Cyber Threat Awareness, Protective Measures and Communication Preferences in Germany: Implications from Three Representative Surveys (2021-2024)

Marc-André Kaufhold
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
kaufhold@peasec.tu-darmstadt.de

Julian Bäumler
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
baeumler@peasec.tu-darmstadt.de

Marius Bajorski
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
marius.bajorski@stud.tu-darmstadt.de

Christian Reuter
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
reuter@peasec.tu-darmstadt.de

Abstract

In light of the increasing vulnerability of citizens against cyberattacks, we conducted three representative surveys with German citizens in 2021 (N=1,093), 2023 (N=1,011), and 2024 (N=1,004) to examine their cyber threat awareness, use of protective security measures, and preferred information channels. While our findings attest large proportions of the German population a high level of cyber threat awareness, many citizens feel inadequately informed about coping with cyberattacks and show little confidence in German security authorities to protect citizens and infrastructures. While age correlated with citizens' awareness and behavior, we only saw minor temporal differences between datasets. Finally, we provide design and policy implications for enhancing citizens' awareness of cyber threats and implementing security measures.

CCS Concepts

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → *Social aspects of security and privacy.*

Keywords

Cyber Threat Awareness, Security Measures, Communication Strategies, Human-Computer Interaction, Representative Citizen Survey

ACM Reference Format:
Marc-André Kaufhold, Julian Bäumler, Marius Bajorski, and Christian Reuter. 2025. Cyber Threat Awareness, Protective Measures and Communication Preferences in Germany: Implications from Three Representative Surveys (2021-2024). In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3706598.3713795

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713795

1 Introduction

Understanding how citizens perceive cybersecurity, the measures they adopt, and the ways they inform themselves about cyber threats is critical for governments and organizations aiming to promote secure behavior and develop effective, user-centered security technologies [101]. The advancing digitization and networking of infrastructures and people towards a post-digital society [20], coupled with the increasing frequency and sophistication of cyberattacks [24], requires of citizens a basic level of threat awareness and security training to implement proper security measures, practices, and tools [39], such as in the case of e-mail and phishing protection [61, 77, 85], Internet of Things (IoT) security [3], password management [93], or web privacy [37, 58]. When designing usable security technologies [36], both developers and citizens are challenged by the need to balance the conflict of objectives between security and usability [89, 91]. In previous research on Human-Computer Interaction (HCI), it was found that the country of residence represents the strongest predictor for the prevalence of privacy and security misconceptions, which potentially impair the proper adoption of security technologies [44].

Furthermore, Germany was identified as a state-oriented risk culture where citizens' trust in state authorities is high, expecting them to prevent and manage incidents, while German citizens showed low awareness, knowledge, and confidence in their respective individual capabilities [21, 81]. However, research on the ransomware attack against a Düsseldorf hospital [88] or the Russian hack disabling thousands of wind turbines in Germany [90] showcase how cyberattacks might undermine public confidence in authorities. In light of this, it seems important to not only examine citizens' behavior and technology use but also their expectations of government communication regarding cyber threats and protective measures. Our literature review revealed that German citizens' cybersecurity behaviors and attitudes have so far only fragmentarily been investigated with regard to correlations with demographic variables [67] and temporal trends. Moreover, the information behavior and expectations of the German population regarding the communication about cyber threats and protective measures have not received scientific attention thus far.

As the findings of surveys with such a focus might be important building blocks to design and evaluate both guidelines and strategies that enhance authorities' and citizens' preparedness and response to cyber threats [53], we seek to answer the following research question: **Using the example of Germany, what are design and policy implications to enhance the awareness, implementation, and communication of cybersecurity information?** To answer these questions, we conducted three representative surveys with German citizens in 2021 (N=1,093), 2023 (N=1,011), and 2024 (N=1,004). By combining three datasets for an advanced descriptive, statistical, and comparative analysis, our study seeks to provide the following contributions to the domain of human-centered cybersecurity research:

- Empirical insights into citizens' awareness of cyber threats, implemented security measures, as well as knowledge about and trust in security agencies (C1).
- Statistical insights into socio-demographic and temporal factors influencing citizen behavior and perceptions with regard to cybersecurity (C2).
- Design and policy implications for enhancing citizens' and employees' awareness of cyber threats and the implementation of security measures (C3).

This paper will present related work on the cybersecurity attitudes, protective measures, and communication preferences of German citizens (Sec. 2) before introducing the method consisting of questionnaire design, data collection, and analysis (Sec. 3). Then it will present the analysis of our representative surveys with German citizens (Sec. 4). Finally, it will discuss design and policy implications for enhancing citizens' and employees' cybersecurity, and compare our results to those of related work (Sec. 5).

2 Related Work

To motivate our survey, key findings with regard to cyber threat perception, exposure and protective measures, and communication of cybersecurity information from the most recent surveys with a focus on Germany are presented below.

2.1 Cyber Threat Awareness and Perception

The awareness and behavior of the German population with regard to cybersecurity have already been investigated in several representative studies with an academic or policy background. In the context of the Russian war of aggression against Ukraine, one 2022 representative survey commissioned by the German digital industry sector association Bitkom (N=1,002) focused on cyberattacks as a means of warfare [83]. It revealed that three quarters of Germans expected wars to be increasingly fought digitally (77%) and were worried about cyber wars being waged against Germany in the future (75%). Already in 2016, a survey of U.S. citizens (N=1,040) found a similar high threat perception; 70% expected major cyberattacks on public infrastructures in the next five years [71].

Although, according to other representative Bitkom surveys from 2021 (N=1,011) and 2023 (N=1,018), most Germans considered themselves primarily responsible for protecting their data ('21: 88%) [5] and their security on the internet ('23: 74%) [28], they articulated need for improvement of governmental cybersecurity activities, particularly regarding the policing of cybercrime. The 2021 and 2022 follow-up surveys (N=1,014) indicate that a large majority wanted the police to show more presence in the digital space ('21: 91%; '22: 93%) and demanded greater state investment in police units specializing in cybercrime ('21: 92%; '22: 97%) [5, 27]. Clear deficits are also seen in the capabilities of the German armed forces; in the 2022 survey on cyberattacks in warfare, only a minority of Germans (10%) believed that the armed forces were sufficiently equipped to defend Germany in cyberspace [83]. Yet, according to Bitkom figures ('19: N=1,004; '20: N=1,016), the proportion of citizens that agree that Germany should actively respond to a cyberattack with counterattacks declined from 2019 to 2020 ('19: 46%; '20: 43%) [7, 79]. Further, a survey (N=707) on the 2020 Düsseldorf hospital hack shows how cyberattacks potentially undermine public confidence in governmental institutions since the public may perceive the authorities as incapable of defending against future threats [88].

The annual surveys by Bitkom further indicate a growing individual threat perception among the German population; the share of people who consider their data to be unsafe on the internet has overall increased between 2020 and 2023 ('20: 68%; '23: 77%) [5, 29, 79, 83]. This corresponds with a rise in the share of the population that assumes a growing threat from cybercriminals ('20: 94%; '21: 98%) and that is more afraid of cybercrime than of analog crime ('20: 39%; '21: 48%) [5, 79]. As regards threat actors on the internet, in 2023, Germans felt most threatened by organized crime (87%), followed by individuals (35%), state actors (24%), and companies (5%) [28]. With regard to the perception of specific cyber threats, the Bitkom surveys also reveal an increase between 2019 and 2021 [5, 7, 79]. This is the case for not only typical cybersecurity and data security threats such as the illegitimate use of data by companies ('19: 79%; '21: 85%), malware infection ('19: 62%; '21: 82%), and the abuse of passwords and accounts ('19: 54%; '21: 62%), but also for phenomena such as hate speech ('19: 11%; '21: 27%), insults and bullying on the internet ('19: 17%; '21: 26%), or sexual harassment online ('19: 17%; '21: 26%). From 2022 onwards, comprehensive data on Germans' perception of these threats is not available.

2.2 Threat Exposure and Protective Measures

According to a 2024 representative survey (N=3,047) commissioned by the Federal Office for Information Security (BSI) and the Police Crime Prevention of the Federal States and the Federation (ProPK), almost one quarter of Germans (24%) have already been personally affected by cybercrime at least once [14]. The proportion of those affected has been relatively stable over the last five years; in surveys by the same institutions in 2020 (N=2,000; 25%), 2021 (N=2,025; 25%), 2022 (N=2,000; 29%) and 2023 (N=3,012; 27%) a similar proportion stated to have been victimized [10–13]. A large-scale victimization study conducted in the German state of Lower Saxony in 2020 (N=4,102) revealed a victimization level of a slightly higher magnitude (30%) [64]. For the Finnish population, Näsi et al. discovered through a representative survey (N=5,455) in 2018 that men were more likely to be affected by malware than women [70]. However, in contrast to [64], a positive correlation was found with regard to age; increasing age is associated with higher malware exposure. Based on a representative survey (N=11,953) of U.S. citizens in 2021, an age correlation was found with regard to the exposure to different types of online fraud [9].

The BSI and ProPK surveys from 2022 to 2024 further requested all self-reported victims of cybercrime to indicate the type of incidents they had experienced [12–14]. While around a quarter of those concerned in 2024 have been affected by online shopping fraud ('22: 25%; '24: 30%) or unauthorized access to an online account ('22: 25%; '24: 24%), around a fifth has become a victim of malware ('22: 24%; '24: 21%) or phishing ('22: 19%; '24: 18%). More than ten percent were affected by identity theft ('22: 19%; '24: 14%), calls from criminals pretending to be IT-support staff ('22: 9%; '24: 13%), and fraud via messenger services ('22: 11%; '24: 10%), whereas online banking fraud ('24: 9%), ransomware ('22: 10%; '24: 6%), and different types abusive content were less common.

Whether Germans actually implement specific protective measures against cybersecurity threats is another topic of the annual surveys by BSI and ProPK [10–14]. Most commonly adopted were up-to-date antivirus programs ('20: 57%; '24: 47%), strong passwords ('20: 48%; '24: 47%), two-factor authentication ('20: 33%; '24: 37%), up-to-date firewalls ('20: 47%; '24: 32%), regular manual updates ('23: 30%; '24: 26%), automated updates ('20: 25%; '24: 22%), regular backups ('20: 20%; '24: 22%), and encrypted e-mail ('20: 18%; '24: 16%) or messenger communication ('23: 17%; '24: 14%). Password managers within the browser ('23: 14%; '24: 15%) or as separate applications ('23: 9%; '24: 10%), as well as virtual private networks (VPNs) ('23: 11%; '24: 11%) were less common. Due to security concerns, some respondents also refrain from using social networks ('20: 10%; '24: 8%), online banking ('20: 10%; '24: 7%), or online shopping ('23: 3%; '24: 3%). For most of the measures surveyed, the degree of adoption among the German population increased between 2020 and 2021 but declined from 2021 to 2024.

2.3 Communication of Cybersecurity Advice

Concerning the communication of cyber threats, protective measures, and advice to the German population, the surveys commissioned by the BSI and ProPK indicate deficits [10–14]. The 2022 survey revealed that almost a third (31%) claim to have never noticed any recommendations on how to protect themselves against cybercrime [12], and from 2022 to 2024, more than one fifth ('22: 23%; '24: 23%) state that they have never informed themselves about cybersecurity [12–14]. By contrast, more than half of respondents ('22: 51%; '24: 57%) inform themselves at least occasionally. Yet, in 2022, only 76% of those who have already encountered cybersecurity recommendations considered them comprehensible [12]. This is consistent with the finding from the 2021 survey that, in addition to a high implementation effort (44%), complicated and difficult-to-understand recommendations (43%) were named as the main barrier to the full implementation of recommendations [11].

The 2023 and 2024 surveys additionally asked those actively searching for cybersecurity information about used information channels and found that they inform themselves most commonly through websites ('23: 64%; '24: 69%), family, friends, and acquaintances ('23: 39%; '24: 39%), social networks ('23: 29%; '24: 34%), television ('23: 26%; '24: 27%), videos or tutorials ('23: 19%; '24: 21%), apps ('23: 15%; '24: 16%), printed or digital newspapers ('23: 15%; '24: 15%), printed or digital specialized journals ('23: 13%; '24: 14%), newsletters ('23: 12%; '24: 13%), and radio ('23: 11%; '24: 11%) [13, 14]. Results from 2023 show that in the future, Germans would like to receive information on cybersecurity through websites (42%), traditional media like TV, radio or newspapers (36%), newsletters (21%), YouTube (18%), and dedicated apps (17%) [13]. The survey conducted by the European Commission further shows that in 2019, 80% of Germans were not aware of any official channel for reporting cybercrime and illegal online behavior, which is roughly in line with the European average (77%) [49].

2.4 Summary of Findings and Research Gaps

The review of existing surveys revealed that a significant share of knowledge about the cybersecurity attitudes and behavior of the German population originates from studies conducted on behalf of government agencies or industry associations [5, 7, 10–12, 15, 79, 83]. Scientifically published studies typically had a more narrow focus and were concerned with cybercrime victimization, general cybersecurity knowledge and behavior, and privacy and security misconceptions [44, 64, 96]. In light of this, this work addresses three distinct research gaps. First, correlations between demographic variables and behaviors and attitudes of the German population have only been studied fragmentarily before. Analyses have only been performed with regard to cybercrime victimization, general cybersecurity knowledge and behavior, and attitudes toward nudging [41, 51, 64, 96].

Second, the studies mostly refer to datasets from a singular survey. None of the scientific publications uses longitudinal data and analyzes temporal differences and trends. The only data available in this regard is provided by the annual surveys by BSI and ProPK [10–14] or Bitkom [5, 7, 79]. In addition, the respective research reports only compare data on selected topics for different years. Moreover, an explicit analysis and interpretation of trends rarely takes place. Third, the information behavior and expectations of the population regarding the communication about cyber threats and protective measures have not received scientific attention thus far. Surveys of German authorities, however, have already provided initial descriptive information on perceived information deficits [11–14], currently used information sources [13, 14], as well as requested information types [12–15] and channels [13].

3 Method

To answer this paper's research questions, we designed a questionnaire with practitioners, considered measures to mitigate biases that are inherent in survey-based research, commissioned the data collection through an online panel provider in three iterations (2021, 2023, 2024), and performed a descriptive, comparative, and statistical data analysis (Figure 1).

