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

Nina Gerber, *Technical University of Darmstadt;*
Karola Marky, *Leibniz University Hannover and University of Glasgow*

https://www.usenix.org/conference/soups2022/presentation/gerber

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

Nina Gerber
Technical University of Darmstadt

Karola Marky
Leibniz University Hannover, University of Glasgow

Abstract

There are several ways to inform individuals about secure and privacy-preserving behavior in private social environments. Experts who are versed in security and privacy (S&P), who might be social peers, such as family members or friends, can provide advice or give recommendations. In this paper, we specifically investigate how S&P adepts inform peers in their private social environment about security and privacy. For this, we first conducted thirteen in-depth interviews with S&P adepts, revealing 1) their own S&P behavior and strategies in their personal lives, 2) obstacles in S&P conversations with peers, 3) situations in which S&P adepts intervene in the behavior of others, and 4) the perception of S&P adepts and stereotypes. Based on the interview results, we conducted three co-design workshop sessions with S&P adepts to explore options to better support S&P adepts informing their peers about secure and privacy-preserving behavior.

1 Introduction

In 2022, more than 22 years after Adams and Sasse's seminal paper "Users are not the enemy" [3], many users are still struggling to protect their IT security and privacy (S&P). Those of us who are relatively well versed in the subject know that users are indeed not the enemy, but we still struggle to help users in their efforts. Accordingly, while many researchers and developers are engaged in understanding lay users' mental models and developing tools to help them protect their S&P; direct, interpersonal one-on-one help or influence among friends and family rarely happens.

Yet, from investigations in other domains, such as general technology support [52], home security [51, 54], or professional contexts [38, 62, 63], we learned that help from knowledgeable peers has a high potential to impact the behavior of lay users positively. The idea of helping lay users through the social influence of people with technical backgrounds is not novel: In 2012, Lipford and Zurko [48] proposed a new paradigm for influencing people to behave securely. Instead of focusing on the usability of security tools, they argued for using social processes (e.g., building a security "neighborhood watch") where people from a user's social network watch over their security decisions. Four years later, Redmiles et al. [56] stated that people with technical backgrounds should be supported in responding to security advice requests from their peers, since even a small set of essential security advice might have a large possible impact on lay users.

Still, little research has been conducted in this area to date. Findings from related studies tend to suggest that tech-savvy individuals have little interest in actively intervening in the security and privacy behavior of their social environment [52]. Our research addresses this issue and seeks to determine what barriers underlie this and how those can be overcome.

Our goal is to (1) investigate the status quo of S&P support-giving in the private context (i.e., when, how and why do S&P adepts (not) support people in their private social environment), and (2) explore options to overcome existing barriers. To this end, we first conducted in-depth interviews with 13 S&P adepts, i.e., people who are fairly versed in IT security and privacy. Building on the results, we then conducted three co-creation workshops with another 11 S&P adepts.

We find that S&P adepts only try to educate people from their social environment about S&P with whom they have a close social relationship. This may be because a trusting relationship is essential for S&P adepts to feel able to address what they consider to be a sensitive topic, where the interlocutor may quickly feel criticized or lectured. Unsolicited advice is given mainly for S&P issues that require explicit interaction, such as passwords. One reason for this could be that for more complex technical issues a common terminology has

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

to be found first, and S&P adepts often have to struggle with users having wrong mental models of what they are trying to explain to them. Opportunities to promote exchange between experts might help them to build a better knowledge foundation for promising approaches in assisting lay users. Finally, we learned that S&P adepts require possibilities to improve their knowledge further (e.g., through open access publications) and that rewards might motivate them, such as recognizing support-giving as a professional achievement. Our paper makes the following contributions:

- We provide an in-depth investigation of S&P knowledge exchange and support between S&P-savvy individuals and their peers in a social context.
- We explore several avenues to overcome existing barriers to S&P support.
- We provide recommendations for S&P adepts and the research community that help to facilitate the development of S&P adepts as a social resource for the improvement of users' S&P behavior.

2 Related Work

To set the scene for our work, we report research about the social influence on S&P behavior, social support and S&P advice, as well as the perspective of S&P experts.

2.1 Social Influence on S&P Behavior

The role of social influence on people's S&P behavior has been extensively investigated by Das et al. [12–16]. They conducted a survey to investigate triggers that impact S&P behavior [12], and found that 39% of the triggers were social. The reported sharing rates were rather low and reasons included perceived obligations to protect others and noticing insecure actions. Primary reasons for not sharing were lack of desire and that others did not need to know about one's S&P practices. Das et al. [13] further explored under which circumstances and for which purposes people talk about S&P with others. Their results confirmed that social interactions, e.g., observing others, were powerful triggers for improving S&P behavior. Reasons for starting S&P conversations either focus on warning others or seeking advice. However, S&P experts are often considered paranoid, "hyper-secure", and behaving "above and beyond" (p.153) [13], a finding that has also been shown in previous studies, e.g., email encryption was considered paranoid [32]. Many security-savvy participants avoided the topic since they worried about being socially inappropriate or, e.g., too preachy [13]. This suggests a large untapped potential: if we better understand how S&P adepts can be motivated to share their knowledge with their social environment, this in turn, could act as an effective trigger to improve the S&P behavior of less tech-savvy individuals. This paper represents a first step towards achieving this goal. In a subsequent survey study, Das et al. [16] focused on sharing S&P news. They found S&P experts want to share news, e.g., because they feel responsible. In two large-scale studies, Das et al. [14, 15] found that people were influenced by their (Facebook) friends in both directions when adopting or rejecting security features.

Other studies focus on social influence in the privacy context [2, 10, 22]. E.g., Emami-Naeini et al. [22] found in a vignette study with MTurkers that friends denying data collection, and privacy experts allowing data collection mostly influenced people's decisions when interacting with IoT devices. Social influence has also been proven effective in the nudging context, i.e., stating that a minority of users like themselves had accepted cookie use could nudge participants away from accepting cookies [10]. A very recent study by Krsek et al. [45] showed that that non-personal social influence has a high potential to motivate users to apply settings different from the defaults offered by Facebook.

A recent interview study shows that implicit social privacy norms on social media among young adults [55] exist. Yet, sanctions that follow violations are mostly indirect, nonconfronting and consequently offer no possibility for violators to learn. Our participants may be particularly affected by this, as it can be assumed that they have particularly strict norms. Thus, they could benefit from solutions that address this issue, and, at the same time, add value to society as a whole by shifting the general social norms towards greater privacy protection.

2.2 Social Support and S&P Advice

Prior work showed that people rely on their social network for general tech and S&P support [18, 27, 29, 46, 51, 52, 56]. Using a combination of semi-structured interviews and a survey, Nthala and Flechais [51] found that users often seek advice or technical help from others they perceive as competent and trustworthy, mostly family and friends. Further, security support is sometimes delegated and occasionally knowledgeable participants offer unsolicited support, e.g., when noticing insecure behavior. Based on these findings, we chose to focus on relatives and friends as receivers of S&P support, and also include questions about responsibility, advice seeking, and intervening.

Two studies of privacy advice sharing among developers on online platforms (e.g., "Stack Overflow") show that privacy-related conversations are mostly motivated by external events, e.g., updates that require actions from developers [47] and advice is mostly shared as links to official documentation [63].

Poole et al. [52] conducted semi-structured interviews to investigate why and how tech-savvy people provide support for social peers. Usually, tech-savvy people are approached unsolicited and quickly gain a reputation. While most participants were happy to support as teenagers, it became increasingly difficult as they got older. Still, they continued to provide support based on a sense of obligation which inspired our work. Consequently, we focus on (1) how to facilitate S&P behavior among people who are closest in our participants' social network, and (2) how this behavior influences the various aspects of the social relationship. Regarding security, Poole et al.'s participants reported engaging in "digital housekeeping" when visiting family members, e.g., updating software. Although helpers did not promote to be experts, they tried preserving that image by avoiding situations in which they cannot help. We also pick up on this in our interview guide.

In a representative US-survey, Redmiles et al. [56] found people with higher skills to be more likely to get S&P advice from work, whereas others get it from family, friends, and service providers. Fagan et al. [23] found that when deciding about whether to follow security advice, people tend to focus on individual aspects rather than social ones. Further, self-rated security expertise does not make a good predictor for security behavior, which we considered in our recruitment process.

Forget et al. [27] combined behavioral and configuration data with interviews with mostly older adults. System maintenance, including security, was often outsourced to "residual experts", usually family members. However, those were not always experts and sometimes had erroneous problem interpretations, leading to serious security threats. In another interview study with older adults, Frik et al. [29] confirmed that security and privacy settings are often delegated to others, like family or community members or technical experts.

