. However, S&P topics remain under-discussed among non-expert users [22, 77], and experts often hesitate to engage in these conversations with non-experts due to fears of disinterest or negative reactions [35].

To leverage the full potential of social dynamics for improving S&P practices, it is essential to understand why people choose to engage in or to avoid conversations about S&P and identify strategies to encourage these discussions. This leads to our second research question:

**RQ2: What facilitates social interactions on S&P?** *We aim to explore the barriers and enablers of S&P discussions, how frequently people talk about S&P topics, identify opportunities for fostering such conversations, and examine how stereotypes surrounding S&P might influence social interactions.*

By addressing these research questions, our study aims to provide actionable insights into the emotional and social dynamics of S&P, contributing to improved user engagement and reshaping the broader perception of S&P practices.

We conducted a survey study with a representative sample of 496 U.S. participants, combining quantitative Likert-scale ratings and qualitative open-ended questions. Our findings reveal that while S&P is widely recognised as important and predominantly associated with positive traits such as trustworthiness and reliability, security may invoke negative affect with participants feeling overwhelmed and fearful due to perceived knowledge gaps, leading to disengagement. They highlighted the need to enhance knowledge, accessibility, and self-efficacy to make S&P practices more engaging and enjoyable. Privacy, in contrast, was frequently described as a controversial and sensitive topic, which is sometimes perceived as hypocritical and overly complicated. Participants expressed a desire for greater societal attention to S&P, advocating for more frequent discussions.

Still, conversations about S&P topics remain rare, hindered by assumed disinterest of peers and social taboos. Participants suggested that external triggers, such as increased media coverage or organisational training, could encourage more S&P-related dialogue. Fear of being stereotyped might also influence willingness to discuss S&P topics: While S&P-conscious people are typically associated with positive attributes like intelligence, certain privacy practices, such as avoiding social media or using encryption, are sometimes labelled as paranoid. These findings highlight the need for interventions that address both the emotional barriers and social dynamics surrounding S&P to foster better engagement and discourse.

This research supports stakeholders that shape usable S&P practices, including researchers, practitioners responsible for security awareness (e.g., CISOs, privacy and security champions, and leadership roles), and system and software designers who seek to create more positive, socially grounded user interactions through the following contributions:

- Our findings extend the understanding of emotional responses towards S&P. Although S&P are predominantly associated with positive traits such as trustworthiness and reliability, security often evokes negative emotions such as fear and overwhelm, driven by perceived knowledge gaps. Privacy, in contrast, is viewed as controversial and sometimes hypocritical, highlighting a nuanced perception of these domains. These findings add to our understanding of user disengagement and suggest pathways for improving accessibility and user experiences in S&P.
- We identify key social and psychological factors that inhibit S&P discussions, including assumed disinterest of others and social taboos. Interestingly, the participants appeared to overestimate the effectiveness of their own S&P measures, as compared to those of colleagues, acquaintances, and especially parents, while underestimating others' willingness to discuss S&P-related topics. Thus, enhancing communication, e.g., through triggering S&P conversations similar to the social triggers described by Das et al. [20], might not only help in organisational but also in private settings, to overcome negative S&P-related perceptions, increase engagement, and better align users' self-appraisals with the actual effectiveness of S&P measures and behaviours.
- Our results highlight the dual-edged nature of S&P stereotypes, where S&P-conscious individuals are admired for their intelligence but also risk being perceived as paranoid. These insights underline the need for strategies to normalise and facilitate S&P discourse in social and professional contexts to counter such stereotypes.

## 2 Related Work

To set the scene, we summarise related work covering emotional and social dimensions of S&P. We conclude with the implications for our study.

### 2.1 S&P-related Emotions & Perceptions

As participants in prior research faced challenges in clearly identifying emotions [77], often confusing them with similar constructs, we adopt a broader interpretation of the term, which includes both perceptions and emotions.

The American Psychological Association (APA) defines perceptions as *the process or result of becoming aware of objects, relationships, and events by means of the senses, which includes such activities as recognising, observing, and discriminating* [4]. As 'perception' is closely connected to processes organising and interpreting the perceived information [4], we understand perceptions in the context of S&P as going beyond the mere sensory, also including some form of

subjective evaluation as described above. In contrast, ‘emotions’ are short-lived and relatively intense experiences [43]; they colour perceptions, influence decisions, and trigger behaviours [51]. Following that understanding, a few studies explored perceptions and emotions towards S&P from different disciplinary perspectives and for different target groups such as S&P professionals as compared to non-expert users.

Menges et al. [53] analysed public statements and survey data to explore employees’ perceptions of and emotions towards IT staff, revealing patterns of negative language, perceived power imbalances, and mutual blame. Da Silva and Jensen [19] highlighted that perceptions of S&P professionals shape the role of the Chief Information Security Officer (CISO) as both a threat protector and a strategic advisor to management. Despite the significant influence of these perceptions on behaviour, detailed research on attitudes and emotions towards S&P professionals remains limited.

When it comes to S&P as a concept, Squires and Shade [69] examined S&P perceptions using ethnographic methods, finding that mismatched views between S&P professionals and employees, shaped by social relations and workplace practices, led to communication breakdowns and weakened the security link between people and technology. Da Silva and Jensen [19] found that S&P is often perceived as *mystical, unknown, and fearful* by CISOs and organisational leaders. Haney and Lutters [38] identified strategies from security advocates to address negative perceptions of S&P, such as building trust, enhancing communication, and incentivising positive behaviours.

A qualitative study inspired by political perception research [65] used sentence completion tasks (e.g., *My opinion on cybersecurity is that...*) to explore general perceptions of S&P. This study also found a generally negative stance towards cybersecurity, i.e., participants felt overwhelmed, scared, helpless, or confused, often attributed to its complexity. Yet, the authors argue that their results are not yet sufficient to inform behavioural interventions given the complexity and ambivalence of emotions.

To disentangle that complexity and to shed light on cybersecurity-related emotions, a recent literature review of 24 articles [78] explored the role of emotions and the often interchangeably-used terms ‘affect’ and ‘mood’ in the S&P context. First, the review shows that affect plays a central role in the field of cybersecurity. For example, van Schaik et al. [74] demonstrated an effect of affect heuristics on risk perception and Conrad et al. [18] found that notifications cause negative affect during internet browsing, regardless of their communication style. Second, the review revealed a trend towards negatively-valenced emotions. In particular, fear (e.g., [1, 16, 44, 83]), anxiety (e.g., [1, 7, 14, 16]) and sadness (e.g., [7, 10, 83]). Even so, only a few studies clearly differentiate between fear and anxiety (e.g., [1, 16, 63]).

A subsequent qualitative study with  $N=138$  participants explored the complex interplay of antecedents and consequences

of S&P-related emotions [77] based on the circumplex model of affect. The study highlighted various cybersecurity-relevant consequences across behavioural, cognitive and social dimensions, including negative tendencies such as avoidance behaviour, and unfavourable spill-over effects. Notably, positive high-arousal emotions, such as interest, have a positive impact on behavioural tendencies. Additionally, users expressed that security should be enjoyable to foster positive attitudes (including affective ones) and, ultimately, encourage positive behaviours [76]. Acknowledging this need, security and privacy education often incorporates elements of ‘fun’ (e.g., gamification) [8, 68]. Yet, there is still no clear understanding of which aspects truly promote ‘fun’ in the context of cybersecurity and privacy [76]. Prior results, however, highlight social dynamics as one of the major impacting factors on security attitudes and emotions [76, 77].

## 2.2 Social Dimensions of S&P

Das et al. [20] showed that social interactions significantly influence security behaviours, such as adopting secure authentication, updating passwords, and adjusting privacy settings. Their findings highlighted the effect of social triggers, with participants influenced by such interactions being four times more likely to share their behaviour and act as social triggers themselves. Further, Das et al. [23, 24] found that displaying the number of friends who adopted a Facebook security feature increased adoption likelihood. In another study, even non-personal social influence through crowd-sourced suggestions of Facebook users were influential in steering users’ related S&P decisions [46]. Chen et al. [15] extended this work by designing phishing training that fostered social interaction through conversation-based and role-play-based methods. Both approaches improved anti-phishing self-efficacy and participants’ intentions to seek support, reinforcing the value of social interactions in security education. As indicated by this work, social interactions in the form of conversations play a crucial role for shaping cybersecurity-related perceptions, emotions, and behaviours.

Initial research has thus explored how and why people engage in conversations about S&P. Das et al. [22] showed in an interview study that when S&P discussions arise, this is often to warn others, share protection strategies, or seek advice (e.g., when observing novel security tools or configuring new devices). They outline five social triggers that enhance security awareness, motivation, or knowledge: 1) observing others, 2) learning through discussions, 3) pranks and demonstrations, 4) experiencing security breaches, and 5) sharing device access. However, their findings suggest that security experts discussing related topics openly are sometimes perceived as paranoid, leading many to avoid such conversations to prevent being seen as socially inappropriate or preachy. In line with that, a related study by Gerber and Marky [35] found that security experts often hesitate to comment on or

intervene in others' security behaviour due to fear of negative reactions or uncertainty about their moral authority to judge such behaviour.