3.1 Questionnaire Design

In order to design the questionnaire, we conducted two creative workshops with eight participants, thereof four cybersecurity experts from German CERTs representing the roles of an incident manager, IT security officer, public safety answering point, and team leader, and four researchers from the domains of digital humanities, human-computer interaction, IT security, and political science. Following an established approach from previous works, we followed the notion of facilitating individual creativity (e.g., reflection) before collective creativity (e.g., brainstorming) could

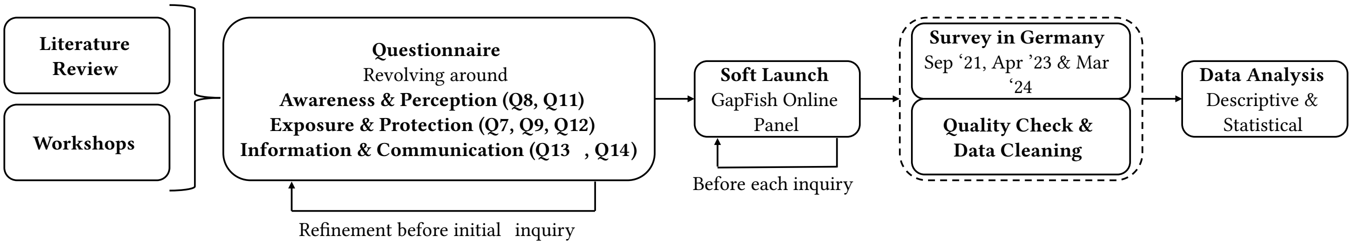
Literature Review
Workshops
Questionnaire
Revolving around
Awareness & Perception (Q8, Q11)
Exposure & Protection (Q7, Q9, Q12)
Information & Communication (Q13 , Q14)
Refinement before initial inquiry
Soft Launch
GapFish Online Panel
Before each inquiry
Survey in Germany
Sep '21, Apr '23 & Mar '24
Quality Check & Data Cleaning
Data Analysis
Descriptive & Statistical

Figure 1: Overview of the methodological approach and timeline of our study on German citizens' cyber threat awareness, protective measures, and communication preferences.

influence individual thoughts [23]. At the beginning of the first workshop, we introduced the overall goal of designing a questionnaire for the conduction of a representative survey. In the following reflection phase, participants were able to note ideas or questions on a digital board, before they used a presentation phase to discuss their ideas and arrange them thematically. Based on this, the authors designed a draft version of the questionnaire. The second workshop was again hosted online to discuss and refine the questions and their items, generate new ones, and reflect upon their thematic grouping and relevance for the underlying research project. We used the participants' feedback to create a second draft of the questionnaire and distributed it via email for a final round of feedback. After conducting a pre-test with 10 persons, we added explanations to difficult terms and thought about potential response biases.

To minimize the potential *question order bias* [47] in our questionnaire design, we took several measures. Firstly, we ensured that respondents were not primed by asking general questions before specific ones. Secondly, we organized similar questions into thematic blocks. Thirdly, we conducted a pre-test to assess if the question order caused any irritation among the respondents. While the questions were presented in the same order for all participants, the rows in matrix questions were randomized. Additionally, obtaining demographic information before the thematic questions was necessary to meet the panel provider's requirement for sample representativeness. Furthermore, in order to address concerns of *unbalanced questions and scales* [35], we carefully worded our questions and items in a neutral and objective manner. We employed balanced scales, such as Likert scales with a neutral option, wherever possible. Moreover, to prevent survey time fatigue and maintain respondents' attention [17], we designed the questionnaire for an average completion time of 20 minutes, as determined during the pre-test. An attention check item, "Please click on 'Rarely' here" (Q12), was included to verify respondents' attentiveness and sincerity. Finally, managing *social desirability bias* [66] proved challenging, especially in measuring cybersecurity behavior [31]. To address this to some extent, we selected the self-administered survey mode, which can enhance respondents' perception of privacy and anonymity, thus encouraging more honest answers [57, 66]. However, as our survey relies on self-reported data, we acknowledge the possibility of biased results. The final version of the questionnaire comprised nineteen questions (Appendix A), asking for the consent of participation (Q1), demographic variables (Q2-6), and then our thematic questions (Q7-14).

3.2 Data Collection

The study was conducted in accordance with the requirements of the ethics committee at our university, such as avoiding unnecessary stress, excluding risk and harm, and anonymizing participants. While the personal data collected were limited to age, gender, education, income, and state (Table 1), participants were transparently informed about the goals of the study and then asked for their informed consent to participate. For the inquiry, we selected GapFish (Berlin) as an ISO-certified panel provider, ensuring panel and data quality, security, and survey quality within their panel of 500,000 active participants. After transmitting the final questionnaire, GapFish programmed and hosted the online survey. Based on data from the German Federal Statistical Office, GapFish set quotas for the different demographic variables to ensure representativity for the German population with regard to age, gender, education, income, and state. After final quality checks, a soft launch, and mutual agreement was achieved, they invited participants from their panel to take part in the surveys in September 2021 (N=1,093, t_{median}: 19.3 min.), April 2023 (N=1,011, t_{median}: 18.0 min.) and March 2024 (N=1,004, t_{median}: 18.2 min.) until the representativity quotas were met (e.g., of ~1,000 participants, ~51% should identify themselves as female and ~49% as male).

Due to the panel size, it is unlikely but still possible that participants took part in more than one of the three inquiries. The rationale for selecting these three specific points of inquiry relates to the potential impact of major global events on public perception of security and risk, including cybersecurity. The 2021 COVID-19 pandemic wave, the 2022 Russian invasion of Ukraine, and the 2023 Hamas-led attack on Israel received intense media coverage and involved heightened public discourse on security, digital threats, and misinformation. We sought to distance our survey collection dates from these events to minimize short-term heightened perceptions that might otherwise skew responses. This timing approach was designed to yield more stable long-term insights into public cybersecurity perceptions rather than capturing potentially reactive, event-driven attitudes. As the projected average length of the survey was 20 minutes, every participant received €2 (i.e., 10 cents per minute of the projected survey length) from the panel provider, which could be redeemed as a payout or voucher as soon as a certain threshold (e.g., €5 or €10) is reached, usually after multiple survey participations. The German original data (i.e., the codebook and survey data from 2021, 2023, and 2024) is provided as supplementary material in the ACM Digital Library.

Variable	Values
Age	18-24 (8.9, 8.1, 8.8%), 25-34 (14.6, 14.5, 14.4%), 35-44 (15.0, 14.7, 14.4%), 45-54 (16.7, 15.8, 16.5%), 55-64 (18.2, 18.8, 18.9%), 65+ (26.5, 28.0, 26.9%)
Gender	Female (50.2, 51.1, 50.9%), male (49.6, 48.7, 49.0%), diverse (0,1%), not stated (0,1, 0,1, 0,0%)
Education	Lower education (28.5, 17.6, 18.3%), middle school (36.0, 36.4, 34.0%), high school or academic degree (35.5, 46.8, 47.7%)
State	BB (2.6, 3.1, 2.8%), BE (4.5, 4.4, 4.6%), BW (13.4, 13.8, 11.9%), BY (15.9, 16.1, 16.0%), HB (0.8, 0.6, 0.8%), HE (7.6, 7.0, 7.3%), HH (2.3, 2.3, 2.2%), MV (1.6, 2.0, 2.0%), NI (9.7, 9.8, 10%), NW (21.7, 21.6, 22.1%), RP (4.9, 4.9, 5.0%), SH (3.6, 3.7, 3.8%), SL (1.2, 1.1, 3.8%), SN (4.9, 4.7, 5.0%), ST (2.7, 2.6, 2.8%), TH (2.6, 2.4, 2.6%)
Income	<1,500€ (24.5, 18.5, 18.7%), 1,500-2,600€ (30.8, 27.0, 26.9%), 2,600-4,500€ (28.9, 35.4, 32.8%), >4,500€ (15.7, 19.1, 21.6%)

Table 1: Demographic variables and values of the samples (2021, 2023, 2024). German states are represented by ISO 3166-2 abbreviations (e.g., BB→Brandenburg).

3.3 Data Analysis

The statistical analysis employed a custom Python script that utilized the SciPy library [95] for statistical calculations and pandas [73, 97] for data storage. An exploratory approach was adopted, calculating effect sizes between all pairs of variables, including demographic ones. Additionally, variables representing the cumulative score of specific questions (Q9, Q11, Q12, Q13) were introduced and correlated. Individuals who failed the "attention check" question were excluded from the study. For certain correlations, specific data points were filtered out. In the case of gender-related correlations, two data points were removed as they reported genders other than male or female. To ensure an ordinal scale, individuals who selected the "Other degrees" option were filtered out from correlations involving the degree as one of the variables. For Q9 and Q11, respondents who chose the option of "do not know" were filtered out when correlating those specific questions. Data points were only filtered out when they affected a particular variable. All correlations not affected by the above considerations were calculated using the entire dataset.

Spearman's rank correlation coefficient [99] was used to assess correlations between ordinal demographic variables (such as age group, income group, or degree) and other ordinal variables. For correlations between two non-demographic ordinal variables, we applied the Pearson correlation coefficient [33]. To compare the results between men and women, as well as between individuals from the western versus eastern German states, we conducted t-tests [94]. Additionally, t-tests were utilized to explore the relationship between ordinal variables and questions where participants could select a limited number of options from a list, comparing groups that did versus those that did not choose a specific option. When analyzing the relationship between two such questions, we employed the Chi-Square test [74]. For comparisons across individual federal states, we conducted one-way ANOVA tests [38].

Effect sizes were calculated for each test and categorized as "no effect," "weak," "moderate," or "strong." Only moderate and strong effects were reported. Spearman's Rho correlations were classified using the rule of thumb by Rea and Parker [76]. For ANOVA tests, the effect size was calculated using η^2 and interpreted based on guidelines from Miles and Shevlin [63]. The remaining tests were interpreted according to Cohen's guidelines [19]: Pearson correlation with r, t-tests with Cohen's d, and Chi-Square tests with Cramer's V as the measure of effect size.

The variables gender and state were measured on a nominal scale. To assess correlations with these variables, Pearson's Chi-square test [74] was employed. Cramer's V [22] was calculated as a measure of effect size, which was then converted to Cohen's ω and interpreted based on Cohen's guidelines [19]. For all other variables measured on an ordinal scale, the correlation was computed using Spearman's rho [65]. These correlations were interpreted by the rule of thumb of Rea and Parker [76]. We also conducted a statistical analysis to examine differences in response patterns between the 2021 and 2024 questionnaires. To compare descriptive results between the two questionnaires, we applied t-tests [94]. To assess whether the relationship between two ordinally scaled variables changed over time, we used the Fisher-Z test [26]. For relationships previously examined using t-tests, ANOVA tests, or Chi-Square tests, we employed a two-factorial ANOVA [38] to compare the results across the different years. For these comparisons, we did not calculate effect sizes, reporting only whether the differences were statistically significant.

3.4 Limitations and Mitigation Strategies

First, a key limitation of this study is the use of an exploratory approach to analyze a large number of individual potential relationships within the data. While this approach is valuable for uncovering new patterns and relationships in the absence of established hypotheses, it also increases the risk of identifying spurious correlations — that is, statistically significant relationships that may not reflect true underlying associations but rather arise by chance due to the number of comparisons being made. To mitigate this risk, we applied a more stringent significance threshold ($p < 0.001$) to minimize the possibility of false positives. Since our approach did not employ joint hypotheses and instead utilized individual rather than disjunction testing, we have decided not to adjust the alpha level further in accordance with the advice set forth by Rubin [84]. However, we acknowledge that the results should be interpreted cautiously, particularly in the absence of prior theoretical grounding or replication [72]. Future research should aim to confirm these findings using hypothesis-driven approaches. Furthermore, we have sought to mitigate the risk of spurious correlations by conducting a longitudinal study, which allows for the testing of these relationships over time. This approach strengthens the robustness of the findings by providing evidence of consistency across different time points, reducing the likelihood that the observed associations are due to chance. Yet, further confirmatory research (e.g., replication in independent samples) could provide additional validation.

Second, as participants were required in Q12 to select from a fixed scale without an option to indicate a lack of understanding, some responses might reflect assumptions or guesses rather than actual behaviors. This suggests that related findings should be interpreted cautiously, particularly for measures that require more technical knowledge, such as firewalls or end-to-end encryption. Third, the study was conducted using an online survey, which provides representative results regarding some demographic factors but only covers people who are willing to do online surveys; thus, they are most likely more familiar with the Internet. Fourth, data on population density was not collected nor investigated in this survey. Future studies could consider a more balanced distribution of participants across states or a larger sample size to examine the influence of rural and urban areas. It would be interesting to observe whether previous findings [6] can be reproduced in Germany, providing insights for developing region-specific cybersecurity education and communication strategies. Fifth, since our sample is based on German citizens, further surveys incorporating and comparing users of other nations with an individual-oriented or fatalistic risk culture [21, 81] could provide additional insights. Finally, we cannot explain the population's low confidence level in German authorities' cybersecurity capabilities. Investigating the reasons for such perceptions, including interviews or open-ended survey questions, represents a promising avenue for future empirical research.

4 Results

Given the large volume of gathered data, we observed numerous weak correlations between variables. However, for the sake of brevity, only moderate and strong relationships are reported in this paper. As a significance level, we chose $p < .001$ for correlations, t-tests, Fisher Z tests, and the ANOVAs. We focus on the latest results from 2024 but indicate the percentage-wise differences since 2021 in brackets (e.g., (+8)) and visualize selected interesting items across all years of inquiry to highlight their temporal change.

4.1 Increasing Use of Mobile and Smart Devices, Especially by Younger Citizens (Q7)

As an introductory question, we asked citizens about their internet devices (Figure 2). Overall, 96% (+2) of respondents stated that they use a smartphone, with the majority (70%, +12) using them for more than 2 hours per day on average, suggesting a noteworthy increase in screen time over the last years. In contrast, mobile devices without touchscreen and with internet access are used by only 21% (-1). A clear shift towards mobile devices becomes visible as the majority of respondents also use a notebook (82%, +6), tablet (63%), or stationary PC (52%, -8), while only 35% use internet-connected game consoles. With the exception of internet-enabled smart TVs, which are used by 78% (+5) of respondents, smart devices have not yet become ubiquitous. Still, smart speakers (40%, +6) and smartwatches (43%, +10) reached a stronger growth than smart lighting (22%, +2), smart heating thermostats (15%, +4), and interconnected cars (10%, +1). The analyses have shown that younger people use smartphones ($\rho(1002) = -0.41$) and gaming consoles ($\rho(1002) = -0.46$) more frequently than older people. Meanwhile, people from households with higher income use smart cars ($\rho(1002) = 0.21$) and smart heaters ($\rho(1002) = 0.21$) more often. Similarly, people with higher degrees of education tend to have higher laptop usage ($\rho(991) = 0.23$).