2.3 The Perspective of S&P Experts

Few studies address the behavior and judgment of experts with respect to helping ordinary users in their S&P efforts. Ion et al. [41] compared security practices of experts and non-experts in a study combining interview and survey data. Not surprisingly, they found experts to show better security practices than non-experts. Further, non-expert users need advice with installing updates, password managers, and two-factor authentication (2FA). In a recent replication study, Busse et al. [7] identified password security, 2FA, links, attachments, and updates as topics that primarily call for expert advice.

Haney and Lutters [39] conducted interviews with security advocates, i.e., individuals who professionally promote security practices. An important aspect of this task is establishing trust. Tahaei et al. [62] investigated privacy-savvy developers in their professional context, identifying motivations, challenges, and strategies to promote privacy-friendly development. Collaborative solutions and guidelines from companies were identified as promising solutions. While Haney and Lutters [39] investigated professionals interacting with strangers, we focus on the potential of S&P-savvy individuals to motivate and facilitate secure and privacy-friendly behavior in their existing social network, where strong relationships of trust should already exist. Existing research on security advocates [37, 38, 62] also confirms the importance of non-technical, interpersonal skills, including the need to make sure people do not feel stupid for knowledge gaps. Perhaps due to this fact, security advocates also have backgrounds in non-technical fields, such as psychology or education [37,38]. This confirms findings about people seeking advice from others in their social network they consider experts, but not necessarily turning to those with a technical background [56]. Likewise, we focus on individuals knowledgeable in the fields of S&P to a certain degree and thus able to facilitate secure and private behavior of others.

Haney and Lutters [39] further identified techniques used by security advocates to overcome negative perceptions like being honest about risks, making one's language understandable, and engaging listeners through reward systems or relatable narratives, and metaphors. Haney and Lutters [39] focus on analyzing the status-quo since security advocates are already doing their best to promote secure behavior, whereas we aim to understand what we would need for S&P-savvy individuals to be tapped as a valuable social resource in the quest for more secure and more privacy-preserving behavior.

The importance of pursuing this line of research is further emphasized by findings of a survey study. Rader et al. [54] showed that stories have great potential to change security attitudes and behavior for the better. Stories told in the home context are more likely to change behavior compared to professional contexts. Yet, stories told by people knowledgeable in security are more likely to be retold, thus influencing more people. In a further analysis, Rader and Wash [53] found experts tend to focus on *how* an attack is conducted and prevented, whereas non-experts were mainly interested in *who* carried out an attack and *why*. The authors recommend experts should consider this in their communication with non-experts.

3 Study I: In-Depth Interviews

First, we wanted to gain a deeper understanding of the topic by conducting in-depth semi-structured interviews with S&P adepts and learn about their experiences with sharing their knowledge or motivating other people in terms of S&P in the private context. We conducted thirteen interviews until we reached data saturation. The interviews were held via a video-call tool, with an average duration of about an hour. All participants received a 20€ gift card for an online shop [34]. The interviews were audio-recorded and transcribed for analysis. We conducted two pilot interviews with experienced researchers to check our questions for clarity and comprehensibility and refined our interview guide based on the feedback.

3.1 Method

Participants. We recruited 13 participants by mailing lists and word-of-mouth. We used university mailing lists (also addressing interested non-students) including those of collaborators, reached out to our professional contacts (researchers and practitioners from various institutions and organizations) and contacts of collaborators, and were open to snowballing. All participants first completed a screening survey to make sure they qualified as S&P adepts (for the detailed scores, the reader is referred to Table 2 in Appendix A.1). All participants had been working intensively on the topic for several years, either in the context of research activity or in another professional context. The participants were between 21 and 56 years old. Two of the participants self-identified as female, eleven as male. All participants were residing in the UK or Germany at the time the study was conducted. For detailed demographics, including occupation and highest education, the reader is referred to Table 1 in Appendix A.1.

Study Procedure. Prior to the interviews, participants were asked to complete a screening survey to ensure that they met the criteria for study participation. We used the Security Behavior Intentions Scale (SEBIS) [20] to measure security intentions, the six-item validated self-report measure of security attitudes (SA-6) [24] to measure security attitudes, the Internet Users' Information Privacy Concerns Scale (IUIPC-8) [35,50] to measure privacy concerns, the Online Privacy Literacy questionnaire (OPLIS) [65] to measure privacy knowledge, the Affinity for Technology Interaction Scale (ATI scale) [28] to measure technical affinity, and two self-constructed items. We then contacted participants who qualified for study participation to set up an appointment and asked them to sign the informed consent form via email. The interviews consisted of six main parts (see Appendix A.2).

First, we thanked the participants, made sure they had signed the informed consent form, and gave them the opportunity to ask questions. We then asked about *their S&P behavior*, including social aspects such as whether they talked about this with others and how others might have reacted to their behavior in the past. Second, we asked about their experiences with observing insecure or privacy-unfriendly behavior of others, including their feelings on this topic and whether they had ever *interfered* in such a situation. Third, we asked whether other people usually *asked them for advice* on S&P issues, including who, on what issues, and how they responded to that. Forth, we asked whether they *feel responsible* for the S&P of other people, including who, why, and how this manifests itself in their behavior, e.g., by sharing news about security incidents and data breaches, or doing digital housekeeping. Fifth, we asked about *bad experiences* with giving advice to others or interfering and the fears associated with it, such as being socially awkward or straining the relationship. Sixth, we asked whether and why others perceive the participants as *S&P experts* and whether they are afraid of coming across as paranoid or tech nerds. We also asked about gender effects and loosely relied on the repertory grid technique [60] to ask which characteristics of a person they associate with IT security and privacy behavior. Finally, we asked the participants to complete another short questionnaire on their demographic information.

Data Analysis. We used thematic analysis [5] to analyze our transcribed data. The author that conducted most of the interviews first read through all transcripts multiple times and then coded all interviews at sentence level to develop a codebook, going back and forth several times to refine the codebook. That author then went through all transcripts and used the codebook for another round of coding. Next, another author went through the entire coding and marked all the codings they disagreed with, including passages where a code should be added (following recommendations for thematic analysis against conducting multiple independent codings and calculating ICR [6], p.278-279[1]). The authors then came together to discuss the notes of the second author and agree on a final coding. After this, both authors grouped the codes into six main themes.

Ethics. The study met all requirements for studies with human participants given by our ethics commission. Before the study, all participants were informed about the study purpose and conditions, informed that they could quit the study at any time without any negative consequences, and asked to confirm their participation by signing an informed consent sheet. Although we used a video-call software, we only recorded the audio track by using another software, and stored it locally on the interviewer's computer. Further, all participants were free to turn off their cameras for the interview. All data was handled confidentially and any identifiable information was deleted in the transcribing process. We decided to compensate the participants with gift cards for the "Greenpeace Magazine Warehouse" webshop, which is associated with Greenpeace, to support a charitable organization, but reward the participants with a product of their own choice from the store.

Limitations. Like most qualitative and exploratory work, our study is subject to several limitations. First, we rely on self-reported data, which might be biased due to social desirability, availability bias, and wrong recalls or self-assessments. We focus on social aspects, which may be especially sensitive for this kind of bias. Still, we aimed to gain a first understanding of IT security and privacy adepts' mindsets and experiences. Further research is needed to explore this topic in more depth. Second, we used a convenience sample, using personal networks and those of colleagues, as well as word-of-mouth. We wanted to target, inter alia, experienced researchers and practitioners in the field without making our project too public in order to preserve anonymity for the publication process. We thus decided not to recruit participants at public events such as scientific conferences or fairs, as it has been done in some

[1] According to Braun and Clarke [6], qualitative research acknowledges the researcher's influence on the research process. Conducting ICR as a means to "prove" reliability is thus seen as not applicable for thematic analysis, as data should not only be described, but also interpreted.

prior studies which aimed to recruit IT security experts [7,41]. As a result, our sample is skewed towards male and young participants, rather homogeneous in terms of culture (UK and Germany) and background, and also includes university students who may be knowledgeable about security but have limited professional security experience. Hence, our sample is hardly representative of all S&P adepts but rather serves as a first step in shining light on this complex topic. Further research is needed to explore the perspective of S&P adepts with different professional and demographic backgrounds, particularly from non-western cultures. Third, we mainly focus on the status quo in the interviews, i.e., we asked how our participants currently interacted with others in the context of S&P, and explored possible obstacles for interfering or motivating others towards more secure and privacy-preserving behavior. Yet if we aim to use S&P adepts as a social resource, we also need to know how social interactions in this context could be facilitated. We address this point in Study II, drawing on a more solution-oriented, participatory approach, i.e., co-creation workshops.