Rader et al. [61], replicated by Pfeffer et al. [58], demonstrated that stories serve as informal security lessons, influencing attitudes and behaviour. They found that security stories told in home settings are more likely to drive behaviour change than professional contexts, though stories shared by security-savvy individuals are more likely to be retold. In a subsequent analysis Rader and Wash [60] observed that experts and non-experts emphasise different aspects in security narratives: experts focus on attack mechanisms and prevention, while non-experts highlight who executed the attack and their motivations. Combining perspectives from both groups in conversations could address non-experts' knowledge gaps and foster more comprehensive understanding.

Furthermore, Das et al. [25] revealed that security news are typically shared out of responsibility, especially with friends and family, followed by significant others and colleagues. Gender differences emerged, with men being more likely to share security news out of responsibility, while those with lower security behavioural intentions shared news based on observing insecure behaviours. Lopez et al. [48] analysed conversations among security developers on platforms like Stack Overflow, revealing that exchanges increase awareness, enhance knowledge, and provide valuable assistance.

### 2.3 User Engagement

A variety of engagement strategies has been proposed in similar fields, where topics might be perceived as too complex or intimidating by lay users. For example, in mathematics, courses that target collaborative learning [54], enrichment classes that provide hands-on tasks and real-world applications of the topic [49], awareness campaigns that include, e.g., posters, public lectures, or articles in non-expert magazines [39], and gamified apps [45] have been found to increase engagement. Other examples include habit-building budgeting tools, that have been found to increase financial engagement and understanding [11, 33], and simulations that increase civic engagement [6, 67]. Further, storytelling has been found to help making complex topics more approachable and increase engagement in domains such as health policy [80] and environmental science [3]. S&P share similar barriers of perceived complexity and disengagement as those topics, while also carrying great emotional weight and personal risk, often evoking fear or avoidance, which makes engagement particularly challenging.

### 2.4 Implications for this Research

Previous research has demonstrated connections between S&P-related social interactions, perceptions, emotions, and behaviours across various disciplines. For instance, percep-

tions of S&P influence the roles of professionals, such as CISOs, and how they are viewed within organisations [19]. Negative emotions can impact both thinking and motivation to adopt secure practices [58]. Moreover, much of the existing work paints a negative view of S&P, portraying it as complex, fearful, and even mystical [19, 38, 63], with emotions like fear, anxiety, and sadness commonly reported in response to S&P issues [7, 16, 83].

We build on this work and shift the focus towards positive S&P associations, striving to identify pathways to counter negative emotional responses and ultimately increase user engagement and experience in the S&P context. For this, we asked our participants what would make S&P more fun. Fun is a recognised hedonic quality in User Experience (UX) [27] that can help to make complex topics like S&P more approachable. We particularly selected fun as a high-arousal form of enjoyment, as such emotions have been found to foster secure behaviour [77]. By asking what would make S&P *more* fun, we also seek to identify barriers for enjoyment.

Further, while social interactions in the form of conversations, including stories and anecdotes, have been found successful in triggering secure behaviour, research so far has been limited on identifying conversation barriers for S&P expert users. Our study extends prior findings in identifying obstacles and potential facilitators for S&P conversations also among non-expert users. This exploration will lay the groundwork for future research, enabling the development of more holistic human-centred S&P interventions that consider socio-emotional influences and responses.

## 3 Method

We used an online survey hosted on SoSciSurvey with a representative sample of  $N = 496$  U.S. citizens to explore how to make S&P more enjoyable and what facilitates conversations on that context. The sample was recruited via Prolific. All participants were reimbursed with an hourly rate of \$13, based on a 20-minute duration (average time  $M = 19.5$  minutes,  $SD = 8.21$ ,  $Med = 18$ ). We included two simple attention checks. The study was pre-tested with 10 participants who were also recruited via Prolific. The pre-test comments only concerned typos and sentence structure, which we used to refine the survey.

### 3.1 Ethical Considerations

All recommendations for conducting studies with human participants provided by our university's ethics commission were met. We followed their provided checklist and the APA guidelines for ethical psychological research involving humans [5]. As such, all participants were informed about the study purpose and procedure prior to giving their consent. They had the right to withdraw from the study at any time and also to have their data deleted after they had completed the study.

We did not collect personally-identifiable information. All demographic questions were voluntary and age was collected in ranges instead of exact age to further enhance anonymity. All data was stored on German servers that are subject to strict EU data protection law. Participation was voluntarily and participants were reimbursed with an hourly rate of \$13, which exceeded minimum wage in the U.S. at the time the study was conducted and in line with the Prolific platform's recommendations for fair payment<sup>1</sup>.

## 3.2 Procedure

The study comprised six main steps, as visualised in Figure 1. More details and all questions are provided in Appendix A:

*First*, the participants were asked for informed consent.

*Second*, we used open text questions to capture general privacy perceptions. For this, we asked our participants:

- to complete the sentences *Privacy is a topic that...* and *It would be so much more fun to protect my (digital) privacy if...*
- to imagine that (digital) privacy was a person (more specifically, a colleague of theirs) and to provide three character traits they would use to describe this person.
- to indicate how well they protected their privacy, as compared to other people in their social circle, such as their colleagues, friends, or parents, using a slider on a scale ranging from *less* to *more*.

While the first points target at measuring the participants' beliefs, the last point assesses self-reported behaviour [31].

*Third*, we repeated the questions from the second block for IT security.

*Fourth*, we focused on S&P conversations, asking them to indicate how often they talked to other people about: (1) privacy issues, and (2) IT security issues on a scale ranging from "1=very infrequently" to "7=very frequently" with *never* as a fallback option. We then asked the participants to rate different reasons for not talking to others frequently about privacy on a 7-Point Likert scale (with 1=strongly disagree and 7=strongly agree) based on answers given in an interview study on that topic by Gerber and Marky [35]. Then, the participants were asked to finish the sentence *I would talk about privacy much more often with others if...* The last two questions were repeated for IT security.

*Fifth*, we asked about perceptions of S&P-savvy people. We used a 7-Point Likert scale to indicate whether our participants thought that people who used different strategies to protect their S&P, including, e.g., encrypting their devices or refraining from using social media, were paranoid. Again, the answers were selected based on Geber and Marky [35]. This

was followed by the Nerd-Genius scale [70] on people protecting their privacy (in the first question) and their IT security (in the second question). This scale asks about stereotypes typically associated with *nerds* or *geniuses*, such as being socially awkward, obsessed with computers, or gifted in math.

*Sixth*, we asked for several S&P-related and general demographics, using two questions based on Nthala and Flechais [55] to assess S&P skills and security support for other people, the ATI scale [32] to capture technical affinity, the Security Attitude scale (SA-6) [30] to measure security attitudes, the Internet Users' Information Privacy Concerns scale (IUIPC-8) [36, 50] to measure privacy concerns, and the technical sub scale of the Online Privacy Literacy Scale (OPLIS) [73] to assess privacy literacy. Finally, we asked for gender, age, education, and employment status, thanked our participants, and redirected them to Prolific.

## 3.3 Sample

We recruited a sample representative of the adult U.S. population via Prolific. A total of 511 participants completed the questionnaire, of whom 15 were excluded since they failed at least one of the two attention checks. Our final sample thus included 496 participants. Of those, 258 were women, 234 men, 2 agender, and 1 non-binary. For the participants' detailed demographics and skills and attitudes with regard to S&P, the reader is referred to Tables 1 and 2.

## 3.4 Limitations

We conducted a survey study that provided a large, diverse sample, but the qualitative data may not be as rich as that from in-depth interviews. Future studies can enrich our understanding of how S&P are perceived as a concept by pursuing alternative study designs such as interviews or experience sampling. In addition, we relied on self-reported data, which might be affected by social desirability or false recalls. We further focused on the U.S. population, for which Prolific provides the opportunity to recruit a sample that is representative in terms of age, sex, and ethnicity. The S&P perception might be different for people with other cultural backgrounds, since, for example, people in the U.S. may value different aspects in terms of privacy than people in Europe [79]. Furthermore, although balanced in terms of age, sex, and ethnicity, our sample may not be representative with regards to other socio-demographic characteristics, such as being slightly skewed towards users with a Bachelor's degree [13]. This might have influenced our findings, as, for example, individuals with higher education levels have been found to rely less on automated tools for security guidance [62].