4.2 High Awareness, Moderate Preparedness, and Low Trust in Authorities (Q8)

When asking about cyber threat awareness on individual and societal levels, a large proportion of respondents evaluate the *current threat level* as quite high (Figure 3). First, on an individual level, 54% (+8) agree or strongly agree that cyber threats pose a serious risk to them. To enhance their security, 72% (+2) of participants support the assessment that internet use should be avoided without security software, and a further 62% (+2) state that they restrict their internet use to commonly known websites. Second, in terms of the *prospective threat level*, an even clearer pattern emerges: 83% (+11) agree that the individual risk of cyber threat victimization will increase, and 77% (+7) think a large-scale cyberattack on German public infrastructure is a realistic scenario in the next five years.

Furthermore, we asked our participants to estimate their individual cybersecurity abilities. With a large increase since 2021, 57% (+8) of our participants said that they feel insufficiently informed about cyber threats. This indicates a moderate *cybersecurity competence* of our participants, supplemented by the fact that only 39% (+1)

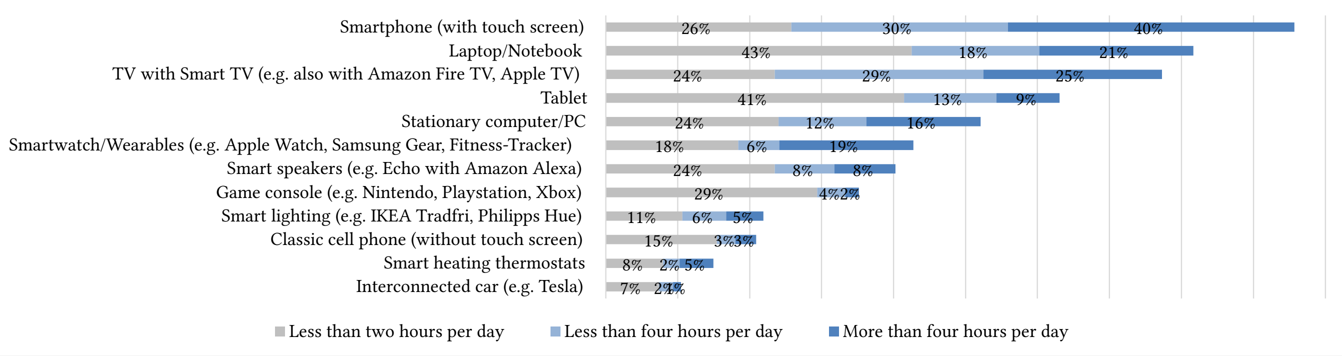

Figure 2: Which devices do you use to connect to the Internet at work and at home, and how often do you use them (Q7, 2024)? The option "Do not own" is not visualized for better comparability in this figure.

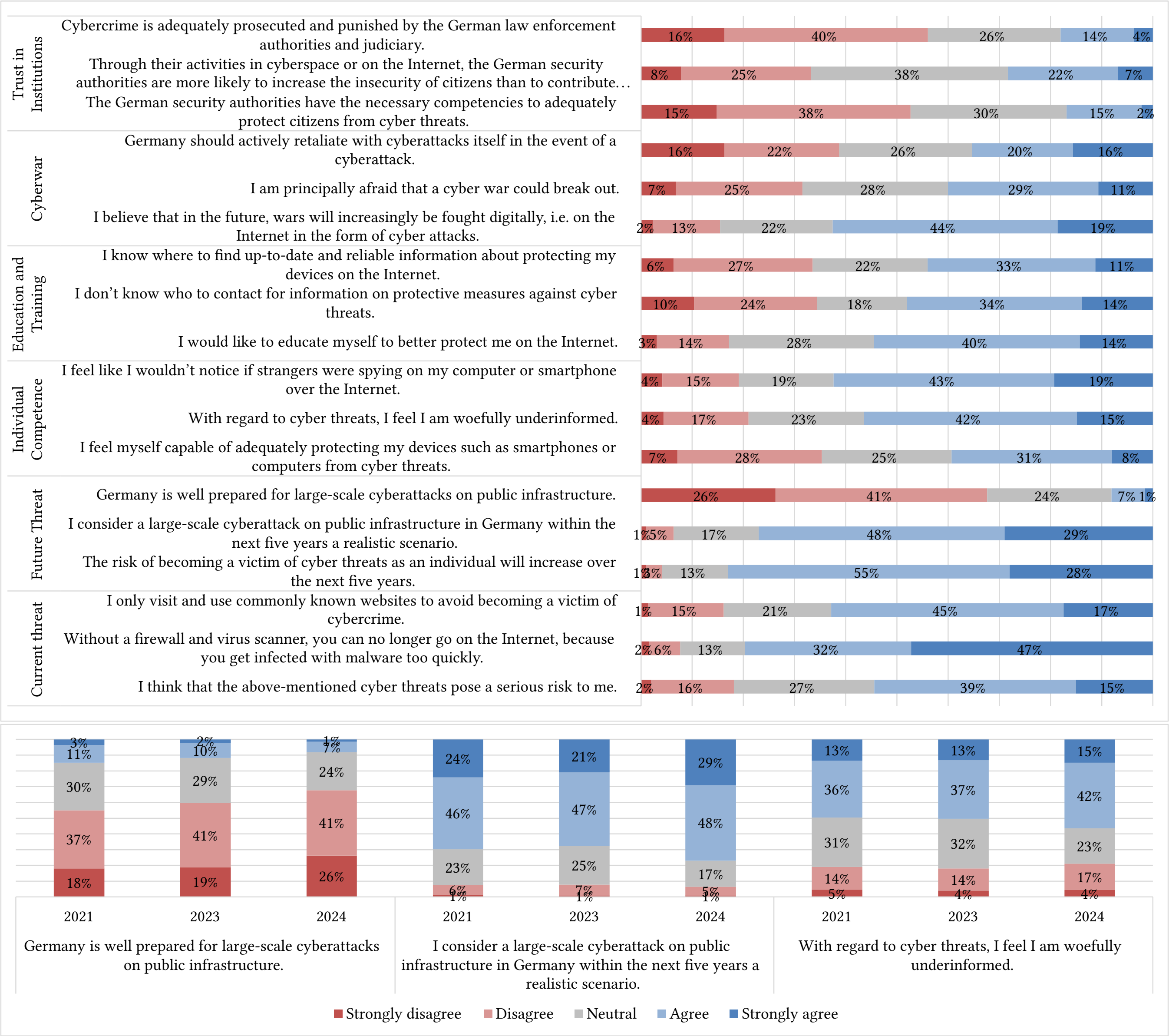

Figure 3: How much do you agree with the following statements regarding cyber threats, i.e., threats on the Internet (Q8, 2024)?

found themselves confident of protecting their own devices from cyber threats, whereas more than 62% (+3) do not feel confident of detecting spy attacks on the internet properly. Correspondingly, a *qualification demand* can be identified since 54% (-1) indicate that they would like to educate themselves about protection on the internet. However, 48% (-1) of interviewees state they don't know who to contact for information on protective measures, and 33% (-1) lack knowledge about internet sources on up-to-date and reliable information about device protection. The correlation analysis has shown that higher age strongly correlates with the agreement to the statement that "in the absence of a firewall and virus scanner, it is no longer possible to access the Internet, given the significant risk of infection with malware." ($\rho(1002) = 0.34$). According to the performed Fisher-Z test, this correlation is significantly higher than it was in the data of our previous questionnaire from 2021 ($z = 3.454$), where the correlation index was only $\rho(1091) = 0.20$.

To our surprise, only 8% (-6) consider Germany as well prepared for large-scale cyberattacks on public infrastructure, which steadily decreased since 2021 (Figure 2), and only 17% (-6) of respondents agree that German security authorities have the necessary competencies to adequately protect citizens from cyber threats, indicating low *trust in governmental institutions* (Figure 2). Furthermore, only 18% (-2) agree that cybercrime is adequately prosecuted and punished by German law enforcement agencies. However, a

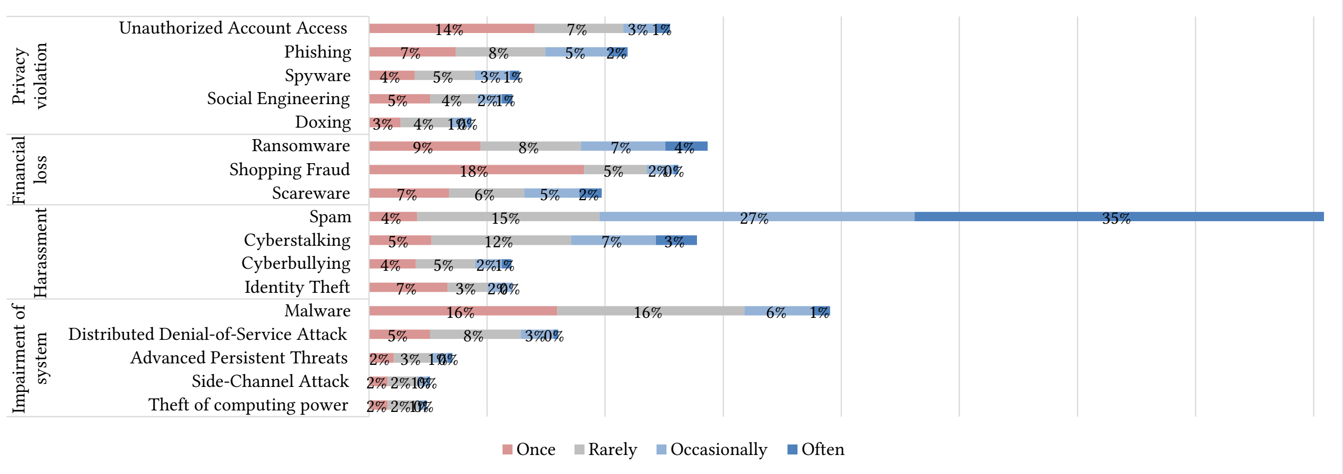

Figure 4: In the last five years, how often have you personally been a victim of the following types of cyber threats (Q09, 2024)? The options "Don't know" and "Never" are not visualized for better comparability in this figure.

majority of 63% of respondents think that wars will increasingly be fought digitally, but only 40% (+3) are generally afraid that a *cyberwar* could break out. Regarding the question of whether Germany should retaliate against cyberattacks with its own cyberattacks (e.g., hackback), the respondents are divided; 36% (-1) view this measure positively, and 28% (+1) negatively. Yet, we found that men view retaliation measures significantly more positively ($p < .001, t(1001) = 9.18, d = 0.58$). Analyzing the correlation between items, we found that the opinion that Germany is well prepared for large-scale cyberattacks on public infrastructure is strongly tied to the trust in German security authorities to have the necessary expertise to adequately protect citizens from cyber threats ($r(1002) = 0.58$). Similarly, the confidence in adequately protecting devices from cyber threats is strongly tied to the perceived knowledge of where to find up-to-date and reliable information on protecting end devices ($r(1002) = 0.52$).

4.3 Spam, Malware, and Ransomware Are the Most Prevalent Threat Types (Q9)

When it comes to susceptibility to cyberattacks (Figure 4), as many as 81% (+11) of respondents said they had been affected by spam at least once in the last five years; indeed, 62% (+11) have been affected by it occasionally or frequently. Moreover, 39% (-1) were affected by malware in the same period (7% (-3) of them occasionally or frequently) and 28% (-6) by ransomware (11% of them occasionally or frequently). In addition, 27% (+3) have already suffered financial losses due to online shopping fraud, and 20% (+4) due to scareware. More serious types of harassment than spam also affected a fraction of respondents, such as identity theft (12%, -4), cyberbullying (12%, -4), cyberstalking (27%, +13), and doxing (9%, -3). Furthermore, participants have been affected by unauthorized third-party access to an online or social media account (26%, +5) or a phishing attack (22%, +3) while being less exposed to the privacy threats

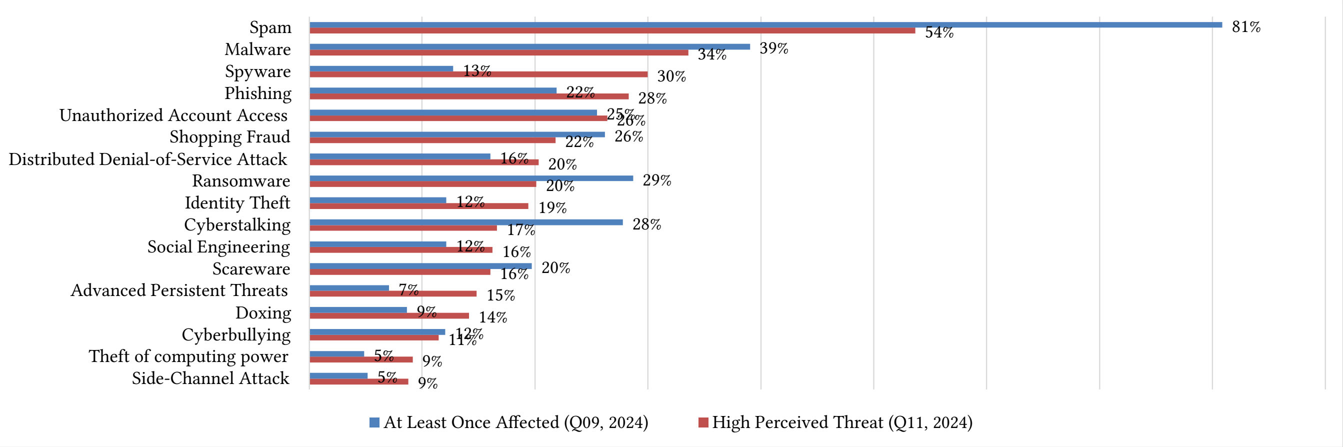

Figure 5: In the last five years, how often have you personally been a victim of the following cyber threats (Q09, 2024), and how high do you estimate the risk of becoming a victim of one of the following cyberattacks in the next five years (Q11, 2024)?

of spyware (12%, -5) and social engineering (12%, +3). Finally, few participants indicate that they have been affected by more complex cyber threats that interfere with the proper functioning of a system. Whereas 16% of respondents have been impacted by a DDoS attack at least once in the last five years, this is the case for only 5% (-3) of respondents with regard to side-channel attacks, only 7% with regard to advance persistent threats, and only 5% (-1) with regard to crypto mining programs. The analysis revealed that young people more often reported to have fallen victim to various types of cyberattacks than older people, specifically online sexual harassment ($\rho(969) = -0.20$), cyberbullying ($\rho(961) = -0.23$) and violent threats ($\rho(987) = -0.25$).