3.2 Results

In the following, we describe our results and provide quotes where applicable. Considering the explorative nature of our study and the limited sample size, we deliberately refrain from reporting exact numbers to avoid the appearance of generalizability. Instead, we will mention a rough frequency frame to emphasize topics that were mentioned by many participants.

3.2.1 Own S&P Behavior

Protection Strategies. When asked about what protection measures they applied in a everyday context, most of our participants referred to using secure authentication mechanisms, i.e., unique, secure passwords, 2FA, and locking devices. Other important security measures include using antivirus programs, updates, and checking emails for phishing. Reported privacy protection measures focused on avoiding tracking (e.g., by blocking or deleting cookies, using private modes in browsers, or VPN), and minimizing data collection (e.g., refrain from using social media and soft- or hardware from certain vendors, and covering one's webcam).

Social Conflicts. Half of our participants mentioned to have experienced social conflicts due to their S&P behavior, mostly with friends and family members or significant others. These conflicts arose from our participants not wanting IoT devices in their homes due to privacy concerns or expressing these concerns when visiting other IoT-equipped households, not wanting to share their passwords or location, and not wanting to use social media although the significant other wanted to tag their spouse on Facebook. Further, very few participants reported foregoing security or privacy to avoid delaying others (e.g., in a meeting), and to avoid being socially excluded.

3.2.2 Intervening in Others' S&P Behavior

Less than half of our participants said they had ever actively interfered in someone's S&P behavior. Basically, our participants only get involved if it affects them (e.g., their own data is involved or they personally would suffer from the consequences) or if they feel a responsibility (professionally or privately, because people rely on their advice or are close to them) (the latter confirming [13,16,51,52]). Only very few participants reported to have negative experiences with giving solicited or unsolicited advice, this includes recipients of the advice having problems with their OS after an update, and data loss after data encryption.

Raising Awareness. Almost all participants reported that at some point, they had tried to raise someone's S&P awareness. In most cases, the recipients of these efforts were family members or friends. Explicitly not addressed were persons with whom our participants have no close relationship. The topics addressed varied, and included data breaches, hacking attacks, scams, exploits, changes in privacy policies, eavesdropping, and new as well as established protection tools such as 2FA or the Tor browser. About half of our participants referred to possible consequences of neglecting S&P protection to make the importance of this protection clear. Other reported strategies were checking the recipient's email address on websites like "Have I Been Pwned", pranks, and trying to initiate a cost-benefit analysis for data sharing. Further, some participants emphasized that a negative framing should be avoided.

Motivating. Half of our participants reported efforts to motivate others in terms of S&P protection. Still, most of these efforts were limited to authentication (i.e., choosing secure passwords, keeping and entering them secretly, using 2FA). Only one participant each referred to the use of secure messenger apps, and operating systems, as well as doing updates.

Being Asked for Advice. Almost all participants reported to be asked for advice on S&P topics regularly. The most popular topics for advice focus on authentication (secure passwords, 2FA), which tools can be used for protection, and data collection (e.g., which services collect what kind of data, how does personalized advertisement work). Some participants also reported to be asked about whether it is advisable to use certain services and devices such as Google smartphones from a S&P point of view, and to give advice on (potential) spam and phishing emails. Most of our participants reported that family members, especially their parents, asked them for S&P advice frequently. Also, about a third said they were asked for advice by friends, and only a few mentioned acquaintances, colleagues, or others (confirming earlier findings [51, 52]). Most of our participants liked to be asked for advice as they feel valued and enjoy being perceived as an expert in this field, while others are primarily pleased that their social network is dealing with the topic at all. Still, about a third of our participants also mentioned negative aspects of being asked for advice, such as the pressure of giving good advice, being asked too often about the same topics, and being asked questions without clear answers (e.g., P5: *"Especially the question 'Is it really secure then?'. I mean, nothing is ever secure.")*

Feeling Responsible. Half of our participants felt responsible for the S&P behavior of their parents, mainly because they had more expertise in this area, had given them S&P advice previously, and their close relationship. Most of these participants also said they would engage in "digital housekeeping" [52]. Only one participant said they also felt responsible for the S&P behavior of other family members and close friends, and another participant who worked as IT admin for their customers' S&P behavior. Yet, these results should be taken with a grain of salt, because our sample was rather young, which might be a reason why no (older) children were considered, for whom they might also would feel responsible. Interestingly, most participants said they did not feel responsible for the S&P behavior of their social network since they felt that the decision to (not) act securely and privacy-preservingly was a personal one that they had no right to interfere with. Seemingly, this did not apply to their parents, perhaps because adult children also frequently interfere in other areas of their parents' lives, e.g., in medical matters. Very few participants also said that they did not feel responsible for others' S&P behavior as this would involve too much effort.

3.2.3 Conversations about S&P

Trigger. Our participants reported several opportunities that sparked conversations about S&P: sitting together with others in front of the computer, which offers the additional opportunity for others to observe one's own S&P behavior (e.g., using 2FA, tracing blocker, the Tor browser) and ask questions, if they were using someone else's computer and thus saw their security and privacy settings (both confirming [13]), giving general technical support, or if others received spam emails, were asked to take security measures by their provider, or saw news about current hacking attacks or scams.

Topics. Most participants reported talking with others about S&P-related topics, mainly to share experiences with protection measures and tools, discuss the pros and cons of not using social media and messengers, and inform others about data breaches or security incidents. More than half of our participants said they would primarily talk to other knowledgeable, tech-savvy people about S&P, as these were – in contrast to less tech-savvy people – interested in these topics.

3.2.4 Obstacles

All participants mentioned obstacles to improving the S&P behavior of their social network, e.g., by giving solicited or unsolicited advice.

Lack of Interest. More than a third of our participants complained about a lack of genuine interest in these topics (P2: *"It's like when someone tells me something about brass band music. I would nod my head and say 'That's interesting'. But that wouldn't really interest me, and that's exactly how I feel the other way around."*), confirming prior work in the professional context [39].

Social Aspects. Others referred to social aspects, such as not wanting to bother others, wanting to avoid negative reactions, not wanting to criticize others, and avoid being perceived as preachy or intrusive.

Lack of Resources and Opportunities. A few participants also mentioned a lack of resources, i.e., facilitating others' S&P behavior being too time-consuming or too much effort, and triggers, mainly because S&P behavior is not directly observable in most cases.

Lack of Legitimacy. Some participants were also reluctant to give advice or interfere in others' behavior since they themselves did not always act as securely and privacy-preservingly as they want. Regarding privacy, one participant each also explained that there is no "right" level of privacy and thus people have to make their own decisions, and that privacy is an especially sensitive topic as some people may be quickly offended because you imply that they are trying to hide something.

3.2.5 Reactions

Others' Reactions. Overall, our participants reported more positive than negative reactions when they gave solicited or unsolicited S&P advice. Positive reactions included interest, gratitude, sympathy, and acceptance, whereas negative reactions mainly refer to disinterest. If others observed their S&P-aware behaviors, our participants mainly got neutral reactions, i.e., others were non-judgmentally surprised about their behavior. Still, like in [13], a few also reported being smiled upon (e.g., P3: *"I think if you're interested in data security, you always get these joking sayings that you're one of the tin foil hatters or paranoid people."*) Most participants said their advice had not brought about any long-term change in the recipients. Only one participant reported to have had a lasting influence on others S&P behavior.

Own Reactions. About half of our participants said they understood that other people's behavior was not always secure and privacy-preserving, because they also knew the costs of such behavior and could well understand if other people were not willing to accept them. Accordingly, most people tend not to take it personally when other people ignore their (solicited or unsolicited) advice. Very occasionally, however, participants reported that such ignorance of the topic was perceived as a personal attack, as it was *"part of one's own identity"* (P1) and that they felt thus somewhat *"affronted"* (P4).

3.2.6 Perception as Expert and Stereotypes

Expert. Prior research [27,51,56] indicates that people do not only delegate their S&P to people who have a professional background in IT security or computer science, but also to knowledgeable people with a non-technical background. This also applies to "security advocates" [37–39] who deliberately chose this path for themselves. Still, about two-third of our participants reported being considered an expert in S&P due to a technical study or profession. Some participants, however, attributed their expert status to their private interest in the topic, and on support provided in the past. Most participants, self-identifying as female and male, thought gender has an impact on whether someone is perceived as an expert, with all agreeing that it tends to be more difficult for females (who have the same knowledge as males) to be seen as experts. This is attributed to common stereotypes, e.g., P9: *"The technology nerd is imagined as an overweight, male basement dweller."*

Stereotypes. S&P behavior of non-experts was often associated with age. Our participants tended to rate younger people (i.e., teenagers) as oversharers on social media and thus privacy-unfriendly and older people (i.e., over 50) as insecure due to lacking technical knowledge. Further, technical expertise and awareness of possible consequences were associated with adequately secure and privacy-preserving behavior. Very secure and privacy-friendly behavior, on the other hand, was associated with anxiety.