<sup>1</sup><https://www.prolific.com/calculator>

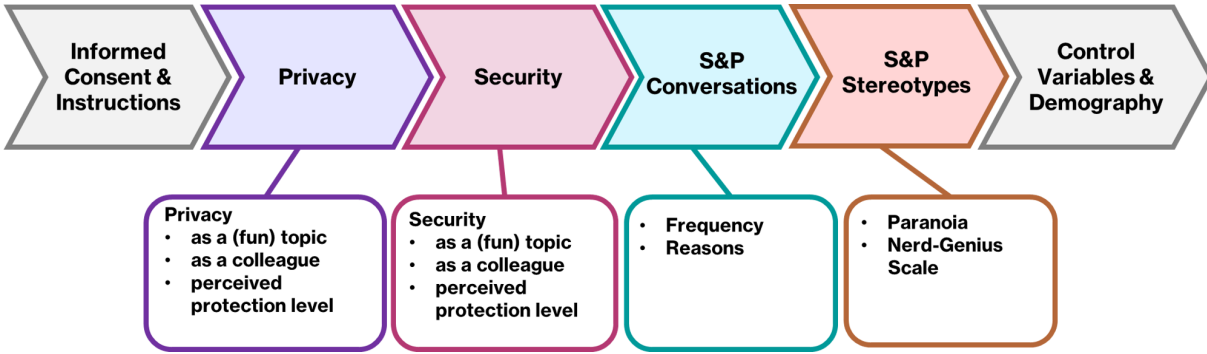


Figure 1: Visualisation of the study procedure.

Age in years: N (%)	Education: N (%)	Employment: N (%)
18-20: 30 (6.1%)	School student: 6 (1.2%)	Employed full time: 182 (36.7%)
21-25: 44 (8.9%)	High School Diploma: 156 (31.5%)	Employed part-time: 64 (12.9%)
26-30: 50 (10.1%)	Bachelor's Degree: 186 (37.5%)	Unemployed and on the lookout: 41 (8.3%)
31-35: 44 (8.9%)	Master's Degree: 78 (15.7%)	Unemployed and not on the lookout: 13 (2.6%)
36-40: 39 (7.9%)	Ph.D. or higher: 21 (4.2%)	Student: 41 (8.3%)
41-45: 42 (8.5%)	Other: 48 (9.7%)	Retired: 66 (13.3%)
46-50: 43 (8.7%)		Homemaker: 20 (4%)
51-55: 42 (8.5%)		Self-employed: 50 (10.1%)
56-60: 64 (12.9%)		Incapacitated for work: 10 (2%)
61-65: 52 (10.5%)		Other: 4 (0.8%)
66-70: 25 (5.0%)		
>70: 2 (4.2%)		

Table 1: Participants' demographic values.

### 3.5 Data Analysis

The open-text responses were analysed using thematic analysis [12]. Two authors initially coded 20% of the responses independently and iteratively developed a codebook. They then discussed and agreed on a unified codebook. Given the simplicity of many responses, such as short text snippets or one-word answers, we followed Ortloff et al.'s recommendations [56]. One author coded all responses using the agreed codebook and added new codes as necessary. The second author reviewed the codings, and noted discrepancies, and the authors then resolved these through discussion, refining the codebook and adding new codes. The first author subsequently re-coded the responses using the updated codebook. The codebook is available in Appendix B.

## 4 Results

This section presents findings on the perceptions of S&P in terms of associations, protection measures, conversations, and stereotypes. We report the frequency of notions for each code with *s* for security-related and *p* for privacy-related notions.

### 4.1 S&P-related Associations

S&P was most often described as **important** ( $s=144$  (29.03%),  $p=226$ , (45.56%)), yet only few participants also found it interesting ( $s=22$  (4.44%),  $p=11$  (2.22%)), e.g.:

*“Security is really uncool but really important.”*  
(P305)

Instead, participants highlighted the **complexity** and overwhelming nature of S&P ( $s=57$  (11.49%),  $p=16$  (3.23%)), and reported feelings of **worry and fear** ( $s=17$  (3.43%),  $p=36$  (7.26%)) in line with previous results [19, 47, 65, 77], e.g.:

*“[Security is a topic that] invokes fear and concern.”*  
(P417); *“[Security is a topic that] sounds scary.”*  
(P159)

For security, these feelings were associated with severe **knowledge and experience gaps** ( $s=83$  (16.73%)) mirroring prior research [47, 65, 77]. Interestingly, hardly any participants reported to have limited privacy knowledge ( $p=4$  (0.81%)). Instead, privacy was described as a **controversial** and thus sensitive topic ( $p=31$  (6.25%)). Although S&P was generally not perceived as particularly engaging, only a small number of participants explicitly characterised it as **uninteresting or boring** ( $s=17$  (3.43%),  $p=11$  (2.22%)), contrary to

S&P skill: N (%)	ATI scale	SA-6	IUIPC-8			OPLIS
			Control	Awareness	Collection	
Novice: 158 (31.9%)	M=3.37	M=3.15	M=5.86	M=6.30	M=5.86	M=3.85
Competent: 308 (62.1%)	SD=1.01	SD=0.95	SD=1.22	SD=1.02	SD=1.20	SD=1.27
Expert: 30 (6%)	Med=3.33	Med=3.17	Med=6.00	Med=7.00	Med=6.25	Med=4.00
	Min=1.11	Min=1.00	Min=1.00	Min=1.00	Min=1.00	Min=0.00
	Max=6.00	Max=7.00	Max=7.00	Max=7.00	Max=7.00	Max=5.00

Table 2: Participants' level of S&P skills and attitudes.

prior assumptions [38], and thus something they do not wish to discuss, e.g.:

*“Security is a topic I am sick of hearing about.”*  
(P192)

Our data showed disagreement about the attention paid to S&P: While privacy was noted as a current **public interest** topic by several participants (p=37), a larger number of participants demanded **greater attention** to S&P (s=63 (12.70%), p=91 (18.35%)) – an obstacle also identified previously [35, 38], stating it should be more frequently discussed (s=22 (4.44%), p=27 (5.44%)) or taken more seriously (s=41 (8.27%), p=64 (12.90%)), e.g.:

*“[Security] gets a lot of publicity, but not enough attention”* (P236); *“If we are not willing to talk openly about [privacy] we will continue to lose it.”*  
(P179)

## 4.2 How to Make S&P Fun

Participants provided several insights on making S&P protection more engaging.

**Simplification** was key to enjoyment, with participants frequently emphasising the need to reduce complexity (s=116 (23.39%), p=103 (20.77%)). In that same vein, many participants blamed **inadequate knowledge** for S&P not being fun (s=89 (17.94%), p=35 (7.06%)), e.g.:

*“It would be more fun to protect my IT security if I learned more about it.”* (P5)

This complexity also contributed to perceptions that S&P was not **accessible** enough to be enjoyable (s=73 (14.72%), p=84 (16.94%)), with participants criticising cumbersome processes and costs (s=20 (4.03%), p=11 (2.22%)).

Participants also expressed a strong desire for enhanced **self-efficacy**, seeking greater control over their data security and visibility online (s=33 (6.65%); p=46 (9.27%)), and highlighting the importance of feeling that their actions could make a meaningful impact (s=26 (5.24%), p=51 (10.28%)), e.g.:

*“If there was tangible proof that my efforts kept my data secure.”* (P467)

Conversely, a substantial proportion of participants viewed the complete **relinquishment of responsibility** for their S&P as the only viable solution (s=75 (15.12%), p=111 (22.38%)). They favoured either reliance on automated systems (s=9, p=16) or the transfer of responsibility to competent peers or institutions such as the government (s=20 (4.03%), p=29 (5.85%)), e.g.:

*“If government and internet providers did more to secure the internet.”* (P473)

Some participants emphasised the emotional dimension, identifying **negative emotions** as a barrier to making S&P enjoyable (s=21 (4.23%), p=24 (4.84%)), e.g.:

*“If it was not talked about in such a doomsday way.”*  
(P185)

Surprisingly, relatively few participants proposed **gamification** or similar engaging methods as a way to enhance the enjoyment of S&P (s=16 (3.23%), p=27 (5.44%)). Still, several participants advocated for **incentives**, including monetary rewards (s=27 (5.44%), p=30 (6.05%)), e.g.:

*“If we got cake every month there were no breaches.”*  
(P317)

Although only a minority, some participants perceived S&P as **too serious** to be made enjoyable (s=8 (1.61%), p=16 (3.23%)), while others felt that **nothing** could make S&P fun (s=20 (4.03%), p=11 (2.22%)).



Figure 2: Character traits associated with privacy.



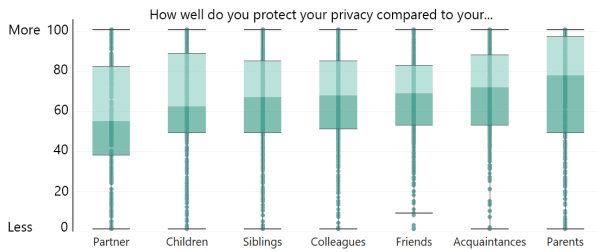


Figure 4: Boxplots showing the data distribution regarding how well participants think they protect their privacy compared to their peers and family.

