More than Usability:
Differential Access to Digital Security and Privacy

Annalina Buckmann
Ruhr University Bochum

Jan Magnus Nold
Ruhr University Bochum

Yasemin Acar
Paderborn University & The George Washington University

Yixin Zou
Max Planck Institute for Security and Privacy

Abstract

Despite over two decades of usable security and privacy (S&P) research, there remains a yawning gap between expert-recommended S&P advice and user behavior. The Security and Privacy Acceptance Framework (SPAF) identifies awareness, motivation, and ability as main factors influencing S&P behavior. The inclusive S&P literature highlights the importance of user diversity, yet there are open questions regarding how and why sociodemographic differences in S&P emerge. We apply SPAF to analyze interview data from 47 participants with varying age, gender, education, income, (dis)ability, and expertise. Our findings highlight seven new underlying factors not covered by SPAF (e.g., how experiences with threats and doing one's own research contribute to awareness) and four barriers (e.g., limited social support). Drawing from our findings, we establish the notion of *differential access* as a new concept to consider for inclusive S&P research beyond system-level accessibility: Users' access to S&P protections and information largely hinges on their social and relational position within the society and access to resources, which varies across sociodemographics.

1 Introduction

Despite over two decades of research in usable security and privacy (S&P), there remains a yawning gap between expert-recommended S&P measures and user behavior [15, 27, 49]. As stated by Das et al. [27], "If enough people employed basic, expert-recommended best practices [...] the cybercrime industry would be hamstrung." Yet the reality is far more complicated: The Security and Privacy Acceptance Framework (SPAF) [27] identifies *awareness*, *motivation*, and *ability* as main factors influencing S&P behaviors. Other work highlights *"differential vulnerabilities"* [70], *"at-risk users"* [98], and the diversity of people's needs that call for inclusive approaches in building S&P mechanisms [77, 96, 97]. Yet there are still contradictory results and vast unknowns about how sociodemographic factors shape S&P behaviors [101].

To address this gap, we present a qualitative interview study with 47 participants with diverse backgrounds in Germany to shed new light on the SPAF framework [27]. Germany presents an interesting context, as past work has found its population more aware of S&P risks [46, 48]. Meanwhile, the country's infrastructure still lags behind in digitization [22], and there is a substantial gap in digital skills between IT specialists and laypeople in the German society [22, 48]. Our participants span various age groups, education and income levels, different levels of IT expertise; some of them had chronic diseases and disabilities and others did not. We did this deliberate sampling as all of these factors have been shown to influence S&P behaviors [98, 101]. In the interviews, we probed participants about their S&P perceptions, experiences, practices, challenges, and needs for improvement. Our research addresses the following questions:

RQ1: To what extent does SPAF apply to explain S&P behaviors for a diverse sample in Germany?

RQ2: What barriers does this diverse sample experience when engaging with S&P topics and advice?

RQ3: How do participants wish to improve S&P in digital societies?

We contribute one of the first systematic applications of SPAF to a diverse sample that covers several at-risk user groups, including older adults, people with disabilities, and people with low socioeconomic status [98]. Our findings empirically validate SPAF and the importance of awareness, motivation, and ability in shaping S&P behaviors. We also identify new underlying factors not covered by SPAF (Table 2), such

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

as how S&P awareness can also originate from interactions with organizations, and how motivation is intrinsically tied to the enthusiasm about technology and learning new things. We further provide insights into the specific barriers to accepting S&P practices, ranging from poor communication to a lack of digital skills and social support. Altogether, our findings highlight the notion of *differential access* to S&P — one's access to resources needed for S&P protections fundamentally hinges on the different relational positions individuals have within digital societies [70].

Key insights from our research include:

- **A refined version of SPAF** drawing from a diverse sample, including seven new underlying factors and four barriers.
- **Substantial gaps** exist between enthusiasts (those with expertise in IT and sometimes S&P) and everyday users in terms of perceived threats and adopted practices, yet they shared similar concerns.
- **Differential access** emerges when observing patterns across diverse user groups; accessibility applies to not only systems but also resources (e.g., finances, time, mental, and social).

2 Background and Related Work

2.1 The Security and Privacy Acceptance Framework (SPAF)

Early usable S&P literature argues that a lack of usability is *the* reason why people do not engage in expert-recommended S&P behaviors [103]: tools and measures that are not built with end-users in mind become too complex and cause friction [6, 7, 47, 85]. To this date, studies consistently show a mismatch between expert and everyday user perspectives on appropriate S&P measures [4, 15, 49, 50, 75, 99, 107]. In 2022, Das et al. proposed SPAF [27] as a framework to explain why users accept or reject S&P practices, identifying *awareness*, *motivation*, and *ability* as three key factors. *Awareness* refers to a person's knowledge and understanding of threats and countermeasures. *Motivation* captures one's willingness to engage in and adopt expert-recommended practices and tools. *Ability* defines to what extent a person can convert motivation into action. SPAF posits that prevalent models of human behavior and technology adoption do not apply in the context of S&P as the practices are abstract, secondary, and not tangible [27]. Moreover, there is increasing evidence for the effect of social influence on all three stages [26, 37, 38, 106].

While some research referred to SPAF [1, 37, 52, 59, 85, 86, 105, 109] since its publication, to the best of our knowledge, we are the first to systematically apply the framework to analyze data from a diverse sample. Our analysis confirms the importance of awareness, motivation, and ability while revealing new underlying factors not covered by SPAF.

2.2 From Usable to Inclusive S&P

Recent work has identified knowledge gaps regarding user diversity and how solutions for "average users" are not enough [40, 42, 51, 97, 101]. Accessible and inclusive S&P research [76, 77, 96, 97] aims at developing S&P mechanisms that are inclusive to people with various characteristics, abilities, needs, and values [96]. Under this wave, studies with specific user groups—such as older adults [9, 63, 88, 111], children [56, 108], and people with different abilities [36, 43]—are emerging. Still, Wei et al. conclude there remain "contradictory results and vast unknowns" about *why* correlations exist between sociodemographic factors and S&P behaviors, and answering the "why" requires an epistemic diversity of methods, including in-depth qualitative methods and analyzing intersectionality [101]. The concept of intersectionality urges us to not look at individual socio-demographic factors and identities in isolation, but to engage their overlaps and intersections that create distinct experiences and struggles [20, 25, 30, 31, 41, 58, 104]. Further, the accessibility literature and the capability approach suggest focusing on "universal barriers", i.e., why someone is struggling with a service, rather than segmenting the people who experience the struggles [29, 84].

Drawing from the concept of universal barriers [84], our work shows how these barriers manifest in our sample of participants with diverse backgrounds. Pierce et al. established the notion of "differential vulnerabilities" to capture "how different populations face different types and degrees of security risks" [70]. Along this line, our findings inform the concept of *differential access*, i.e., access to S&P protections is similarly contingent on the different relational positions individuals have within digital societies.

2.3 The S&P Landscape in Germany

Studies on digitalization and S&P in Germany present a mixed picture, making it an interesting site of inquiry. According to the EU's "Digital Economy and Society Index 2022" [22], Germany ranks 13th of 27 EU member states, despite being the EU's largest economy. While Germany excels in connectivity, it lags behind in the provision of digital public services and human capital: even though the number of IT specialists is above average, there is a gap in digital skills and competencies among the population [22], amplified by factors like gender, education, and occupation [48].

The German population has a high privacy awareness [48] and holds fewer S&P misconceptions [46]. Yet studies show pronounced differences among population groups within Germany [45, 68, 94]. The uptake of protective measures also increases with age [68]. Herbert found four at-risk groups in

Germany (older adults, teenagers, people with migration backgrounds, and those with low formal education) experience more cybercrime than the average German population [45]. Moreover, low-income users in Germany face specific S&P risks due to limited financial resources, resulting in practices such as using an untrusted cloud because they could not afford more storage space [55]. Our research complements prior quantitative studies by providing qualitative insights on German users' everyday S&P awareness, motivation, ability, and associated barriers. Going beyond the low-income sample in Kostan et al.'s study [55], we draw our insights from a sample diverse in age, education, income, and chronic diseases.

3 Research Method

3.1 In-Depth Interviews

Interview Procedure. With semi-structured interviews, we explored the topics (perceptions, understandings, feelings, experiences, and practices related to S&P) in depth while having the flexibility of delving into themes important to the interviewee. We provide our full interview guide in Appendix C, sorted by thematic blocks. The interviews were conducted in German by native speakers. We conducted three pilot interviews (not included in the analysis) and mildly adjusted the phrasing and order of questions. Questions and themes were derived from related work [26, 73, 79, 87, 94] to facilitate understanding of S&P awareness, motivation, and ability. The interview started with broad questions about the role of the internet in participants' lives. Next, we probed concerns, threat models, practices, and problems, and sources for S&P awareness and support. The interview ended with participants' thoughts on S&P responsibility and wishes for improvement. Rather than strictly following the thematic blocks, we gave participants the freedom and time to set their own emphases and probed topics brought up by participants.

To reach a diverse sample across urban and rural areas, we conducted all interviews remotely via video calls using Zoom or via telephone calls using Skype. Interviews were scheduled for two hours, and we collected a total of 52:30h of recordings (average time per interview: 1:07h, ranging from 0:27h to 1:55h). To avoid fatigue, we reminded participants that they did not have to answer all questions and could stop the interview at any time. Most participants were keen to discuss the topics at length.

