Small Talk, Big Impact: The Role of Everyday Conversations in Cybersecurity Practices

Doruntina Murtezaj
University of the Bundeswehr Munich
Munich, Germany
LMU Munich
Munich, Germany
doruntina.murtezaj@unibw.de

Leonard Johannes Rössert
LMU Munich
Munich, Germany
leo.roessert@campus.lmu.de

Yomna Abdelrahman
University of the Bundeswehr Munich
Munich, Germany
yomna.abdelrahman@unibw.de

Viktorija Paneva
LMU Munich
Munich, Germany
viktorija.paneva@ifi.lmu.de

Florian Alt
LMU Munich
Munich, Germany
University of the Bundeswehr Munich
Munich, Germany
florian.alt@ifi.lmu.de

Abstract

Everyday talk is often treated as casual chatter, yet it plays a crucial role in how people acquire and share knowledge. Typically, cybersecurity practices are informed by formal training, but they often overlook the impact of social exchanges. This paper investigates how informal conversations can act as a socio-technical mechanism for shaping cybersecurity awareness and practices. We conducted an online survey (N=215) where participants described recent discussions about cybersecurity, including who was involved, where they took place, and what triggered them. Quantitative and thematic analysis revealed common contexts, social settings, and topics. Most conversations occurred spontaneously in private environments, with personal experiences being the most frequent trigger. We contribute empirical insights on informal security conversations to inform the design of human-centered technologies that surface and mediate security-related discussions in everyday contexts, to ensure implicit and continuous security awareness.

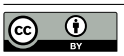
CCS Concepts

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

Keywords

cybersecurity, human-centered security, everyday conversations, security awareness, peer influence, usable security, informal learning

ACM Reference Format:
Doruntina Murtezaj, Leonard Johannes Rössert, Yomna Abdelrahman, Viktorija Paneva, and Florian Alt. 2026. Small Talk, Big Impact: The Role of Everyday Conversations in Cybersecurity Practices. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 26 pages. https://doi.org/10.1145/3772318.3791412



CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791412

1 Introduction

Cybersecurity is often focused on technical solutions and individual user responsibility: users are expected to protect their digital lives by following best practices, such as choosing strong passwords, updating software, or identifying phishing emails. This framing positions security as a matter of personal responsibility and risk management [42]. However, a growing body of research suggests that cybersecurity behaviors are not shaped by knowledge or tools alone. Rather, they are deeply embedded in *social contexts*, influenced by interpersonal relationships, cultural norms, and everyday interactions [3].

Security-related decisions rarely happen in isolation. People routinely discuss digital threats, protective tools, or personal incidents with others, whether to seek advice, offer support, or simply share a story [15, 31]. These *informal conversations* can strongly influence how people perceive risks and choose to act [30]. Prior work has shown that peer interactions can trigger behavioral change, reinforce norms, or serve as emotional support in the face of online threats [11]. Yet despite this recognition, relatively little is known about these conversations: *When do they occur? What prompts them? Who participates? And what impact, if any, do they have on people's security behaviors or attitudes*? To this end, the main research questions guiding this study are:

RQ1 In what contexts (e.g., group sizes, place, situation) do people engage in conversations about cybersecurity?
RQ2 What types of cybersecurity topics are most commonly discussed in everyday conversations?
RQ3 With whom do individuals typically discuss security-related topics, and how does the relationship influence the emotional tone of the conversation?
RQ4 What are the typical triggers that lead to security-related conversations, and what, if any, follow-up actions result from the conversations?

The research questions target central dimensions of everyday security talk and their relevance for design. *RQ1* examines the contexts in which conversations occur, pointing to opportune moments for support. *RQ2* identifies the topics that are frequently discussed as well as those that remain underrepresented, thereby pointing to areas where awareness strategies may require reinforcement. *RQ3* considers the role of social relationships in shaping the exchange of advice and perspectives, with implications for the design of peer-oriented approaches to security support. *RQ4* focuses on the triggers that initiate conversations, contributing knowledge on how such triggers can be deliberately incorporated into education strategies. It also considers whether these conversations resulted in any follow-up actions, offering insights into how initial prompts may connect to sustained engagement with security practices. Collectively, the questions connect empirical insights on security conversations with directions for designing interventions and technologies in human-centered security.

This paper focuses on everyday cybersecurity conversations as a meaningful unit of analysis. We conducted an *online survey* asking participants (N=215) to recall a real-world conversation they had about a security topic. Participants were asked to describe the conversation and answer follow-up questions about it. By collecting first-person accounts of recent conversations, we gain empirical insight into the *social dimension of cybersecurity* that often remains hidden in technical or policy-focused research.

Contribution Statement. Our study contributes in three key ways: (1) *Situational insights:* we provide empirical insights into the situational aspects of cybersecurity conversations, including when, where, with whom, and why people talk about security; (2) *Overview of topics and triggers:* we offer an overview of the common topics and triggers that shape these conversations, spanning personal incidents, news events, and social media posts as well as advice seeking and peer support; and (3) *Implications for awareness:* we discuss the implications of our findings for awareness and education strategies, suggesting that informal peer communication can be incorporated into efforts to promote secure practices in everyday life.

This work contributes to the view that cybersecurity is not merely an individual technical task but a social process [24]. By foregrounding conversations as a site of security learning, negotiation, and decision-making, our findings extend existing literature on security behavior. We highlight how knowledge is circulated, internalized, and acted upon through interaction, and argue that these informal exchanges deserve greater attention from both researchers and practitioners. As digital risks continue to evolve, designing for security must involve not only more effective tools and policies but also a deeper understanding of the social dynamics through which security norms are built and shared. For Human–Computer Interaction (HCI), this emphasizes the need to create technologies and interfaces that support these social processes, enabling users to discuss, learn, and adopt secure practices in their everyday interactions.

2 Related Work

Cybersecurity involves protecting digital systems, networks, and data from unauthorized access, damage, or disruption [2, 9]. As digital technologies have become integral to everyday life, cybersecurity has expanded beyond technical measures to include organizational and human factors as well [1, 22, 23]. This shift reflects a growing recognition that cybersecurity is as much a social issue as it is a technical one. For instance, despite advances in security technologies, industry reports[1] suggest that a majority of breaches occur due to human factors. This might be caused by users often ignoring security advice. In some cases, following security protocols may even appear economically or practically irrational to users when weighed against their immediate goals [19]. Hence, it is essential to support users in adopting more secure behaviors.

Early work in usable security and human-computer interaction addressed these challenges by focusing on individual users. Researchers proposed design frameworks and models that improve interface design, modeling risk perception, and accommodating users' mental models and cognitive limitations in security decisions [1, 8, 10, 38]. For instance, previous research has focused on enhancing users' attention to and compliance with security warnings, which are often overlooked or followed reluctantly [14, 17]. However, a growing body of research suggests that user behavior in cybersecurity cannot be fully understood without considering the social context in which it occurs [4]. In line with this perspective, we contribute by investigating how cybersecurity topics surface in everyday interpersonal conversations.

2.1 Learning Security Through Stories and Triggers

Rader et al. [34] show how users learn about cybersecurity through *informal storytelling*. Their study revealed that stories, especially emotionally resonant ones, can significantly shape listeners' *risk perceptions* and *protective behaviors*. Such stories often convey implicit lessons and circulate more effectively within social networks than advice from experts or formal training [5, 33].

Wash's [40] work on *folk models* provides further insight into this phenomenon. He found that non-experts often rely on simplified mental models of security threats, developed primarily through anecdotes and peer narratives. These folk models influence users' decision-making more strongly than technical knowledge or official guidelines.

Recent work has extended this perspective to the domain of Internet of Things (IoT) security. Zhang-Kennedy et al. [45] examined the influence of personal narratives and social stories on users' perceptions, trust, and adoption behaviors concerning smart home devices. Their findings show that *negative stories* about breaches, privacy violations, or unreliability reduce trust and willingness to adopt IoT technologies, while *positive stories* emphasizing safety and quality of life increase acceptance. This illustrates how narratives serve as powerful *triggers* for shaping security-related attitudes, while also highlighting the risks of misinformation in security storytelling.