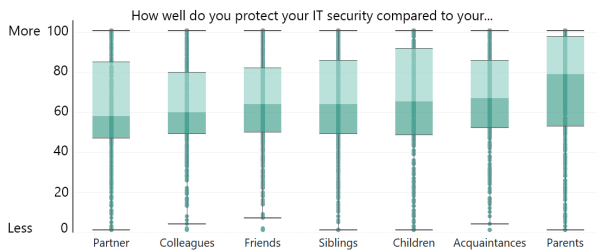


Figure 5: Boxplots showing the data distribution regarding how well participants think they protect their IT security compared to their peers and family.

Figure 6). Common reasons were the lack of relevant conversation starters, perceived complexity, or disinterest from others (see Figures 8 and 7) extending prior literature identifying lack of interest, social aspects, lack of resources/opportunities and lack of legitimacy [35]. However, contrasting results by Gerber and Marky [35], most participants disagreed with the idea that they themselves lacked interest or that they feared negative reactions when raising these topics. Two ANOVAs showed a main effect of self-reported skill level on conversation frequency for privacy ( $F(2, 460) = 13.74, p < .001, \eta_p^2 = .06$ ) and security ( $F(2, 432) = 36.29, p < .001, \eta_p^2 = .14$ ). Post-hoc tests using independent sample t-tests with Bonferroni-Holm corrections revealed that self-identified experts talk more frequently about S&P than participants who consider themselves to be novices or competent, while participants who consider themselves to be competent talk more frequently about S&P than self-identified novices. The detailed results for the post-hoc comparison analyses are provided in Appendix B.

Our qualitative analysis, based on responses to the prompt *I would talk about security/privacy much more often if...*, confirmed the quantitative findings regarding conversation barriers. Such barriers for S&P conversations included **knowledge gaps**. While many participants felt they themselves lacked sufficient knowledge ( $s=140$  (28.23%),  $p=64$  (12.90%)), oth-

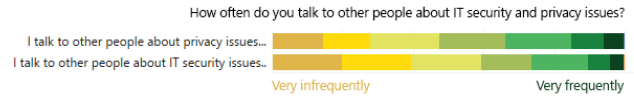


Figure 6: Answers to statements about the frequency with which participants talk to others about privacy and IT security issues.



Figure 7: Answers to statements about reasons for not talking frequently with others about privacy, based on Gerber and Marky [35].

ers felt peers lacked understanding ( $s=33$  (6.65%),  $p=26$  (5.24%)):

*“If they could relate. Sometimes they don’t understand what I’m talking about.”* (P123)

Interestingly, considerably more participants thought others were **not interested** ( $s=63$  (12.71%);  $p=65$  (13.10%)) in the topic than reporting disinterest themselves ( $s=17$  (3.43%),  $p=13$  (2.62%)), e.g.:

*“If others were as interested in the subject as me.”* (P39)

Participants also noted **social norms** ( $s=50$  (10.08%),  $p=80$  (16.13%)), where security and privacy were seen as uncommon topics to address ( $s=30$  (6.05%);  $p=47$  (9.48%)), or only worth discussing with those sharing similar knowledge or interest ( $s=20$  (4.03%);  $p=47$  (9.48%)). For privacy especially, some participants felt it was socially unacceptable to bring it up ( $p=27$  (5.44%)), e.g.:

*“I would talk about privacy more often if it wasn’t taboo.”* (P66)

Additionally, the **perception** of S&P as negative and complex ( $s=33$  (6.65%);  $p=30$  (6.05%)), or uncontrollable and thus futile to discuss ( $s=14$  (2.82%);  $p=18$  (3.63%)) further hindered conversations, e.g.:

*“Just talking about it without being able to do anything is just stressful.”* (P284)

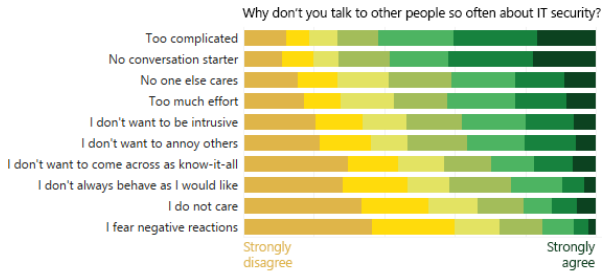


Figure 8: Answers to statements about reasons for not talking frequently with others about IT security, based on Gerber and Marky [35].

Finally, participants highlighted a **need for conversation facilitators** ( $s=104$  (20.97%),  $p=127$  (25-60%)), such as others initiating discussions ( $s=43$  (8.67%),  $p=67$  (13.51%)) or external triggers like media coverage or workplace training ( $s=61$  (12.30%),  $p=60$  (12.10%)).

#### 4.6 S&P Stereotypes

Most participants did **not** perceive individuals who follow basic security practices – such as using antivirus software or regularly updating devices – as **paranoid** (see Figure 9). However, behaviours such as covering device cameras, avoiding social media, reading privacy policies, and encrypting devices were more likely to be viewed as paranoid, reflecting differing connotations associated with security and privacy protection behaviours.

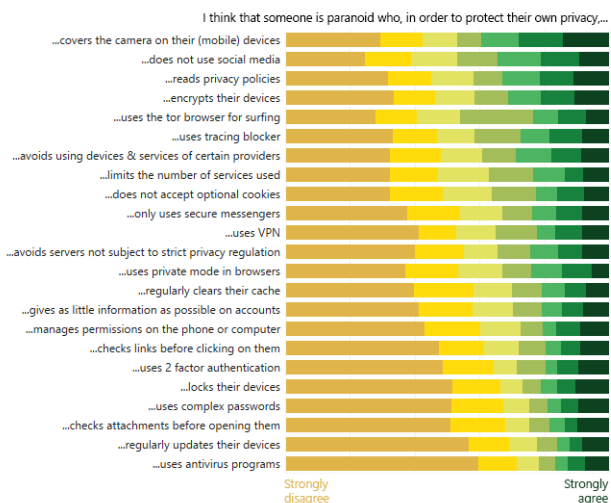


Figure 9: Answers to statements about whether someone is paranoid who uses privacy protection measures, based on Gerber and Marky [35].

Utilising the Nerd-Genius scale [70], we assessed the stereotypes attributed to individuals who actively protect their privacy and security. This scale includes traits associated with both *geniuses* and *nerds*. Participants predominantly associated these individuals with *genius* traits, such as intelligence, genius-level aptitude, computer obsession, and mathematical proficiency (see Figure 10 and 11), again underscoring the perception of S&P as a complex topic that warrants high levels of expertise. The trait 'introvert' from the *nerd* category received the highest agreement, though fewer than 25% strongly or somewhat agreed with this attribution. The results provide a promising foundation for bridging the gap between experts and lay users and fostering a more positive interaction between them.

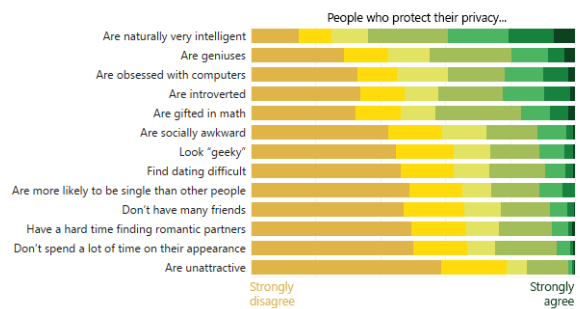


Figure 10: Answers to the Nerd-Genius scale [70] capturing perceptions of people who protect their privacy.

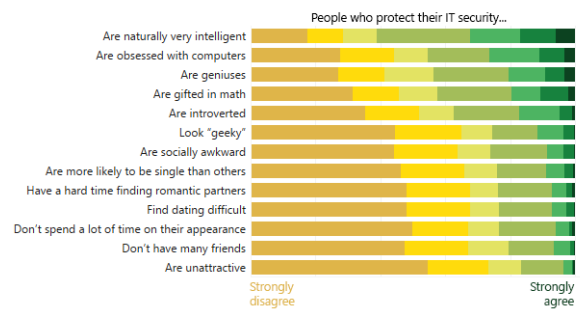


Figure 11: Answers to the Nerd-Genius scale [70] capturing perceptions of people who protect their IT security.

## 5 Discussion

In the following sections, we discuss our overall findings and additional relevant findings and also practical implications with regard to the RQs.

**S&P is perceived as negative yet important.** Consistent with previous studies, our research reveals mixed perceptions of S&P. Participants acknowledged its importance but also found it complex, overwhelming, and frightening, aligning with findings from Renaud et al. [65] and Da Silva and Jensen [19]. This complexity and associated fear underscore the need to address the emotional and social dimensions of S&P research. While fear has been a focus in prior studies [1, 16, 44, 83], efforts to reduce fear and foster positive emotions are still scarce [78]. Our findings on suggested measures for fostering positive user engagement with S&P align with Haney and Lutters' [38] strategies, highlighting trust-building, engaging conversations, and incentivisation. In summary, our findings suggest that S&P needs to be more engaging and enjoyable to address current negative perceptions. While gamification intuitively appears to be a promising solution, perceptions of gamifying S&P were mixed.