3.2.7 Summary of Interview Findings

S&P adepts mostly only try raising awareness of people they are close to (friends and family), but enjoy being asked for advice. Negative aspects of being asked for advice, however, include the pressure of giving good advice, being asked too often about the same topics, and being asked questions without clear answers. While reactions to (un)solicited S&P advice are mostly positive to neutral, S&P adepts are nevertheless afraid of negative reactions and struggle with the fact that primarily unsolicited meddling can lead to socially awkward situations. One difficulty is also getting started on the topic, since there are not many triggers for talking about S&P. Communication on S&P topics, therefore, takes place primarily between S&P adepts, as it is assumed that others are not interested in the topic. In general, privacy in particular is seen as a matter for everyone to decide for themselves. An exception seems to be parents, for whom S&P adepts feel responsible.

4 Study II: Co-Creation Workshops

While the interviews in Study I primarily focused on the status quo and aimed to identify potential barriers to S&P support from social peers, we took a more solution-oriented perspective in the second study. We conducted three co-creation workshops with three to four S&P adepts each to explore how S&P adepts can be supported to improve the S&P behavior of people in their social environment. The co-creation workshops were held via a video-call tool, with an average duration of about two hours. We used a Mural whiteboard[2] for facilitating the collaboration. Participants were offered compensation of €25 or £20, however, eight of the eleven participants chose not to be paid as their primary interest in participating was to support research in this area. The workshops were audio-recorded and transcribed for analysis. We conducted a pilot workshop with experienced researchers to check the procedure and materials and refined our workshop guide based on the feedback.

4.1 Method

Participants. We recruited 11 participants for three co-creation workshops by mailing lists and word-of-mouth. Like in the interviews, all participants had been working intensively on the topic for several years, either in the context of a research activity or as practitioners, and were currently residing in the UK or Germany. Four of the participants self-identified as female, seven as male. For detailed demographics and the screening data, the reader is referred to Appendix B.1.

Workshop Procedure. The co-creation workshop followed the first steps of a design sprint [44]. Before the study, participants were asked to complete a shorter version of the screening survey from the interview study (based on the interview participants' feedback that the survey was too long, we removed the SEBIS and all OPLIS scales except for the most relevant *technical aspects*) to ensure that they met the criteria for study participation. The screening survey started with a consent form that covered the entire co-creation workshop. The workshop started with an icebreaker session (approx. 7 min) where participants were asked to draw their mood to familiarize themselves with the Mural board and then introduce themselves to the others. During that time, small talk about social S&P situations was possible.

Map and Target. Next, the participants were introduced to the scenario by watching a 2-minute presentation held by the moderator. After the presentation, the participants' attention was drawn back to the Mural board. Their first task was brainstorming facilitators and obstacles of supporting their social peers in behaving securely and privacy-preservingly. This task was meant to provide a neutral introduction to the topic and initiate an exchange between the participants. In the further course, the brainstorming results served as a source of inspiration for the development of the co-creation solutions. To support the brainstorming, we used the miracle question [17], which originates from systemic therapy and in which clients adopt a solution-oriented perspective in which they are asked to imagine that a particular problem no longer exists. Furthermore, the S&P adepts were instructed to write down their

[2] https://www.mural.co/ last-accessed Feb. 16 2022

thoughts on sticky notes and discuss them. After the brainstorming, the S&P adepts were asked to agree on a common goal for the remainder of the workshop by collaboratively formulating the problem as a "How Might We" question [11].

Sketch. Once the goal was clear, we used the 5-3-4 method [58] to co-create solutions. Using this method, each participant first wrote three ideas on sticky notes. Second, the S&P adepts shifted clockwise and could either add three new ideas or extend the ideas from their successor. This was repeated until the S&P adepts fully rotated once. Each rotation was limited to three minutes. After that, each participant gave a short presentation (approx. 1 min) of their ideas. The others were allowed to ask questions.

Decide. Once the ideas were clear, the participants were asked to vote for ideas following the how-now-wow principle [66]. This approach addresses the issue that people tend to brainstorm highly original ideas, but usually settle on well-known solutions in the further development process. Brainstorming ideas are evaluated on two dimensions, originality and easiness to implement: now-ideas are normal ideas that are easy to implement, how-ideas are original ideas that are (too) hard to implement, and wow-ideas are original ideas that are easy (enough) to implement. For this, each participant received 15 dots (5 per category) and was asked to place these dots on the sticky notes from the previous round. Next, the ideas were sorted into the how-now-wow matrix based on the voting. After the sorting, the S&P adepts discussed the results. They were specifically asked to explain their voting and discuss how wow-ideas could be realized as solutions.

Finally, the adepts were thanked for participation, could ask questions, provide comments and were reimbursed.

Data Analysis. To analyze the results, we had two iterations – one for the data collected on the Mural board and one for the transcribed recordings. Similar to the interview analysis, we used thematic analysis [5]. First, one author, who was present at all workshops, familiarized with the Mural boards and then developed a codebook based on the sticky notes. The codebook was then applied to all data collected. Next, a second coder went through the coding and marked disagreements that were discussed later on. To analyze the transcripts, both authors coded all transcripts at the sentence level to iteratively develop a codebook considering also the first round of coding the board. One author then went through all transcripts once more to apply the codebook. The coding was verified by the second author. The authors then came together to discuss the notes of the second author and agree on a final coding considering the data on the board and the transcripts. After this, both authors grouped the codes into four main themes.

Ethics. For the co-creation workshops, we took the same precautions like in the interview study. Since the co-creation workshop involved other participants, the co-creation participants were informed about that before the study. During the workshop, participants were encouraged to have the camera on but were not required to do so. With a screen-recording software, we captured the Mural board but not the video call.

Limitations. There are several limitations based on the used method and sample. First, since the sample is rather small and homogeneous, our results should be considered as first insights that should be validated and broadened by future investigations. Considering the sample composition, it was biased towards researchers because more researchers than practitioners participated. Practitioners might struggle with other issues than researchers who are used to teaching. Yet Usable S&P researchers are particularly versed in the topic and thus might come up with a plethora of solutions in a shorter amount of time compared to other S&P adepts. Furthermore, the sample was slightly skewed towards male and young participants, of whom all had a university degree and were currently residing in the UK or Germany. Due to COVID-19, we opted for an online workshop, since capturing qualitative data online can be suitable [49]. This allowed for a more diverse and international sample. Still, in-person co-creation workshops are better for designing solutions using paper and sketching, while online workshops lead to more text-based co-creation. Our workshops thus focus more on generating concepts and identifying obstacles and facilitators. As a consequence, the co-creation serves rather to generate research data instead of designing solutions for actual use. The results hence must be enhanced by in-person workshops in the future.

4.2 Results

Four themes for the co-created solutions emerged during the analysis, which are described below.

4.2.1 Set a Constructive Dialogue Space

Create a Constructive Atmosphere. A reoccurring theme during the workshops reflected in various co-created solutions is the issue of addressing S&P topics in "normal" conversations without being judgmental or preachy. Some participants, hence, thought it would be helpful to establish social norms for such discussions. An important point here is finding a balance between creating awareness and accepting the user's S&P attitude, which often differs from that of the S&P adepts. In addition, the use case of the person seeking help and their lack of knowledge should be accepted. Furthermore, users seeking support should be able to address their problem without the S&P adept making a big deal out of it, e.g., P1WS1: *"[It works] as soon as someone has the feeling, I can now also ask a question and say I have but only five minutes time. And somehow you get an answer in five minutes that you can work with."* Last but not least, the recipient should be given time to reflect on what has been said, i.e., the S&P adept should take up the topic again after a period of reflection if necessary, but should not push it too hard in the initial conversation.