4.4 The Risk of Cyber Threats Is Rated as High, Regardless of Past Exposure (Q11)

When we asked our participants for their risk perception of attack types within the next five years (Figure 5), many respondents indicated that they perceive a high personal risk with regard to the classic cybersecurity threats of spam (54%, +11), malware (33%, +4), spyware (30%, +5), and phishing (29%, +4) as well as unauthorized third-party access to online and social media accounts (27%, +4), which increased across all previous items since 2021. In contrast, only a smaller number of respondents have a comparable high risk awareness of the dangers posed by online shopping fraud (22%, +2) and serious forms of online harassment, such as identity theft (19%, +2), doxing (14%, -2), cyberbullying (11%, -3), and cyberstalking (17%, +3). The same applies to scareware (16%, +1), social engineering (16%, +2), and technically complex cyber threats, such as DDoS attacks (20%, +3), advanced persistent threats (15%, +2), crypto mining programs (9%, -3), and side-channel attacks (9%, -2). Especially remarkable is the observation that even though ransomware constitutes one of the most frequent cyber threats, only 20% (+2) associate rather high or very high risks with it.

As highlighted in Figure 5, we could not observe a stable relationship between respondents being affected by a cyber threat at least once and the resulting threat perception, suggesting that other factors at least moderate threat perception. When looking at the perceived probability of falling victim in the future, this applies to even more different attacks compared to past victimhood: Younger age correlates with the perceived risk of online sexual harassment ($\rho(848) = -0.27$), spam ($\rho(917) = -0.25$), cyberbullying ($\rho(854) = -0.23$), hate speech ($\rho(840) = -0.24$), violent threats ($\rho(839) = -0.31$), online shopping scams ($\rho(874) = -0.21$), blackmailing ($\rho(806) = -0.21$) and social media hacks ($\rho(838) = -0.21$). Furthermore, we analyzed the correlation between the current and the future susceptibility for each specific attack by calculating the Pearson r coefficient for each attack. First, the current and future susceptibility correlated for every attack, with a significance level of $p < .001$. Second, this correlation was especially strong for sexual harassment ($r(828) = 0.56$) and spam ($r(900) = 0.57$).

4.5 Easy-To-Use and Mandatory Security Measures Are More Prevalent (Q12)

Looking at security measures and tools (Figure 6), it is noticeable that a large number of respondents often or always use security solutions that have been configured once and are then permanently

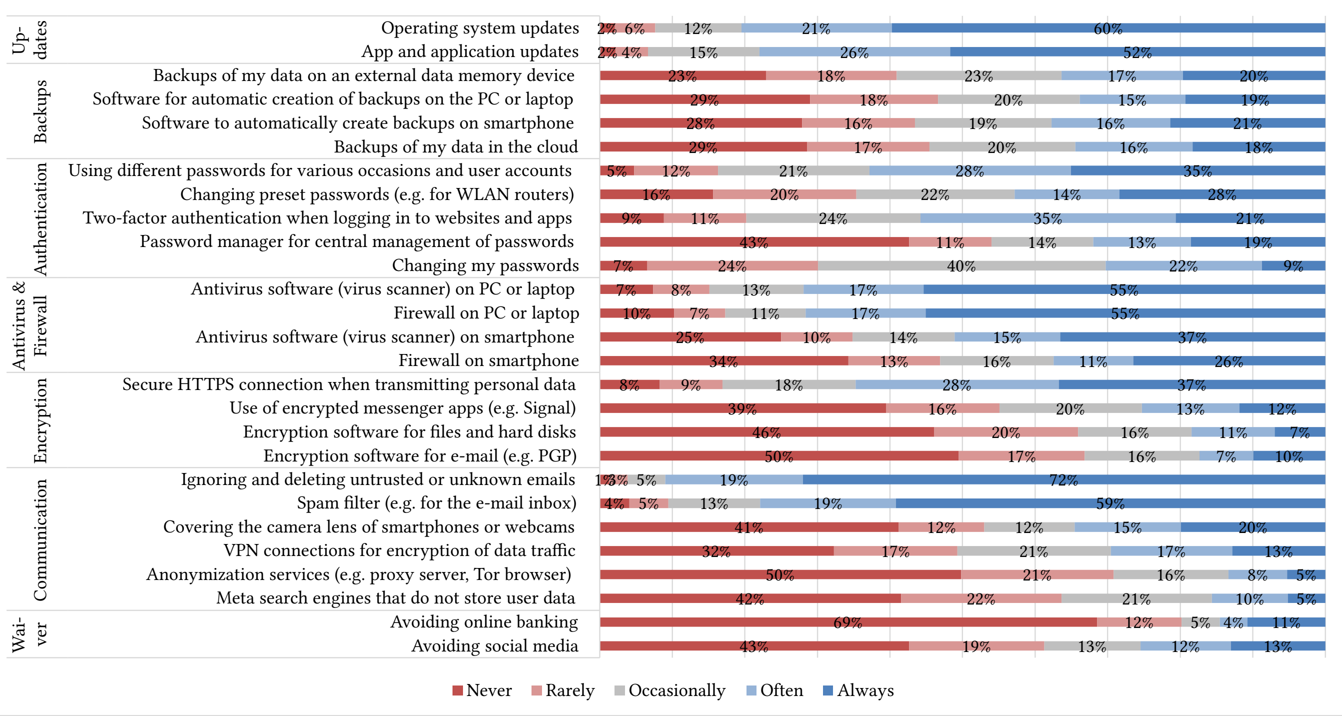

Figure 6: How continuously do you use security measures on your personal devices to protect against cyber threats (Q12, 2024)?

active, such as spam filters (78%, +8), firewalls (72%, +4) and antivirus software (72%, +4) on the PC or laptop, as well as firewalls (37%, -6) and antivirus software (52%, +3) on the smartphone. Also common is regularly updating programs and apps (78%, +7) and the operating system of devices (81%, +10). While fewer respondents use software for automated backups, the use of storage media (37%, +4) and cloud services (34%, +4) for backups enjoy similar approval levels. Further, 35% (+1) cover the lenses of cameras on their devices.

With 56% (+14) of our participants, an increasing number often use two-factor authentication when logging into services, and fewer use specific encryption measures, such as encrypted messengers (25%, -4), encryption software for e-mails (17%, -6), or encryption software for files and hard disks (18%, -5). Still, a slight increase in the use of tools that require regular user interventions like password managers (32%, +3) or VPN services (30%, +3), but not anonymization services (13%, -4) or meta-search engines (15%, +1), could be observed. Furthermore, older people use antivirus software ($\rho(1002) = 0.29$) and firewalls ($\rho(1002) = 0.24$) to protect their computers more often. They are also more likely to abstain from using social media ($\rho(1002) = 0.27$).

4.6 Conversations, Security Software, and TV are Widespread Information Sources (Q13)

When asking citizens which channels citizens would prefer to receive cyber threat information (Figure 7), around half of respondents reported that they sometimes or more frequently obtain information from family or friends (61%, +1), installed security software (55%, -4), television (49%, -7), and security software vendor websites (46%, -5). A slightly smaller proportion but still more than a third said they at least sometimes consult the websites of software or hardware manufacturers (45%, +1), the radio (41%, -1), messengers (36%), warning apps (40%, +6), school, university, or workplace (38%, +4), multimedia services such as YouTube (31%, -2), and newsletters (33%) to access cybersecurity information, while social networks (28%, -2), security news websites (31%, +2), specialized publications (25%, -3), and security authority websites (24%, -2) were cited less frequently. Finally, only a small and annually decreasing proportion of participants mention blogs (11%, -8), microblogging services (9%, -6), or podcasts (12%, -4) as at least occasional sources.

According to our results, people of higher ages are less likely to utilize their workplace, school, or university as such a channel ($\rho(1002) = -0.38$). However, they are more likely to use the press (such as newspapers) ($\rho(1002) = 0.20$), newsletters ($\rho(1002) = 0.24$), installed software ($\rho(1002) = 0.29$) and websites of manufacturers of security software ($\rho(1002) = 0.21$). Interestingly, some of these correlations have become stronger since our first survey in 2021, as shown by the Fisher-Z-Tests: The correlation between age and the utilization of newsletters as a channel inside the data from those years ($p < .001, \rho(1091) = 0.08$) has increased significantly ($z = 3.756$). Similar effects could be observed in the correlations between age and the use of installed software as a channel (old correlation: $\rho(1091) = 0.15$, z-Results: $z = 3.364$). Furthermore, people with higher income ($\rho(1002) = 0.29$) and people with higher degrees ($\rho(991) = 0.23$) are more likely to retrieve such information from their workplace, school, or university.

4.7 Security Software, TV, and Warning Apps Are Preferred Information Channels (Q14)

We asked respondents to indicate their three preferred channels for receiving cyber threat, vulnerability, and problem resolution

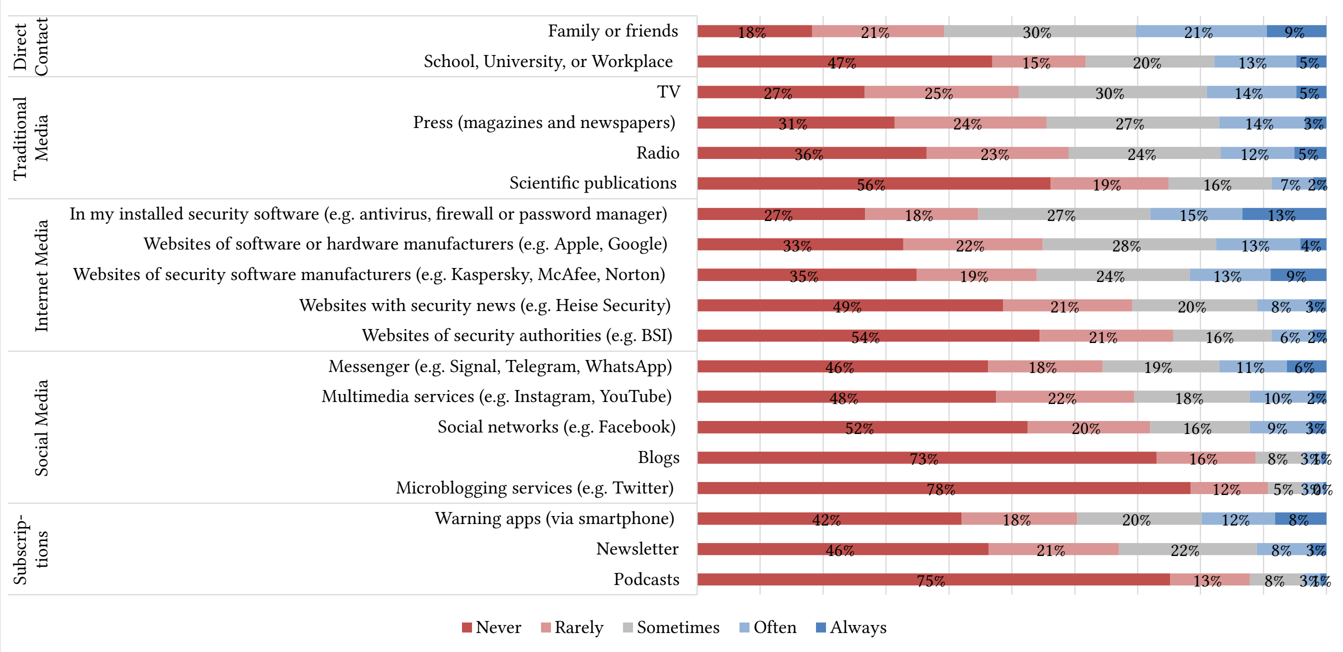

Figure 7: Which channels do you currently use to find out about cyber threats, vulnerabilities, and solutions (Q13, 2024)?