**Gamification of S&P topics is ambiguous.** Surprisingly, while gamification is often associated with enhancing user engagement, it was mentioned infrequently by participants. Instead, they emphasised the need for reducing complexity and improving usability. This suggests a greater focus on making S&P solutions more user-friendly rather than simply adding gamified elements. A minority of participants even expressed the view that S&P should not, or cannot, be made fun, indicating that it should not be gamified. This sentiment may reflect concerns about diminishing the seriousness of the topic or deep-seated negative perceptions, suggesting a need for further investigation into these attitudes.

Overall, the results indicate that addressing pragmatic usability aspects – such as efficacy and ease of use – may be more crucial than introducing fun or hedonic elements. Gamification alone may not enhance engagement if underlying usability issues are not resolved. This reflects the distinction between pragmatic usability, which concerns task efficiency, and hedonic usability, which relates to aspects like fun and stimulation [40]. Addressing users' hedonic needs may be ineffective or even counterproductive if basic usability requirements are not met. When users feel stressed or out of control, introducing stimulating elements that elevate arousal could exacerbate negative experiences rather than enhance engagement. Participants' preference for usability improvements over gamification suggests that not all users or S&P contexts may benefit from gamification. Perhaps S&P is not automatically fun when a gamified element is introduced, while it might well be fun in training scenarios. Future research should explore the balance between gamification and usability enhancements, particularly in different S&P scenarios.

Additionally, the desire for more control over personal data versus automation or externalisation of S&P tasks indicates a mixed preference for responsibility management, aligning with Renaud et al.'s [64] findings on de-responsibilisation.

**Security and Privacy are not articulated – but for different reasons.** While participants personally expressed interest in discussing S&P, they assumed that others were disinterested, resulting in a collective silence on the topic.

Privacy discussions were further constrained by social norms and the topic's controversial nature, drawing parallels to politics or religion. Participants feared negative reactions or being perceived as overly cautious, leading them to avoid conversations on privacy even when recognizing its importance. In contrast, security was rarely discussed due to a lack of knowledge rather than controversy. This distinction suggests different barriers to engagement: while privacy discussions are hindered by social discomfort and fear of judgment, security discussions are avoided due to knowledge gaps.

Yet, even though the participants rated their own knowledge and experience levels as low, they consistently perceived their level of protection to be greater than other family members, friends or colleagues. This hints at a potential mismatch between their perceived and their actual level of protection compared to others or the illusory superiority effect [75] manifesting in yet another domain. Participants indicated that S&P would be more engaging if they had more knowledge. This suggests a need for improved S&P education integrated into curricula and for engaging interactive experiences as proposed by Wiederhold [81]. Based on our findings, S&P education measures in school curricula and workplace trainings should use positive formats like role-play to reduce intimidation and build confidence.

**Security advocates are intelligent whereas privacy advocates are paranoid?** By differentiating between security and privacy, our study uncovered distinct perceptions for each construct, highlighting the need to address these differences in both research and organisational measures. Participants perceived security-related measures (e.g., antivirus software, device updates) as less paranoid than privacy-focused actions (e.g., covering cameras, avoiding social media). Notably, security was more frequently associated with intelligence and expertise, while privacy was linked to traits like introversion, discreteness, or secretiveness, reflecting the more personal and intimate nature of privacy concerns.

These findings have implications for organisational S&P initiatives, such as appointing "security champions" or "privacy champions" [34, 37, 72]. While research already established that the approach comes with its own challenges, e.g., related to the selection of appropriate people [9, 34] and lack of management support [37], our research indicates that security as compared to privacy champions might need to be introduced and supported differently. Specifically, privacy champions may need assistance in countering stereotypes that frame privacy-conscious behaviours as overly cautious or secretive and in reinforcing the legitimacy and importance of privacy measures within the organisation. This could involve targeted training, executive endorsement, and strategic

communication to shift organisational perceptions and ensure privacy initiatives receive the same level of recognition and support as security measures. The same likely applies to data protection officers, i.e., the people responsible to advocate for, check compliance with, and consult on privacy-related topics. They might benefit from strategic communication explaining the value of privacy measures beyond mere compliance, e.g., highlighting privacy as a business case for new products or the potential reputation loss and costs associated with data leaks in case of insufficient privacy considerations.

## 5.1 Conclusion & Recommendations

Our findings reveal a surprising and simple way to enhance engagement with S&P through initiating S&P-related conversations. Six key points emerge:

**Fostering positive engagement with S&P.** Consistent with previous research, our study reveals mixed feelings towards S&P. Positive perceptions generally highlight the importance of S&P and associate it with professionalism and intelligence. Conversely, negative perceptions focus on complexity, mysticism, ambiguity, and frustration. This dichotomy suggests that while S&P may be valued on a general level, personal experiences with S&P are often negative. Future work should explore this distinction further, focusing on enabling users to make positive social and emotional experiences with S&P. The framework developed by Faklaris et al. [29] can provide initial guidance on what type of social influence to use in which step of S&P learning and adoption. For example, storytelling might be helpful for raising threat awareness whereas social proof may better support S&P learning. Further, strengthening users' self-efficacy by highlighting the security relevance of everyday actions like device locking or updating and promoting security practices like password managers and 2FA as empowering choices rather than obligatory tasks may help to overcome fears and negative perceptions.

**Integrating S&P conversations into work routines.** Although individuals express a willingness to discuss S&P with peers, they often perceive others as uninterested and lack conversation starters. This gap, also identified by Gerber and Marky for expert users [35], suggests that fostering S&P discussions could be beneficial. Examples of positive effects on S&P behaviours triggered by peer influence through conversations are also summarized by Wu et al. [82]. The workplace presents an opportunity to foster more organic S&P discussions. Initiatives such as workplace S&P meet-ups, public awareness days (e.g., Safer Internet Day), or integrating S&P elements into unexpected settings (e.g., on frequently used office material or informational posters) might stimulate S&P conversations. For example, routine security updates could be utilised as conversation starters, e.g., by encouraging a collective coffee break when updates are installed. In this break,

employees could casually discuss the necessity and benefits of updates and other security measures. Such low-stakes, structured interactions could normalise S&P discussions and reduce perceived barriers.

### **Integrating S&P conversations beyond on-site work places.**

As work does not only happen in classical on-site settings any more and is increasingly intertwined with private life, it is also important to consider remote and private settings. Widely used services such as Google services and apps such as messenger apps or social media platforms offer options for peer-to-peer learning and informal exchange in everyday interactions. For example, private persons as well as remote workers participating in team communications online could be reached through integrated prompts in meetings or chat platforms. In-person discussions in private contexts among friends or family could be triggered through many ways including cybersecurity education in schools, poster campaigns in public settings such as bus stops, or through prompts integrated in everyday objects such as water bottle labels.

### **Making privacy protective practices less paranoid.**

Privacy, in particular, may benefit from a cultural shift within organisations to counteract the view of privacy as “paranoid”. A strong error culture, psychological safety, and visible support from leadership could help reduce shame, and guilt associated with privacy-related mistakes. Likewise, increasing privacy visibility might help in reducing social taboos around the topic, e.g., through media coverage also in entertainment formats, highlighting privacy features in apps and devices, and legal framings that treat privacy as a valuable and achievable goal rather than an abstract ideal.

### **Supporting calibration of perceived vs. actual protection levels.**

Participants tended to overestimate their S&P knowledge compared to others, reflecting the illusory superiority effect [75] or optimism bias [66]. Similar to overestimations in driving ability [26], individuals rated their S&P protection as superior to that of their peers. To address this, providing realistic assessments of one's protection level and incorporating social cues (e.g., social password meters or visibility of friends' security practices) could help align perceptions and motivate improvements in S&P.

### **Fostering interactions between experts and lay users.**

Positive perceptions of S&P-conscious individuals, who were associated with genius but not nerd attributes in our study, point towards untapped potential of facilitating interactions between S&P experts and lay users to leverage expert knowledge more effectively, potentially improving S&P practices privately and within organisations. Positioning S&P professionals as approachable role models could encourage broader engagement and reduce the perceived exclusivity of S&P discussions, which are often confined to expert circles.

## Acknowledgments

This research work has partially been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

## Data Availability Statement

Due to the high sensitivity of survey data with regards to the potential identification of participants, we do not make the data publicly available. Detailed information on the sample, the survey guide, codebook, and exemplary quotes are provided in the Appendix. For further information or access to the original survey data, please contact the authors.