Establish Contact Between S&P Adepts and Users. Among the most important issues for our participants was how to establish contact between supporters and recipients. Like in Study I, our participants were reluctant to raise S&P issues themselves for fear of violating social norms. The challenge of not being in a position to give advice because of doubts about having enough expertise (security) or not always behaving optimally (privacy), an aspect that was also mentioned in Study I, also plays a role here. Accordingly, some of the considerations in the co-creation process related to how to make it clear to the outside world that one is a suitable contact person for the topic. There are officially defined roles and responsibilities for this in the professional context, e.g., P1WS1: *"For example, I was never asked about data protection until I was a data protection officer, because then it was clear that I am in charge."*, which could possibly also be transferred to the private context. One option for this, which has already proven itself unofficially in practice [27, 29, 51], is to officially delegate S&P. Like P1WS1 reported on his experience as a data protection officer: *"People were much more likely to bring things up to me if they felt it wasn't their problem afterward."* Another co-created solution that might fit this point was to offer oneself as an S&P adept in clubs and communities, as this reaches a lot of people, and word of availability as an advisor spreads quickly in the local environment.

If S&P adepts do want to proactively approach people, finding an entry point is challenging, as it is not a common topic when talking to one's social environment, e.g., P2WS2: *"I don't usually come into situations were my friends or family ask me about like security and privacy behavior and when I speak to those people I usually have other topics in mind than just randomly starting giving advice on internet security."* Certain publicly effective events, such as changes in legislation [59], changes in terms and conditions (T&Cs) of popular products like WhatsApp [40], or contact tracing apps [8] reported in the media can serve as an icebreaker for conversations. In this case, either people approach the S&P adepts, or the topic serves as a reminder for the S&P adepts that they could approach people. Movies could also be a good conversation starter. Although they often paint an unrealistic picture of S&P [30], they can serve as a starting point to explain how something actually works. A broader approach to this would be to conduct awareness campaigns. Although this has already been suggested in the literature [33], the goal would not be to raise S&P awareness per se, but, as P2WS2 put it: *"It is probably mostly about giving experts a stage. This one is mostly about providing like the pressing issue are for the public to actually be motivated to learn about privacy and security issues or find their experts of trust and to ask questions."* One suggestion was to do this in conjunction with action days such as Safer Internet Day or Password Day [25, 64].

Build Trust. Many S&P adepts were concerned with the question of how they could give those seeking help confidence in their abilities as supporters. Possible solutions for this were discussed, e.g., a kind of certification or score that changes depending on the quality of the help provided or the advice given. This would not only strengthen the subjective trust of the user, but also of the S&P adepts in their own abilities. Tools that enable users to experience S&P settings, such as AmIUnique [26], could also be used to enable users to judge the quality of advice themselves. One participant also noted that S&P are sensitive topics that are better discussed in (confidential) face-to-face conversations rather than, for example, via texts or in public. Still, some participants thought that credibility could only be achieved if there are large, trustworthy institutions, such as courts, that back up certain statements on S&P, as these are often difficult to believe: P4WS1: *"[They need to say] 'That's how tracking works on the internet. Yeah, that's super creepy. I'm sure you guys don't want that.' If you do it as individuals, doesn't matter how great people think you are, then you sound like a conspiracy theorist."*

4.2.2 Harness the Potential of Exchange

Promote Exchange Between S&P Adepts. Another topic that came up multiple times during the workshops was the desire to share successful tactics and strategies for support with other S&P adepts. This wish, however, remained on the surface, the participants had no concrete idea of how such an exchange could be designed, except for the vague idea of a platform. Still, a concrete co-creation idea, which aims in a similar direction, is to refer people seeking help to other specialists who are more knowledgeable in the area concerned, similar to the way it is done in medicine. This approach would offer the possibility to admit without loss of face that one does not know something and still have the feeling that one has helped the person seeking help (at least a little) by referring them to the right place. On the other hand, this could lead to helping people with whom one does not have a close relationship. Since most S&P adepts tend to help out of a sense of responsibility for their immediate social environment [51, 52], different facilitating conditions might have to be created at this point. One example of this was to give the S&P adepts the opportunity to offer consultation hours during their working hours.

Promote Exchange Between Users. Another idea of relieving the S&P adepts was to refer people seeking help to other users who had already been helped with the same problem, in a kind of snowball system, e.g., P1WS3: *"That you say, hey, I've already explained something similar to this guy, go see him. If this guy then explains it again to a buddy, then it becomes even clearer for him."* This idea also emerged in a more institutionalized context such as a school, where existing peer systems such as dispute resolution or mentoring programs are maintained by having each new generation step up and pass on their knowledge to the next generation.

4.2.3 Facilitate Knowledge Transfer

Find Common Ground. Two challenges that can arise when communicating knowledge are the question of a shared language, which must form the basis for successful communication, and the fact that users often have incorrect mental models of the matter concerned. The first problem has been addressed in several co-creation solutions, e.g., via the development of a dictionary that translates terms between S&P adepts and users, but also via the specification of certain terms, such as virus/malware, that do not keep changing over the years. With regard to the latter point, e.g., the development of metaphors was suggested (confirming earlier findings [39]), which offers great potential for presenting technical issues such as end-to-end encryption (E2EE) in a comprehensible way [61]. There was also a frequent request for training S&P adepts in explaining facts in a popular scientific way. Since S&P adepts are often asked for advice on specific problems, a flowchart, for example, would be a promising tool for the S&P adepts to use as a basis for deciding what knowledge they need to convey in order to understand the actual matter of interest.

Show S&P Relevance. Several co-creation proposals were aimed at making users aware of the relevance of S&P to create a basis for conversation. The S&P adepts found it most promising to illustrate the possible consequences of IT security and privacy violations, e.g., through real-life stories. In addition, the participants reported that it is easier to discuss S&P tools with users that require explicit interaction, such as passwords, than those that primarily take place in the background. This could be helped by tools that visualize the influence of different settings on a device or in a program, so that users can try out what influence a certain setting has, for example, on the collection of their data.

Enable Remote Access. Some participants dealt with the problem of helping someone across a distance with a technical S&P problem. While this works easily via screen sharing and remote access on some devices, such solutions are lacking to date, e.g., for mobile devices. Still, this option should be taken with caution, as it tempts S&P adepts to *"just do things quickly themselves"* (P1WS3), although it would be more sustainable to explain the solution to the person seeking help.

4.2.4 Strengthen Capabilities and Opportunities

Improve Expert Knowledge. Practitioners face the challenge of keeping up-to-date with the latest findings from S&P research. This is not only a question of the time required, which could be minimized by a convenient news ticker that summarizes the latest research results, but also of paywalls behind which many research papers are hidden. Although open access publications are already an existing solution to this problem, many publishers require a publication fee from the authors, which cannot always be raised by the institutions concerned. To better assess one's skills and knowledge gaps, a "test your knowledge quiz" would also be helpful.

Reward Support-Giving. Ultimately, it should also be worthwhile for the S&P adepts to provide support. One possible way of doing this would be to integrate the support into everyday working life, e.g., by making working time available for this purpose or by recognizing the support as a professional achievement in the context of a scientific or industrial career. A less formalized reward system would be the development of a gamification solution, e.g., P3WS2: *"So, gamification would already like covering ninety percent of all the security experts, because they are all children and want to play games."* Intrinsic motivation, on the other hand, can come from the social relationship itself, e.g., P3WS2: *"I feel stronger about the need of giving friends and family security advice, because I feel socially obliged to help them to prevent mistakes if I can. If a complete stranger maybe would have the same issue, I wouldn't bother to go the extra mile."* An implicit solution would therefore be to emphasize the social aspect of the support, for example, by providing support in a nice setting like a café or by providing some kind of exchange of support in another field where the user is an expert.

4.2.5 Summary of Co-Creation Workshop Findings

It is important to set a constructive, trusting dialogue space to avoid socially awkward situations. As S&P adepts are reluctant to raise the topic themselves for fear of disinterest, media reports, movies, and awareness campaigns could serve as conversation triggers. S&P adepts often do not feel they are in the moral position to give advice, hence, it could be helpful for users to officially delegate privacy and security to S&P adepts in the private context. Encouraging exchange has the potential to counteract the nagging aspects of being asked for advice by referring users to other S&P adepts on topics where they struggle to give good advice, and to other users they have helped before on topics where they are always being asked. Support could be made easier and less time-consuming by facilitating free and easy access to materials, such as flowcharts for knowledge transfer, metaphors, and research results. By rewarding and recognizing support in a professional or social context, motivation can be maintained even in the absence of direct positive responses from users.

5 Discussion

Below, we first recap our findings and then build on them to provide recommendations for S&P adepts who want to support other people as well as the S&P research community.