From a social perspective, cybersecurity behaviors are shaped by three key challenges [12]: *awareness* of security threats and tools, *motivation* to engage with them, and *know how* for effective use. Das et al. [12] investigated how social processes influence individual

[1]Verizon 2025 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/, last accessed 27 June 2025

cybersecurity decisions. Their findings demonstrate that conversations with peers often act as *catalysts for behavior change*. Nearly 50% of all reported changes stemmed from implicit or explicit social interactions, underscoring the interpersonal nature of security awareness and action. Building on this, Das et al. conducted a large-scale survey to categorize the *behavioral triggers* that prompt users to adopt security and privacy practices [11]. They identified three types of triggers:

- **Social triggers:** advice from peers or observing others,
- **Proactive triggers:** self-motivated actions,
- **Forced triggers:** institutionally mandated behavior.

Among these, social triggers were the most prevalent, especially among users with low to medium security behavioral intention. Participants were also more likely to share their own behavioral changes when prompted by a social interaction, illustrating the *cascading effects* of interpersonal influence in shaping cybersecurity practices.

2.2 The Social Life of Security

Several studies have examined when and how individuals choose to engage, or remain silent, in conversations about cybersecurity [3, 39]. Furthermore, Das et al. [12] found that users readily act on advice from trusted peers but hesitate to offer unsolicited guidance due to concerns about social appropriateness or seeming intrusive. These findings suggest that the act of sharing security advice is embedded in relational and cultural dynamics that influence when and how conversations occur. Educational and societal factors also affect how users perceive and engage with cybersecurity.

In a large-scale study in China, Hong et al. [20] used a *Knowledge-Attitude-Behavior* model to analyze how exposure to less-educated social environments, such as colleagues without formal training, can erode the cybersecurity attitudes and behaviors of university-educated individuals. That study highlights that cybersecurity behaviors are influenced by the broader social and cultural context in which individuals operate, not solely by personal knowledge. Jenkins et al. [21] explored how organizational environments can foster or inhibit open dialogue about security. During a two-week trial of an anonymous discussion platform at a large academic institution, they discovered that anonymity allowed employees to voice concerns, provide feedback on policy changes, and suggest improvements to training. Depending on the source, people from different socioeconomic backgrounds respond differently to security advice. Those from lower socioeconomic backgrounds tend to favor informal sources, such as peers, over formal institutional advice [36].

Beyond individual or organizational settings, Wu et al. [44] systematize how security and privacy practices vary across different social scales, from intimate relationships and families to broader social networks and the public domain. They identify four core behavioral domains through which security and privacy interactions manifest: *negotiating access to shared resources, shared and social authentication, managing self-presentation, and influencing others' behaviors*. Their taxonomy reveals that security and privacy are not merely individual concerns but a socially embedded phenomenon shaped by interpersonal trust, shared norms, and collective responsibilities across various contexts.

Together, prior work suggests that cybersecurity is shaped by relationships, social norms, and organizational contexts, rather than solely through formal training. Much of this knowledge, however, has been derived from interviews or observational logs. Less is known about how people themselves recall and describe their everyday conversations about security, which is the focus of our work.

2.3 Conversations Beyond Formal Security Settings

Prior research has emphasized the importance of structured security dialogues in professional and organizational settings. Parkin et al. [28], for instance, explored how conversations between business leaders and IT advisors can be supported through ontologies and case-based recommendations, helping organizations contextualize incidents and make informed decisions. Complementing this organizational perspective, our work shifts the focus toward informal conversations among everyday users, outside of formal business contexts.

Watson et al. [41] examined how small social groups, such as families or roommates, collectively approach cybersecurity and privacy in everyday life. The authors emphasize that these groups often rely on implicit agreements and individual accountability.

Moju-Igbene et al. [26] explored how small groups negotiate social controls for securing shared digital resources through participatory design jams. They highlight how conversations about privacy and security intertwine with maintaining trust and avoiding social friction, illustrating that securing shared accounts or devices often requires balancing relational harmony with protective measures.

Another line of work addresses privacy disclosures in routine digital interactions: Prange et al. [32] studied situations where individuals unintentionally revealed personal information during video conferences, while Windl et al. [43] examined privacy slip-ups caused by ambient technologies such as cameras and smart devices. Both studies highlight how social settings and contextual factors shape privacy outcomes in daily life, reinforcing the view that security and privacy are lived experiences rather than abstract technical concerns. Beyond co-present interactions, Song et al. [37] analyzed online discussions following the overturn of Roe v. Wade, showing how people collectively engaged in privacy sensemaking around period and fertility tracking apps. Their study illustrates how informal online conversations can evolve into collective reasoning and privacy activism, revealing both the strengths and pitfalls of community-driven privacy discourse.

A related stream of research examined the linguistic dimensions of professional security discourse. Meyers et al. [25] analyzed bug report conversations in the Chromium project[2], identifying pragmatic features such as formality, politeness, and uncertainty that distinguish security from non-security dialogues. While situated in a software engineering environment, their work demonstrated how communication styles shape security mindsets; in contrast, our study places greater emphasis on how non-expert users engage in security talk in everyday settings.

[2]https://www.chromium.org, last accessed: 4 September 2025

Working outside the cybersecurity field highlights the importance of social interaction in awareness building. Peltonen et al.'s CityWall project [29] and Davies et al.'s research on pervasive displays [13] demonstrate how interactive installations in public spaces can foster shared learning and casual engagement. Although not focused on security, these studies highlight the importance of visibility, shared experience, and co-present interaction, which are increasingly relevant for understanding how cybersecurity awareness circulates in everyday contexts.

Summary. Taken together, these studies demonstrate the importance of the social context for understanding how people perceive and act on security issues. Yet most prior work has focused on structured environments such as workplaces, professional platforms, or controlled deployments. Our work contributes by documenting everyday, unstructured conversations about cybersecurity among general users across diverse contexts. Recent work has begun to explore these dynamics across different social scales and informal settings, from small-group interactions to collective sensemaking in online communities. However, much of this research focuses on specific scenarios or mediated environments, such as workplaces, shared digital resources, or online discussions. Our work complements these perspectives by documenting how everyday, unstructured conversations about cybersecurity arise across a wide variety of real-life contexts and among people with diverse backgrounds and levels of expertise. This lens offers insights that can inform the design of future awareness strategies and HCI interventions that meet users where security concerns actually surface.

3 Methodology

This study systematically documents how people discuss cybersecurity in their everyday lives. To achieve this, we designed and deployed an online survey that asked participants to recall and describe recent conversations about cybersecurity, followed by structured follow-up questions on the context, participants, and outcomes of these interactions. This approach enabled us to capture both qualitative narratives and quantitative measures, offering complementary perspectives on the social dynamics of security talk. In the following subsections, we describe the procedure for developing and piloting the survey instrument, the survey's structure, and the tools used for data analysis. We also outline the participant recruitment process, as well as address ethical considerations and methodological limitations.

3.1 Survey Development

We conducted the study using an online survey (see Appendix A) that collected detailed information about participants' recent conversations about cybersecurity. Participants were first prompted to recall a specific discussion they had about cybersecurity topics, followed by a set of structured questions about the context, participants, and outcomes of that conversation. The survey was divided into three main parts: *(1) narrative description of the recalled cybersecurity conversation, (2) follow-up questions regarding the conversation's context and effects, and (3) demographic questions.*

Participants were informed that there were no right or wrong answers and were encouraged to provide as much detail as possible. Based on pilot testing, the estimated completion time for the survey was, on average, seven minutes. Participation was anonymous and voluntary, with participants able to skip questions they did not wish to answer.

After developing the initial version of the survey instrument, we conducted a three-step testing and deployment process: first, we consulted with domain experts; second, we conducted pilot testing with a small sample of participants; third, we deployed the survey.