## References

- [1] H. Abroshan, J. Devos, G. Poels, and E Laermans. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, 9:121916–121929, 2021. <https://doi.org/10.1109/ACCESS.2021.3109091>.
- [2] Krishnashree Achuthan, Sugandh Khobragade, and Robin Kowalski. Public sentiment and engagement on cybersecurity: Insights from reddit discussions. *Computers in Human Behavior Reports*, 17:100573, 2025.
- [3] Karolin Andersson, Anneli Sundin, and Robert Watt. Rethinking communication: integrating storytelling for increased stakeholder engagement in environmental evidence synthesis. *Environmental Evidence*, 7(6), 02 2018.
- [4] APA. APA Dictionary of Psychology, 2023. Retrieved 16 February 2023 from: <https://dictionary.apa.org/perception>.
- [5] American Psychological Association. Ethical principles of psychologists and code of conduct. 2016.
- [6] Christine Bachen, Pedro Hernández-Ramos, Chad Raphael, and Amanda Waldron. Civic play and civic gaps: Can life simulation games advance educational equity? *Journal of Information Technology & Politics*, 12, 11 2015.
- [7] Eric Bachura, Rohit Valecha, Rui Chen, and H Raghav Rao. The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter. *MIS Quarterly*, 46(2):881–910, 2022. <https://doi.org/10.25300/MISQ/2022/15596>.
- [8] Ryan J Baxter, D Kip Holderness Jr, and David A Wood. Applying basic gamification techniques to it compliance training: Evidence from the lab and field. *Journal of information systems*, 30(3):119–133, 2016.
- [9] Ingolf Becker, Simon Parkin, and M. Angela Sasse. Finding security champions in blends of organisational culture. In *Proceedings of the 2nd European Workshop on Usable Security*. Internet Society, 2017.
- [10] O. Beris, A. Beutement, and M. A. Sasse. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In A. Somayaji, R. Böhme, P. van Oorschot, and M. Mannan, editors, *Proceedings of the 2015 New Security Paradigms Workshop*, page 73–84, 2015. <https://doi.org/10.1145/2841113.2841119>.
- [11] Paula Bitrián Arcas, Isabel Buil, and Sara Catalán. Making finance fun: the gamification of personal financial management apps. *International Journal of Bank Marketing*, 39:1310–1332, 06 2021.
- [12] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006. <https://doi.org/10.1191/1478088706qp063oa>.
- [13] United States Census Bureau. Census Bureau Releases New Educational Attainment Data, 2023. Retrieved 19th May 2025 from: <https://www.census.gov/newsroom/press-releases/2023/educational-attainment-data.html>.
- [14] AJ Burns, Tom L Roberts, Clay Posey, and Paul Benjamin Lowry. The adaptive roles of positive and negative emotions in organizational insiders’ security-based precaution taking. *Information Systems Research*, 30(4):1228–1247, 2019. <https://doi.org/10.1287/isre.2019.0860>.
- [15] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails: Evidence from a mixed-design experiment. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI ’24, New York, NY, USA, 2024. Association for Computing Machinery.
- [16] Violet Cheung-Blunden, Kiefer Cropper, Aleesa Panis, and Kamilah Davis. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion*, 19(8):1353–1365, 2019. <https://doi.org/10.1037/emo0000508>.

- [17] Kevin Collier. Ransomware attack delays patient care at hospitals across the U.S., 2022. Retrieved 15th November 2022 from: <https://www.nbcnews.com/tech/security/ransomware-attack-delays-patient-care-hospitals-us-rcna50919>.
- [18] Colin Conrad, Jasmine Aziz, Natalie Smith, and Aaron Newman. What Do Users Feel? Towards Affective EEG Correlates of Cybersecurity Notifications. In *NeuroIS Retreat*, pages 153–162. Springer, 2020. [https://doi.org/10.1007/978-3-030-60073-0\\_17](https://doi.org/10.1007/978-3-030-60073-0_17).
- [19] Joseph Da Silva and Rikke Bjerg Jensen. "cyber security is a dark art": The ciso as soothsayer. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), November 2022.
- [20] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. A typology of perceived triggers for End-User security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 97–115, Santa Clara, CA, August 2019. USENIX Association.
- [21] Sauvik Das, Cori Faklaris, Jason I. Hong, and Laura A. Dabbish. The security & privacy acceptance framework (spaf). *Foundations and Trends® in Privacy and Security*, 5(1-2):1–143, 2022.
- [22] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, Menlo Park, CA, July 2014. USENIX Association.
- [23] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the SIGSAC Conference on Computer and Communications Security, CCS '14*, pages 739–749, New York, NY, USA, 2014. Association for Computing Machinery. <https://doi.org/10.1145/2660267.2660271>.
- [24] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. The role of social influence in security feature adoption. In *Proceedings of the Conference on Computer Supported Cooperative Work & Social Computing, CSCW '15*, pages 1416–1426, New York, NY, USA, 2015. Association for Computing Machinery. <https://doi.org/10.1145/2675133.2675225>.
- [25] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. Breaking! A typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18*, pages 1–12, New York, NY, USA, 2018. Association for Computing Machinery.
- [26] David M DeJoy. The optimism bias and traffic accident risk perception. *Accident Analysis & Prevention*, 21(4):333–340, 1989. [https://doi.org/10.1016/0001-4575\(89\)90024-9](https://doi.org/10.1016/0001-4575(89)90024-9).
- [27] Sarah Diefenbach, Nina Kolb, and Marc Hassenzahl. The 'hedonic' in human-computer interaction: history, contributions, and future research directions. In *Proceedings of the 2014 Conference on Designing Interactive Systems, DIS '14*, page 305–314, New York, NY, USA, 2014. Association for Computing Machinery.
- [28] Pardis Emami Naeini, Martin Degeling, Lujó Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghghat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), 11 2018.
- [29] Cori Faklaris, Laura Dabbish, and Jason I. Hong. A framework for reasoning about social influences on security and privacy adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, CHI EA '24*, New York, NY, USA, 2024. Association for Computing Machinery.
- [30] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. A Self-Report measure of End-User security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 61–77, Santa Clara, CA, August 2019. USENIX Association. <https://www.usenix.org/conference/soups2019/presentation/faklaris>.
- [31] M. Fishbein and Icek Ajzen. *Belief, attitude, intention and behaviour: An introduction to theory and research*. Addison-Wesley, Reading, MA, 1975.
- [32] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human-Computer Interaction*, 35(6):456–467, 2019. <https://doi.org/10.1080/10447318.2018.1456150>.
- [33] Veronica Frisancho, Alejandro Herrera, and Silvia Prina. Can a mobile-app-based behavioral intervention teach financial skills to youth? experimental evidence from a financial diaries study. *Journal of Economic Behavior & Organization*, 214:595–614, 2023.
- [34] Trevor Gabriel and Steven Furnell. Selecting security champions. *Computer Fraud & Security*, 2011(8):8–12, 2011.
- [35] Nina Gerber and Karola Marky. The nerd factor: The potential of S&P adepts to serve as a social

- resource in the user's quest for more secure and Privacy-Preserving behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 57–76, Boston, MA, August 2022. USENIX Association. <https://www.usenix.org/conference/soups2022/presentation/gerber>.
- [36] Thomas Groß. Validity and reliability of the scale internet users' information privacy concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies*, 2021:235–258, 2021.
- [37] Marco Gutfleisch, Markus Schöps, Stefan Albert Horstmann, Daniel Wichmann, and M Angela Sasse. Security champions without support: Results from a case study with owasp samm in a large-scale e-commerce enterprise. In *Proceedings of the 2023 European Symposium on Usable Security*, pages 260–276, 2023.
- [38] Julie M. Haney and Wayne G. Lutters. "it's Scary... It's Confusing... It's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 411–425, Baltimore, MD, August 2018. USENIX Association.
- [39] Vagn Lundsgaard Hansen. Popularizing mathematics: from eight to infinity, 2003. <https://arxiv.org/abs/math/0305019>.
- [40] Mark Hassenzahl. The hedonic/pragmatic model of user experience. In Effie Law, Arnold Vermeeren, Marc Hassenzahl, and Mark Blythe, editors, *Towards a UX manifesto. COST294-MAUSE affiliated workshop*, volume 10, pages 10–14, 3rd September 2007, Lancaster, UK, 2007.
- [41] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Durmuth, Yixin Zou, and M. Angela Sasse. Digital Security — A Question of Perspective A Large-Scale Telephone Survey with Four At-Risk User Groups . In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 697–716, Los Alamitos, CA, USA, May 2024. IEEE Computer Society.
- [42] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. A world full of privacy and security (mis)conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.
- [43] Alice M Isen. Toward understanding the role of affect in cognition. In Jr. R. S. Wyer and T. K. Srull, editors, *Handbook of Social Cognition*, volume 3, pages 179—236. Lawrence Erlbaum Associates Publishers, 1984.
- [44] Allen C Johnston and Merrill Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3):549–566, 2010. <https://doi.org/10.2307/25750691>.
- [45] Noizzie Jutin and Siti Maat. The effectiveness of gamification in teaching and learning mathematics: A systematic literature review. *International Journal of Academic Research in Progressive Education and Development*, 13(1), 02 2024.
- [46] Isadora Krsek, Kimi Wenzel, Sauvik Das, Jason I. Hong, and Laura Dabbish. To self-persuade or be persuaded: Examining interventions for users' privacy setting selection. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.
- [47] Oksana Kulyk, Karen Renaud, and Stefan Costica. People want reassurance when making privacy-related decisions—not technicalities. *Journal of Systems and Software*, 200:111620, 2023. <https://doi.org/10.1016/j.jss.2023.111620>.
- [48] Tamara Lopez, Thein Tun, Arosha Bandara, Levine Mark, Bashar Nuseibeh, and Helen Sharp. An anatomy of security conversations in stack overflow. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)*, pages 31–40. IEEE, 2019.
- [49] Sofya Lyakhova and Andrew Neate. Engagement and online mathematics enrichment for secondary students. *Teaching Mathematics and its Applications: An International Journal of the IMA*, 43(3):224–245, September 2024.
- [50] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004. <https://doi.org/10.1287/isre.1040.0032>.
- [51] Leonard L Martin, David W Ward, John W Achee, and Robert S Wyer. Mood as input: People have to interpret the motivational implications of their moods. *Journal of Personality and Social Psychology*, 64(3):317–326, 1993. <https://doi.org/10.1037/0022-3514.64.3.317>.
- [52] John McAlaney and Vladlena Benson. Cybersecurity as a social phenomenon. In Vladlena Benson and John Mcalaney, editors, *Cyber influence and cognitive threats*, pages 1–8. Elsevier, 2020.