5.1 Summary of Main Findings

Prior research showed that social triggers have great potential of influencing people's security and privacy behavior for the better [10, 12–16, 22, 45, 55]. Indeed, people tend to rely on their social network for tech, but also for S&P advice and support [18, 27, 29, 46, 51, 52, 56]. Few studies have focused on the support-givers' perspective so far. We fill in this gap by adding knowledge about when, how, and why S&P adepts give advice and support to people from their social circle, and how they could be supported in this task.

It has been shown that when giving advice, it is especially important to establish trust, hence social skills are important [38, 39, 62]. We confirm these findings and enhance them by showing that S&P adepts often struggle to comment on or intervene in others' S&P behavior due to fear of negative reactions. Consequently, although they are often *asked by relatives and friends for advice*, they primarily proactively *talk to other S&P-savvy individuals* about S&P-related topics.

A major obstacle to communication between S&P adepts and users is that S&P adepts do not feel in the *(moral) position to judge* the behavior of others. If we want to use the potential of S&P adepts to improve the S&P behavior of users in their social environment, we have to find solutions that create a conversation where users ask the S&P adept directly for advice. This could be facilitated, e.g., via the official delegation of S&P in a private context to the S&P adepts. S&P adepts should also be supported in *finding the right tone* for such conversations for which no social norms exist yet, i.e., positive, non-judgmental, and non-moralizing.

It is further important to consider the *users' mental models* in conversations, which may differ from those of the S&P adepts [43, 53, 54]. This can be supported by prepared materials that use metaphors to explain complex issues in a comprehensible way. It could also be helpful for different S&P adepts to *exchange information about strategies and explanations* that have been used successfully – in cases where one is not familiar enough with the topic, one might even *refer the person seeking help to another S&P adept*. To reduce the sometimes daunting effort of S&P adepts, which is not always rewarded by the gratitude of those seeking help, it should be as easy as possible for S&P adepts to *obtain information*. Another option would be to *reward support-giving* in the official context or to *highlight the social aspects* of the process.

5.2 Recommendations: S&P Adepts

We first give four recommendations for S&P adepts based on the results reported in Section 4.2.1 and 4.2.3 considering methods to establish a constructive dialogue space and facilitate knowledge transfer.

Signal Availability. Our participants stated that if someone wants to help people, it must first be clear that this is the appropriate contact person for the topic. To achieve this, we recommend S&P adepts to *be approachable* and address the problem without opening a huge can of worms. This could be realized by transferring the principle of official roles, like data protection officers, from professional to private contexts. For example, S&P adepts could ask their peers whether they would like to *delegate their S&P* to them. To reach a large number of people seeking help and having word of their expertise spread quickly, S&P adepts should actively *offer their skills in associations and communities*, e.g., by having a special badge on social media profiles, or organizing workshops. S&P adepts should also *openly admit when their knowledge in a particular area is not sufficient* and, if possible, put the person seeking advice in touch with a more suitable S&P adept, e.g., by forwarding a message.

Use Conversation Starters to Talk about S&P. S&P are usually not common topics when talking to people from one's social circle. To find an easy entry into the topic, we recommend S&P adepts to *use media coverage of events*, e.g., legislative changes or the introduction of new technologies such as contact tracing apps as an icebreaker for conversations. They should further *rely on action days*, such as the Safer Internet Day as an occasion and reminder to raise the issue in their social environment. Another suitable conversation starter is to *use popular, unrealistic movies and TV shows* to explain how something really works. To realize this, experts could be supported by publicly available online collections of movie clips for different topics that they could either show their peers or share with them. In the interests of sustainability, if an S&P adept is asked for help with a technical problem, one should also *not just make all the settings themselves*, but explain to the person seeking help what they are doing and why.

Stay Positive. Talking about others' S&P behavior can be socially difficult, because one does not want to criticize the other person as stated in both studies. To address this issue, we recommend S&P adepts to stick to *positive, non-judgmental language*, do *not moralize*, and give users *time to reflect*, i.e., by revisiting the topic after a while. S&P adepts could be supported here by publicly available informative materials and educational videos that help them strengthening their communication skills. Since not all S&P adepts have the capabilities for this, it would also make sense to integrate communication training into curricula for technical subjects.

Establish a Common Ground. Another challenge is to find a common basis for discussion. For this purpose, we recommend S&P adepts to be aware that people asking for help might have *erroneous mental models*. To address this, S&P adepts should use *metaphors* to explain the technical background of solutions, such as E2EE. To lay the groundwork for this, security curricula should include human factors to strengthen understanding of the lay user perspective. Also, they should use *consistent (technical) terms* in the long term. As stated above, S&P adepts could be supported by informative materials or educated within specific workshops. Such materials would ideally be standardized and use a common terminology. Further, awareness for existing materials, such as those offered by the National Cybersecurity Alliance

(U.S. [4]), the National Cyber Security Centre (U.K., [9]), or the BSI (Germany, [31]) should be raised, e.g., by using professional networks or mailing-lists.

Considering the four recommendations above, there are several obstacles and challenges. Since security experts might *not agree on what the most important, useful tips for non-tech-savvy users are* [57], there is a risk that they will not even recognize where their knowledge is insufficient or where an acute need for action is. To address this, an exchange between S&P adepts is also important with regard to sensible security and privacy advice (see Section 5.3). Further, S&P adepts must ensure that they *do not refer help seekers to malicious actors* who, for example, want to gain access to systems or passwords. Since S&P adepts first have to find the necessary *time* and *motivation*, the following recommendations refer to how the research community can support them in doing so.

5.3 Recommendations: Research Community

We further propose to implement the following measures in the S&P research community to strengthen the capabilities and opportunities for S&P adepts and harness the potential of exchange (see Section 4.2.4 and 4.2.2):

Reward Support-Giving. S&P adepts' desire to support others often conflicts with other commitments and goals. To address this, we recommend that commitment to user support should somehow be *recognized as a career achievement*, e.g., by awarding specific certifications or social media badges. To further enhance the S&P adepts' motivation, *gamification solutions* should not only be developed for the S&P behavior of users, but also for the support giving of S&P adepts. For this, one could also introduce a *rating system for advice quality* similar to online platforms like StackOverflow or as part of existing social networks, which strengthens user trust in the S&P adept and the adepts' trust in their own abilities.

Facilitate Access to Information. In order to facilitate access to research results also for S&P adepts from industry and researchers from institutions with less funding, *open access* should be specifically promoted since participants in our study who were practitioners voiced interest in research papers that is hindered by closed access. This could be realized by primarily applying for projects with funding for open access fees or by preferentially publishing at conferences and journals that publish the publications free of charge under an open-access license. Furthermore, the research community could offer a *newsletter* summarizing the most important recent research findings. Another option is strengthening the link between practitioners and researchers, for instance, by offering practitioner tracks at scientific conferences and publishing in practitioner magazines.

Establish a Peer-System. Furthermore, to increase outreach and relieve S&P adepts, a *peer system* could be introduced by passing on knowledge to the next generation, similar to mentoring programs. For this purpose, people seeking advice could also be referred directly to other users who have already been helped on the same topic. There are several ways to realize this: a standalone online platform, as part of a social network, or within organizations and schools.

Create a Platform for Professional Exchange. A platform should be created that enables the *exchange between S&P adepts* on this topic, e.g., in the context of workshops or as a Slack channel. This could also serve as a discussion space to gain consensus on what is effective and actionable S&P advice.

6 Conclusion and Future Work

We add to existing work on social support in the S&P context by investigating how and under which circumstances S&P adepts support people in their private social environment, the challenges they face and ways to overcome them. For this, we first analyze the status quo by conducting in-depth interviews with 13 S&P adepts, and then explore options to assist S&P adepts in their efforts to help others in three co-creation workshops with 11 S&P adepts. We find that S&P adepts often struggle finding the right tone in conversations with lay users, partly because they do not see themselves in a moral position to give advice. Once contact is established, another challenge is to find a shared language. Since lay users often have different mental models than S&P adepts, it can be helpful to use metaphors for this purpose.

Some of the findings from our exploratory studies need to be confirmed and analyzed in more detail, such as what obstacles S&P adepts face in improving others' behavior. The effectiveness of the recommendations proposed by us should be investigated in field studies. For this, the introduction of a peer system and a platform for professional exchange would be a good idea. Another possible next step is the creation and evaluation of guidelines and training for the social aspects of conversations. Focusing on risks of S&P failures seems promising for emphasizing the relevance of S&P. Further research is needed to understand how such risks should be communicated [1, 21, 42]. Since it is easier to communicate about S&P tools that are observable, research should identify solutions that improve the visibility of S&P issues, such as privacy icons [19, 36]. Finally, since the lack of motivation is a main obstacle for providing S&P advice, future work should identify and validate techniques that motivate S&P adepts.