Recruitment. We distributed our recruitment material among various organizations and associations; some of them serve specific groups (e.g., older adults and people with disabilities). This partnership further ensured participants had contacts in the organization to turn to if needed. After getting an initial set of participants, we conducted snowball sampling, asking participants to share our recruitment message in their circles. Our recruitment material consisted of a letter and a flyer of the study overview, including a QR code/link to our pre-questionnaire. After the participant gave informed consent, the pre-questionnaire asked for demographic questions: age, gender, migration backgrounds, chronic illness or disability, education level, income level, size of their hometown, and open questions on internet and device usage. We used information from the pre-questionnaire to generate prompts for the interviews. Participants could choose to skip questions about migration backgrounds and existing illnesses. At the end, participants could schedule a two-hour slot for the interview.

Qualitative Data Analysis. The interviews were transcribed verbatim by a GDPR-compliant transcription service and then manually reviewed, edited, and anonymized. Two researchers analyzed the transcripts, following the six phases of thematic analysis [11, 12, 14]: After familiarizing themselves with the data (I), the researchers agreed on an initial codebook (II), accounting for the high-level themes identified in the data and from the interview guide. Both coded the same set of 14 interviews independently to account for more specific themes (III). After synthesizing themes, one researcher coded the remaining data, refined the categories in ongoing discussions (IV). The researchers continued the discussions during the coding process to refine the top and sub-categories and ensure consensus and saturation [13] (V). The second researcher reviewed the final coding to ensure that categories were matched before writing the findings (VI) [11]. We then mapped our findings to the SPAF factors (awareness, motivation, and ability) and analyzed the prevalence of themes and patterns among different sociodemographics and their intersections [62, 104]. As emerging disagreements were resolved and a consensus was reached throughout the coding process, we do not report inter-rater reliability, following established practices in the HCI community [14, 16, 55, 60]. All quotes were translated into English by one researcher.

3.2 Research Ethics and Limitations

Positionality Statement. As human-centered security researchers, we bring a special perspective of data collection and analysis, mainly focusing on human factors and IT security. We strive to represent the participants' experiences as accurately as possible through triangulation among researchers: the data was analyzed by researchers of different gender and age with backgrounds in social sciences and IT security.

Ethics & Data Protection. When we conducted the study, our institution did not have an ethics review board. We designed our study with strict ethical considerations according to the Menlo report [54] and obtained approval from our institution's data protection officer. Before filling out the pre-questionnaire, participants agreed to participate in a consent form, including information on data handling and possible risks. Before beginning the interviews, we guided participants through the consent form again, so that they could ask questions before giving their consent once more. All data was collected and processed according to the GDPR and stored encrypted on our institution's servers. Each participant was compensated with 40€.

Limitations. Our study has several limitations typical for interview studies, including self-report, recall, and social desirability biases. To counter these, we encouraged participants to be open about their thoughts, emphasized the study was not about right or wrong answers, and took care to create rapport and provide an open, relaxed atmosphere for dialogue. As the interviews were conducted remotely, only people with the necessary conditions could participate. We made great efforts to reach less tech-savvy participants and offered the opportunity to conduct the interview via landline. Our sample consisted of German residents only, so the results might not transfer to other countries or societies; they are also not representative of the whole German population or any specific groups due to the study's qualitative nature. For example, we did not identify distinct patterns across the urban vs. rural divide or people with vs. without migration backgrounds, unlike other quantitative surveys [22, 45].

4 Results

After describing the sample in 4.1, we present our findings on S&P awareness (4.2), motivation (4.3), and ability (4.4) along SPAF. The new underlying factors derived from our findings and not covered by SPAF are highlighted by ★. We then present findings about participants' barriers to S&P protections (4.5) and wishes for how S&P can be improved (4.6). Table 2 summarizes an overview of our findings.

4.1 Sample Description

We conducted 47 semi-structured interviews with participants of diverse sociodemographics. Table 1 provides an aggregated overview, and Table 3 in Appendix A shows details and intersections per participant. Twelve participants had prior knowledge of IT, and some in S&P specifically, drawing from their work experience, education, or private interests. To differentiate those with more structural mental models from those with more functional mental models [50, 67], we name the former "enthusiasts", and the latter "everyday users" [18, 44]. Since these categories overlap with each other (i.e., one participant can belong to multiple groups), we report the results in aggregate for the most part. However, we also identify distinct group-based patterns and intersections when they emerge.

4.2 Awareness and Concerns

Our findings confirm the role of SPAF factors – *social engagement, digital literacy and mental models, media exposure, warnings and notifications* – in shaping awareness. We also identify additional factors: ★*threat experiences and incidents,* ★*organizations and institutions*, and doing one's ★*own research*. Additionally, everyday users struggled to name concrete threats but raised various S&P ★*concerns*.

Table 1: Aggregated demographic overview (N=47).

Demographic	**abs.**	**rel. %**	**Demographic**	**abs.**	**rel. %**
Gender			**Age**		
woman	23	48.90%	young (18-27)	9	19.10%
man	23	48.90%	adult	22	46.60%
non-binary	1	2.10%	older (60+)	16	34.00%
Education			**Income**		
lower	13	27.70%	low	23	48.90%
higher	13	27.70%	middle	11	23.40%
university/college	21	44.70%	high and upper	13	27.70%
Chronic Disease or Disability			**City Size**		
yes	20	42.60%	rural & small	7	14.89%
no	26	55.30%	medium	14	29.79%
n/a	1	2.10%	(major) city	26	55.32%
Migration Backgrounds			**Enthusiast**		
yes	8	17.00%	yes	12	25.53%
no	39	83.00%	no	35	74.46%

Social Engagement. Participants referred to different social sources for getting awareness, advice, and support on S&P. Some mentioned their workplace, where they learned from other colleagues, asked S&P experts, or participated in specific courses. Most participants learned about S&P from their social circle and friends, general conversations about the topic, or stories about incidents. The family was mentioned as a source predominantly by women: they asked their husbands or partners, fathers, or brothers. Older women would ask their children and grandchildren, emphasizing they needed to trust the person, and seeing them as more knowledgeable due to being "digital natives". Advice was passed through generations, from children to their parents and grandparents.

While enthusiasts would exclusively turn to persons with expertise, only a few everyday users had expert sources to turn to – and those were usually men. This pattern may stem from gender stereotypes [100] more than actual gender differences, and the reliance on men was not perceived positively by all: *"That's another thing: as a woman, do I have to call a man again and ask for help?"* [P09]

Mental Models and Digital Literacy. Participants discussed their knowledge and understanding of S&P. Some showed limited awareness of possible threats, which in turn caused them insecurity when using the Internet: *"I never feel secure. There's always a bit of tension"* [P19]. Others – especially older women – expressed a strong avoidance of learning: *"I don't want to go online with shaky fingers"* [P02]. Others stated that "knowing too much" would make one paranoid, in turn causing non-use or disengagement.

S&P was perceived as *"master's knowledge"* [P44], reserved for experts, *"as if you have to have studied computer science [to] have a chance"* [P09]. Enthusiasts, predominantly men with middle or higher income and education, built elaborate knowledge ecosystems having more stable flows of S&P information and available support sources to turn to. In contrast, everyday users pieced together information from different and random channels and resources, resulting in fragmented mental models.

Media Exposure. Information in the media was mostly encountered by chance on TV, radio, print, or social media, featuring reports about recent attacks on organizations. Only a few participants encountered S&P advice, e.g., in shows for consumers. Generally, media exposure was described as frightening, featuring *"horror scenarios"* [P08], causing one to *"want to delete everything"* [P14].

Warnings & Notifications. These channels were primarily brought up in the context of firewalls and antivirus software. Rather than facilitating awareness, they were described as disruptive and burdensome: *"You never know what it is. You have to do the research yourself, think for yourself, and understand it yourself"* [P17]. This was particularly salient for tools prompted by the device. In contrast, participants appreciated prompts to use multi-factor authentication (MFA) and warnings when accessing insecure websites.

★Threat Experiences and Incidents. Participants recalled certain incidents that shaped their S&P awareness. The most prevalent was phishing (via e-mail, phone, or SMS), which they referred to as *"spam"* or *"fake"*. Most felt fairly confident in dealing with it, elaborating on protective practices. Still, everyday users lacked understanding and were left wondering how it worked and what specific risk was associated with it: *"How did they get my e-mail address? [What] happens should I eventually click on such a thing?"* [P01].

For other incidents, everyday users noticeably struggled to express their experience and used broad phrases such as "*having been hacked*" and "*data abuse*", whereas the actual incidents ranged from identity theft to external access to accounts or devices and malware. Others described receiving targeted content and ads as a threat and feeling personally manipulated: *"I [find] that scary. Then I'm wondering, how is it all connected?"* [P24]. The lack of words to describe their experience was coupled with a lack of understanding of how the attacks worked and suitable protective measures.

★Institutions and Organizations. These places were predominantly mentioned by everyday users as a source for cultivating awareness, even though S&P may not be the focal point of their service. For instance, older participants turned to senior-specific organizations to learn about S&P through lectures, courses, or 1-1 support. Some participants also mentioned support offered by banks, where they get information about online banking and learn about MFA: *"They explained everything to me, and gave me a feeling of security"* [P06]. Schools or universities were primarily mentioned by younger adults, referring to the provided information as *"rudimentary"* [P17], while some adults and older adults referred to courses and experts at the workplace facilitating awareness.

Institutions and organizations also intersect with incident support as learning opportunities. Participants reported turning to the police, banks, or IT support for help when dealing with the aftermath of an incident. While banks or IT support could usually solve the issue, the police take on crime reports but would not offer further support or explanation: *"They did not help me, they said: 'No, we are overloaded'"* [P29].