- [53] U. Menges, J. Hielscher, A. Buckmann, A. Kluge, M. A. Sasse, and I. Verret. Why IT Security Needs Therapy. In S. Katsikas, C. Lambrinouidakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, and M. A. Sotelo Monge, editors, *Lecture Notes in Computer Science. Computer Security. ESORICS 2021 International Workshops Vol. 13106*, page 335–356, 2022. [https://doi.org/10.1007/978-3-030-95484-0\\_20](https://doi.org/10.1007/978-3-030-95484-0_20).
- [54] Nagham Mohammad, Mihai Nica, Kimberly Levere, and Rachel Okner. Promoting engagement via engaged mathematics labs and supportive learning. *International Electronic Journal of Mathematics Education*, 18(2):em0732, 04 2023.
- [55] Norbert Nthala and Ivan Flechais. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 63–82, Baltimore, MD, August 2018. USENIX Association.
- [56] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. Different researchers, different results? analyzing the influence of researcher experience and data type during qualitative analysis of an interview and survey study on security advice. In *Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI '23*, New York, NY, USA, 2023. Association for Computing Machinery.
- [57] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 319–338, Santa Clara, CA, August 2019. USENIX Association.
- [58] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 1–18, Boston, MA, August 2022. USENIX Association. <https://www.usenix.org/conference/soups2022/presentation/pfeffer>.
- [59] Jakub Przetacznik and Simona Tarpova. Russia's war on Ukraine: Timeline of cyber-attacks. Technical Report March, European Parliament, 2022. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS\\_BRI\(2022\)733549\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf) Accessed 5 April 2023.
- [60] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 12 2015.
- [61] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS 2012*, New York, NY, USA, 2012. Association for Computing Machinery.
- [62] 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, CCS '16*, page 666–677, New York, NY, USA, 2016. Association for Computing Machinery.
- [63] Karen Renaud and Marc Dupuis. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*, pages 42–56, Costa Rica, 2019. <https://doi.org/10.1145/3368860.3368864>.
- [64] Karen Renaud, Stephen Flowerday, and Karl van der Schyff. Uncertainty in cyber de-responsibilisation. *Computer Fraud & Security*, 2021(8):13–19, 2021. [https://doi.org/10.1016/S1361-3723\(21\)00086-5](https://doi.org/10.1016/S1361-3723(21)00086-5).
- [65] Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1):1–17, 2021. <https://doi.org/10.1057/s41599-021-00746-5>.
- [66] Tali Sharot. The optimism bias. *Current Biology*, 21(23):R941–R945, 2011. <https://doi.org/10.1016/j.cub.2011.10.030>.
- [67] Kelly Siegel-Stechler and Gretchen Gee. Political and international affairs simulations and college students' civic development. *International Studies Perspectives*, 24(2):115–127, 2023.
- [68] Mario Silic and Paul Benjamin Lowry. Using design-science based gamification to improve organizational security training and compliance. *Journal of management information systems*, 37(1):129–161, 2020.
- [69] SUSAN Squires and MOLLY Shade. People, the weak link in cyber-security: Can ethnography bridge the gap? In *Ethnographic Praxis in Industry Conference Proceedings*, pages 47–57. Wiley Online Library, 2015. <https://doi.org/10.1111/1559-8918.2015.01039>.

- [70] Christine R. Starr. “I’m Not a Science Nerd!”: STEM Stereotypes, Identity, and Motivation Among Undergraduate Women. *Psychology of Women Quarterly*, 42(4):489–503, 2018. <https://doi.org/10.1177/0361684318793848>.
- [71] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, 07 2021. <https://doi.org/10.2478/popets-2021-0049>.
- [72] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21, New York, NY, USA, 2021. Association for Computing Machinery.
- [73] Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. Do People Know About Privacy and Data Protection Strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In Serge Gutwirth, Ronald Leenes, and Paul de Hert, editors, *Reforming European Data Protection Law*, pages 333–365. Springer Netherlands, Dordrecht, 2015. [https://doi.org/10.1007/978-94-017-9385-8\\_14](https://doi.org/10.1007/978-94-017-9385-8_14).
- [74] P. van Schaik, K. Renaud, C. Wilson, J. Jansen, and J. Onibokun. Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, 90:101651, 2020. <https://doi.org/10.1016/j.cose.2019.101651>.
- [75] N Van Yperen, BP Buunk, and J Van der Pligt. Illusoire superioriteit: Het verband met het belang en van de verificerbaarheid van de vergelijkingsdimensies [illusory superiority: The relation with importance and verifiability of comparison dimensions]. *Fundamentele Sociale Psychologie*, 5:186–200, 1991.
- [76] Alexandra von Preuschen, Carolin Benda, Monika Christine Schuhmacher, and Verena Zimmermann. Fear, fun or none: A qualitative quest towards unlocking cybersecurity attitudes. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI ’25, New York, NY, USA, 2025. Association for Computing Machinery.
- [77] Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. Beyond fear and frustration - towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 623–642, Philadelphia, PA, August 2024. USENIX Association.
- [78] Alexandra von Preuschen, Verena Zimmermann, and Monika Schuhmacher. How do you Feel about Cybersecurity? – A Literature Review on Emotions in Cybersecurity. In Nina Gerber and Verena Zimmermann, editors, *Proceedings of the International Symposium on Technikpsychologie (TecPsy)*. Sciendo, 2023. <https://sciendo.com/book/9788366675896>.
- [79] James Q. Whitman. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal*, 113(6):1151–1221, 2004.
- [80] Corrie Whitmore and Kathryn Schild. Exploring complex concepts through storytelling: A synchronous online health policy course case study and recommendations for implementing across disciplines. *Open Praxis*, 14:242–248, 09 2022.
- [81] Brenda K Wiederhold. Increasing cybersecurity through emotional engagement. *Cyberpsychology, Behavior and Social Networking*, 24(9):579–580, 2021. <https://doi.org/10.1089/cyber.2021.29224.editorial>.
- [82] Yuxi Wu, W. Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879, 2022.
- [83] Xiaochen Angela Zhang and Jonathan Borden. How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 23(10):1336–1352, 2020. <https://doi.org/10.1080/13669877.2019.1646315>.

## A Survey

### Informed Consent for participating in a scientific study on IT security and privacy

Thank you for your interest in our study on IT security and privacy! Before you start, we would like to provide you with some more information: The German Research Association requires explicit consent to voluntarily participating in empirical research. Therefore, we kindly ask you to read the following information on the study, and to confirm the informed consent statement below if you agree to participate. In this study, you will answer some questionnaires and provide some personal information. Completing the study will take approximately 20 minutes. Your participation will be compensated with the amount indicated on the Prolific platform. The collected data (questionnaire responses, demographic information) will only be used for research purposes. Participants in this study will not be exposed to any risk greater than that experienced in everyday life. You can abort the study at any time if you wish without having to provide a reason. All data collected until then will be deleted.

### Data protection

The data collection and handling in this study are in accordance with the European General Data Protection Regulation (GDPR) .

The data will only be used for the purposes stated in this informed consent and not be forwarded to a third party for any other purpose. Within this study the following types of data will be collected:

- questionnaire responses, and
- demographic information

As demographic information we will collect:

- gender,
- age (in groups),
- education,
- occupation, and
- experience with IT security and privacy

#### Confidentiality

The collected data will only be used for research and publication purposes (e.g., a scientific journal) in an aggregated (e.g., as means) and anonymized form. Demographic information such as age and gender do not permit inference to you as a person. At no point in time will we store your name or other definite information.

#### Data storage

The collected data will be handled by researchers at Technische Universität Darmstadt, Germany. As soon as the research purpose allows it, we will delete all personal data or store it separately from the rest of your answers respectively. Possibly provided personal information will be replaced by a placeholder. The data will be stored in an anonymised form.