First Step: Pilot Testing with Domain Experts. We conducted initial pilot testing with PhD-level researchers (N=3): two experts in in human-computer interaction and one in usable security and privacy. Their expertise in survey design and human-centered security research ensured that the instrument was reviewed with attention to methodological rigor and domain relevance. Using pen-and-paper versions of the survey, participants completed the questionnaire while thinking aloud, followed by structured feedback discussions that focused on wording clarity, logical flow, appropriateness of answer options, and completion time.

Based on expert feedback, several targeted adjustments were made. To clarify the scope of certain questions, we refined the wording for clarity and precision. The survey logic was revised so that participants who indicated no prior conversation would still proceed to the demographic section. In addition, example topics—such as large-scale hacks, ransomware attacks on municipalities or universities, choosing secure passwords, or adopting password managers—were added to help participants better understand what qualifies as a cybersecurity conversation. Further refinements focused on restructuring response categories, expanding emotional response options, and ensuring greater alignment between questions about participants' own perceptions and those of their conversation partners.

Second Step: Technical Pilot with Broader Sample. After incorporating expert feedback, we conducted a technical pilot with participants (N=15) from our academic environment. They completed the survey independently using the live online link. The aim was to confirm the average completion time and to identify potential usability or comprehension challenges. No substantial content changes were required based on this pilot. Minor refinements were made to styling and formatting, such as emphasizing key words, since no comprehension issues were reported.

Third Step: Survey Ready for Deployment. A final internal review (N=2) was conducted to verify the survey's functionality and logical consistency. This step confirmed that the instrument was ready for large-scale deployment. By integrating expert feedback, pilot testing with participants, and iterative refinements, the survey was optimized for accessibility to a general audience while ensuring methodological rigor in capturing everyday cybersecurity conversations.

3.2 Apparatus

This subsection describes both the structure of the online survey presented to participants and the software environments used for data collection and analysis.

3.2.1 Survey Structure. The survey was designed to capture how cybersecurity conversations unfold in everyday life, from the context in which they occur to the people involved and their perceived outcomes. To achieve this, the survey combined open-ended and structured items, allowing participants to both narrate their own experiences and provide corresponding categorical data. Accordingly, the survey was divided into three main parts:

(1) Narrative description: Participants were asked to recall and describe, in as much detail as possible, a recent conversation they had about cybersecurity.
(2) Follow-up questions: The multiple-choice and Likert-style items aimed to provide context for the narrative description and collect comparable data.
(3) Demographics: These include questions on age, gender, country of residence, and occupation/field of study.

Participants could also describe an additional conversation if they had more than one to report. Table 1 provides an overview with example items. The complete questionnaire is included in Appendix A.

3.2.2 Data Collection and Processing Tools. The survey was hosted on the Qualtrics platform[3], which supports responsive layouts for desktop and mobile devices. Participants accessed the survey via a URL distributed through the recruitment channel described in Section 3.4. Responses were securely stored on Qualtrics servers and later exported in CSV format.

3.3 Data Analysis

The collected survey data comprised both quantitative responses from structured items and qualitative narratives from open-ended questions, requiring a mixed-methods approach to analysis.

3.3.1 Quantitative Data Analysis. The quantitative data from the closed-ended survey items were analyzed using descriptive and inferential statistics. Descriptive analyses summarized the distributions of responses across key variables, including conversation settings, triggers, initiators, and reported outcomes. Where applicable, chi-square tests of independence were conducted to examine relationships between categorical variables (e.g., whether particular triggers were more likely to result in reported behavior change). Likert-scale items (e.g., self-assessed confidence in discussing security topics) were analyzed using measures of central tendency and dispersion. Additionally, exploratory analyses examined correlations between confidence, emotional tone, and conversation outcomes. Together, these analyses helped identify patterns in how situational and relational aspects of conversations may shape participants' perceptions and reported behavioral changes. Quantitative data were analyzed using Jupyter Notebook[4], which provides an open-source environment for statistical analysis and visualization.

3.3.2 Qualitative Data Analysis. All entries were imported into the ATLAS.ti analysis software[5]. We used thematic analysis with open coding [6]. We followed the six stages of thematic analysis proposed by Braun and Clarke [7]. These stages include becoming familiar with the data, creating an initial set of codes, grouping codes into themes, discussing those themes, defining and naming them, and finally presenting the findings. These steps support a thorough analysis of the qualitative participants' responses. Two authors independently read 43 transcripts (20%) to familiarize themselves with the data and generated open codes. Through repeated discussions, they developed a coding book (generating the initial codes stage). The remaining transcripts were divided between the researchers, who coded them individually. After all materials were coded, the team met again to refine and finalize the codebook (see Appendix B). Following this, the researchers collaboratively identified emerging themes through an iterative process that involved grouping codes, assessing theme coherence, and defining clear theme labels. This approach resulted in four main themes: *Incident-Based and Social Triggers for Cybersecurity Talk*, *Everyday Security Learning through Advice*, *Social and Emotional Aspects of Cybersecurity Conversations*, and *Conversations as Drivers of Behavior Change*.

Table 1: Overview of the survey structure with illustrative example questions from each section. The survey was organized into three parts: (1) an open-ended *narrative description* of a recent conversation about cybersecurity, where participants were encouraged to recall and narrate their experience in detail; (2) *follow-up questions* capturing the context, triggers, emotions, and outcomes of the conversation, including whether it led to changes in security practices; and (3) *demographic* questions providing background information about participants' age, gender, country of residence, and occupation/field of study. This structure ensured that both qualitative narratives and comparable quantitative measures could be collected, enabling a multi-faceted analysis of everyday cybersecurity conversations.

Part	Example Questions
(1) Narrative description	Do you remember having a conversation about any cybersecurity topic? (Yes/No/I do not know) Please describe, in as much detail as possible, the last time you talked about cybersecurity (e.g., Who was involved? Where did it take place?).
(2) Follow-up questions	Who started the conversation? (Myself/Other/I do not know) What led to the topic of cybersecurity coming up (e.g., Personal incident, News story)? What specific cybersecurity issue(s) did you discuss (e.g., Phishing, Password use, Privacy tools)? How did you feel during the conversation (e.g., Interested/curious, Worried/anxious)? Did the conversation lead to any changes in security practices? (Yes/No/I do not know)
(3) Demographics	Age, Gender, Country of residence, Occupation/Field of study

[3]https://www.qualtrics.com, last accessed: 4 September 2025
[4]https://jupyter.org, last accessed: 4 September 2025
[5]https://atlasti.com, last accessed: 4 December 2025

3.4 Participants and Recruitment

Initially, N=258 participants took part in the survey and completed it. Responses were reviewed for completeness and consistency during the data cleaning process. We excluded three participants based on their responses to a self-assessed honesty item included at the end of the survey. Participants rated the statement *I have answered all questions honestly* on a 5-point Likert scale. Participants who did not select the highest point on the scale—indicating maximum honesty levels—were excluded, resulting in a dataset of 255 participants. Of these, 40 participants (16%) either could not recall a cybersecurity conversation or chose not to provide any details. Thus the final analytic sample consisted of the N=215 participants who provided at least one conversation description. Thirteen of these participants (6%) reported two conversations, yielding a total of 228 conversation accounts.

Participants were recruited through the online research platform Prolific[6]. The target population included adults aged above 18 and we used Prolific's quota system to obtain a balanced gender distribution. No restrictions were placed on country of residence, level of education, or technical expertise, and no cybersecurity knowledge was required. Participants were not intentionally prefiltered beyond the platform's basic eligibility criteria. The aim was (1) to avoid introducing additional screening that would disproportionately favor highly engaged or technically knowledgeable individuals, and (2) to maintain ecological validity by allowing a participant pool that reflects the diversity of people who have cybersecurity conversations in their everyday lives.

Recruitment materials briefly described the aim of the study and provided the survey link. The study description informed prospective participants that the survey focused on describing a recent conversation about cybersecurity and invited them to participate if they could recall at least one such conversation. While this may have introduced some degree of self-selection, no explicit screening or filtering was imposed by the researchers. Participants were compensated in line with Prolific's fair payment policy, at an hourly rate of £10.20/hour, consistent with the platform's recommended standards. The study procedure was reviewed and approved by the university's ethics committee.