★Own Research. "Doing my own research" was a prevalent source for S&P awareness among participants. Noticeably, enthusiasts almost exclusively turned to S&P-related online resources such as websites, magazines, online communities, or specific associations; they knew what they were looking for and where they had to look for it. In contrast, everyday users would broadly refer to doing "online research", using search engines and comparing different information they found. Only a few everyday users were aware of official S&P resources provided by authorities or consumer centers.

★Concerns. While everyday users noticeably struggled to describe concrete threats, talking about general concerns – what users care about and fear might happen [21] – was an easier endeavor. A major area of concern was online banking and finances: everyday users (especially women, those with chronic diseases, and low-income participants) found it very important to protect banking information, but also worried about data loss or loss of access. Participants also raised other concerns related to privacy and third-party data management, as "the internet does not forget":

> "*Someone is drawing conclusions. But it's probably not someone, but algorithms. I don't even know who is working with this data everywhere*" [P04].

Concerns about a lack of transparency and data abuse were set in relation to broader concerns about fake news, manipulations, and surveillance: *"It leads to the consolidation of fake news and conspiracy theories. I think that is really dangerous"* [P30]. Similarly, participants discussed the consequences of algorithms and technologies on daily life and society due to rapid developments and increasing complexity: *"Although I wouldn't consider myself particularly old, I feel overwhelmed by some [technological developments]"* [P16]. Some worried that quick technological developments would cause friction to social cohesion and pose a risk if not accompanied by according awareness and education programs:

> "*Too much new knowledge was simply assumed all at once to be able to use the whole thing easily. And this generation, [they can] generally use it, but don't understand [it]*" [P21].

For others, their concerns were overwhelming and resulted in disengagement with S&P altogether:

> "*I can no longer defend myself against this. The data is there, the data is stored permanently, and a third party can process this data without my consent. I find that very unsafe*" [P12].

4.3 Motivation

Motivation is another important factor for S&P acceptance according to SPAF. On top of the underlying factors mentioned by SPAF (*subjective norms, perceived relative advantage, trialability*, and *compatibility*), we identified ★*enthusiasm* and ★*responsibility* as two additional underlying factors that shape motivation.

Subjective Norms. Subjective norms, i.e., perceived expectations from others [3], were prominent in shaping the usage of tools such as firewalls or antivirus software, which were almost exclusively mentioned by everyday users: *"I learned [from my father], the first thing to do with a new PC, is to install antivirus software"* [P39].

We also observe gendered patterns in the adoption of behaviors. For example, women participants identified providing information online as a risk: *"I am a woman, and I am alone. You have to be careful"* [P34]. In addition, women participants recounted being socialized to be scared of technology through past generations. P34 said:

> *"[As] women, we were kept away from technology. I'm still afraid today when I touch something technical, I might break something. Whenever the PC or laptop does something weird, I get scared and think I've broken it."*

Noticeably, these norms and stereotypes were not only encountered by older women. P09, a woman enthusiast, shared: *"The salesman said to me: 'Buy a MacBook. It's a woman's computer. You can't do anything wrong with that."* As such, these prevailing stereotypes [100], ingrained as subjective norms, can deeply inhibit women's self-efficacy and motivation when engaging with S&P.

Perceived Relative Advantage. Several participants stated they felt secure, as they had experienced no incident so far – yet acknowledged that they were not able to assess it. Others, especially women and low-income participants, felt they would not be a target: *"They probably just had a tear in their eye when they saw my account balances"* [P02]. Perceiving attacks as efforts only targeting wealthy, prominent individuals or organizations, they saw no reason to engage in further protective measures. While enthusiasts, and mostly men, felt quite confident in their protective measures, others expressed a sense of futility and powerlessness: *"Experts can of course crack everything"* [P29].

Despite being aware of certain S&P advice regarding secure messengers and social media, some participants felt the associated costs outweighed the benefits of staying in touch with other people. This tradeoff presented a special challenge for participants with chronic diseases or disabilities, who received valuable information and advice from online forums and communities. Other participants refrained from using social media, big platforms or companies, smart home devices, online shops, or cloud services. Some participants refrained from secure messengers or password (PW) managers, contradicting expert advice.

Trialability. In terms of trialability, i.e., "the degree to which an innovation may be experimented with on a limited basis" [82], participants broadly agreed that *"100% security is an unattainable goal"*. The abstractness and invisibility of threats make it hard to assess the benefits of S&P measures through trial [27]; i.e., a *lack of* trialability caused feelings of insecurity. For example, regarding MFA enforced by banks, everyday users still felt a sense of insecurity as they were not able to assess the measure's effectiveness: *"People say it's secure. So I try to believe it's secure"* [P03]. On the other hand, enthusiasts would trial S&P practices by engaging in self-pentesting practices or trying out Linux products.

Compatibility. According to SPAF, compatibility refers to how S&P advice fits with users workflows, identities, and perceptions or values. Interestingly, we observed cases where compatibility with values or concerns outweighed compatibility with workflows. In other words, sometimes participants were willing to sacrifice usable workflows. For example, many participants had pronounced privacy concerns, especially regarding targeted content and cookies, and even some older adults would use tools to prevent tracking: *"[It's] important to me to preserve anonymity, I run it after every use"* [P36].

Concerns with data aggregation motivated participants to engage in various obfuscation techniques, from to providing fake data, to using different pseudonyms and several e-mail addresses, which some also related to phishing prevention. Even though these practices were sometimes at odds with their workflows, or caused friction with their task, the feeling of lacking control over data caused them higher discomfort.

★Enthusiasm. We identified enthusiasm – for technology or for learning new things in general – as a prominent factor in shaping motivation. Enthusiasts usually taught themselves about S&P on their own, perceiving tinkering with tools and settings as a fun-inducing hobby, often dating back to their early childhood or teenage years. P09 explained how she would set S&P challenges to herself that involve additional learning effort: *"As others say: 'We lived vegan for half a year', I only used Linux products for half a year."*

P21 explained hosting his own services, did penetration testing, and continually learned about S&P out of fun:

> *"I am very interested in technology. I naturally enjoy fixing problems. Although I cause most of the problems myself because I'm tinkering with the service."*

Yet, this enthusiasm was not shared by everyone: *"I want to use this thing, and I don't want to know much else"* [P38]. While older adults especially appreciated the new opportunities for learning the Internet gave them, they experienced great frustrations when trying to learn about S&P online.

★Responsibility. Motivation can also stem from the perception of S&P as a (shared) responsibility. Participants largely felt left on their own with taking care of it, calling on institutions, organizations, regulatory bodies, and government to do their part by providing better policies:

> "*The conditions have to be created, by politicians and so on, so this can be implemented. And there must be opportunities for companies to bring in [experts]*" [P06].

For enthusiasts in particular, while they ascribed the responsibility to organizations and governmental institutions, they did not trust organizations and governmental institutions to do it right due to opposing interests or business models. As such, they were highly motivated to engage in elaborated, time-consuming practices, facilitated by their enthusiasm and a balance of the associated costs and benefits. Moreover, they emphasized that current systems and structures were not laid out to ensure S&P, so holding users accountable for their own S&P would be a *"perpetrator-victim reversal"* [P46].

4.4 Ability

Across different groups within our sample, there were noticeable differences in terms of S&P practices they engaged in, the challenges they faced, and how they dealt with the challenges. In addition to *system usability and accessibility*, we identified ★*access to resources* (financial, mental, social, and time) as a new underlying factor shaping ability.

System Usability and Accessibility. Enthusiasts were overall confident in their practices, primarily engaging in technical measures. While it could take them some time to set them up, or they would face technical friction from time to time (e.g., due to a lack of interoperability), they perceived it as an annoyance they could handle or a fun problem to solve. However, they acknowledged their practices were not manageable for everyday users who lacked their enthusiasm and ability: *"What I do is not a model that is somehow generally usable, [most] people can't do that"* [P05].

The dominant theme for everyday users was authentication – participants acknowledged the practice's importance yet talked about it with annoyance. They elaborated on their own PW management systems, including differentiating between accounts of different importance, managing several PW lists, and creating memory aids and PW rules to remember various combinations of letters, symbols, and numbers, like *"a story you can reconstruct"* [P26]. However, they encountered issues with this approach, and some admitted falling back to insecure practices as the workload was too much. Participants welcomed MFA as an additional layer of security, despite the friction it causes. They also appreciated the usability of biometric authentication, yet felt uncertain about its security: *"My ability is limited. [...] If I am always too scared and don't trust its protection, then I can't use it at all"* [P03].

Other participants said they used firewalls and antivirus software, yet faced usability issues, and they felt they were unable to assess these tools' actual workings or security. Secure messengers were also discussed ambivalently by everyday users – not in relation to usability, but rather utility and privacy concerns: *"If everyone uses WhatsApp, you are out of the loop with Signal"* [P04]. Despite being concerned with privacy, only very few everyday users used privacy-enhancing technologies, as high amounts of friction caused abandonment. Further, several participants – especially older adults – refrained from online banking as a protective measure, accepting additional costs and time to work through their finances even as more physical branches were closing down.

★Access to Resources. Beyond general accessibility, often discussed in relation to the user's own characteristics (e.g., different physical abilities, digital literacies, and educational attainment) [27], we identify access to resources as an underlying factor for ability; the resources include finances, time, but also one's mental and emotional capacities.