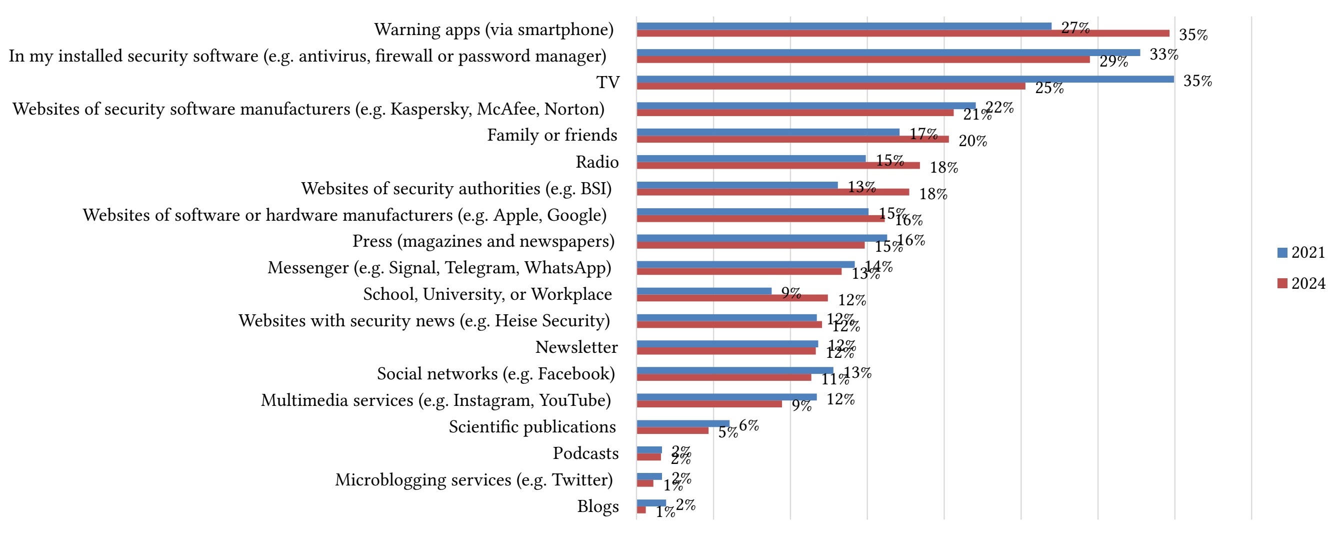

Figure 8: Through which channels would you prefer to receive information on cyber threats, security vulnerabilities, and problem solutions in the future? Please select up to three items (Q14, 2021-2024).

information in the future (Figure 8). Altogether, warning apps on smartphones (35%, +8), installed security software (29%, -4), and television (25%, -10) were mentioned most frequently in 2024, indicating a transition from TV to warning apps as the most preferred future information source. While the websites of security software manufacturers (21%, -1), security authorities (18%, +5), hardware or software manufacturers (n=15%, +1), media specializing in security topics (n=12%), and specialized newsletters (12%) still constitute noteworthy information channels, there is also a strong interest in direct exchange among family or friends (20%, +3) and, to a lesser extent, the school, university or workplace (12%, +3). While most traditional media, including press publications (15%, -1), radio (18%, +3), and scientific publications (5%, -1), remained relatively stable, only a minor decline in social channels such as messengers (13%, -1), social networks like Facebook (11%, -2), and multimedia services like YouTube (9%, -3) is observable.

To analyze the connection to items other than the three picked, we conducted t-tests, with one group being people who did pick a certain channel and the other being people who did not. We found that the people in the groups that picked workplace, school or university ($t(1002) = 11.2, d = 0.97$), multimedia platforms ($t(1002) = -8.36, d = 0.85$), social media platforms ($t(1002) = 5.43, d = 0.50$) and podcasts ($t(1002) = 7.08, d = 1.1$) are each significantly younger. We also analyzed the connection between current and preferred channels. Similarly to the above paragraph, we conducted t-tests, where one group consisted of people who did pick a preferred channel in Q14, and the other consisted of people who didn't. We then analyzed whether one of those groups had a higher average current channel usage according to Q13. Several interesting observations could be made: first, except for blogs ($p = .002, t(1002) = -5.74, d = 2.40$) and microblogging platforms ($p = .003, t(1002) = -3.87, d = 1.83$), there was a significant difference between the groups who did and did not pick a certain channel, with the significance level being $p < .001$. Second, except for warning Apps ($t(1002) = -6.84, d = 0.47$), all effect sizes were moderate or strong. Third, the channel podcasts ($t(1002) = -4.51, d = 1.82$) has an exceptionally high effect size.

5 Discussion and Conclusion

In this study, we examined German citizens' awareness of cyber threats, implementation of security measures, and communication preferences. By combining three datasets for statistical analysis (Table 2), we explored to what extent demographic (age, gender, education, income, region) and temporal factors (2021, 2023, 2024) influenced citizen perceptions towards cybersecurity. While we analyzed three representative datasets of German citizens to reach more generalizable and robust findings for the target population, several assumptions about their generalizability for other countries with similar digital infrastructures and threat landscapes can be made. Yet, a survey by the European Commission highlighted fine-grained and nuanced differences concerning cybersecurity behavior and perception across the 28 European states, suggesting that a "one size fits all" approach is neither effective nor feasible [49].

Since Germany was identified as a state-oriented risk culture [21], similar findings might be replicated in countries with similar characteristics (e.g., Austria, Sweden). However, we also asked for individual security measures, and also in individual-oriented (e.g., the Netherlands) and fatalistic risk cultures (e.g., Italy), a high level of preparedness across authorities and citizens is desirable, requiring high-quality information as a foundation for culture-oriented strategies. In this regard, our recommendations must be customized to the country's risk culture, for instance, by either laying focus on informational push strategies from authorities (in state-oriented risk cultures) or pull strategies by citizens (in individual-oriented risk cultures) [81]. In fatalistic risk cultures, then, authorities are expected to intervene, but the main focus is on the response and recovery phases rather than prevention [21].

Key Statistical Observations
Age
• **Device usage (Q7)**: Smartphone ($\rho = -0.41$), gaming console ($\rho = -0.46$)
• **Threat perception (Q8)**: "Without a firewall and virus scanner, you can no longer go on the Internet." ($\rho = 0.34$)
• **Victimization exposure (Q9)**: Cyberbullying ($\rho = -0.23$)
• **Victimization risk (Q11)**: Cyberbullying ($\rho = -0.23$), shopping fraud ($\rho = -0.21$), unauthorized account access ($\rho = -0.21$), spam ($\rho = -0.25$)
• **Security tools (Q12)**: Firewall on PC/laptop ($\rho = 0.24$), antivirus on PC/laptop ($\rho = 0.29$), avoiding social media ($\rho = 0.27$)
• **Current channels of information (Q13)**: Press ($\rho = 0.20$), websites of security software manufacturers ($\rho = 0.21$), newsletters ($\rho = 0.24$), installed security software ($\rho = 0.29$), school, university, or workplace ($\rho = -0.38$)
• **Preferred channels of information (Q14)**: Social networks ($d = 0.50$), multimedia services ($d = 0.85$), school, university, or workplace ($d = 0.97$), podcasts ($d = 1.1$)
Gender
• **Threat perception (Q8)**: "Germany should actively retaliate with cyberattacks itself in the event of a cyberattack." ($d = 0.58$)
Income
• **Device usage (Q7)**: Interconnected car ($\rho = 0.21$), smart heating thermostats ($\rho = 0.21$)
• **Current channels (Q13)**: School, university, or workplace ($\rho = 0.29$)
Education
• **Device usage (Q7)**: Laptop/Notebook ($\rho = 0.23$)
• **Current channels (Q13)**: School, university, or workplace ($\rho = 0.23$)

Table 2: Key statistical observations of our study, ordered by demographic variables.

Recent usable security research proposed the change from a "human-as-problem", i.e., humans conceptualized as the weakest link in an organization's security, to a "human-as-solution" cybersecurity mindset [100], encouraging expertise, learning, communication, and collaboration to establish resistance and resilience under the complex, emergent, and unpredictable nature of socio-technical systems. Including the potential for the constructive and solution-oriented perspective of humans in cybersecurity, we discuss design and policy implications for enhancing citizens' cybersecurity in the following sections.

5.1 Implications for Design: Foster Learning and Resilience

A central tenet of HCI is that technology should be user-centric, with designs being based on social science findings about users [87]. Based on our empirical data, we suggest four distinct design implications to enhance technology for citizens' cyber threat awareness, their implementation of protective measures, as well as the reception of information and warning messages from authorities and commercial security providers.

Enhance the Availability and Ease of Use of Relevant Everyday Security Technologies (D1). Our results indicate that citizens would rather use enforced security provisions (e.g., updates or 2FA) than independently initiated measures. For instance, in line with our observed adoption rates, the ease of use of some protective measures, such as encryption software for e-mail communication, remains an unresolved issue in usable security practice and research [60, 86]. Enhancing usability can help citizens adopt specific security measures regardless of their underlying risk culture. The relevance of these measures may be communicated by authorities or institutional information resources for self-learning. Alternatively, some measures could be enforced through organizational service design and policies. User tutorials can help citizens adopt specific security measures, such as backups, encryption software, or password managers, in state-oriented risk cultures. In contrast, nudging approaches may facilitate better security decisions [40, 78] in individual-oriented risk cultures, which emphasize personal responsibility for cybersecurity behaviors. While our longitudinal study showcased how citizens increasingly prefer to receive cyber threat information via warning apps, most of these apps still focus on the preparedness for and response to natural hazards [43]. Since IT knowledge and skills vary across different demographic groups, research shows warning messages must be carefully crafted with regard to emotional appeals [48, 62, 75] as well as the level of detail and wording of alerts [4].

Consider Age- and Skill-Related Design Options of Technology (D2). In line with previous research [67], particularly age was found to correlate with cybersecurity behavior and threat perception. In our study, younger people reported higher exposure to cyberbullying and displayed greater threat awareness for spam, cyberbullying, online shopping scams, and unauthorized third-party access to accounts. This could be connected to the higher level of online activity, as increased exposure would make them more susceptible to cybercrime, requiring a higher level of protection. In other words, older people are less active in the online realm, which leads to a lower susceptibility and may induce a lower perceived need for protection. Furthermore, existing usable security research found that age was the strongest predictor for security misconceptions [44]. These findings suggest tailoring cybersecurity protection tools according to age, such as introducing older individuals to user-friendly novel protection tools while emphasizing the significance of foundational safeguards like firewalls and antivirus programs to younger individuals. User-friendly guidelines and tutorials on modern protection tools [53] could constitute appropriate educational material for older age groups while engaging campaigns highlighting the importance and effectiveness of foundational security practices could work for younger individuals. For instance, Demuth et al. [25] used so-called privacy personas to implement distinct views for different levels of expertise for privacy-enhancing technologies.

Inclusive Technology Design with Long-Term Sociodemographic Change in Mind (D3). Overall, our findings indicate a rising individual and public infrastructure risk perception. This is accompanied by an increase in intuitive protection measures, such as application and operating system updates, while the implementation of more complicated measures, such as encryption, even decreased, calling for the design of usable security technologies. Furthermore, a low and declining trust in Germany's preparedness and security authorities' competencies was observed, while the perception of being insufficiently informed about cyber threats increased. Given the observed state-oriented risk culture in Germany [21, 81], the provision of actionable cybersecurity information via public channels (i.e., television and warning apps) could alleviate these issues. While an increase in mobile devices, such as smartphones, notebooks, and smartwatches, was especially observed among younger citizens, classic media, such as radio and television, was used more frequently by older people. In previous work on social media in emergencies, such age-related observations were made across all types of risk cultures [80, 81]. To achieve long-term societal resilience, introducing cybersecurity information through established media and introducing technology for emerging threats (e.g., harassment among younger adults) must be balanced in future research and practice. A standardized usable security and privacy questionnaire, such as currently in development [45], might be useful for the robust and long-term measurement of citizens' knowledge, attitude, and behavior.

Establish Cybersecurity Multi-Channel Warnings for Societal Resilience (D4). Although the BSI and federal CERTs provide security information via newsletter and their website, they are not among the most used and preferred information channels, indicating a mismatch between supply and demand. Authorities and enterprises should intensify their communication through preferred channels, such as security software, television, or warning apps. We assume that warning apps, due to their configurability, and related websites should also be suitable for pull strategies within individual-oriented risk cultures. According to a study, about 61% of German citizens consider it at least quite or highly important to include cybercrime-related warnings in established warning apps [42]. As citizens require different types of information, information could be organized in accordance with the emergency management cycle [2], which encompasses the steps of mitigation (e.g., software updates), preparedness (e.g., information on secure banking), response (e.g., recommendations for contact points), and recovery (e.g., guidance for self-help). However, a challenge arises due to the limited number of active users. For instance, the German Civil Protection's warning app, NINA, had only 8.8 million users in 2021 [16]. Although the use of warning apps may have been positively influenced by the COVID-19 pandemic [42], strategies to increase the user base must be developed concurrently. To account for different channel preferences [67] and ensure resilience through redundancy, the use of multi-channel information systems, such as already established for natural hazards in Germany, should be considered [56].

5.2 Implications for Policy: Promote Communication and Collaboration

While the design of usable technology is suitable to tackle some of the discussed issues, their implementation often requires resources and support of governments and security authorities. Considering the potential of HCI for evidence-based policymaking [92] and the issues that became prevalent in our study, we outline four distinct policy implications not only as a means for improved technology support but also to enhance the quality of security services.

Enhance Information Dissemination for Preparedness and Trust Building (P1). In all samples, we found that large parts of the population feel inadequately informed about cyber threats. Although the BSI and federal CERTs provide security information via newsletter and their website, they are not among the most used and preferred information channels, indicating a mismatch between supply and demand. Thus, we suggest cybersecurity authorities to align and enhance their information dissemination strategies [52, 98], which can be characterized by the provision of supportive resources, cybersecurity news, and advisories on security vulnerabilities via promising information channels. While state-oriented risk cultures would probably expect information about mitigation measures already implemented by authorities, in an individual-oriented risk culture, the communication could focus on empowering individuals (e.g., providing information for mitigation and preparedness) to take responsibility for their own cybersecurity. In fatalistic risk cultures, then, a focus could be set on response (e.g., recommendations for contact points) and recovery (e.g., guidance for self-help) information.

Provide Resources for Enhanced Cybersecurity Response Capabilities (P2). Although Germany was identified as a state-oriented risk culture [21, 81], our participants showed little and decreasing trust in security authorities' ability to effectively protect citizens while expecting an increasing likelihood of large-scale cyberattacks on public infrastructures, probably due to multiple successful cyberattacks on German infrastructure. Beyond the positive impact of prevention [88], more advanced strategies of conversations & coordinated action [98] should be explored to account for a "human-as-solution" perspective [100], enhance the self-efficacy of citizens [8], and improve citizens' trust in authorities' capabilities, including the management of misinformation, direct conversations between authorities and citizens, or the crowdsourcing of cybersecurity tasks. Since emergency managers of security domains often struggle with resource-intensive strategies due to a lack of personnel and technology [54, 82], a German working group (AG KRITIS) proposed a concept for increasing response capacities against large-scale cyberattacks by including trusted volunteers [1]. Similar to the Virtual Operations Support Team of the German Technical Relief Agency [30] and the rich tradition of volunteer fire brigades in Germany [34], the proper deployment of a Cyber Relief Agency could also help to strengthen the bonds between authorities and citizens and provide opportunities for promoting and recruiting young talents and increases networking between experts. Furthermore, usable security research suggested the training and deployment of cybersecurity guardians for peer-to-peer communication, especially among older communities [68].