3.5 Limitations

While this study offers novel insights into everyday cybersecurity conversations, its methodological limitations should be noted to contextualize the findings. The survey relies on participants' memories of past conversations. While this approach is practical for large-scale data collection, it may introduce minor recall inaccuracies and favor interactions that were salient or emotionally charged, while more routine or implicit exchanges may be overlooked. To partially mitigate this, we included follow-up questions about perceived impact, potential behavioral change, and intentions to continue the conversation, which provide additional context. At the same time, this recall-based survey approach remains one of the few practical ways to capture reflections on real-life interactions without the ethical and practical constraints of in-situ observations or the influence of the researcher's presence.

[6]https://www.prolific.com, last accessed September 4, 2025

The open-ended nature of the core questions enabled rich qualitative input. However, some participants provided shorter or less detailed accounts. This variation limits the depth of certain entries, yet it also reflects the natural diversity in how people remember and report such conversations. To support interpretability, the survey included follow-up questions about the described conversations, which helped clarify relevant context.

Another limitation concerns the possibility of *social desirability bias*: participants might have avoided or felt uncomfortable reporting on *less conventional* security conversations or behaviors, given the sensitivity of the topic in a cybersecurity study. The generalizability of our findings is also constrained by the sample size and should therefore be interpreted as indicative patterns rather than population-wide estimates. Cultural and regulatory contexts may likewise have shaped participants' conversations. Although our sample included respondents from multiple countries, the distribution across countries was not balanced, and the study was not designed to examine cross-cultural effects, which prior work suggests can influence security perceptions and responses [35].

Finally, we discouraged participants from using Large Language Models (LLMs) to answer the text-entry question and disabled the ability to paste text into the survey fields. While this required participants to manually type their answers, it cannot be ruled out entirely that some entires may have been generated with external tools.

4 Results

The results present findings based on the cleaned dataset. Percentages are calculated relative to the total number of coded instances within each category. Participant quotes were lightly polished for grammar and readability. We first present the quantitative results (Section 4.2) obtained from the closed-ended questions, followed by the qualitative results (Section 4.3) derived from the open-ended questions.

4.1 Demographics

We report demographic data for our final dataset containing 215 participants who described a cybersecurity conversation. Their ages ranged from 19 to 73 years old, with a median age of 32. The gender distribution was 50% male, 48% female, and 2% other. Participants had diverse educational and professional backgrounds, including students, knowledge workers, and practitioners in fields such as design, law, chemistry, medicine, beauty therapy, and education. A subset of 46 participants reported working in IT-related fields. The largest share of respondents resided in the United Kingdom (20%), followed by Germany (19%) and the United States (15%); the remainder came from other European countries (see Appendix C). The overall completion rate was 77%, with a dropout rate of 23%. With regard to cybersecurity-related practices, participants on average tended to disagree with the statement: *"I often give cybersecurity advice to others"* ($M = 2.76$, $SD = 1.11$). While 33% selected the midpoint of the scale and 26% disagreed, only 21% agreed and a small fraction (6%) strongly agreed, suggesting that giving cybersecurity advice is not a frequent activity for most respondents.

Table 2: Summary of participant demographics (N = 215).

Characteristic	Value
Age	19–73 years (Median: 32 years)
Gender	50% male, 48% female, 2% other
Occupations	Students, professionals (design, law, chemistry, medicine, beauty therapy, education, etc.)
Country of residence	20% UK, 19% Germany, 15% USA, remainder other European countries
Cybersecurity advice	Mean = 2.76 (SD = 1.11); 33% midpoint, 21% agree, 6% strongly agree (5-point Likert scale)

4.2 Quantitative Results

This section reports the quantitative results, summarizing patterns across participants' survey responses.

4.2.1 Do people talk about security? In response to the opening survey question (*"Do you remember having a conversation about any cybersecurity topic?"*), 84% of the respondents (N=215) reported having done so and proceeded to describe such a conversation. The remaining 16% (N=40) answered with *no* or *I do not know*.

4.2.2 A Situational Overview of Cybersecurity Conversations (RQ1).

Group Sizes and Dynamics. The majority of conversations (57%) occurred between two individuals, while an additional 22% involved three participants. Thus, over three-quarters of all discussions took place in dyadic or triadic settings. Larger groups of four or more accounted for only 14%, indicating that cybersecurity conversations predominantly unfold in small, intimate contexts. In 21% of cases, new participants joined partway through the discussion, whereas 79% remained restricted to the original group. Follow-up interactions were less common: 19% of respondents reported having continued the discussion in a subsequent exchange, while the remaining 81% had not yet engaged in follow-up, although some indicated plans to do so.

To explore the relationship between conversational structure and behavioral outcomes, we examined the correlations between group size, additional participant joining, follow-up interactions, and reported changes in cybersecurity practices (see Figure 1). We found a moderate positive correlation between group size and the likelihood of new participants joining ($\rho = 0.55$), suggesting that *larger conversations were more likely to expand*. However, the associations between structural features and reported behavioral change were weak: conversation size ($\rho = 0.11$), new participants joining ($\rho = 0.11$), and follow-up interactions ($\rho = 0.04$) showed no meaningful relationship with behavior change. These results indicate that structural characteristics of conversations alone did not substantially predict whether participants reported behavioral changes within our dataset.

Conversation Settings. The majority of reported conversations took place in domestic or professional settings. Specifically, 42%

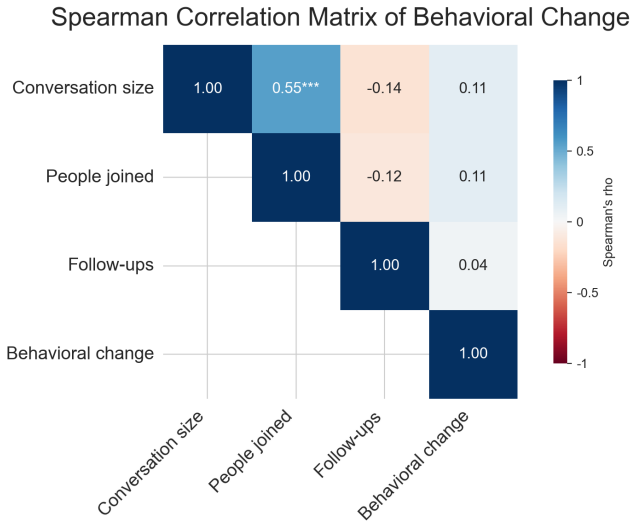


Figure 1: Spearman correlation matrix of conversational metrics and behavioral change. The size of the conversation and the number of people joined are moderately correlated ($\rho = 0.55$), suggesting that larger discussions attract more participants. Follow-ups are weakly negatively correlated with both, while behavioral change shows minimal correlation with other variables ($\rho \leq 0.11$). Color intensity reflects the strength and direction of the correlation, ranging from blue (negative) to red (positive). *Significance levels:* $*p < 0.05$, $**p < 0.01$, $***p < 0.001$.

occurred at home and 34% in workplaces or universities (see Figure 2), together accounting for nearly three-quarters of all interactions. Public spaces, including streets, parks, cafés, and similar environments, represented 15% of the total. The remaining 9% were distributed across diverse contexts such as telephone calls, car rides, or social gatherings. Overall, the findings suggest that *cybersecurity conversations are most often embedded in everyday routines and established social or professional networks.*

Initiators. When asked about who initiated the conversation, participants' responses were nearly evenly divided. In total, 48% reported that they had initiated the discussion themselves, while 52% stated it was initiated by someone else.

4.2.3 Identification of Key Conversation Topics (RQ2). Figure 3 presents the distribution of topics participants reported discussing in their cybersecurity conversations. The most frequently mentioned themes were *incidents* (46%), such as data breaches or ransomware attacks, followed by *security behavior* (43%), including practices like password choice or software updates, and *application areas* (41%), such as social media or smartphone use. Other topics were mentioned less frequently but still played a notable role, with *phishing or scams* reported in 37% of conversations and *security tools* (e.g., password managers or antivirus software) in 31%. These findings indicate that *participants tended to focus their discussions on visible or personally relevant threats*, while more specialized or technical aspects of cybersecurity were addressed less frequently.