The workload for researching S&P information and maintaining practices was perceived as "*not manageable if you don't work on it full-time*" [P19] – even by enthusiasts. Some participants further stressed the financial costs of acquiring additional storage space to do backups or new devices to continue to receive updates. The financial costs put an additional burden on participants with lower income, often intersecting with chronic disease or disability and age.

While enthusiasts tend to comfortably manage the tradeoffs, everyday users resorted to self-blame using phrases like *"I know I should"*. For example, some recounted dealing with several unique passwords was too much for them, causing them to engage in insecure password practices despite better knowledge. This was a pressing issue for older adults and participants with chronic diseases or disabilities – which often overlapped – struggling with fiddly settings, but also limited time and energy to deal with S&P: *"... then the tiredness comes through again"* [P43].

Backups represented another significant challenge. Despite great motivation to prevent data loss, everyday users struggled to remember doing them, did not know what system to use, or had mixed feelings about cloud services. Participants with lower income further explained that they lacked the resources to acquire additional storage space to do so.

Similarly, regular updates were not done either due to past usability issues, or no longer receiving updates when using older devices. However, acquiring newer devices required access to finances – as well as to time, ability, and enthusiasm to adjust habitual behaviors to something new: *"As soon as something new comes up you have to think: 'How do I do that now?', [and] have to be really careful what you do"* [P37].

Being careful was a major practice among participants, e.g., checking for trust signals on websites, or only using trusted sources in general. Being careful as S&P practice was especially pronounced among participants lacking in-depth understanding and awareness of threats and measures. However, even these seemingly simple heuristic-based practices added extra burden on participants, requiring extra cognitive workload. Even when the usability and accessibility of S&P tools and advice are guaranteed, non-adoption might still occur when participants face significant barriers in accessing necessary social, economic, and mental resources.

4.5 Barriers to S&P

We identified several barriers participants face when attempting to learning about S&P and adopting protective practices:

S&P communication, *fear and limited trust*, *limited digital skills* and *limited social support*. These barriers further intersect with participants' sociodemographics.

Poor Communication of S&P. Participants reported communication issues related to S&P knowledge, including jargon, problematic framing, and a lack of shared language. These issues make S&P information and notifications hard to access, often requiring further research:

> "*[They] simply require too much prior knowledge [and] use these very specific, unfamiliar terms. I have to look it up first, what did they mean again?*" [P37].

This lack of accessible language impacts the quality of support from experts and one's social networks. P04 describes her experience of attending a talk by an S&P expert:

> "*[He] certainly made a lot of nice offers, but I can't take advantage of them[.] 35-year-old nerds write for 35-year-old nerds. But we are simply left out.*"

Further, the prevalence of English terminology presented an obstacle to our German participants, especially to older adults: *"There are so many words for which no images can be generated in my head"* [P36].

This lack of common and shared language impeded advice-seeking and caused misunderstandings: supportees struggled to articulate their problems or got lost in technical details, and supporters struggled with where to start. Enthusiasts found it hard to avoid technical language and refrain from discussing complex technicalities in their communication: *"It's hard to teach people, because [the] whole thing is super complex, like how everything works technologically"* [P10]. Supporters highlighted the effort to communicate in a target-group-specific way, focusing on the needs and requirements at hand rather than explaining it from an S&P perspective. However, volunteers in organizations found this easier: *"People say, 'Well, you're not such a computer science nerd, you can explain it well'"* [P09].

Fear and Limited Trust. The impression that S&P information requires expert knowledge to understand, with an exclusive focus on attacks, further induced fear and prevented participants from seeking more information: *"I don't want to go online with shaky fingers"* [P02]. This fear was especially prevalent in older women, who recounted having been socialized to be especially careful when using digital technologies. Several participants highlighted overcoming this fear and establishing trust as a barrier, such as P20:

> "*If I recommend something that doesn't meet their trust, [that] doesn't help, [because] they don't have the feeling that it is secure, even though it is objectively secure.*"

For example, several participants explained not using PW managers or cloud services for backups due to a lack of trust. Older adults, in particular, emphasized the need for a trusted relationship with advice and support givers – which could sometimes only be achieved in 1-1 sessions instead of group support or own research.

Limited Digital Skills. Participants who engaged in their own research but had limited digital skills felt overwhelmed by the amount of information and what to do with it. Finding, comparing, and distinguishing trustworthy sources required a lot of time – with no guarantee of finding actionable advice suiting their use case: *"You can basically find everything on the Internet, but [if] you don't know what you're doing, then you're very lost"* [P17].

Limited digital skills also presented a barrier to giving advice and support, especially to older adults, who often infrequently used devices: *"Sometimes they only have a cell phone because their kids [want them to be reachable]"* [P15]. Supporters had to show and explain "basic" ways of using and handling a device or service, before even getting to S&P: *"If you tell them about VPN [you] won't get anywhere"* [P15]. Additionally, infrequent use caused older adults to forget what they had learned, hindering the solidification of skills:

> "*I tell [them] to make updates, [and they don't know how.] I'll do it for them, but I know as soon as they get home, they'll have forgotten it*" [P15].

Limited Social Support. Barriers can also occur in one's access to social support, which is further intertwined with one's sociodemographics. For most participants, they could only lean on their close ones for support: *"You don't have any contact points for help, so you're really dependent on private contacts"* [P17]. Some emphasized they did not have anyone in their social circles they could even talk to about the topic: *"In my circle of friends, I'm probably the one who has the most Internet knowledge"* [P02].

Associations and organizations offering courses and support were mostly available in bigger cities. As such, barriers to accessing social support were more pronounced for participants who lived in rural areas, alone, or with chronic diseases or disabilities, as the condition made them unable to leave the house as much; the latter two conditions also often intersect with older age. Due to limited sources, some older adults hired a personal IT specialist for support – if they could afford it. However, not being able to assess the advice they received and having to trust unknown persons left them feeling insecure and exploited. Two older women shared they felt *"scammed"* by their IT support, who tried to sell them services they did not need *"for security reasons."*

On the other hand, enthusiasts supporting their social circles would get easily frustrated, avoid the topic, only help when directly asked, and sometimes simply take over the task to avoid friction. While volunteers in associations were more aware of group-specific needs, they lacked resources to meet the high demands and costs associated with advice- and support giving: in terms of time, finances, devices, know-how, and patience, but also simply having access to a commonplace for 1-1 support: *"There are so many people who want to learn all this. It is simply not manageable. There is a tremendous need and perhaps we should address it"* [P37].

4.6 Improving S&P in Digital Societies

Throughout the interviews, participants discussed S&P as a social and cultural issue, requiring efforts from not only individual users but also multiple stakeholders. We present findings about participants' suggestions for improving S&P in digital societies.

Usable and Accessible Information and Mechanisms. Sometimes participants identified the need for usable and accessible S&P broadly, wishing things were *"less complicated"* [P28]. Others mentioned specific use cases or applications, especially tools for data management and backups, identity management, handling cookies and targeted advertising, and usable authentication. Beyond specific tools, accessibility desires also apply to advice and information. Here, participants generally demanded less technical jargon and suggested advice should preferably be provided as checklists and step-by-step instructions, like *"ready meals for IT"* [P09]. Others emphasized the importance of a participatory approach in developing tools and advice by including and engaging with various user groups: *"[They] should be developed much more closely with users, including those from different generations, [to] make an offer [that] is okay for the user"* [P04]. Several participants referred to the need for better defaults and standards across software and hardware.

Socio-Technical Implementation. Participants highlighted the necessity to implement S&P on a societal and governmental level, with involvement from the state, organizations, service providers, administrative bodies, and critical infrastructure joining forces. Some specifically called for digital sovereignty, i.e., laws and infrastructures enabling the self-determination of one's digital destiny [24]. Another topic was data minimization and transparency in data handling, often referring to the GDPR not being sufficiently implemented. In line with this, participants called for more control over data and its protection – individually and socially – as well as the need for offline alternatives.

There was a general call for more support. Everyday users emphasized human and local support, such as dedicated professionals citizens can turn to in order to recover from attacks. Further, participants stressed the need to build more S&P competence in a group-specific manner – such as by targeting older adults and schools to disseminate S&P knowledge and skills into society. To achieve this goal, better infrastructure, laws and regulations, proper funding, and cooperation between stakeholders were seen as necessary. Everyday users envisioned S&P being ingrained into society and culture as *"traffic rules"* [P17] or *"as popular as going hiking, or driving to the sea"* [P09].

5 Discussion

For all factors – awareness, motivation, ability – we observe gendered patterns that proliferate with increasing age and sparse technical expertise. Further, amplified concerns and barriers occur when older age intersects with chronic disease/disability, lower income, and a lack of exposure to digital technologies and S&P during the life course, e.g., at school or workplace. Additionally, we identified barriers running across awareness, motivation, and ability. To counter these barriers, participants called for embedding S&P in society and culture, by addressing usability and accessibility of measures, and engaging infrastructures and policies.

5.1 New Insights Compared to SPAF

Applying SPAF to a diverse sample of participants, our study reveals seven new underlying factors for awareness, motivation, and ability as well as four barriers that cut across them. Table 2 illustrates the findings as a refined and more holistic version of SPAF. We now discuss our key insights.

The Interdependence Between Awareness, Motivation, and Ability. Our results indicate S&P awareness, motivation, and ability are not separate factors as they interrelate and influence each other. For example, perceiving S&P practices as futile or avoiding them altogether (4.2) limits motivation and ability, even when system usability is guaranteed. A lack of awareness of measures, or lack of trust in them, limits ability, even when motivation is high (4.3).