Acknowledgments

This work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, grant number 251805230/GRK 2050) and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758, 2020.

[2] Alessandro Acquisti, Leslie K. John, and George Loewenstein. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2):160–174, 2012.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, dec 1999.

[4] National Cybersecurity Alliance. Stay safe online, 2022. https://staysafeonline.org (Accessed 30-May-2022).

[5] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[6] Virginia Braun and Victoria Clarke. *Successful qualitative research: A practical guide for beginners*. SAGE Publications, 2013.

[7] 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, pages 117–136, Santa Clara, CA, August 2019. USENIX Association.

[8] Rory Cellan-Jones and Leo Kelion. Coronavirus: The great contact-tracing apps mystery, 2021. https://www.bbc.com/news/technology-53485569 (Accessed 16-February-2022).

[9] National Cyber Security Centre. Information for individuals & families, 2022. https://www.ncsc.gov.uk/section/information-for/individuals-families (Accessed 30-May-2022).

[10] Lynne M. Coventry, Debora Jeske, John M. Blythe, James Turland, and Pam Briggs. Personality and social framing in privacy decision-making: A study on cookie acceptance. *Frontiers in Psychology*, 7, 2016.

[11] Rikke Friis Dam and Teo Yu Siang. Define and frame your design challenge by creating your point of view and ask "how might we", 2021. https://www.interaction-design.org/literature/article/define-and-frame-your-design-challenge-by-creating-your-point-of-view-and-ask-how-might-we (Accessed 02-February-2022).

[12] 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.

[13] 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.

[14] 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 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 739—-749, New York, NY, USA, 2014. Association for Computing Machinery.

[15] 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 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '15, pages 1416—-1426, New York, NY, USA, 2015. Association for Computing Machinery.

[16] 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.

[17] Steve De Shazer, Yvonne Dolan, Harry Korman, Terry Trepper, Eric McCollum, and Insoo Kim Berg. *More than miracles: The state of the art of solution-focused brief therapy*. Routledge, 2021.

[18] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8:391–401, 2004.

[19] Serge Egelman, Raghudeep Kannavara, and Richard Chow. Is this thing on? Crowdsourcing privacy indicators for ubiquitous sensing platforms. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1669—-1678, New York, NY, USA, 2015. Association for Computing Machinery.

[20] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 2873—-2882, New York, NY, USA, 2015. Association for Computing Machinery.

[21] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 447–464, 2020.

[22] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), Nov 2018.

[23] 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, pages 59–75, Denver, CO, June 2016. USENIX Association.

[24] 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.

[25] Better Internet for Kids. Safer internet day. https://www.saferinternetday.org/ (Accessed 16-February-2022).

[26] Inria National Institute for Research in Digital Science and Technology. Amiunique. https://amiunique.org/ (Accessed 16-February-2022).

[27] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: User engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security*, SOUPS 2016, pages 97–111, Denver, CO, June 2016. USENIX Association.

[28] 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.

[29] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security*, SOUPS 2019, pages 21–40, Santa Clara, CA, August 2019. USENIX Association.

[30] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L. Mazurek. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security*, SOUPS 2019, pages 79–95, Santa Clara, CA, August 2019. USENIX Association.

[31] Bundesamt für Sicherheit in der Informationstechnik. Digitaler verbraucherschutz, 2022. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html (Accessed 30-May-2022).

[32] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 591—600, New York, NY, USA, 2006. Association for Computing Machinery.

[33] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. Investigating people's privacy risk perception. *Proceedings on Privacy Enhancing Technologies*, 2019(3):267–288, 2019.

[34] Greenpeace Media GmbH. Greenpeace magazin. warenhaus. https://warenhaus.greenpeace-magazin.de/ (Accessed 16-February-2022).

[35] Thomas Gross. Validity and reliability of the scale internet users' information privacy concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies*, 2021:235 – 258, 2021.

[36] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. Toggles, dollar signs, and triangles: How to (in)effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[37] Julie Haney and Wayne Lutters. Cybersecurity advocates: Discovering the characteristics and skills for an emergent role. *Information & Computer Security*, 29, 2021.

[38] Julie Haney, Wayne Lutters, and Jody Jacobs. Cybersecurity advocates: Force multipliers in security behavior change. *IEEE Security Privacy*, 19(4):54–59, 2021.

[39] 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.

[40] Alex Hern. Whatsapp to try again to change privacy policy in mid-may, 2021. `https://www.theguardian.com/technology/2021/feb/22/whatsapp-to-try-again-to-change-privacy-policy-in-mid-may` (Accessed 16-February-2022).

[41] 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, pages 327–346, Ottawa, July 2015. USENIX Association.

[42] Timo Jakobi, Sameer Patil, Dave Randall, Gunnar Stevens, and Volker Wulf. It Is About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Trans. Comput.-Hum. Interact.*, 26(1):2:1–2:44, 2019.

[43] 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, pages 39–52, Ottawa, July 2015. USENIX Association.

[44] Joonas Koivumaa. *Sprint: How to Solve Big Problems and Test New Ideas in just Five Days*. Lapin ammattikorkeakoulu, 2017.

[45] Isadora Krsek, Kimi V Wenzel, Sauvik Das, Jason I. Hong, and Laura A. 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.

[46] Amanda Lenhart, Mary Madden, Sandra Cortesi, Urs Gasser, and Aaron Smith. Where teens seek online privacy advice), 2013. `https://www.pewresearch.org/internet/2013/08/15/where-teens-seek-online-privacy-advice/` (Accessed 17-January-2022).

[47] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. How developers talk about personal data and what it means for user privacy: A case study of a developer forum on reddit. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW3), jan 2021.

[48] Heather Richter Lipford and Mary Ellen Zurko. Someone to watch over me. In *Proceedings of the 2012 New Security Paradigms Workshop*, NSPW '12, pages 67—76, New York, NY, USA, 2012. Association for Computing Machinery.

[49] Bojana Lobe, David Morgan, and Kim A. Hoffman. Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods*, 19:1609406920937875, 2020.

[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.

[51] 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.

[52] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E. Grinter, and W. Keith Edwards. Computer help at home: Methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 739 — 748, New York, NY, USA, 2009. Association for Computing Machinery.

[53] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 12 2015.

[54] 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.

[55] Yasmeen Rashidi, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. "It's easier than causing confrontation": Sanctioning strategies to maintain social norms and privacy on social media. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW1), may 2020.

[56] 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, pages 666—-677, New York, NY, USA, 2016. Association for Computing Machinery.

[57] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security Privacy*, 15(5):55–64, 2017.

[58] Curedale Robert. *Design Thinking: Process and Methods Manual*. Design Community College Inc, 2013.

[59] Adam Satariano. U.s. news outlets block european readers over new privacy rules, 2021. https://www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html (Accessed 16-February-2022).

[60] Luis Angel Saúl, M. Angeles López-González, Alexis Moreno-Pulido, Sergi Corbella, Victoria Compañ, and Guillem Feixas. Bibliometric review of the repertory grid technique: 1998–2007. *Journal of Constructivist Psychology*, 25(2):112–131, 2012.

[61] Leonie Schaewitz, David Lakotta, M. Angela Sasse, and Nikol Rummel. Peeking into the black box: Towards understanding user understanding of E2EE. In *European Symposium on Usable Security*, EuroUSEC '21, pages 129—140, New York, NY, USA, 2021. Association for Computing Machinery.

[62] 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.

[63] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. Understanding privacy-related advice on Stack Overflow. *Proceedings on Privacy Enhancing Technologies*, 1:18, 2022.

[64] National Today. World password day. https://nationaltoday.com/world-password-day/ (Accessed 16-February-2022).

[65] 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)*, pages 333–365. Springer Netherlands, Dordrecht, 2015.

[66] Ramon Vullings, Godelieve Spaas, and Igor Byttebier. *Creativity Today*. BIS Publishers, 2009.

A Study I: Interview Study

A.1 Interview Demographics and Screening

In this section. we provide detailed demographics from the interviews (Table 1) and screening data (Table 2).

Table 1: Demographics of the interview sample.