Prioritize Age-Oriented Education and Preparedness Measures (P3). Overall, the demographic variables of education, gender, income, and region have a lower impact on cybersecurity behavior, suggesting that strategies focusing on age-related differences and requirements should be effective, e.g., to bridge the gap between cybersecurity knowledge and actual behavior [59, 69]. In terms of age, younger subjects were observed to use internet-connected devices more frequently and demonstrated a preference for utilizing different cybersecurity measures compared to older individuals. Older individuals tended to favor traditional approaches such as antivirus programs, firewalls, and password changes, whereas younger individuals showed a greater inclination towards using backups, encryption, and anonymization software. A possible reason for this may be generational differences in technology affinity [32]. Beyond age, individuals with higher income and education were more inclined to acquire cybersecurity education from their workplace, school, or university. Apart from a singular item regarding retaliation measures in cyberwar, no moderate or strong correlations involving gender could be observed. One possible reason for this result could be a change in societal norms and advancements in gender equality. In terms of location, no moderate or strong impact of the federal state on perceptions and behavior could be observed, and people from the new states of Germany (BB, MV, SN, ST, TH) did not appear to answer differently.

Consider Enhanced Public-Private Partnerships for Information Exchange (P4). Authorities and enterprises should explore the potentials of public-private partnerships, as established in the domain of critical infrastructures [18], to enhance the security education and preparedness of citizens and employees. Considering the channels of cybersecurity information dissemination, in our study, citizens valued both commercial channels (i.e., installed security software and websites of security software manufacturers) and public channels (i.e., television and warning apps), but also private exchange (i.e., family and friends; school, university, or workplace). Thus, intensified cooperation between cybersecurity authorities, commercial enterprises, and universities seems a promising approach to reach citizens effectively across different information channels. Recently, the BSI introduced an obtainable IT Security Label for manufacturers and service providers, which is intended to enhance transparency for consumers by making the basic security features of IT products, including current security vulnerabilities, recognizable at a glance [55]. Although it allows the scanning of a QR code on the packaging of a certified product, there is still a lack of usable applications and interfaces integrated into the concept to provide a permanent overview of scanned products.

5.3 Comparison to Related Work

This study has examined a number of topics that have received little attention in previous representative surveys of the German population (see Section 2). While there is knowledge on used cybersecurity information channels [13, 14] and desired information types [12–15], there is only limited data on preferred future information channels [13], and no data on favored contact points in the event of cyberattacks. Beyond the thematic focus, this study extends the state of research in two primary aspects. On the one hand, besides our study, the only longitudinal data on cybersecurity attitudes and behaviors of Germans is provided by the annual surveys of Bitkom [5, 7, 79] or BSI and ProPK [10–14], whose primary research motivation are not scientific. Even though our three datasets cannot reveal any long-term trends, the temporal differences uncovered in this study may provide initial indications. On the other hand, for the German population, correlations with demographic factors have only been explored for cybercrime victimization [64, 96], general cybersecurity knowledge and behavior [46], and attitudes toward nudging in cybersecurity [40]. Our study examines all variables for potential correlations with demographic factors. Thus, it yields preliminary evidence on a variety of correlations that have not yet been discussed in research and merit scrutiny in future work.

We are able to corroborate some results from previous studies, while there are also several deviating observations. First, we observe that the trend towards a growing individual threat perception between 2019 and 2021, as evident in Bitkom's annual surveys [5, 7, 79], seems to continue for the time between 2021 and 2024. Further, risk perceptions of all individual threat types, with the exception of doxing, cyberbullying, crypto mining programs, and side-channel attacks, also increased. Further, it is noteworthy that the 2024 proportions of respondents thinking that wars are increasingly being fought digitally (63% vs. 77%) and fearing the outbreak of cyber war (40% vs. 75%) are both significantly lower than Bitkom's 2022 figures [83]. An explanation for this could be priming effects, as the Bitkom survey had an explicit focus on the Ukraine war.

Second, we were able to substantiate previous evidence concerning a widespread perception of deficits in the capacities and competencies of German state institutions such as the police [5, 27] and the armed forces [83]. In our samples, less than one of four respondents think that cybercrime is adequately prosecuted and punished by German law enforcement agencies and that these agencies have the necessary competencies to adequately protect citizens from cyber threats. Third, our results cannot corroborate previously observed correlations between self-reported cyber threat exposure and demographic variables. We were not able to observe the finding of Müller et al. [64] that exposure decreases with increasing age for our 2024 data. A corresponding moderate or strong negative correlation was only found for cyberbullying. Also in contrast to them, we found no correlations between exposure and respondents' gender, and all correlations observed by Weber and Wührl [96] were not present in our data.

Fourth, while previous surveys indicate that between 2020 and 2024 Germans' overall cybercrime exposure remains relatively stable with a slight decrease since 2022 [10–14], our study shows a more differentiated picture with regard to specific cybersecurity threats. Whereas the proportion of those at least once affected by cyberstalking, spam, unauthorized third-party account access, scareware, online shopping fraud, phishing, and social engineering in the five years prior to the surveys increased between 2021 and 2024, the proportion of those affected by DDoS attacks and advanced persistent threats remained stable, and the percentage of malware, ransomware, spyware, identity theft, cyberbullying, doxing and side-channel attack victims decreased.

Fifth, while shopping fraud, unauthorized account access, and malware were the most common threat types in the latest BSI and ProPK survey [14], spam, malware, and ransomware were the most prevalent in ours. Further, in our study, a higher proportion reported being exposed to most threat types that were included in both surveys. These disparities might be related to differences in framing. The BSI and ProPK only asked self-reported victims of cybercrime and not all respondents about their exposure, whereas we asked all respondents without any explicit reference to crime. Sixth, the BSI and ProPK surveys also indicate an overall decline in the adoption of all security measures that they continuously surveyed between 2021 and 2024 [10–14]. Our results do not confirm this pattern. The proportion of those stating that they often or always use a measure increased for 15 measures between 2021 and 2024, while it decreased for five and remained constant for one.

Finally, differences can also be observed with regard to the information behavior and requirements of the German population. Whereas in the BSI and ProPK surveys of 2023 and 2024, websites, family, friends and acquaintances, social networks, television, and videos or tutorials were the most common sources of cybersecurity information [13, 14], in our samples, family or friends, installed security software, television, and security software vendor websites are most prevalent. There are also some differences regarding preferred future communication channels for cyber security information. While websites, traditional media, and newsletters were mentioned most frequently in the 2023 BSI and ProPK survey [13], in our survey, it was warning apps, installed security software, and television. Furthermore, in contrast to surveys that observed increasing information requirements between 2020 and 2022 [10–12], our study suggests that perceived demand for cybersecurity information stagnated between 2021 and 2024. In this period, the share of respondents who articulated a wish for the provision of further cybersecurity education remained almost constant.

Acknowledgments

This research work has been co-funded by the German Federal Ministry of Education and Research (BMBF) and the Hessian Ministry of Higher Education, Research, Science and the Arts (HMWK) within their joint support of the National Research Center for Applied Cybersecurity ATHENE, as well as by the BMBF in the project CYLENCE (13N16636) [50].

References

[1] Manuel Atug. 2021. Das Cyber-Hilfswerk: Ein Konzept der unabhängigen AG KRITIS zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen. *Recht Innovativ* 5, 1 (Dec. 2021), 1–8. doi:10.1007/s43442-021-0058-0

[2] Malcolm E. Baird. 2010. *The "Phases" of Emergency Management.* Background Paper. Vanderbilt Center for Transportation Research (VECTOR), Nashville, TN, USA. 1–46 pages. https://www.memphis.edu/ifti/pdfs/cait_phases_of_emergency_mngt.pdf

[3] David Barrera, Christopher Bellman, and Paul Van Oorschot. 2023. Security Best Practices: A Critical Analysis Using IoT as a Case Study. *ACM Trans. Priv. Secur.* 26, 2, Article 13 (mar 2023), 30 pages. doi:10.1145/3563392

[4] Ali Sercan Basyurt, Jennifer Fromm, Philipp Kuehn, Marc-André Kaufhold, and Milad Mirabaie. 2022. Help Wanted - Challenges in Data Collection, Analysis and Communication of Cyber Threats in Security Operation Centers. In *Wirtschaftsinformatik 2022 Proceedings* (Nuremberg, Germany) *(WI)*. Association for Information Systems, Atlanta, GA, USA, Article 20, 16 pages. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/20/

[5] Achim Berg. 2021. *IT- und Cybersicherheit 2021.* Presentation. Bitkom e.V., Berlin. https://www.bitkom.org/sites/main/files/2021-12/bitkom-charts-it-und-cybersicherheit-14-12-2021.pdf

[6] Igor Bernik, Kaja Prislan, and Anže Mihelič. 2022. Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia. *Sustainability* 14, 21, Article 14487 (2022), 16 pages. doi:10.3390/su142114487

[7] Bitkom Research. 2020. *Vertrauen & IT-Sicherheit.* Presentation. Bitkom e.V., Berlin. https://www.bitkom.org/sites/default/files/2020-02/bitkom_vertrauenitsicherheit2020.pdf

[8] Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M. Angela Sasse, and Malte Elson. 2024. Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 973, 32 pages. doi:10.1145/3613904.3642432

[9] Casey Breen, Cormac Herley, and Elissa M. Redmiles. 2022. A Large-Scale Measurement of Cybercrime Against Individuals. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 122, 41 pages. doi:10.1145/3491102.3517613

[10] Bundesamt für Sicherheit in der Informationstechnik and Polizeiliche Kriminalprävention der Länder und des Bundes. 2020. *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.* Research Report. Bundesamt für Sicherheit in der Informationstechnik, Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2020.pdf?__blob=publicationFile&v=1

[11] Bundesamt für Sicherheit in der Informationstechnik and Polizeiliche Kriminalprävention der Länder und des Bundes. 2021. *Digitalbarometer 2021: Bürgerbefragung zur Cyber-Sicherheit.* Research Report. Bundesamt für Sicherheit in der Informationstechnik, Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.pdf?__blob=publicationFile&v=2

[12] Bundesamt für Sicherheit in der Informationstechnik and Polizeiliche Kriminalprävention der Länder und des Bundes. 2022. *Digitalbarometer. Bürgerbefragung zur Cyber-Sicherheit 2022.* Research Report. Bundesamt für Sicherheit in der Informationstechnik, Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2022.pdf?__blob=publicationFile&v=3

[13] Bundesamt für Sicherheit in der Informationstechnik and Polizeiliche Kriminalprävention der Länder und des Bundes. 2023. *CyMon – der Cybersicherheitsmonitor. Befragung zur Cybersicherheit 2023.* Research Report. Bundesamt für Sicherheit in der Informationstechnik, Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2023_Kurzbericht.pdf?__blob=publicationFile&v=2

[14] Bundesamt für Sicherheit in der Informationstechnik and Polizeiliche Kriminalprävention der Länder und des Bundes. 2024. *CyMon – der Cybersicherheitsmonitor. Befragung zur Cybersicherheit 2024.* Research Report. Bundesamt für Sicherheit in der Informationstechnik, Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2024_Kurzbericht.pdf?__blob=publicationFile&v=2

[15] Bundesministerium des Innern, für Bau und Heimat and Bundesamt für Sicherheit in der Informationstechnik. 2020. *Bundesweite Themenabfrage zur Internetsicherheit mit Civey.* Presentation. Bundesministerium des Innern, für Bau und Heimat and Bundesamt für Sicherheit in der Informationstechnik, Berlin. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/anlage-1-pm-sid.pdf;jsessionid=F267B0E2F27B93F8B813EEB00D569AEB.1_cid364?__blob=publicationFile&v=1

[16] Bundesregierung. 2021. Warn-App NINA mit lokalen Hinweisen zu Gefahrenlagen. https://www.bundesregierung.de/breg-de/aktuelles/warn-app-nina-1942330

[17] Brendan Burchell and Catherine Marsh. 1992. The effect of questionnaire length on survey response. *Quality and quantity* 26, 3 (1992), 233–244. doi:10.1007/BF00172427

[18] Nathan E. Busch and Austen D. Givens. 2013. Achieving Resilience in Disaster Management: The Role of Public-Private Partnerships. *Journal of Strategic Security* 6, 2 (2013), 1–19. doi:10.5038/1944-0472.6.2.1

[19] Jacob Cohen. 2013. *Statistical power analysis for the behavioral sciences.* Academic press, New York, NY, USA. doi:10.4324/9780203771587

[20] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude P. R. Heath. 2020. Too Much Information: Questioning Security in a Post-Digital Society. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3313831.3376214

[21] Alessio Cornia, Kerstin Dressel, and Patricia Pfeil. 2016. Risk cultures and dominant approaches towards disasters in seven European countries. *Journal of Risk Research* 19, 3 (2016), 288–304. doi:10.1080/13669877.2014.961520

[22] Harald Cramér. 1999. *Mathematical methods of statistics.* Princeton Mathematical Series, Vol. 26. Princeton University Press, Princeton. https://press.princeton.edu/books/paperback/9780691005478/mathematical-methods-of-statistics-pms-9-volume-9

[23] Mihaly Csikszentmihalyi. 2013. *Creativity: the psychology of discovery and invention* (first harper perennial modern classics edition ed.). Harper Perennial Modern Classics, New York.

[24] John S. II Davis, Benjamin Boudreaux, Jonathan William Welburn, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace.* Technical Report. RAND Corporation, Arlington, VA, USA. doi:10.7249/RR2081

[25] Kilian Demuth, Sebastian Linsner, Tom Biselli, Marc-André Kaufhold, and Christian Reuter. 2024. Support Personas: A Concept for Tailored Support of Users of Privacy-Enhancing Technologies. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (Oct. 2024), 797–817. doi:10.56553/popets-2024-0142

[26] Michael Eid, Mario Gollwitzer, and Manfred Schmitt. 2016. *Formelsammlung Statistik und Forschungsmethoden.* Beltz Verlag, Weinheim.