Prior work that aims to promote S&P acceptance has primarily targeted one factor at a time, and it was mostly ability [27]. Nevertheless, this interdependence showcased by our findings emphasizes the need for integrative approaches to address S&P acceptance by considering awareness, motivation, and ability altogether [27]. Along this line, the four barriers we identified (4.5) are also intertwined with awareness, motivation, and ability, further validating that the three factors operate concurrently.

Institutional Support in Learning About Security and Privacy. We found *threat experiences and incidents* (4.2) as a prominent factor influencing awareness, similar to other prior work identifying threats as a trigger for the uptake of protective measures [65, 110]. However, a lack of in-depth understanding of threats caused friction when participants sought advice and appropriate countermeasures. In some cases, incidents caused participants to seek help from institutions and organizations, with varying results.

Our findings also highlight the role of *organizations and institutions* (4.2) in providing support and awareness, which is not covered in SPAF, but has been documented by other work [19, 70, 72, 98]. While everyday user participants were largely unaware of S&P specific organizations, those working in voluntary and non-governmental organizations were more aware of differential vulnerabilities [66, 70]. These participants are better equipped to provide tailored interventions and support, but they are also in dire need of *resources* (4.4) to do so efficiently and meet the demand [19]. A possible direction for future work is seeking to empower these in-

Table 2: A refined version of SPAF informed by our findings, including seven new underlying factors and four barriers.

	SPAF Factors	New Factors		Barriers
Awareness	•Social Engagement •Mental Models & Digital Literacy •Media Exposure •Warnings & Notifications	•Threat Experiences •Own Research •Institutions & Organizations •Concerns	Differential Access	•S&P Communication •Fear and Limited Trust •Limited Digital Skills •Limited Social Support
Motivation	•Subjective Norms •Perceived Relative Advantage •Trialability •Compatibility	•Enthusiasm •(Shared) Responsibility		
Ability	•System Usability •Accessibility	•Access to Resources (material, mental, social, time)		
Embedded in Society & Culture				

dividuals in disseminating knowledge and best practices as security champions; while prior work has mostly investigated security champions in the workplace [8], such efforts can be broadened to NGO settings.

Self-Learning Tied to Digital Skills and Literacy. A prevalent source for S&P awareness among our participants was doing their *own research* (4.2), another factor our findings add to SPAF. This finding highlights the proactiveness in even everyday users, contrasting the framing of users being passive recipients of expert advice [28]. However, doing own research requires *digital skills* [92, 93] (4.5) to find appropriate sources, as well as the *resources* (such as time) (4.4) to understand and assess them. Currently, the S&P advice landscape is still fragmented [5, 64, 74, 75, 89] and overwhelms everyday users. Future research should investigate how to improve *communication of S&P*, e.g, using creative methods to establish folklore [39, 95], and fostering positive security narratives [18, 61, 81] to reduce fear and build trust (4.5).

The Promises and Downstream Effects of Concerns. SPAF notes S&P as secondary concerns to users but does not highlight concerns as a prominent factor [27]. In contrast, our findings emphasize that S&P *concerns* (4.2) – i.e., what users care about or fear might happen [21] – are deeply intertwined with participants' awareness and have downstream effects on motivation and ability. While some participants had overwhelming concerns, inhibiting motivation and ability, others were willing to face the extra workload to meet their concerns. Moreover, especially for everyday users, talking about concerns is more effective than talking about threats, suggesting that efforts to address concerns are a fruitful starting point for research and interventions [18, 27]. Despite a disparity in threat models between enthusiasts and everyday users, they shared similar concerns. As such, we see concerns as an integral part of understanding users' acceptance and rejection of S&P practices and conducting human-centered threat modeling [27, 91].

Toward the goal of improving motivation, we also identified *enthusiasm* (4.3) as a new factor not covered by SPAF: the enthusiasm to tinker with technology, solve problems, and learn something new motivated users to overcome challenges and inconveniences. This opens up avenues for research on how to increase enthusiasm and make S&P more fun for less tech-savvy users.

Going Beyond System-level Usability and Accessibility. On issues related to usability and accessibility (4.4), our findings also suggest the dual role of friction. In certain instances, such as MFA, participants tolerated and sometimes even appreciated friction, as it gave them a sense of security. Everyday users engaged with social strategies (e.g., asking others for support), distancing behaviors (e.g., censoring online sharing and disclosure), and non-use (4.2,4.4) [83, 98], all of which came with the cost of missing out benefits provided by a digital society. These findings support recent work on "security-enhancing friction" [32], opening up avenues for research on how much and what kind of friction is tolerable or may even be desirable for users.

Moreover, as our findings show, *digital skills* (4.5) – as a pre-requisite for handling tools efficiently – are a major barrier to S&P awareness, motivation, and ability. While digital literacy (4.2) refers to mental operations of understanding and knowledge, digital skills involve active interactions and operations with hardware and software, and communication [92]. As usability mainly aims at ease and efficiency of use, the goal of achieving usability might actually counteract the acquisition of digital skills. Further, one's *access to resources* (in terms of material, mental, and social resources as well as time) significantly impacts S&P ability. While usability aims at reducing time and mental workload, future work aiming at inclusive S&P solutions should take into account resources in other formats as well.

Toward Shared Responsibility. While SPAF is primarily for characterizing end-users, it highlights *shared responsibility* as an avenue for future work, as the "wider ecosystem of interactors who work to ensure a secure and trustworthy cyberspace" [27]. Our findings suggest that this ecosystem should include experts, organizations, regulators, legislative bodies, and people in one's social support network. We – and our participants (4.3, 4.6) – see the necessity of examining and improving the broader ecosystem in order to ensure the acceptability of S&P practices and re-distributing responsibility from individual users to more privileged stakeholders to counter cyber-attacks [79].

5.2 Differential Access to Security and Privacy

Our interview study based on a diverse sample enables us to dive into the possible "why" of sociodemographic differences [101], especially when several identities that make individuals "at-risk" [98] intersect with one another [20, 25]. For instance, older age intersects with and amplifies varying physio-cognitive abilities, chronic illness, and lower income, increasing the burden and cost of adopting S&P measures. A key takeaway from our findings is the notion of *differential access*: the S&P risks and vulnerabilities faced by individual users hinge on their social and relational positions in the society [70, 98], intersecting identities [41, 58] and the resources they can access.

Impact from Limited Resources. Similar to Kostan et al. [55], we found that lower-income participants continued using older devices and software no longer supported by updates; some could not afford storage space for backups (4.4). In contrast, those with higher incomes could afford to hire professional IT support, yet at times felt scammed as they could not assess the given advice (4.5). Our findings add to the limited research on the interplay between income and security behaviors [101], which remains understudied and is an important topic for future work.

In addition to limited financial resources, our findings capture resources in a broader sense, also including access to time, mental and emotional capacities, and social capital (4.4, 4.5) [77, 93]. For participants with less time and mental/emotional capacities, the workload of maintaining common S&P practices could become too high. To obtain S&P information and support, our participants relied heavily on their own research and social contacts (4.2, 4.5) [37, 45], but those who lacked access to such resources were left alone in dealing with S&P. Future work should look into opportunities for intervention in streamlining and equalizing access to S&P by enabling individuals to obtain support from *institutions and organizations* (4.2), especially organizations specializing in S&P topics, which were largely unheard of among everyday users.

Gendered Stereotypes and Gaps. Across all age groups, women participants showed less self-efficacy [10] when engaging with S&P; while they sometimes did their own research, they also heavily relied on men for support and advice. Some women participants reported being talked down upon when doing so, encountering the assumption they would not understand or be interested, inhibiting motivation. Older women, in particular, recounted having been socialized to be especially careful with technical devices, decreasing trust and increasing fear (4.2, 4.3, 4.5). Our findings confirm prior work on gendered gaps in digital skills [48].

Nonetheless, prevailing gender stereotypes related to S&P [100] might serve as a deeper explanation of the observed gaps and behaviors. Our findings also suggest the existence of gender stereotypes (4.3): Women are less confident, while men might be overconfident. Related work found that women and men prefer different S&P advice sources [23, 72], and show differences in the uptake of S&P practices [101], further emphasizing the need for tailored interventions and researching gender in relation to other factors and barriers.

The Interplay Between Age and Other Sociodemographic Factors. While the importance of age in studying S&P behaviors is not new, our findings highlight the interplay between age and other sociodemographic factors: 1. gender; 2. different physical and cognitive abilities; 3. education and income; 4. experience and exposure to digital technologies over the life course [27, 77]. For example, older adults drawing on former experience with digital technologies at the workplace showed less fear and greater self-efficacy [10] when dealing with S&P, and would also support others. Yet, especially older women expressed avoidance of S&P, or reverted to non-use out of fear – especially when lacking social support, or access to resources (4.2, 4.3, 4.5). On the other hand, young adults who've grown up with digital technologies recounted less friction in usage, yet studies show this does not correlate with S&P usage [68, 94, 101]. Our work indicates that the mixed findings on age's influence on S&P [101] may be explained by other intersecting factors, emphasizing the need to take them into account in future work.