ID	age	gender	occupation	highest education
P1	29	f	PhD Student	Master Degree
P2	43	m	Computer Scientist	Diploma
P3	34	m	Researcher at University	PhD or higher
P4	56	m	Production Plant Manager	Master Degree
P5	25	m	Student	Bachelor Degree
P6	23	m	Student	Bachelor Degree
P7	22	m	Intern in a company & student	Bachelor Degree
P8	53	m	Head of IT	Apprenticeship
P9	21	f	Student	High School Diploma
P10	22	m	Student	High School Diploma
P11	25	m	Development Engineer	Master Degree
P12	48	m	System Administrator	High School Diploma
P13	21	m	Student	School Student

Table 2: Screening of the interview sample.

	median	minimum	maximum	percentile		
				25	50	75
SEBIS_Device Securement	4.5000	4.00	5.00	4.2500	4.5000	4.7500
SEBIS_Password Generation	4.2500	3.00	5.00	3.5000	4.2500	4.3750
SEBIS_Proactive Awareness	3.6000	2.80	4.60	3.4000	3.6000	4.3000
SEBIS_Updating	4.3333	3.00	5.00	3.8333	4.3333	4.6667
SA6	3.8333	3.00	4.83	3.3333	3.8333	4.2500
ATI	5.1111	3.00	5.78	4.7222	5.1111	5.3333
IUIPC8_Control	6.5000	3.50	7.00	5.7500	6.5000	6.7500
IUIPC8_Awareness	7.0000	4.00	7.00	6.2500	7.0000	7.0000
IUIPC8_Collection	6.2500	3.75	7.00	5.0000	6.2500	6.8750
OPLIS_Knowledge	4.0000	2.00	5.00	3.5000	4.0000	5.0000
OPLIS_Technical Aspects	5.0000	4.00	5.00	5.0000	5.0000	5.0000
OPLIS_Law	3.0000	0.00	4.00	2.0000	3.0000	4.0000
OPLIS_Protection	4.0000	1.00	5.00	2.0000	4.0000	4.0000

Note: Cut off scores were SEBIS (average of all scales): 3.7, SA6: 3, ATI: 3, IUIPC-8 (average of all scales): 3.7, OPLIS (average of all scales): 2.5. Please note that these are the absolute lowest limits, but the values of most participants were significantly higher. We also considered the whole picture and made sure that someone scoring low on one scale (e.g., privacy concerns) scored considerably higher on other scales, e.g., security behavioral intention.

A.2 Interview Guide

- Welcoming the participant
- Security and Privacy Behavior
  - What do you do to protect your S&P in everyday life?
  - Do you share this behavior in interactions with others? Do others recognize your S&P in everyday life?
  - How do others react to it?
  - How do you feel when others respond to your behavior?
  - Is this a topic of conversation? (E.g., refraining from using social networks, or use of certain messengers)
  - Have there ever been situations where others reacted with surprise to your S&P behavior?
  - Have there ever been situations where you felt uncomfortable acting according to your S&P ideas?
    - How did you resolve this?
    - What did you take away from this for future situations?

  - In conversations, do you generally hold an S&P opinion, e.g., about using certain products and services?
    - (If yes:) How do you feel about this?
    - (If not:) Why not?

- Interference
  - Do you ever observe insecure or privacy-unfriendly behavior in others?
    - Could you give an example?
    - What are your thoughts and feelings about it?
    - Do you intervene in the other person's behavior?
      - (If yes:) How and why?
      - (If no:) Why not?
    - Do you potentially fear of coming across as arrogant?
    - Do you potentially fear of coming across as preachy?

- Advice
  - Do others ask you for advice about S&P?
    - Who?
    - About what specifically?
    - How do you respond to that?
    - Can you give examples for what advice you give?

- Responsibility
  - Do you feel responsible for the S&P of others?
    - Of whom?
    - Why?
    - How does this affect your behavior?
  - Do you engage in "digital housekeeping" with relatives or friends?
  - Do you share news about changes (e.g., new privacy regulations, E2E encryption), data breaches, or security incidents?
    - (If yes:) With whom and why?
    - (If not:) Why not?

- Bad experiences
  - Have you ever had a bad experience giving S&P advice to someone?
  - Have you ever had a bad experience when intervening without being asked?
  - Are you afraid that intervening might somehow be socially inappropriate/awkward?
  - Are you afraid that it might strain social relationships if
    - People are annoyed by interventions?
    - You notice that people don't follow your advice?
  - Are you afraid that helping might be too much work/you will be asked all the time in the future?
  - Are you afraid that you don't know some things and that this will damage your reputation as an expert?

- Perception
  - Would you say that others think you are an S&P expert?
  - Why do others think you are an S&P expert?
  - Generally regarding own behavior or when interfering/advising others ...
    - ... are you sometimes afraid of coming across as paranoid/as a "tin foil hat wearer"?

        - ∗ ... are you sometimes afraid of coming across as a tech nerd?
        - ∗ Would you say that S&P expertise has anything to do with gender? Is being an S&P expert different for women than for men?
    - – Repertory Grid: With which characteristics would you describe someone who ...
        - ∗ ... behaves too insecurely?
        - ∗ ... behaves in just the right secure way?
        - ∗ ... behaves too securely?
        - ∗ ... behaves too privacy-unfriendly?
        - ∗ ... behaves in exactly the right privacy-friendly way?
        - ∗ ... behaves too privacy-friendly?

- End and reimbursement

A.3 Codebook

The codebook is available at https://www.arbing.psychologie.tu-darmstadt.de/media/ag_arbeits_und_ingenieurpsychologie/responsive_design/forschungsergebnisse_1/TheNerdFactor_Codebooks.pdf.

B Study II: Co-Creation

B.1 Workshop Demographics and Screening

In this section, we provide detailed demographics from workshops (Table 3) and screening data (Table 4).

Table 3: Demographics of the co-creation sample. Please note that P1WS1 refers to Participant 1 from the first workshop, P1WS2 to Participant 1 from the second workshop etc.

ID	age	gender	occupation	highest education
P1WS1	31–35	m	Employed Full-time & Privacy Officer	Bachelor Degree
P2WS1	26–30	f	Scientific Employee	Master Degree
P3WS1	31–35	m	Post-doc Researcher	PhD or higher
P4WS1	26–30	m	Usable Security Researcher (PhD)	Master Degree
P1WS2	31–35	f	Post-doc Researcher	PhD or higher
P2WS2	26–30	m	Software Developer	Master Degree
P3WS2	31–35	m	Post-doc Researcher	PhD or higher
P1WS3	26–30	m	Doctoral Candidate	Master Degree
P2WS3	31–35	f	Post-doc Researcher	PhD or higher
P3WS3	36–40	m	Professor, computer science	PhD or higher
P4WS3	26–30	f	Usable Security Researcher (PhD)	Master Degree

Table 4: Screening of the workshop sample.

	median	minimum	maximum	percentile		
				25	50	75
SA6	3.6667	3.00	4.67	3.1667	3.6667	4.3333
ATI	4.5556	2.89	5.78	4.1111	4.5556	5.2222
IUIPC8_Control	6.0000	5.00	7.00	5.5000	6.0000	7.0000
IUIPC8_Awareness	7.0000	6.00	7.00	6.5000	7.0000	7.0000
IUIPC8_Collection	6.5000	3.25	7.00	5.5000	6.5000	6.7500
OPLIS_Technical Aspects	5.0000	4.00	5.00	4.0000	5.0000	5.0000

Note: Cut off scores were SA6: 3, ATI: 2.7, IUIPC-8 (average of all scales): 3.7, OPLIS: 4. Please note that these are the absolute lowest limits, but the values of most participants were significantly higher. We also considered the whole picture and made sure that someone scoring low on one scale (e.g., privacy concerns) scored considerably higher on other scales, e.g., knowledge about technical privacy aspects.

B.2 Workshop Guide

- Welcome (3 min)
- Icebreaker (7 min):
  - paint your current mood on Mural (paint & introduce)
  - meanwhile small talk about social S&P situations
- Introduction to the topic (2 min)
- Brainstorming: Facilitators and obstacles, using the miracle question
- Formulate "How Might We" question (2 min)
- Develop solutions: 5-3-4
  - everyone creates 3 ideas on sticky notes (writing and/or drawing)
  - after 3 min: go clockwise, everyone creates 3 more ideas (inspired by existing or new), repeat until rotation is complete
  - Remember: The target group is you! You should develop solutions that help you to support others.
- Short presentation of your own thoughts (1 min each), everyone can ask comprehension questions until all ideas are reasonably clear
- Decision: Dotmocracy with How-Now-Wow matrix
- Discussion: everyone explains what they think is good and why and what is difficult and why, then open discussion where wow ideas can be developed into solutions
- Wrap up, farewell, payment

B.3 Codebook

The codebook is available at `https://www.arbing.psychologie.tu-darmstadt.de/media/ag_arbeits_und_ingenieurpsychologie/responsive_design/forschungsergebnisse_1/TheNerdFactor_Codebooks.pdf`.