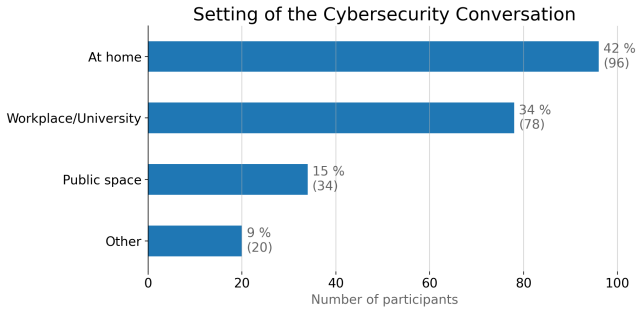


Figure 2: Distribution of settings where cybersecurity conversations took place. Most participants reported having these discussions at home (42%, N=96), followed by the workplace or university (34%, N=78). Fewer conversations occurred in public spaces (15%, N=34) or other settings (9%, N=20). Percentages are shown alongside absolute counts.

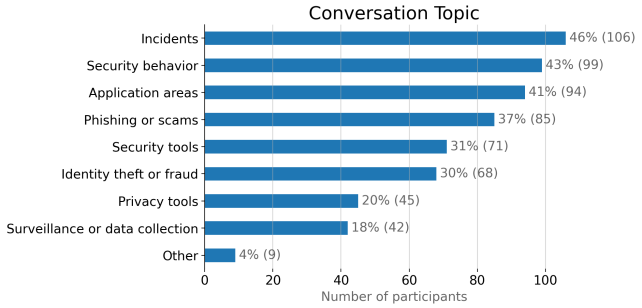


Figure 3: Topics discussed in cybersecurity conversations. The most frequent topics were incidents (46%, N=106), security behavior (43%, N=99), and application areas (41%, N=94). Other common themes included phishing or scams (37%, N=85), security tools (31%, N=71), and identity theft or fraud (30%, N=68). Less frequent topics were privacy tools (20%, N=45), surveillance or data collection (18%, N=42), and other issues (4%, N=9).

This pattern highlights the importance of concrete incidents and everyday practices in shaping informal security discussions, while abstract or technical issues seem to play a more peripheral role.

A chi-square test of independence was applied to examine the relationship between age range and the topics discussed. The analysis revealed no statistically significant association: $\chi^2(40, N = 619) = 40.41$, $p = .45$. This indicates that, overall, topic choice was not strongly dependent on age group. Nevertheless, standardized residuals (see Figure 4) highlight certain tendencies. For instance, discussions of *surveillance or data collection* were more frequent than expected among respondents aged 18–24, whereas they were less frequent among the 25–34 and 35–44 groups. Conversely, *incidents* were somewhat more common among respondents aged 55–64, while *application areas* appeared less often than expected in

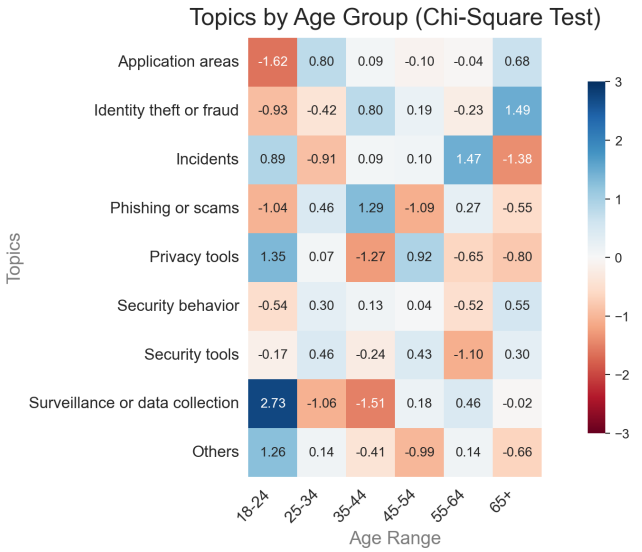


Figure 4: Standardized residuals from the chi-square test of independence between age groups and topics discussed. Residuals indicate whether a topic was mentioned more frequently (positive, blue) or less frequently (negative, red) than expected under independence. No overall significant association was found ($\chi^2(40, N = 619) = 40.41$, $p = .45$), but deviations suggest exploratory patterns such as increased discussion of *surveillance or data collection* among respondents aged 18–24.

the 18–24 group. While these deviations are not statistically significant, they suggest possible age-related patterns in conversational focus that could be explored in future studies.

4.2.4 *Insights into Social Dynamics and Emotional Tone of the Conversations (RQ3).*

Relationship. Cybersecurity conversations were most frequently reported with *friends* (34%) and *colleagues* (33%), which together accounted for more than two-thirds of all responses. A substantial proportion of participants also indicated discussions with *family members* (22%) or a *partner* (14%). These findings suggest that *cybersecurity concerns are most often addressed within established personal and professional networks.* Conversations with more distant contacts were relatively uncommon. Only 4% of respondents mentioned discussing cybersecurity with an *acquaintance*, and conversations with *strangers* accounted for just 2%. A small percentage (2%) selected the category *other*. These results suggest that *cybersecurity discussions predominantly occur in settings characterized by trust and regular interaction, such as friendships, workplaces, and family.* Ad hoc interactions seem to play only a minor role.

Emotions. The most frequently reported emotion in cybersecurity conversations was *interest or curiosity*, selected by 64% of participants for themselves and by 59% as perceived in others (see Figure 5). *Worry or anxiety* and *confidence or informedness* were also

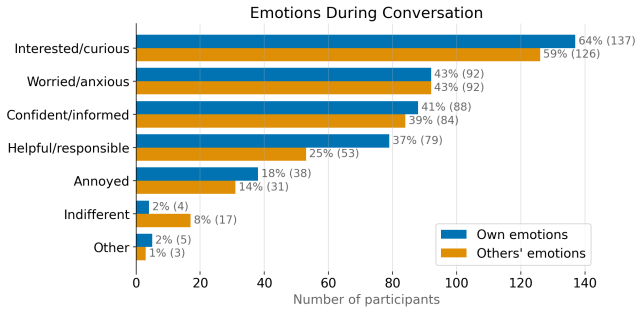


Figure 5: Emotions expressed during cybersecurity conversations, comparing participants' own feelings with perceptions of others' emotions. The most common emotions were interest/curiosity (64% own, 59% others), worry/anxiety (43% each), and confidence/informedness (41% own, 39% others). Participants also reported feeling helpful/responsible (37%) or perceiving others that way (25%). Less frequent were annoyance (14–18%), indifference (2–8%), and other emotions (1–2%).

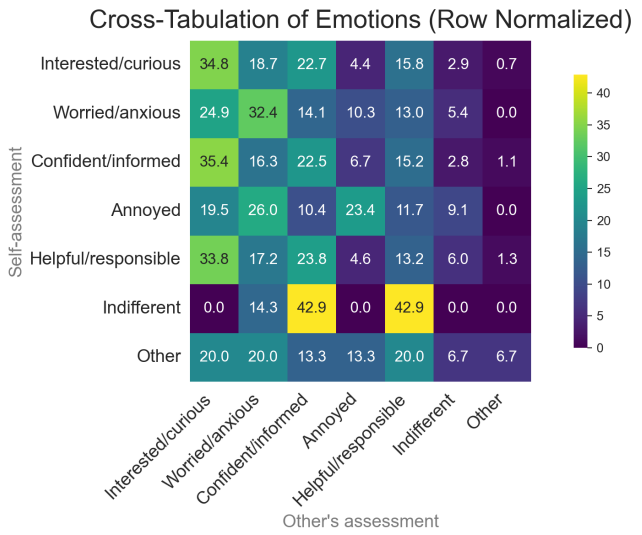


Figure 6: Cross-tabulation of emotions reported in cybersecurity conversations (row-normalized). Rows represent participants' self-assessed emotions, while columns show how they perceived others' emotions. Lighter cells indicate higher proportions within each row. For example, participants who felt interested/curious often also perceived others as interested/curious (35%), while those reporting indifference most frequently perceived others as indifferent (43%). The matrix highlights both alignment and divergence between self- and other-assessed emotions.

common, with 43% of respondents attributing each of these feelings to both themselves and their conversation partners. Feelings of *helpfulness or responsibility* appeared more asymmetrical, reported by 37% of participants as their own emotion but by only 25% for others. Negative emotions were less frequent overall: *annoyance* was mentioned by 18% for oneself and 14% for others, while *indifference* was rarely selected (2% self, 8% others). These findings indicate that most conversations were perceived as engaging and constructive, although they were often accompanied by elements of uncertainty or concern.