Adding Differential Access to Universal Access. Altogether, our findings suggest that access to S&P is differentiated and heavily tied to accessibility across the physical, cognitive, emotional, financial, and social dimensions (4.4, 4.5) [70, 77, 93]. Currently, access to S&P largely hinges on the contingency of one's social and relational position within society [70] and having access to resources, which varies depending on intersecting socio-demographic factors and identities. As such, intersectionality [20, 25] results in *differential access*. Further, Schauberger's "universal barriers to access" framework posits there are fundamental reasons why someone is struggling with a service, and focusing on these barriers might be a more sustainable approach than segmenting the people who experience them, as it results in an infinite list of different conditions or characteristics [84]. Our findings echo the strength of thinking along the line of universal access as we identified common barriers across participants from a wide range of demographics (4.5). Moreover, by focusing on S&P, we identified new barriers compared to Schauberger's framework drawn from governmental digital services broadly, namely barriers in social support [37], digital skills [92, 93], and how S&P is framed and communicated [57, 95]. Thus, we argue, that combining the concepts of intersectionality and *differential access* offers a powerful approach to uncover the underlying "whys" of user behavior, as well as pinpointing barriers to S&P in design and socio-cultural environment.

Overall, the prevailing friction and remarkably persistent sense of futility and resignation regarding S&P [102] among participants indicate we, as the S&P community, need to become better at being "persuasive" [102]: not only in usability, but in the stories we tell about S&P, and the way we tell them, to embed S&P in the digital society and culture sustainably.

5.3 Security and Privacy in Digital Societies

Our results show that everyday users faced significant barriers to S&P. *Differential access* requires differential interventions to enable S&P behaviors among diverse user groups, rather than delegating responsibility to individual users (4.3, 4.6) [47, 79, 80]. Our findings suggest the importance of integrative approaches to accessible and usable S&P, that address awareness, motivation, and ability at the same time [27]. Tailored interventions and support can facilitate competencies and capabilities [28, 29] to implement S&P in digital societies (4.5, 4.6). Further, our results align with prior work [19, 70] suggesting that voluntary S&P supporters, provided with necessary resources, could serve as security champions [8, 53, 66], facilitate assisted access [19], and address individual concerns rather than amplifying threats [87].

Different user groups face different risks [70, 98], and require different skills based on their experiences. To address the digital skills gap [22, 48, 92, 93], more efforts should be directed at increasing a society's digital competencies and capabilities, enabling individual users to acquire the S&P advice and skill they need in their individual circumstances and contexts, facilitating the life-long learning that is required by rapid technological developments (4.2, 4.5, 4.6). Our findings further support the relevance of participatory, human-centered approaches [17, 34, 78], including users from different backgrounds [77, 97], to ensure acceptability of S&P measures.

Some wishes from our participants involve making S&P *"common knowledge"*, habitual like *"traffic rules"*, and *"as popular as going hiking"* (4.6). Achieving these goals requires a holistic re-conceptualization of security culture [71, 90], i.e., the ways we think about and do security, and the role of humans as both users of technologies but also citizens in a society [33]. Researchers have proposed "learning from safety science" [35] and "cyber resilience" [33] as ways forward, requiring cooperation among different societal stakeholders and across different fields of expertise.

Our participants were largely aware of – and concerned with – this: they perceived S&P as a societal and cultural issue, embedded in larger structures and processes of regulation and policy (4.6). We encourage future work to take up on this, and identify potentials and obstacles of policies to facilitate usable and accessible S&P, co-develop tailored interventions for S&P capabilities, and further engage the socio-technical gap "between what we know we must support socially and what we can support technically" [2].

6 Conclusion

> "[The] dynamics of computational artifacts extend beyond the interface narrowly defined, to relations of people with each other and to the place of computing in their ongoing activities. System design, it follows, must include not only the design of innovative technologies, but their artful integration with the rest of the social and material world."
>
> – Lucy Suchman [69]

Our study aimed at addressing the prevailing gap between expert-recommended S&P advice and user behavior, as well as the knowledge gap on the interplay of user diversity and S&P behaviors. We represent results of the first systematic application of the SPAF to a diverse sample with 47 participants from different socio-demographic backgrounds, including age, gender, income, education, chronic illness and disabilities, and different levels of expertise.

Our analysis of the in-depth interviews reveals additional underlying factors affecting S&P awareness, motivation, and ability that are so far not included in SPAF: threat experiences and incidents, organizations and institutions, own research, and S&P concerns influence awareness, enthusiuasm and shared responsibility affect motivation, access to resources is a pre-requisites for ability. We further identify barriers running along awareness, motivation, and ability, inhibiting access to S&P: S&P communication, fear and limited trust, and lack of digital skills as well as social support.

Analyzing the intersections of socio-demographic factors, such as gender, age, income, education, chronic disease and disability, as well as technical expertise, we contribute the notion of *differential access* to S&P, requiring differential interventions such as tailored S&P communication and skill-building, and addressing universal barriers in design. The notion of differential access can support future work in explaining contradictory results on the interplay of socio-demographics and S&P behavior.

Based on our results, we contribute a refined version of SPAF to further inform research and interventions.

We conclude that *usability is not enough*: participants saw S&P embedded in larger social and cultural processes of policy and regulation. In face of rapid technological advancements, digital S&P requires lifelong learning, social support, and attention to different circumstances and contexts users find themselves during the course of their lives.

We encourage researchers and practitioners to tailor their engagements and interventions, co-develop accessible and inclusive measures that are adaptable to different and changing contexts, support social S&P multipliers and champions, and to foster cooperation between different societal stakeholders and disciplines to cultivate holistic security cultures.

Acknowledgments

We thank everyone involved in this project, from our participants who enabled the study, to our student assistants supporting our work, Angela Sasse for valuable support and advice, and our reviewers for their thorough feedback. The research was partially funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under the Germany's Excellence Strategy—EXC 2092 CASA—390781972, by the Federal Ministry of Education and Research (BMBF) under the project 16KIS1646K "Digi-Fit", and the Max Planck Society.

References

[1] Jad Al Aaraj, Olivia Figueira, Tu Le, Isabela Figueira, Rahmadi Trimananda, and Athina Markopoulou. Vbit: Towards enhancing privacy control over iot devices. *arXiv preprint arXiv:2409.06233*, 2024.

[2] Mark S Ackerman. The intellectual challenge of cscw: The gap between social requirements and technical feasibility. *Human–Computer Interaction*, 15(2-3):179–203, 2000.

[3] Icek Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 1991.

[4] Simon Anell, Lea Gröber, and Katharina Krombholz. End user and expert perceptions of threats and potential countermeasures. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 230–239. IEEE, 2020.

[5] David Barrera, Christopher Bellman, and Paul C. van Oorschot. Security Best Practices: A Critical Analysis Using IoT as a Case Study, September 2022.

[6] Adam Beautement and Angela Sasse. The economics of user effort in information security. *Computer Fraud & Security*, 2009(10):8–12, 2009.

[7] Adam Beautement, M Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 new security paradigms workshop*, pages 47–58, 2008.

[8] Ingolf Becker, Simon Parkin, and M Angela Sasse. Finding security champions in blends of organisational culture. *Proc. USEC*, 11:124, 2017.

[9] Clara Berridge, Yuanjin Zhou, Amanda Lazar, Anupreet Porwal, Nora Mattek, Sarah Gothard, and Jeffrey Kaye. Control matters in elder care technology: Evidence and direction for designing it in. In *Proceedings of the 2022 ACM Designing Interactive Systems Conference*, pages 1831–1848, 2022.

[10] Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M Angela Sasse, and Malte Elson. Self-efficacy and security behavior: Results from a systematic review of research methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–32, 2024.

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

[12] Virginia Braun and Victoria Clarke. *Thematic analysis.* American Psychological Association, 2012.

[13] Virginia Braun and Victoria Clarke. To saturate or not to saturate? questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative research in sport, exercise and health*, 13(2):201–216, 2021.

[14] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. *Thematic Analysis*, pages 843–860. Springer Singapore, Singapore, 2019.

[15] 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, 2019.

[16] Nicholas Cofie, Heather Braund, and Nancy Dalgarno. Eight ways to get a grip on intercoder reliability using qualitative-based measures. *Canadian Medical Education Journal*, 13(2):73–76, 2022.

[17] Lizzie Coles-Kemp et al. Inclusive security: digital security meets web science. *Foundations and Trends® in Web Science*, 7(2):88–241, 2020.

[18] Lizzie Coles-Kemp and René Rydhof Hansen. Walking the line: The everyday security ties that bind. In *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5*, pages 464–480. Springer, 2017.

[19] Lizzie Coles-Kemp, Nick Robinson, and Claude PR Heath. Protecting the vulnerable: Dimensions of assisted digital access. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–26, 2022.

[20] Patricia Hill Collins. Intersectionality's definitional dilemmas. *Annual review of sociology*, 41(1):1–20, 2015.

[21] Jessica Colnago, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Stanton. Is it a concern or a preference? an investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 331–346, 2022.

[22] European Commission. Germany in the Digital Economy and Society Index. https://digital-strategy.ec.europa.eu/en/policies/desi-germany.

[23] Kovila PL Coopamootoo and Magdalene Ng. "Un-Equal online safety?" a gender analysis of security and privacy protection advice and behaviour patterns. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 5611–5628, 2023.

[24] Stephane Couture and Sophie Toupin. What does the notion of "sovereignty" mean when referring to the digital? *New media & society*, 21(10):2305–2322, 2019.

[25] W Crenshaw Kimberlé. On intersectionality: Essential writings, 2017.

[26] Sauvik Das. Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *it-Information Technology*, 58(5):237–245, 2016.

[27] Sauvik Das, Cori Faklaris, Jason I. Hong, and Laura A. Dabbish. The security & privacy acceptance framework. *Foundations and Trends® in Privacy and Security*, 5(1-2):1–143, 2022.