#### Voluntariness & Rights of the Participants

Answering the questions of this study and agreeing to the analysis of your data (especially the collection, storage and publication) is voluntary. You have the right to abort the study any time, to refuse participation, to be informed about the personal data we store and to have the personal data corrected, limited or deleted if you wish. You can revoke the handling of your personal data any time, without this having an influence on the legitimacy on the data analysis done until the moment of revocation. To revoke your agreement please inform the contact person named below verbally or in written form. You also have the right on data portability and the right to complain to a regulator. If you have read and understood the information, and agree to participate in the study, please tick the box next to the agreement below.

I hereby confirm that I have read and understood the information on this study, want to take part in the study and agree to the designated handling of personal data (especially the data collection, storage and publication).

If you have an questions or concerns please contact: [Contact details of the authors]

#### Survey Items

Please finish the following sentences. Just complete the sentence in the way that comes to your mind first, there are no right or wrong answers. We are interested in your personal associations with this topic.

1. Privacy is a topic that...[text field]
2. It would be so much more fun to protect my (digital) privacy if...[text field]

3. Imagine (digital) privacy was a person, or more precisely, a colleague of yours. Which three character traits would you use to describe him or her? Please use one line per character trait.

text field

text field

text field

1. How would you define privacy? [text field]
2. What is important to you in terms of your privacy? [text field]
1. How well do you protect your privacy compared to...  
Please answer the question only in relation to such people who are in your life, i.e. if you do not have any siblings, please just do not make any statement in relation to your siblings. [Visual analogue scale from 1="less" to 101="more"; randomised order]
  - (a) ...your children?
  - (b) ...your acquaintances?
  - (c) ...your colleagues?
  - (d) ...your parents?
  - (e) ...your siblings? your partner?
  - (f) ...your friends?

Please finish the following sentences. Just complete the sentence in the way that comes to your mind first, there are no right or wrong answers. We are interested in your personal associations with this topic.

1. IT Security is a topic that...[text field]
2. It would be so much more fun to protect my IT security if...[text field]
3. Imagine IT security was a person, or more precisely, a colleague of yours. Which three character traits would you use to describe him or her? Please use one line per character trait.

text field

text field

text field

1. How well do you protect your IT security compared to...  
Please answer the question only in relation to such people who are in your life, i.e. if you do not have any siblings, please just do not make any statement in relation to your siblings. [Visual analogue scale from 1="less" to 101="more"; randomised order]
  - (a) ...your children?
  - (b) ...your acquaintances?
  - (c) ...your colleagues?
  - (d) ...your parents?
  - (e) ...your siblings?
  - (f) ...your partner?
  - (g) ...your friends?

1. How often do you talk to other people about IT security and privacy issues?
  - (a) I talk to other people about privacy issues...[7-point Likert-like scale from 1="very infrequently" to 7="very frequently"; fallback option="never"]
  - (b) I talk to other people about IT security issues...[7-point Likert-like scale from 1="very infrequently" to 7="very frequently"; fallback option="never"]
2. In case you do not talk very frequently to others about privacy: Why don't you talk to other people so often about privacy? [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order; based on the results from [35]]
  - (a) Because it is too much effort
  - (b) Because I don't want to come across as know-it-all
  - (c) Because no one else cares
  - (d) Because I do not care
  - (e) Because I don't always behave as I would like in this area
  - (f) Because I don't want to annoy others
  - (g) Because I fear negative reactions
  - (h) Because I don't want to be intrusive
  - (i) Because there are no opportunities for this to serve as a conversation starter
  - (j) Because it is too complicated
  - (k) other: [text field]
3. I would talk about privacy much more often with others if...[text field]
4. In case you do not talk very frequently to others about IT security: Why don't you talk to other people so often about IT security? [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order; based on the results from [35]]
  - (a) Because it is too much effort
  - (b) Because I don't want to come across as know-it-all
  - (c) Because no one else cares
  - (d) Because I do not care
  - (e) Because I don't always behave as I would like in this area
  - (f) Because I don't want to annoy others
  - (g) Because I fear negative reactions
  - (h) Because I don't want to be intrusive
  - (i) Because there are no opportunities for this to serve as a conversation starter
  - (j) Because it is too complicated
  - (k) other: [text field]
5. I would talk about IT security much more often with others if...[text field]
6. It is important you pay attention to the statements. Please agree by choosing "strongly agree". [[7-point Likert scale, 1="strongly disagree", 7="strongly agree"]
  - (a) I'm paying attention to the questions in this questionnaire. I confirm this by choosing "strongly agree".
1. I think that someone is paranoid who, in order to protect their own privacy...[7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order; based on the results from [35]]
  - (a) ...uses private mode in browsers.
  - (b) ...encrypts their devices.
  - (c) ...covers the camera on their (mobile) devices.
  - (d) ...uses 2 factor authentication.
  - (e) ...only uses messengers that are considered secure.
  - (f) ...avoids to use the devices and services of certain providers.
  - (g) ...avoids having private data stored on servers that are not subject to strict privacy regulation.
  - (h) ...checks attachments before opening them.
  - (i) ...uses the tor browser for surfing.
  - (j) ...uses complex passwords.
  - (k) ...uses tracing blocker.
  - (l) ...regularly updates their devices.
  - (m) ...does not use social media.
  - (n) ...reads privacy policies.
  - (o) ...checks links before clicking on them.
  - (p) ...locks their devices when they are not using them.
  - (q) ...gives as little information as possible on user accounts.
  - (r) ...manages permissions on the phone or computer.
  - (s) ...uses antivirus programs.
  - (t) ...uses VPN.
  - (u) ...does not accept optional cookies.
  - (v) ...regularly clears their cache.
  - (w) ...limits the number of services used.
1. Nerd-Genius scale [70]: What do you think about people who protect their privacy? [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order]
1. How would you rate your general skills in computer security and privacy (e.g., understanding threats, vulnerabilities, and countermeasures)? [single choice; based on [55]]
  - (a) Novice
  - (b) Competent
  - (c) Expert
2. Assuming you believe each of the following to be less competent than you in data security, if they ask you for advice or help with data security, how likely are you to offer it? [7-point Likert-like scale, 1="Very unlikely", 7="Very likely"; randomised order; ; based on [55]]
  - (a) Relative
  - (b) Friend

- (c) Work colleague
  - (d) Others
3. ATI scale [32] [6-point Likert scale, 1=“strongly disagree”, 6=“strongly agree”; randomised order]
  4. SA-6 [30] [5-point Likert scale, 1=“strongly disagree”, 5=“strongly agree”; randomised order]
  5. IUIPC-8 [36, 50] [7-point Likert scale, 1=“strongly disagree”, 7=“strongly agree”; randomised order]
  6. To confirm that you are paying attention to the questions in the questionnaire, please select the second option from the left on the scale. [7-point Likert scale, 1=“strongly disagree”, 7=“strongly agree”]
    - (a) Paying attention to the questions in this questionnaire is important. I agree by choosing the second option from the left of the scale.
  7. OPLIS technical scale [73]: In the following you will find different questions about the Internet. Some of the questions are not easy to answer, in order to be able to assess as many people as possible with different levels of knowledge. Therefore, it is not a big deal if you do not know an answer. In that case, simply select “Don’t know”.

#### Demographic Information

1. With which gender do you identify most? [single choice]
  - (a) female
  - (b) male
  - (c) other
  - (d) prefer not to say
2. How old are you? [single choice]
  - (a) 18-20 years
  - (b) 21-25 years
  - (c) 26-30 years
  - (d) 31-35 years
  - (e) 36-40 years
  - (f) 41-45 years
  - (g) 46-50 years
  - (h) 51-55 years
  - (i) 56-60 years
  - (j) 61-65 years
  - (k) 66-70 years
  - (l) 71-75 years
  - (m) 76-80 years
  - (n) >80 years
  - (o) Prefer not to say
3. What is your highest degree of education? [single choice]
  - (a) School student
  - (b) High School Diploma
  - (c) Bachelor’s Degree
  - (d) Master’s Degree
  - (e) Ph.D. or higher
  - (f) Other, namely: [text field]
  - (g) Prefer not to say
4. What describes your current employment status best? [single choice]
  - (a) employed full time
  - (b) employed part-time
  - (c) unemployed and on the lookout
  - (d) unemployed and not on the lookout
  - (e) student
  - (f) retired
  - (g) homemaker
  - (h) self-employed
  - (i) incapacitated for work
  - (j) other:[text field]
  - (k) Prefer not to say

Thank you for completing this questionnaire!  
 We would like to thank you very much for helping us.  
 Your answers were transmitted. We will now redirect you to Prolific.

## B Online Appendix

This article is supplemented by an Online Appendix that provides details on the character traits associated with security and privacy, the codebook, and the statistical analyses results on OSF: <https://osf.io/z7hsj/files/osfstorage/68346bfd8ae20e827053930b>.