[27] Bitkom e.V. 2023. *Drei Viertel von Cyberkriminalität betroffen.* Press release. Bitkom e.V., Berlin. https://www.bitkom.org/print/pdf/node/17694

[28] Bitkom e.V. 2023. *Fast jeder fühlt sich im Internet bedroht – vor allem durch organisierte Kriminalität.* Press release. Bitkom e.V., Berlin. https://www.bitkom.org/print/pdf/node/20232

[29] Bitkom e.V. 2024. *Datenschutz: Deutsche Anbieter genießen das größte Vertrauen.* Technical Report. Bitkom e.V., Berlin. https://www.bitkom.org/print/pdf/node/20661

[30] Ramian Fathi, Dennis Thom, Steffen Koch, Thomas Ertl, and Frank Fiedrich. 2020. VOST: A case study in voluntary digital participation for collaborative emergency management. *Information Processing and Management* 57, 4 (2020), 102174. doi:10.1016/j.ipm.2019.102174

[31] Tobias Fertig and Andreas Schütz. 2020. About the measuring of information security awareness: a systematic literature review. In *Proceedings of the 53rd Annual Hawaii International Conference on System Sciences* (Grand Wailea, HI, USA) *(HICSS)*. HICSS, Honolulu, HI, USA, 6518–6527. https://scholarspace.manoa.hawaii.edu/items/bc46ac13-2f4b-4d70-add9-ce10527f7015

[32] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. doi:10.1080/10447318.2018.1456150

[33] David Freedman, Robert Pisani, and Roger Purves. 2007. *Statistics* (international student ed., 4. ed ed.). Norton, New York.

[34] Matthias Freise and Andrea Walter. 2024. Motivations and expectations of German volunteer firefighters. *Journal of Civil Society* 20, 2 (2024), 190–208. doi:10.1080/17448689.2024.2357081

[35] Hershey H Friedman and Taiwo Amoo. 1999. Rating the rating scales. *Friedman, Hershey H. and Amoo, Taiwo (1999)." Rating the Rating Scales." Journal of Marketing Management, Winter* 9, 3 (1999), 114–123. https://ssrn.com/abstract=2333648

[36] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable security: History, themes, and challenges.* Morgan & Claypool Publishers, San Rafael, CA, USA. doi:10.1007/978-3-031-02343-9

[37] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261. doi:10.1016/j.cose.2018.04.002

[38] Ellen A. Girden. 1992. *ANOVA. Repeated Measures.* SAGE Publications, Newbury Park.

[39] Magdalena Glas, Manfred Vielberth, and Guenther Pernul. 2023. Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 622, 19 pages. doi:10.1145/3544548.3581046

[40] Katrin Hartwig and Christian Reuter. 2021. Nudge or Restraint: How do People Assess Nudging in Cybersecurity - A Representative Study in Germany. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 141–150. doi:10.1145/3481357.3481514

[41] Katrin Hartwig and Christian Reuter. 2022. Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour & Information Technology (BIT)* 41, 7 (2022), 1357–1380. doi:10.1080/0144929X.2021.1876167

[42] Jasmin Haunschild, Marc-André Kaufhold, and Christian Reuter. 2022. Perceptions and Use of Warning Apps – Did Recent Crises Lead to Changes in Germany?. In *Proceedings of Mensch Und Computer 2022* (Darmstadt, Germany) *(MuC '22)*. Association for Computing Machinery, New York, NY, USA, 25–40. doi:10.1145/3543758.3543770

[43] Andrin Hauri, Kevin Kohler, and Benjamin Scharte. 2022. *A Comparative Assessment of Mobile Device-Based Multi-Hazard Warnings: Saving Lives through Public Alerts in Europe.* Technical Report. ETH Zurich. 46 p. pages. doi:10.3929/ETHZ-B-000533908

[44] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. 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* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 582, 23 pages. doi:10.1145/3544548.3581410

[45] Franziska Herbert, Florian M. Farke, Marvin Kowalewski, and Markus Dürmuth. 2021. Vision: Developing a Broad Usable Security & Privacy Questionnaire. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 76–82. doi:10.1145/3481357.3481526

[46] Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. 2020. Differences in IT Security Behavior and Knowledge of Private Users in Germany. In *Proceedings of the 15th International Conference on Wirtschaftsinformatik* (Potsdam, Germany). Association for Information Systems, Atlanta, GA, USA, 168–184. doi:10.30844/wi_2020_v3-herbert

[47] Glenn D Israel and CL Taylor. 1990. Can response order bias evaluations? *Evaluation and Program Planning* 13, 4 (1990), 365–371. doi:10.1016/0149-7189(90)90021-N

[48] Allen C Johnston, Merrill Warkentin, Alan R Dennis, and Mikko Siponen. 2019. Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences* 50, 2 (2019), 245–284. doi:10.1111/deci.12328

[49] Kantar. 2020. *Special Eurobarometer 499. Europeans' attitudes towards cyber security.* Technical Report. European Commission, Brussels. https://op.europa.eu/en/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1

[50] Marc-André Kaufhold, Markus Bayer, Julian Bäumler, Christian Reuter, Stefan Stieglitz, Ali Sercan Basyurt, Milad Mirabaie, Christoph Fuchß, and Kaan Eyilmez. 2023. CYLENCE: Strategies and Tools for Cross-Media Reporting, Detection, and Treatment of Cyberbullying and Hatespeech in Law Enforcement Agencies. In *Mensch und Computer 2023 - Workshopband.* Gesellschaft für Informatik e.V., Rapperswil, Switzerland, 8 pages. doi:10.18420/muc2023-mci-ws01-211

[51] Marc-André Kaufhold, Julian Bäumler, and Christian Reuter. 2022. The Implementation of Protective Measures and Communication of Cybersecurity Alerts in Germany - A Representative Survey of the Population. In *Workshop-Proceedings Mensch und Computer (Mensch und Computer 2022 - Workshopband).* Gesellschaft für Informatik e.V., Darmstadt, 12 pages. doi:10.18420/muc2022-mci-ws01-228

[52] Marc-André Kaufhold, Jennifer Fromm, Thea Riebe, Milad Mirbabaie, Philipp Kuehn, Ali Sercan Basyurt, Markus Bayer, Marc Stöttinger, Kaan Eyilmez, Reinhard Möller, Christoph Fuchß, Stefan Stieglitz, and Christian Reuter. 2021. CYWARN: Strategy and Technology Development for Cross-Platform Cyber Situational Awareness and Actor-Specific Cyber Threat Communication. In *Workshop-Proceedings Mensch und Computer (Mensch und Computer 2021 - Workshopband).* Gesellschaft für Informatik e.V., Bonn, 9 pages. doi:10.18420/muc2021-mci-ws08-263

[53] Marc-André Kaufhold, Alexis Gizikis, Christian Reuter, Matthias Habdank, and Margarita Grinko. 2019. Avoiding Chaotic Use of Social Media before, during, and after Emergencies: Design and Evaluation of Citizens' Guidelines. *Journal of Contingencies and Crisis Management (JCCM)* 27, 3 (2019), 198–213. doi:10.1111/1468-5973.12249

[54] Marc-André Kaufhold, Thea Riebe, Markus Bayer, and Christian Reuter. 2024. 'We Do Not Have the Capacity to Monitor All Media': A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 580, 16 pages. doi:10.1145/3613904.3642368

[55] Dennis-Kenji Kipker and Dario E Scholz. 2021. Das IT-Sicherheitsgesetz 2.0: Eine kritische Analyse. *Datenschutz und Datensicherheit-DuD* 45, 1 (2021), 40–45. doi:10.1007/s11623-020-1387-9

[56] Michael Klafft. 2013. Diffusion of emergency warnings via multi-channel communication systems an empirical analysis. In *Eleventh International Symposium on Autonomous Decentralized Systems (ISADS).* IEEE, Mexico City, 1–5. doi:10.1109/ISADS.2013.6513437

[57] Ivar Krumpal. 2013. Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & quantity* 47, 4 (2013), 2025–2047. doi:10.1007/s11135-011-9640-9

[58] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. In *Proceedings 3rd European Workshop on Usable Security* (London, England). Internet Society, Reston, VI, USA, 11 pages. doi:10.14722/eurousec.2018.23012

[59] Maria Lamond, Karen Renaud, Lara Wood, and Suzanne Prior. 2022. SOK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review. In *Proceedings of the 2022 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '22)*. Association for Computing Machinery, New York, NY, USA, 14–27. doi:10.1145/3549015.3554207

[60] Ada Lerner, Eric Zeng, and Franziska Roesner. 2017. Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P).* IEEE, New York, NY, USA, 385–400. doi:10.1109/EuroSP.2017.41

[61] Ioana Andreea Marin, Pavlo Burda, Nicola Zannone, and Luca Allodi. 2023. The Influence of Human Factors on the Intention to Report Phishing Emails. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*

(Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 620, 18 pages. doi:10.1145/3544548.3580985

[62] Philip Menard, Gregory J Bott, and Robert E Crossler. 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems* 34, 4 (2017), 1203–1230. doi:10.1080/07421222.2017.1394083

[63] Jeremy Miles and Mark Shevlin. 2014. *Applying regression and correlation: a guide for students and researchers*. SAGE, Los Angeles. OCLC: 890939337.

[64] Philipp Müller, Arne Dreißigacker, and Anna Isenhardt. 2022. *Cybercrime gegen Privatpersonen. Ergebnisse einer repräsentativen Bevölkerungsbefragung in Niedersachsen.* Research Report No. 168. Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover. https://kfn.de/wp-content/uploads/Forschungsberichte/FB_168.pdf

[65] Jerome L. Myers, Arnold D. Well, Robert Frederick Lorch, and Arnold Well. 2010. *Research design and statistical analysis* (3. ed ed.). Routledge, New York, NY.

[66] Anton J Nederhof. 1985. Methods of coping with social desirability bias: A review. *European journal of social psychology* 15, 3 (1985), 263–280. doi:10.1002/ejsp.2420150303

[67] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–11. doi:10.1145/3290605.3300579

[68] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities.. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 86, 15 pages. doi:10.1145/3411764.3445078

[69] James Nicholson, Julia Terry, Helen Beckett, and Pardeep Kumar. 2021. Understanding Young People's Experiences of Cybersecurity. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 200–210. doi:10.1145/3481357.3481520

[70] Matti Näsi, Petri Danielsson, and Markus Kaakinen. 2023. Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors. *European Journal on Criminal Policy and Research* 29, 2 (June 2023), 283–301. doi:10.1007/s10610-021-09497-0

[71] Kenneth Olmstead and Aaron Smith. 2017. *Americans and Cybersecurity.* Research Report. Pew Research Center, Washington, D.C. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/01/Americans-and-Cyber-Security-final.pdf

[72] Anna-Marie Ortloff, Maike Vossen, and Christian Tiefenau. 2021. Replicating a Study of Ransomware in Germany. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 151–164. doi:10.1145/3481357.3481508

[73] The pandas development team. 2020. *pandas-dev/pandas: Pandas.* The pandas development team, Geneva, Switzerland. doi:10.5281/zenodo.3509134

[74] Karl Pearson. 1900. X. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 50, 302 (July 1900), 157–175. doi:10.1080/14786440009463897

[75] Miloslava Plachkinova and Philip Menard. 2022. An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs. *Information Systems Frontiers* 24, 5 (Oct. 2022), 1395–1416. doi:10.1007/s10796-019-09970-6

[76] Louis M. Rea and Richard A. Parker. 2014. *Designing and conducting survey research: a comprehensive guide* (4th, rev. ed ed.). Jossey-Bass, San Francisco.

[77] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landsberger, and Melanie Volkamer. 2020. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (Boston, MA, USA). USENIX Association, Berkeley, CA, USA, 259–284. https://www.usenix.org/conference/soups2020/presentation/reinheimer

[78] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (2018), 22–35. doi:10.1016/j.ijhcs.2018.05.011

[79] Bitkom Research. 2021. *Vertrauen und Sicherheit in der digitalen Welt.* Presentation. Bitkom e.V., Berlin. https://www.bitkom.org/sites/main/files/2021-07/bitkom_vertrauenitsicherheit2021.pdf

[80] Christian Reuter, Marc-André Kaufhold, Tom Biselli, and Helene Pleil. 2023. Increasing Adoption Despite Perceived Limitations of Social Media in Emergencies: Representative Insights on German Citizens' Perception and Trends from 2017 to 2021. *International Journal of Disaster Risk Reduction (IJDRR)* 96 (2023), 20 pages. doi:10.1016/j.ijdrr.2023.103880

[81] Christian Reuter, Marc-André Kaufhold, Stefka Schmid, Thomas Spielhofer, and Anna Sophie Hahne. 2019. The Impact of Risk Cultures: Citizens' Perception of Social Media Use in Emergencies across Europe. *Technological Forecasting and Social Change* 148, 119724 (2019), 1–17. doi:10.1016/j.techfore.2019.119724

[82] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 2021. The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 478 (Oct. 2021), 30 pages. doi:10.1145/3479865

[83] Bernhard Rohleder. 2022. *Wie die Deutschen auf den Ukraine-Krieg reagieren.* Presentation. Bitkom, Berlin. https://www.bitkom.org/sites/main/files/2022-03/Bitkom-ChartsVerbraucherumfrageUkraine22032022.pdf

[84] Mark Rubin. 2021. When to adjust alpha during multiple testing: a consideration of disjunction, conjunction, and individual testing. *Synthese* 199, 3-4 (Dec. 2021), 10969–11000. doi:10.1007/s11229-021-03276-4

[85] Scott Ruoti, Jeff Andersen, Luke Dickinson, Scott Heidbrink, Tyler Monson, Mark O'neill, Ken Reese, Brad Spendlove, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. 2019. A Usability Study of Four Secure Email Tools Using Paired Participants. *ACM Trans. Priv. Secur.* 22, 2, Article 13 (April 2019), 33 pages. doi:10.1145/3313761

[86] Scott Ruoti, Jeff Andersen, Tyler Monson, Daniel Zappala, and Kent Seamons. 2018. A Comparative Usability Study of Key Management in Secure Email. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (Baltimore, MD, USA). USENIX Association, Berkeley, CA, USA, 375–394. https://www.usenix.org/conference/soups2018/presentation/ruoti

[87] Corina Sas, Steve Whittaker, Steven Dow, Jodi Forlizzi, and John Zimmerman. 2014. Generating implications for design through design research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 1971–1980. doi:10.1145/2556288.2557357

[88] Ryan Shandler and Miguel Alberto Gomez. 2023. The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics* 20, 4 (Oct. 2023), 359–374. doi:10.1080/19331681.2022.2112796

[89] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Designing Password Policies for Strength and Usability. *ACM Trans. Inf. Syst. Secur.* 18, 4, Article 13 (May 2016), 34 pages. doi:10.1145/2891411