[28] Partha Das Chowdhury, Andrés Domínguez Hernández, Kopo Marvin Ramokapane, and Awais Rashid. From utility to capability: A new paradigm to conceptualize and develop inclusive pets. In *Proceedings of the 2022 New Security Paradigms Workshop*, NSPW '22, page 60–74, New York, NY, USA, 2023. Association for Computing Machinery.

[29] Partha Das Chowdhury and Karen Renaud. 'ought' should not assume 'can'? basic capabilities in cybersecurity to ground sen's capability approach. In *Proceedings of the 2023 New Security Paradigms Workshop*, NSPW '23, page 76–91, New York, NY, USA, 2023. Association for Computing Machinery.

[30] Michael Ann DeVito. How transfeminine tiktok creators navigate the algorithmic trap of visibility via folk theorization. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–31, 2022.

[31] Michael Ann DeVito, Jessica L Feuston, Erika Melder, Christen Malloy, Cade Ponder, and Jed R Brubaker. Safety and community context: Exploring a transfeminist approach to sapphic relationship platforms. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1):1–34, 2024.

[32] Verena Distler, Gabriele Lenzini, Carine Lallemand, and Vincent Koenig. The framework of security-enhancing friction: How ux can help users behave more securely. In *Proceedings of the New Security Paradigms Workshop 2020*, pages 45–58, 2020.

[33] Myriam Dunn Cavelty, Christine Eriksen, and Benjamin Scharte. Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*, 26(7):801–814, 2023.

[34] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. Understanding the experience-centeredness of privacy and security technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*, pages 83–94, 2014.

[35] Nico Ebert, Thierry Schaltegger, Benjamin Ambuehl, Lorin Schöni, Verena Zimmermann, and Melanie Knieps. Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, page 103435, 2023.

[36] Ahmet Erinola, Annalina Buckmann, Jennifer Friedauer, Aslı Yardım, and M Angela Sasse. "as usual, i needed assistance of a seeing person": Experiences and challenges of people with disabilities and authentication methods. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 575–593. IEEE, 2023.

[37] Cori Faklaris, Laura Dabbish, and Jason I Hong. A framework for reasoning about social influences on security and privacy adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2024.

[38] Matthias Fassl and Katharina Krombholz. Why i can't authenticate—understanding the low adoption of authentication ceremonies with autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2023.

[39] Matthias Fassl, Alexander Ponticello, Adrian Dabrowski, and Katharina Krombholz. Investigating security folklore: A case study on the tor over vpn phenomenon. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2):1–26, 2023.

[40] Lothar Fritsch, Kristin Skeide Fuglerud, and Ivar Solheim. Towards inclusive identity management. *Identity in the Information Society*, 3:515–538, 2010.

[41] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. " like lesbians walking the perimeter": Experiences of {US}.{LGBTQ+} folks with

online security, safety, and privacy advice. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 305–322, 2022.

[42] Ayako A. Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How WEIRD is usable privacy and security research? In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 3241–3258, Philadelphia, PA, August 2024. USENIX Association.

[43] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 1–20, 2019.

[44] Claude PR Heath and Lizzie Coles-Kemp. Drawing out the everyday hyper-[in] securities of digital identity. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2022.

[45] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. Digital security—a question of perspective. a large-scale telephone survey with four at-risk user groups. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 27–27. IEEE Computer Society, 2023.

[46] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. A world full of privacy and security (mis) conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–23, 2023.

[47] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, 2009.

[48] Initiative D21 e.V. Digital Skills Gap: So (unterschiedlich) digital kompetent ist die deutsche Bevölkerung. https://initiatived21.de/uploads/03_Studien-Publikationen/Digital-SKills-Gap/digital-skills-gap_so-unterschiedlich-digital-kompetent-ist-die-deutsche-bevoelkerung.pdf.

[49] 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, 2015.

[50] 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, 2015.

[51] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. Human factors in security research: Lessons learned from 2008-2018. *arXiv preprint arXiv:2103.13287*, 2021.

[52] Smirity Kaushik, Natã M Barbosa, Yaman Yu, Tanusree Sharma, Zachary Kilhoffer, JooYoung Seo, Sauvik Das, and Yang Wang. GuardLens: Supporting safer online browsing for people with visual impairments. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 361–380, 2023.

[53] Becky Kazansky. 'it depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society*, 8(1):2053951720985557, 2021.

[54] Erin Kenneally and David Dittrich. The menlo report: Ethical principles guiding information and communication technology research. *Available at SSRN 2445102*, 2012.

[55] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in germany through qualitative interviews. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2029–2046, 2024.

[56] Maria Lamond, Karen Renaud, Lara Wood, and Suzanne Prior. *SoK: Young Children's Cybersecurity Knowledge, Skills Practice: A Systematic Literature Review*, page 14–27. Association for Computing Machinery, New York, NY, USA, 2022.

[57] Genevieve Liveley. Stories of cyber security combined report. *Research Institute for Sociotechnical Cyber Security*, 2022.

[58] Abby Marsh and Ada Lerner. Privacy norms of transformative fandom: A case study of an activity-defined community. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1):1–29, 2024.

[59] Peter Mayer, Yixin Zou, Byron M Lowens, Hunter A Dyer, Khue Le, Florian Schaub, and Adam J Aviv. Awareness, intention,(in) action: Individuals' reactions to data breaches. *ACM Transactions on Computer-Human Interaction*, 30(5):1–53, 2023.

[60] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proc. ACM Hum.-Comput. Interact. (CSCW)*, 2019.

[61] Bill McSweeney. *Security, identity and interests: a sociology of international relations*. Number 69. Cambridge University Press, 1999.

[62] Joya Misra, Celeste Vaughan Curington, and Venus Mary Green. Methods of intersectional research. In *Intersectional Experiences and Marginalized Voices*, pages 10–29. Routledge, 2024.

[63] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–24, 2021.

[64] Lorenzo Neil, Harshini Sri Ramulu, Yasemin Acar, and Bradley Reaves. Who comes up with this stuff? interviewing authors to understand how they produce security advice. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 283–299, 2023.

[65] Magdalene Ng, Maria Bada, and Kovila PL Coopamootoo. What we do in the shadows: How does experiencing cybercrime affect response actions & protective practices? In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 659–672. IEEE, 2023.

[66] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. Training and embedding cybersecurity guardians in older communities. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2021.

[67] Donald A Norman. Some observations on mental models. In *Mental models*, pages 15–22. Psychology Press, 2014.

[68] Annika Onemichl and Carolin Bolz. Digitalbarometer - Bürgerbefragung zur Cyber-Sicherheit 2022. Technical report, Bundesamt für Sicherheit in der Informationstechnik, November 2022.

[69] Steven Pemberton, K Ehrlich, and A Henderson. Design:(inter) facing the millennium: where are we (going)? *Interactions*, 7(1):19–30, 2000.

[70] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–24, 2018.

[71] Alessandro Pollini, Tiziana C Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, 24(2):371–390, 2022.

[72] 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*, pages 666–677, 2016.

[73] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *IEEE Symposium on Security and Privacy*, SP '16, pages 272–288, San Jose, California, USA, May 2016. IEEE.

[74] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium*, pages 89–100. USENIX, 2020.

[75] 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, October 2017.

[76] Karen Renaud. Accessible cyber security: the next frontier? In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pages 9–18, 2021.

[77] Karen Renaud and Lizzie Coles-Kemp. Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, 3(5):346, 2022.

[78] Karen Renaud and Stephen Flowerday. Contemplating human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications*, 34:76–81, 2017.

[79] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, 78:198–211, 2018.

[80] Karen Renaud, Craig Orgeron, Merrill Warkentin, and P Edward French. Cyber security responsibilization: an evaluation of the intervention approaches adopted

by the five eyes countries and china. *Public Administration Review*, 80(4):577–589, 2020.

[81] Paul Roe. The ‘value’of positive security. *Review of international studies*, 34(4):777–794, 2008.

[82] Everett M Rogers, Arvind Singhal, and Margaret M Quinlan. Diffusion of innovations. In *An integrated approach to communication theory and research*, pages 432–448. Routledge, 2014.

[83] Shruti Sannon and Andrea Forte. Privacy research with marginalized groups: What we know, what’s needed, and what’s next. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–33, 2022.

[84] Ute Schauberger. Universal barriers to access. https://uteschauberger.com/barrierstoaccess.html. [Accessed 07-11-2024].

[85] Shirin Shams and Delphine Reinhardt. Vision: Supporting citizens in adopting privacy enhancing technologies. In *Proceedings of the 2023 European Symposium on Usable Security*, pages 253–259, 2023.

[86] Xiaoxin Shen, Eman Alashwali, and Lorrie Faith Cranor. What do privacy advertisements communicate to consumers? *arXiv preprint arXiv:2405.13857*, 2024.

[87] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *extended abstracts of the 2021 CHI conference on human factors in computing systems*, pages 1–6, 2021.

[88] Xinru Tang, Yuling Sun, Bowen Zhang, Zimi Liu, RAY Lc, Zhicong Lu, and Xin Tong. " i never imagined grandma could do so well with technology" evolving roles of younger family members in older adults’ technology learning and use. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–29, 2022.

[89] Sarah Turner, Jason Nurse, and Shujun Li. When Googling It Doesn’t Work: The Challenge of Finding Security Advice for Smart Home Devices. In Steven Furnell and Nathan Clarke, editors, *Human Aspects of Information Security and Assurance*, IFIP Advances in Information and Communication Technology, pages 115–126, Cham, 2021. Springer International Publishing.