To better understand how emotions shaped conversational experiences, we compared participants' self-reported emotions with their perceptions of their conversation partners' emotions (Figure 6). Cross-tabulations revealed varying degrees of overlap: 52 participants (23%, 95% CI [18–29]) reported perfect alignment, 100 (44%, CI [38–50]) showed partial overlap, and 76 (33%, CI [28–40]) indicated no alignment, highlighting frequent discrepancy between one's own emotional state and that of others. To further explore these dynamics, we applied k-means clustering ($k = 3$) to the combined emotion profiles. The three-cluster solution had a low silhouette score ($s = 0.17$), indicating modest separation, but was highly stable across re-runs (mean ARI = 0.92, range 0.85–1.00), suggesting the clusters capture reproducible conversational profiles. The largest cluster, *Confident/Helpful/Curious*, comprised 126 participants (55%, CI [49–62]) and reflected predominantly positive and constructive emotions. The second cluster, *Anxious/Annoyed*, included 98 participants (43%, CI [37–50]) and was marked by feelings of uncertainty, worry, and frustration. A small cluster, *Neutral/Indifferent* ($N = 4$, 2%, CI [0.7–4.4]), also emerged, though its size makes interpretation tentative. These results suggest that, *although many conversations are perceived as constructive, a notable proportion evoke anxiety or annoyance.* Also mismatches between one's own emotions and those perceived in others are common.

Confidence. Participants rated their confidence in discussing cybersecurity on a 5-point Likert scale. Overall, responses indicated high levels of confidence. The majority selected agreement values, with 40% choosing *agree* and 26% choosing *strongly agree*. *Neutral* responses accounted for 22% of the sample, while only 8% and 3% reported lower confidence levels. These results suggest that most participants felt comfortable and assured when engaging in security-related conversations, with relatively few expressing uncertainty or low confidence.

An independent samples t-test was conducted to examine differences in self-confidence between male and female participants. Results indicated that males ($M = 3.94$, $n = 113$) reported significantly higher self-confidence compared to females ($M = 3.58$, $n = 109$), $t(217.4) = 2.67$, $p = .008$. To explore how confidence related to other factors, we conducted correlation analyses between confidence, self-reported behavioral change, willingness to give advice, and age (see Figure 7). Confidence showed a moderate positive correlation with willingness to give advice ($\rho = 0.45$), but only weak associations with behavioral change ($\rho = 0.06$) and age ($\rho = 0.13$). Similarly, behavioral change exhibited weak correlations with both willingness to give advice ($\rho = 0.14$) and age ($\rho = 0.06$), while age and advisory intentions were virtually unrelated ($\rho = 0.02$). Collectively, these findings suggest that *while confidence may encourage intentions to advise others, it does not strongly predict whether participants actually adopt new behaviors themselves.*

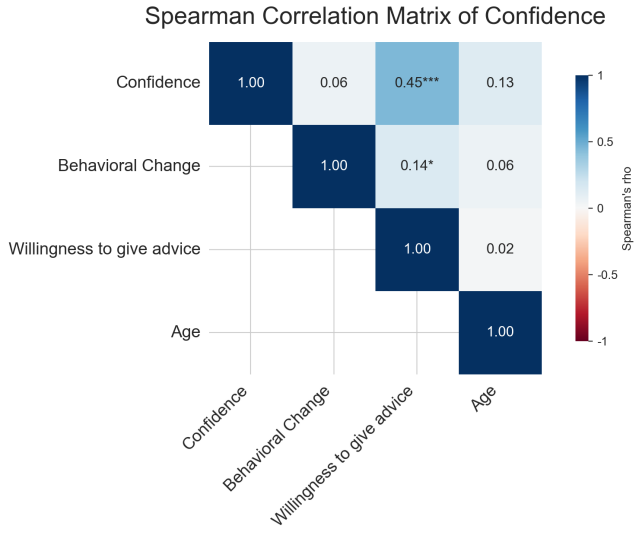


Figure 7: Spearman correlation matrix of confidence, behavioral change, willingness to give advice, and age. Confidence shows a moderate positive correlation with willingness to give advice ($\rho = 0.45$), while all other relationships are weak ($\rho \leq 0.14$). Color intensity represents correlation strength and direction, ranging from blue (negative) to red (positive). *Significance levels:* $*p < 0.05$, $**p < 0.01$, $***p < 0.001$.

To examine these relationships further, we ran an ordinal regression predicting confidence from willingness to give advice, behavioral change, age, gender, and country. Willingness to give advice emerged as a robust predictor ($\beta = 0.82$, $p < 0.001$), with each one-point increase on the advice scale more than doubling the odds of reporting higher confidence. By contrast, behavioral change was not significant ($\beta = -0.20$, $p = 0.53$), suggesting that adopting new practices does not systematically explain confidence levels. Age showed a small positive trend ($\beta = 0.02$, $p = 0.09$), indicating that older participants may report slightly greater confidence, yet the effect was not reliable at conventional significance levels. Neither gender nor country of residence contributed significantly, with wide confidence intervals around their estimates. Together, these results reinforce the interpretation that *confidence is primarily linked to advisory intentions, with demographic and behavioral factors playing a minimal role.*

4.2.5 Conversation Triggers and Follow-Up Actions (RQ4). About half of the participants (51%) indicated that their conversations were triggered by a *personal experience*, often involving a security or privacy incident such as receiving a suspicious email or noticing unusual account activity (see Figure 8). The second most common trigger was *exposure to an external information source*, reported by 27% of participants. These included news articles or social media posts, which participants noted as prompts to raise the topic in conversation. Work- or school-related requirements accounted for 21% of triggers, reflecting institutional contexts where cybersecurity was mandated or discussed. In 14% of cases, conversations began when someone explicitly sought advice, positioning the participant as an information source. The remaining 11% were categorized as *other*, covering a variety of less frequent circumstances, such as overhearing related discussions, encountering unfamiliar technologies, or reflecting on past events without a direct external stimulus.

Impactful Conversations Leading to Follow-Up Actions. When asked if the conversation led to any changes in cybersecurity practices, 62% (N=117) of participants reported that it did not, while 38% (N=71) said that they had adopted new practices or influenced others to do so. *Although some respondents reported a change in their cybersecurity behavior, most did not make direct adjustments following the conversation.*

We applied logistic regression to identify conversational factors associated with changes in cybersecurity behavior. The model demonstrated moderate discriminatory ability. Cross-validation yielded a mean ROC AUC of 0.661 (SD = 0.082, $n = 5$ folds), which was consistent with the holdout ROC AUC of 0.661, indicating stable model performance. The overall classification accuracy was 0.649. Examination of the confusion matrix (22 TN, 13 FP, 7 FN, 15 TP) and classification report revealed asymmetries between classes: the model achieved relatively high precision for the negative class ($P = 0.76$, $R = 0.63$, $F_1 = 0.69$), while the positive class was characterized by lower precision but higher recall ($P = 0.54$, $R = 0.68$, $F_1 = 0.60$). This pattern reveals that the model was more effective at identifying true positives than at avoiding false positives.