[90] Veronika Slakaityte, Izabela Surwillo, and Trine Villumsen Berling. 2023. A new cooperation agenda for European energy security. *Nature Energy* 8, 10 (Aug. 2023), 1051–1053. doi:10.1038/s41560-023-01322-8

[91] D. K. Smetters and R. E. Grinter. 2002. Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the 2002 Workshop on New Security Paradigms* (Virginia Beach, Virginia) *(NSPW '02)*. Association for Computing Machinery, New York, NY, USA, 82–89. doi:10.1145/844102.844117

[92] Anne Spaa, Abigail Durrant, Chris Elsden, and John Vines. 2019. Understanding the Boundaries between Policymaking and HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. doi:10.1145/3290605.3300314

[93] Elizabeth Stobert and Robert Biddle. 2018. The Password Life Cycle. *ACM Trans. Priv. Secur.* 21, 3, Article 13 (April 2018), 32 pages. doi:10.1145/3183341

[94] Student. 1908. The Probable Error of a Mean. *Biometrika* 6, 1 (March 1908), 1–25. doi:10.2307/2331554

[95] Pauli Virtanen, Ralf Gommers, Travis E. Oliphant, Matt Haberland, Tyler Reddy, David Cournapeau, Evgeni Burovski, Pearu Peterson, Warren Weckesser, Jonathan Bright, Stéfan J. van der Walt, Matthew Brett, Joshua Wilson, K. Jarrod Millman, Nikolay Mayorov, Andrew R. J. Nelson, Eric Jones, Robert Kern, Eric Larson, C J Carey, İlhan Polat, Yu Feng, Eric W. Moore, Jake VanderPlas, Denis Laxalde, Josef Perktold, Robert Cimrman, Ian Henriksen, E. A. Quintero, Charles R. Harris, Anne M. Archibald, Antônio H. Ribeiro, Fabian Pedregosa, Paul van Mulbregt, and SciPy 1.0 Contributors. 2020. SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python. *Nature Methods* 17, 3 (March 2020), 261–272. doi:10.1038/s41592-019-0686-2

[96] Christine Weber and Johanna Marie Wührl. 2022. Opfererfahrungen im Internet – Ergebnisse des Deutschen Viktimisierungssurvey (DVS). In *Handbuch Cyberkriminologie*, Thomas-Gabriel Rüdiger and P. Saskia Bayerl (Eds.). Springer Fachmedien Wiesbaden, Wiesbaden, 1–42. doi:10.1007/978-3-658-35450-3_44-1

[97] Wes McKinney. 2010. Data Structures for Statistical Computing in Python. In *Proceedings of the 9th Python in Science Conference*, Stéfan van der Walt and Jarrod Millman (Eds.). Curvenote, Calgary, Canada, 56–61. doi:10.25080/Majora-92bf1922-00a

[98] Clayton Wukich. 2015. Social media use in emergency management. *Journal of Emergency Management* 13, 4 (2015), 281–294. doi:10.5055/jem.2015.0242

[99] Jerrold H. Zar. 2005. Spearman Rank Correlation. In *Encyclopedia of Biostatistics* (2nd ed.), Peter Armitage and Theodore Colton (Eds.). Vol. 7. Wiley, Hoboken, NJ, USA. doi:10.1002/0470011815.b2a15150

[100] Verena Zimmermann and Karen Renaud. 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies* 131 (2019), 169–187. doi:10.1016/j.ijhcs.2019.05.005

[101] Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. 2022. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems* 62, 1 (2022), 82–97. doi:10.1080/08874417.2020.1712269

A Questionnaire

This is the English translation of the German questionnaire used in the survey.

Q1: I agree to complete this questionnaire for the ANONYMIZED project, which asks about my attitudes toward cybersecurity and that my participation is voluntary. The results of this survey will be further processed for scientific purposes only and not for commercial use; all information collected in this survey will be kept, retrieved, and analyzed by researchers only for the purpose of this project. My anonymity is assured, and I will not be identified in publications or otherwise without my explicit written consent (Selected, Not Selected)

Q2: How old are you? (18-24, 25-34, 35-44, 45-54, 55-64, 65+)

Q3: You are... (male, female, diverse, not specified)

Q4: What is your highest educational qualification? (No degree, Hauptschulabschluss, Polytechnische Oberschule, Realschulabschluss, Fachabitur, Abitur, Fachhochschulabschluss, university degree, other degree)

Q5: In which federal state do you live? (Baden-Wuerttemberg, Bavaria, Berlin, Brandenburg, Bremen, Hamburg, Hesse, Mecklenburg-Western Pomerania, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt, Schleswig-Holstein, Thuringia)

Q6: If you add up all the incomes in your household: In which of the following income groups does your monthly household net income fall? (under 900 EUR, 900 EUR to under 1300 EUR, 1300 EUR to under 1500 EUR, 1500 EUR to under 2000 EUR, 2000 EUR to under 2600 EUR, 2600 EUR to under 3200 EUR, 3200 EUR to under 4500 EUR, 4500 EUR to under 6000 EUR, 6000 EUR and more)

Q7: Which of the following devices do you use to connect to the Internet at work and at home, and how often do you use them? (I do not own, Less than two hours a day, Less than four hours a day, More than four hours a day)

- Laptop/Notebook
- Classic cell phone (without touch screen)
- Smartphone (with touch screen)
- Tablet
- Smartwatch/Wearables (e.g., Apple Watch, Samsung Gear, Fitness-Tracker)
- Interconnected car (e.g., Tesla)
- Stationary computer/PC
- TV with Smart TV (e.g., also with Amazon Fire TV, Apple TV)
- Game console (e.g., Nintendo, Playstation, Xbox)
- Smart lighting (e.g. IKEA Tradfri, Philipps Hue)
- Smart heating thermostats
- Smart speakers (e.g., Echo with Amazon Alexa)

Q8: How much do you agree with the following statements regarding cyber threats, i.e., threats on the internet? Note: cyber threats on the internet include, for example, malware such as computer viruses, data misuse, password and account theft, data espionage, online banking fraud, online shopping scams, insults and bullying, sexual harassment, and hate speech (Strongly disagree, Tend to disagree, Neutral, Tend to agree, Strongly agree)

- I think that the above-mentioned cyber threats pose a serious risk to me.
- Without a firewall and virus scanner, you can no longer go on the Internet because you get infected with malware too quickly.
- I only visit and use commonly known websites to avoid becoming a victim of cybercrime.
- The risk of becoming a victim of cyber threats as an individual will increase over the next five years.
- I consider a large-scale cyberattack on public infrastructure in Germany within the next five years a realistic scenario.
- Germany is well prepared for large-scale cyberattacks on public infrastructure.
- I feel capable of adequately protecting my devices, such as smartphones or computers, from cyber threats.
- With regard to cyber threats, I feel I am woefully underinformed.
- I feel like I wouldn't notice if strangers were spying on my computer or smartphone over the Internet.
- I would like to educate myself to better protect myself on the Internet.
- I don't know who to contact for information on protective measures against cyber threats.
- I know where to find up-to-date and reliable information about protecting my devices on the Internet.
- I believe that in the future, wars will increasingly be fought digitally, i.e., on the Internet in the form of cyber attacks.
- I am principally afraid that a cyber war could break out.
- Germany should actively retaliate with cyberattacks itself in the event of a cyberattack.
- The German security authorities have the necessary competencies to adequately protect citizens from cyber threats.
- Through their activities in cyberspace or on the Internet, the German security authorities are more likely to increase the insecurity of citizens than to contribute to a higher level of protection.
- Cybercrime is adequately prosecuted and punished by the German law enforcement authorities and judiciary.

Q09: In the last five years, how often have you personally been a victim of the following types of cyber threats? (Don't know, Never, Once, Rarely, Occasionally, Often)

- Malicious software such as viruses or worms

- No access to online services due to a cyber attack (DDoS attack)
- Theft of computing power, for example, by cryptomining
- Ongoing complex, targeted, and effective attacks against IT infrastructures (Advanced Persistent Threats)
- Unwanted transmission of sexually explicit messages and content (sexual harassment)
- Extraction of information from the physical behavior of hardware (side-channel attack)
- Unwanted, mass delivery of messages (spam)
- Exclusion, insults, or harassment on the internet over a longer period of time (cyberbullying)
- Repeated unwanted contact and approach attempts or digital stalking (cyberstalking)
- Hostility or disparagement based on my supposed or actual affiliation to a social group, e.g., because of my religion, origin, or sexual orientation on the internet (hate speech)
- A person steals your personal data and pretends to be you (identity theft)
- Threat of physical violence on the internet
- Request for payment to regain control over data or devices (ransomware or extortion software)
- Loss of money or goods due to online shopping fraud
- Extortion or intimidation via the Internet to force certain actions (blackmailing)
- Malware that coerced me into buying security software (scareware)
- Software that spies on me in the background (spyware)
- Spying on or stealing confidential data (phishing)
- Involuntary publication of private data on the Internet (doxing)
- Disclosure of confidential information through manipulation (social engineering)
- Unauthorized third-party access to an online or social media account

Q10: Which people or organizations do you or would you seek help from if you were the victim of a cyberattack (e.g., malware)? (Never, Rarely, Occasionally, Often, Always)

- Federal Criminal Police Office (BSI)
- Computer Emergency Response Teams (CERTs) of the federal states
- Police
- Operator or manufacturer of the affected hardware, software or website
- Internet service provider (e.g., Telekom)
- Consumer information and advice centers
- IT security department of my employer
- PC specialist shop/IT service provider
- Public service broadcasting media
- Private media
- Internet forums on IT security (e.g., Heise Security)
- Influential security experts on the Internet
- Influential individuals on social media (influencers)
- Family, friends, or acquaintances with IT skills
- Colleagues with IT skills
- I solve the problem myself

Q11: How high do you estimate the risk of becoming a victim of one of the following types of cyberattacks in the next five years? (I cannot say, Very low, Rather low, Average, Rather high, Very high)

- Malicious software such as viruses or worms
- No access to online services due to a cyber attack (DDoS attack)
- Theft of computing power, for example, by cryptomining
- Ongoing complex, targeted, and effective attacks against IT infrastructures (Advanced Persistent Threats)
- Unwanted transmission of sexually explicit messages and content (sexual harassment)
- Extraction of information from the physical behavior of hardware (side-channel attack)
- Unwanted, mass delivery of messages (spam)
- Exclusion, insults, or harassment on the internet over a longer period of time (cyberbullying)
- Repeated unwanted contact and approach attempts or digital stalking (cyberstalking)
- Hostility or disparagement based on my supposed or actual affiliation to a social group, e.g., because of my religion, origin, or sexual orientation on the internet (hate speech)
- A person steals your personal data and pretends to be you (identity theft)
- Threat of physical violence on the internet
- Request for payment in order to regain control over data or devices (ransomware or extortion software)
- Loss of money or goods due to online shopping fraud
- Extortion or intimidation via the Internet to force certain actions (blackmailing)
- Malware that coerced me into buying security software (scareware)
- Software that spies on me in the background (spyware)
- Spying on or stealing confidential data (phishing)
- Involuntary publication of private data on the Internet (doxing)
- Disclosure of confidential information through manipulation (social engineering)
- Unauthorized third-party access to an online or social media account

Q12: How continuously do you use the following security programs or security measures on your personal devices (computer, smartphone, etc.) to protect against cyber threats? (Never, Rarely, Occasionally, Often, Always)

- Antivirus software (virus scanner) on PC or laptop
- Antivirus software (virus scanner) on smartphone
- Software for automatic creation of backups on the PC or laptop
- Software to automatically create backups on smartphone
- Firewall on PC or laptop
- Firewall on smartphone
- Use of encrypted messenger apps (e.g., Signal)
- Spam filter (e.g., for the e-mail inbox)
- Encryption software for files and hard disks
- Encryption software for e-mail (e.g., PGP)
- Anonymization services (e.g., proxy server, Tor browser)

- VPN connections for encryption of data traffic
- Password manager for central management of passwords
- Two-factor authentication when logging in to websites and apps
- Operating system updates
- App and application updates
- Covering the camera lens of smartphones or webcams
- Changing preset passwords (e.g., for WLAN routers)
- Backups of my data on an external data memory device
- Backups of my data in the cloud
- Meta search engines that do not store user data
- Use of complex passwords (e.g., with special characters, numbers, and uppercase letters)
- Ignoring and deleting untrusted or unknown emails
- Changing my passwords
- Using different passwords for various occasions and user accounts
- Secure HTTPS connection when transmitting personal data
- Avoiding online banking
- Avoiding social media
- Please click on 'Rarely' here

Q13: Which channels do you currently use to find out about cyber threats, security vulnerabilities, and solutions to problems? (Never, Rarely, Occasionally, Often, Always)

- School, University, or Workplace
- Family or friends
- Press (magazines and newspapers)
- Scientific publications
- TV
- Radio
- Websites of security authorities (e.g., BSI)
- Websites with security news (e.g., Heise Security)
- Websites of software or hardware manufacturers (e.g., Apple, Google)
- Websites of security software manufacturers (e.g., Kaspersky, McAfee, Norton)
- Blogs
- Microblogging services (e.g. Twitter)
- Multimedia services (e.g., Instagram, YouTube)
- Social networks (e.g., Facebook)
- Messenger (e.g., Signal, Telegram, WhatsApp)
- Newsletter
- Podcasts
- Warning apps (via smartphone)
- In my installed security software (e.g., antivirus, firewall, or password manager)

Q14: Which channels would you prefer to receive information about cyber threats, vulnerabilities, and problem solutions in the future? Select up to three of the channels you consider most important (Not selected, Selected)

- School, University, or Workplace
- Family or friends
- Press (magazines and newspapers)
- Scientific publications
- TV
- Radio
- Websites of security authorities (e.g., BSI)
- Websites with security news (e.g., Heise Security)
- Websites of software or hardware manufacturers (e.g., Apple, Google)
- Websites of security software manufacturers (e.g., Kaspersky, McAfee, Norton)
- Blogs
- Microblogging services (e.g. Twitter)
- Multimedia services (e.g., Instagram, YouTube)
- Social networks (e.g., Facebook)
- Messenger (e.g., Signal, Telegram, WhatsApp)
- Newsletter
- Podcasts
- Warning apps (via smartphone)
- In my installed security software (e.g., antivirus, firewall, or password manager)