[90] Betsy Uchendu, Jason RC Nurse, Maria Bada, and Steven Furnell. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109:102387, 2021.

[91] Warda Usman and Daniel Zappala. Sok: A framework and guide for human-centered threat modeling in security and privacy research. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 33–33. IEEE Computer Society, 2024.

[92] Alexander JAM Van Deursen and Jan AGM Van Dijk. *Digital skills: Unlocking the information society*. Springer, 2014.

[93] Jan AGM Van Dijk. Digital divide: Impact of access. *The international encyclopedia of media effects*, pages 1–11, 2017.

[94] Lea van Nek and Carolin Bolz. Digitalbarometer 2021: Bürgerbefragung zur Cyber-Sicherheit. Technical report, Bundesamt für Sicherheit in der Informationstechnik, September 2021.

[95] Luca Viganò. The cybersecurity of fairy tales. *Journal of Cybersecurity*, 10(1):tyae005, 2024.

[96] Yang Wang. The third wave? inclusive privacy and security. In *Proceedings of the 2017 new security paradigms workshop*, pages 122–130, 2017.

[97] Yang Wang. Inclusive security and privacy. *IEEE Security & Privacy*, 16(4):82–87, 2018.

[98] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2344–2360. IEEE, 2022.

[99] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS ’10, pages 1–16, New York, NY, USA, July 2010. Association for Computing Machinery.

[100] Miranda Wei, Pardis Emami-Naeini, Franziska Roesner, and Tadayoshi Kohno. Skilled or gullible? gender stereotypes related to computer security and privacy. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2050–2067. IEEE, 2023.

[101] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M. Redmiles, and Franziska Roesner. Sok (or solk?): On the quantitative study of sociodemographic factors and computer security behaviors. *CoRR*, abs/2404.10187, 2024.

[102] Dirk Weirich and Martina Angela Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms*, pages 137–143, 2001.

[103] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium*, volume 348, pages 169–184, 1999.

[104] Marisol Wong-Villacres, Arkadeep Kumar, Aditya Vishwanath, Naveena Karusala, Betsy DiSalvo, and Neha Kumar. Designing for intersections. In *Proceedings of the 2018 Designing Interactive Systems Conference*, pages 45–58, 2018.

[105] Yuxi Wu, Sydney Bice, W Keith Edwards, and Sauvik Das. The slow violence of surveillance capitalism: How online behavioral advertising harms people. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, pages 1826–1837, 2023.

[106] Yuxi Wu, W Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879. IEEE, 2022.

[107] Yaxing Yao, Davide Lo Re, and Yang Wang. Folk models of online behavioral advertising. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 1957–1969, 2017.

[108] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 'i make up a silly name': Understanding children's perception of privacy risks online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[109] Zhixuan Zhou, Tanusree Sharma, Luke Emano, Sauvik Das, and Yang Wang. Iterative design of an accessible crypto wallet for blind users. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 381–398, 2023.

[110] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2020.

[111] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. Cross-contextual examination of older adults' privacy concerns, behaviors, and vulnerabilities. *Proceedings on Privacy Enhancing Technologies*, 2024.

A Participants

Table 3 shows the participants' detailed demographics.

Table 3: Participant sample (n=47).

	Age	**Gender**	**Migration backg.**	**Chron. Disease**	**Education**	**Income**	**City Size**	**Enthusiast**
P01	older	w	×	✓	lower ed.	low	medium	×
P02	older	w	×	✓	lower ed.	middle	(major) city	×
P03	older	w	✓	×	higher ed.	low	(major) city	×
P04	older	w	×	✓	higher ed.	upper	medium	×
P05	adult	m	×	×	university	upper	(major) city	✓
P06	young	w	×	✓	higher ed.	middle	medium	×
P07	adult	m	×	×	university	middle	rural & small	✓
P08	adult	m	×	×	university	middle	medium	×
P09	adult	w	×	✓	university	upper	(major) city	✓
P10	young	m	×	×	lower ed.	middle	rural & small	✓
P11	adult	n.b.	×	×	higher ed.	low	(major) city	×
P12	adult	m	×	×	university	upper	medium	✓
P13	young	w	×	×	higher ed.	middle	medium	×
P14	young	m	×	×	university	low	(major) city	×
P15	older	w	✓	✓	university	low	(major) city	×
P16	adult	m	✓	×	university	upper	(major) city	×
P17	adult	m	×	×	lower ed.	low	(major) city	×
P18	older	m	×	–	higher ed.	low	(major) city	×
P19	adult	m	×	✓	lower ed.	low	rural & small	×
P20	young	m	×	×	higher ed.	low	(major) city	✓
P21	adult	m	✓	✓	university	upper	medium	✓
P22	adult	w	×	✓	lower ed.	low	medium	×
P23	older	w	×	×	university	low	(major) city	×
P24	adult	w	×	×	higher ed.	low	(major) city	×
P25	adult	w	✓	×	university	low	(major) city	×
P26	adult	m	×	×	lower ed.	upper	(major) city	×
P27	adult	w	×	✓	university	middle	(major) city	×
P28	adult	m	✓	×	higher ed.	low	rural & small	✓
P29	young	m	×	×	lower ed.	low	medium	×
P30	older	w	×	✓	lower ed.	low	(major) city	×
P31	adult	m	×	×	higher ed.	middle	medium	×
P32	older	w	×	✓	lower ed.	middle	medium	×
P33	young	w	×	×	university	low	medium	×
P34	adult	w	×	✓	university	low	(major) city	×
P35	adult	m	×	✓	university	upper	(major) city	✓
P36	older	w	×	✓	university	low	(major) city	×
P37	older	w	×	×	lower ed.	middle	medium	×
P38	older	w	×	✓	university	low	(major) city	×
P39	young	w	×	×	higher ed.	low	(major) city	×
P40	adult	m	×	×	higher ed.	low	medium	×
P41	adult	m	✓	✓	university	upper	(major) city	✓
P42	young	m	✓	×	lower ed.	low	rural & small	×
P43	older	w	×	✓	lower ed.	middle	(major) city	×
P44	older	m	×	×	higher ed.	upper	(major) city	×
P45	older	w	×	✓	university	upper	(major) city	×
P46	adult	m	×	×	university	upper	rural & small	✓
P47	older	m	×	✓	university	upper	rural & small	✓

B Codebook

Table 4 shows our high-level codes.

Table 4: Code table with high-level codes.

Code	Explanation
Security perception	Understanding of, attitudes towards, and meaning of security
Security practices	Practices to ensure security
Security experiences	Experienced threats to security
Privacy perception	Understanding of, attitudes towards, and meaning of privacy
Privacy practices	Practices to protect privacy
Privacy experiences	Experienced threats to privacy
Threat actors	Actors who could pose a threat or carry out an attack
Threat Models	Known threats and attacks
Concerns	Concerns and worries regarding security and privacy and the Internet
Non-Use	Non-Use due to S&P concerns
S&P Learning	Where participants learned about S&P
S&P support and advice seeking	Where and how participants seek support and advice regarding S&P
S&P support and advice giving	How and to whom participants give support and advice regarding S&P
Friction and Challenges	Experienced friction, barriers, and obstacles when engaging S&P
S&P needs, wishes, requirements	Participants' S&P needs, requirements, and wishes for improvement
Responsibility	Assigned responsibility for S&P
Role of social position	Influence of social position on S&P
Role of knowledge	Influence of knowledge on S&P

C Interview Guide

Our interview guide translated from German to English. All interviews were conducted in German.

Introductory block

- What role does the internet play in your live?
- What devices and services do you use regularly?
- Which data, devices, or services do you consider very important or very private?
- What about your workplace, or expierences with authorities?

Deeper into Assets and Priorities

- What does "[internet] security" mean to you?
- what do you want to protect?
- (pick up: What data, devices, services are especially important to you?) What do you need them for?
- Who do you share it with? what should remain private? Who shouldn't see it?
- What would happen if you lost it? What would happen if someone saw [it/them]?

S&P Practices

- How do you deal with them (tools, data)?
- Does it bother you when using?
- How do you know or feel you are safe?
- What are you doing to achieve this?
- You have tried to change something? What was that? How did it go?
- Has something disturbed or bothered you you?
- Have you had problems during use? what happened and what did you do?

Advice and Support Seeking

- How come you are doing it like this? Where and how have you learnt about it?
- How and where do you learn such S&P behavior in general?
- Is there something you don't follow? Why not?
- Do you also give advice to others? who and what?
- Who helps you? Do you help someone?

Concerns and Threats

- How safe/competent/though you feel when using this services?
- Have you ever felt insecure, uneasy, or concerned in the digital world / when using the internet? What happened?
- Are there services you also know analogue, and do you feel different online?
- Are you worried about losing data? or someone accessing it?
- Is there anything else bothering you regarding digital services and data?

- Have you ever had to use the internet, although you felt uncomfortable? Why did you feel uncomfortable? What did you do?
- What could happen if...? (pick up attack)
- who could have an interest? Who carries out (attacks)? Why? what could they do? what would happen? what would you do?
- What else are you concerned with?

Responsibility for S&P

- who is responsible for keeping your data secure / private?
- Someone else? Who should be responsible?

Improvements

- How satisfied are you regarding S&P?
- What bothers you?
- How to support you? What would make it easier for you?
- If you had a wish for improvement, what would that be?