Coefficient analysis using regularized logistic regression further highlighted the variables most strongly associated with the outcome. Positive predictors included feeling helpful and responsible (OR = 1.94), feeling worried or anxious (OR = 1.67), and being asked for advice (OR = 1.58). Country indicators such as Greece, Poland, and the USA were also linked to higher odds of a positive prediction (OR range 1.17–1.33), as were work- or school-related requirements (OR = 1.25). Conversely, negative predictors included confidence in being well-informed (OR = 0.72), colleague influence (OR = 0.80), and professional fields such as IT (e.g., computer science, cybersecurity, software development) (OR = 0.82) and medicine (OR = 0.81). In addition, country indicators such as Spain, the UK, and Germany were associated with lower odds of a positive classification (OR range 0.71–0.87). These findings suggest that *psychological dispositions and social context are stronger determinants of the predicted outcome than professional or demographic variables alone.*

Decision Flow. The Sankey diagram (see Figure 9) illustrates how reported conversation triggers shaped the topics and eventual outcomes of cybersecurity discussions, including whether participants reported changes in their own behaviour. As participants could select multiple triggers and topics when describing a single conversation, the flows capture the complexity and overlap in how these discussions emerged and developed. Overall, *the triggers were relatively evenly distributed across the different conversation topics*, suggesting that no single entry point dominated the way cybersecurity issues were framed. The subsequent flows from conversation topics to outcomes reveal a similar pattern: *individual topics map onto behavioural outcomes in proportions that broadly mirror the overall distribution.* This indicates that, *while triggers and topics varied, their relationship to reported behavioural change was diffuse rather than concentrated in one pathway*, highlighting the diversity

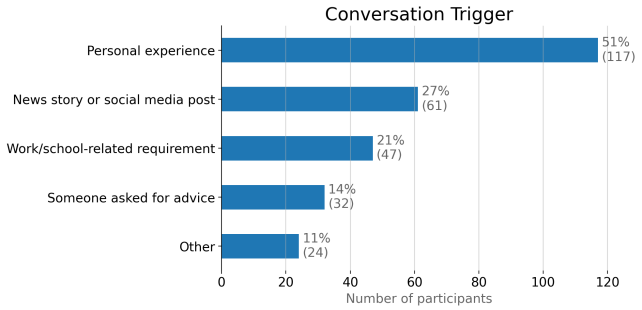


Figure 8: Triggers for cybersecurity conversations. The most common trigger was personal experience (51%, N=117), followed by a news story or social media post (27%, N=61) and work/school-related requirements (21%, N=47). Fewer conversations were initiated when someone asked for advice (14%, N=32) or due to other reasons (11%, N=24).

of ways in which everyday conversations about cybersecurity unfolded.

Key Quantitative Takeaways. Everyday cybersecurity talk was most often reported at home (42%) and at work/university (34%), typically triggered by personal experience (51%) and centered on incidents (46%), security behavior (43%), and application areas (41%). Interested/curious was the dominant emotion (64% self; 59% others), with worried/anxious also common (43% each). Correlational patterns were sparse: conversation size correlated with more people joining ($\rho = .55$, $p < .001$); confidence correlated with willingness to give advice ($\rho = .45$, $p < .001$); and behavioral change showed a small positive link with advice-giving ($\rho = .14$, $p < .05$). Other associations, including those with age, were weak, and the topic × age chi-square test showed no overall significant association; residuals suggested only exploratory, small deviations. In outcomes, 38% reported a behavior change following a conversation (62% did not). A cross-tabulation of emotions indicated frequent alignment between how participants felt and how they perceived others felt (stronger values along the diagonal).

4.3 Qualitative Results

The average length of the conversation description was 415 characters (74 words). Participants did not describe their conversations as isolated incidents but rather as part of social interactions shaped by feelings, relationships, and attempts to understand these incidents. In the following, we present the themes that emerged from the participants' responses.

4.3.1 Incident-Based and Social Triggers for Cybersecurity Talk. A prominent theme concerned how cybersecurity incidents acted as spontaneous conversation triggers. Participants often began discussing cybersecurity after *personally experiencing* or knowing someone who experienced phishing attempts, suspicious emails, hacked accounts, or financial fraud. For instance, one participant noted that they "were talking to [a] friend at university about a cybersecurity attack that happened at my school, and was explaining what happened to me" (P90). Similarly, workplace exchanges often arose after experiencing an issue; as one participant noted, their colleague "told [them] his email had been hacked and used to send phishing messages," which "sparked a quick discussion at lunch" (P43). Conversations were also triggered by cyberattacks *reported in the news or online*, which served as shared reference points for discussing security concerns: "we talked after hearing about a Marks&Spencer data leak and wondered if we might be affected" (P45).

Beyond concrete incidents, participants also described how *Social and Emotional Concerns* — such as sense of responsibility, fear, or worry for family members, played an important role in initiating conversations. Many framed their motivation as a desire to protect people close to them from potential harm. For example, one participant "talked with [their] relatives about the increase in scamming and how careful you must be when you are online" (P170). Others felt an obligation to share their knowledge, with one noting that they "know a lot/enough about the topic where I think people will benefit from my advice" (P50). In summary, experienced (by self or acquaintance) or witnessed incidents (reported in news), as well as social responsibility, acted as triggers that transformed everyday interactions into opportunities to reflect on security.

4.3.2 Everyday Security Learning through Advice. This theme describes the evolution of the conversations. Once conversations were started, they often evolved into informal educational moments in which practical advice was exchanged. Participants shared *actionable security advice*, such as how to create strong passwords, how to identify phishing attempts, or why multifactor authentication should be enabled. For example, one participant explained how they and their son "spoke about not clicking bad links and using strong passwords" (P112). Similarly, another participant, advising their mother, emphasized the importance of carefully reviewing message senders: "I advised her to always check the email address that sent the email and to be skeptical when receiving texts like "urgent" etc." (P76).

Participants who reported being personally affected by a recent incident discussed *post-incident recovery strategies*, such as locking down accounts, updating credentials, or monitoring financial activity. One participant described telling their brother, whose credit card details had been stolen, to "call the credit card company to freeze the card and to get a new one" (P198). In another case, when a partner received a suspicious call from a bank, the participant recounted that "we didn't know if they could do something to the bank account, and we were watching it closely" (P254).

Informal learning also extended to *recommending security tools* and helping others in securely configuring their devices and accounts. For example, one participant described "recommending a new VPN to my colleague" (P209), while another noted that their colleague was "using an app on the phone that stores passwords and syncs with their computer so they don't have to remember anything" (P205).

4.3.3 Social and Emotional Aspects of Cybersecurity Conversations. Conversations were shaped by social and emotional dynamics, with many participants expressing concern for the digital safety of others (e.g., warning a partner or a parent), attempting to reduce others' anxiety after an incident, or correcting misconceptions. Parent-child interactions appeared frequently, highlighting how security norms were shared across generations. For example, one participant

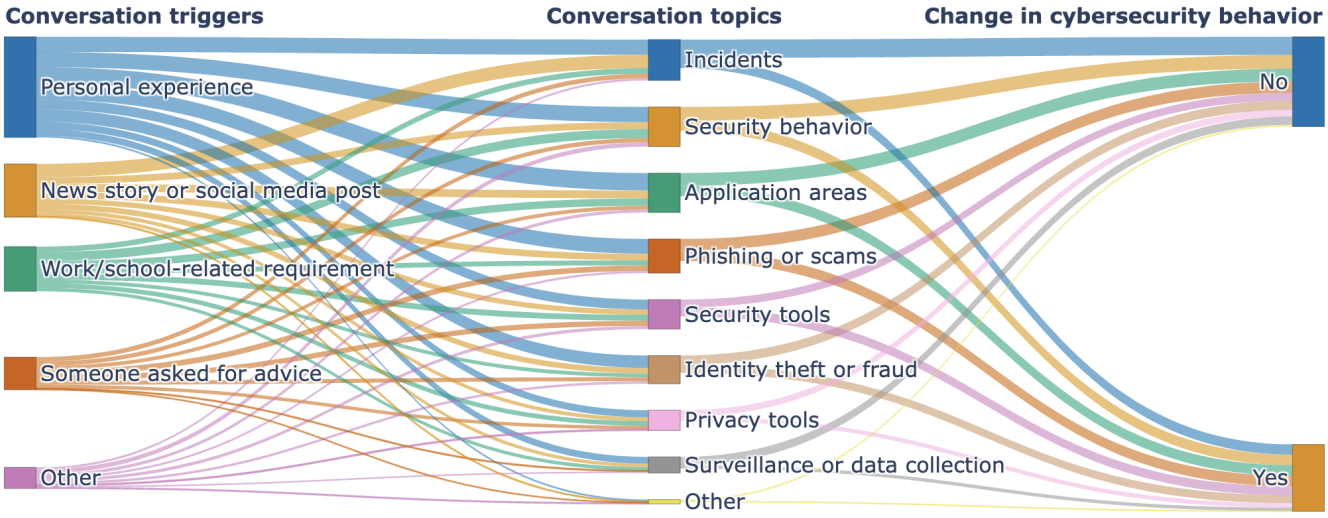


Figure 9: Flow of cybersecurity conversations from triggers (left) through topics (center) to reported behavioral change (right). Personal experience and news or social media posts were common triggers, leading primarily to discussions about incidents, security behavior, and application areas. These conversations varied in whether they were associated with self-reported behavioral change (Yes/No). The diagram highlights how different triggers and topics relate to outcomes.

described feeling "worried that [their] daughter would fall for the scam" and explained that they "gave her advice about falling for scams like this" (P139). Another participant expressed helplessness in the aftermath of an incident, they "felt annoyed that [their] mother's account was hacked and it felt like we couldn't do much after the fact" P(191).

Trust and mistrust in technological systems also surfaced as conversational topics, revealing how emotional responses shaped participants' interpretations of digital risks. One participant described asking a friend about website cookies because they "feel like I am giving websites access to use my personal information by accepting them" (P65). Another expressed broader skepticism, remarking that "..you can never trust even the big tech companies themselves" (P29).

In a few instances, misconceptions about security practices also surfaced within these exchanges. For example, one participant described discussing recently introduced two-factor authentication at their university, noting that "everyone else found it annoying too" and that "no one saw the point of it, as there is no particularly sensitive data on university accounts" (P47). Similarly, another conversation led participants to conclude that "probably nobody cares about either one of us [our] data or texts or whatever" (P235), illustrating how social dynamics can normalize inaccurate assumptions about risk. Together, these accounts highlight how cybersecurity awareness is jointly constructed through emotional investment, interpersonal relationships, and shared attempts to make sense of digital uncertainty.

4.3.4 Conversations as Drivers of Behavior Change. Although 38% of participants reported behavioral change, their accounts reveal valuable insights into how conversations can effectively motivate more secure practices. Many reported strengthening their personal security routines in direct response to discussions, such as updating passwords, enabling stronger authentication, or avoiding risky online behavior. In one case, after a participant told their sister about losing a notebook that contained important customer-related information, the sister subsequently "made sure to change her passwords every 6 months to ensure data security" (P90). Others reflected on shifts in their own habits: "I am much more careful now on email" (P99). Notably, these changes were not limited to individuals but influenced collective practices within organizations and households. For example, one participant explained that "we updated our security on our platform to avoid potential attacks" (P195). While another described a workplace discussion in which "my manager and I discussed this and concluded that we could not share any details with them" P(194), signaling a shift towards more cautious information handling.

Participants also described adopting new tools based on recommendations exchanged during these conversations, such as password managers, VPNs, or antivirus solutions. One participant, for example, reflected on a conversation about VPNs at work: "we talked about VPN usage in the workplace, and how it protects us. I was recommending a new VPN to my colleague...afterwards my colleague was satisfied with using the VPN" P(209). To sum up, these accounts show how everyday conversations can produce concrete and sustained behavioral changes, such as regularly updating login credentials, monitoring accounts, and adopting tools that support safer digital practices.

Key Qualitative Takeaways. Participants described cybersecurity conversations as situated exchanges that frequently begin with a concrete incident or media story prompt. Such incidents often generated emotions such as worry, fear, or frustration, which in turn prompted people to seek reassurance or advice from family,

friends, or colleagues. These accounts suggest that moments of heightened vulnerability can create openings for discussing cybersecurity issues, particularly when risks feel immediate or personally relevant.

Our analysis indicates that informal conversations serve an important socio-technical role, with many functioning as brief exchanges of guidance or clarification embedded within everyday talk. Through these interactions, participants learned about protective behaviors, tools, and recovery strategies in ways that complemented formal training. These conversations were also deeply relational, driven by feelings of care, responsibility, and trust, highlighting that cybersecurity awareness is not only technical but also emotional and socially negotiated.

5 Discussion

Our findings show that everyday cybersecurity conversations are not merely isolated discussions about specific incidents, but they are situated within broader social interactions embedded in daily routines, shaped by emotions, relationships, and practical concerns. Participants often approached security tasks collaboratively, suggesting that informal talk can act as a subtle form of situated support that influences how people understand and manage security in practice. Below, we highlight the key findings and their implications.

First, conversations emerged naturally from ordinary situations. In line with **RQ1: Contexts of Cybersecurity Conversations**, participants described discussions happening in kitchens, offices, and living rooms, typically prompted by small disruptions, e.g., a suspicious email, an unexpected notification, a browser warning. These moments served as micro-training sessions, enabling people to examine digital threats together. Unlike formal training, which is structured and abstracted from everyday life, these interactions were spontaneous, interpersonal, and grounded in existing concerns. This situational embeddedness broadens traditional views of security learning by demonstrating that understanding and action develop through lived experience, rather than solely through planned instruction.

This embeddedness also aligns with prior work showing that security practices are integrated in daily life rather than occurring in isolation [3, 41, 44]. Consistent with Watson et al. [41], we found that conversations frequently took place within small social groups, especially among family members and close friends. However, our findings diverge from the assumption that such conversations are rare, exceptional, or primarily reactive in nature. Watson et al. [41] noted that household discussions tended to be infrequent and often triggered by major news events. In contrast, participants in our study described conversations arising from routine, low-stakes cues, suggesting that opportunities are far more common and distributed across daily routines than previously recognized. Our results thus extend prior work by showing that conversations are not solely responses to high-profile incidents or institutional pressures but also emerge from personal, everyday triggers that prompt users to seek guidance or share concerns. Furthermore, while earlier research emphasized organizational influences on security talk [21, 28], our findings demonstrate that similar dynamics unfold in non-organizational and social contexts.

Regarding **RQ2: Topics of Cybersecurity Conversations**, participants focused on personally relevant topics such as phishing and passwords, consistent with prior findings that everyday security learning is driven by concrete examples rather than abstract concepts [12, 34, 40]. Rader et al. [34] and Wash [40] have demonstrated that narratives substantially influence users' mental models; our findings support this pattern, showing that participants frequently used stories – either personal or second-hand. At the same time, participants sometimes circulated incomplete or incorrect understandings, such as misconceptions about the "lack of necessity" for two-factor authentication or low perceived risk of data sharing. These findings are consistent with prior work on "*folk models*" [40], but our study also shows how these models are collectively shaped in conversation rather than solely held individually. This suggests a more socially distributed process of model formation, extending existing research that primarily examines *folk models* at the individual level. Additionally, this finding implies that informal talk might act as a double-edged sword: it spreads useful heuristics, but it can also reinforce misleading or incomplete models of cybersecurity. Moreover, while prior work emphasizes the role of large-scale incidents in shaping awareness [15, 31, 34], our participants frequently discussed subtler, less dramatic triggers (e.g., unfamiliar security settings). This suggests that the range of topics that spark security conversations may be broader and simpler than reported by previous work.

Participants described emotions, including curiosity, anxiety, frustration, and protectiveness. This dimension addresses **RQ3: The Social and Emotional Dynamics of Cybersecurity** and aligns with recent work highlighting the role of affect in cybersecurity attitudes [39] and the importance of social support for navigating online threats [11]. Our findings reinforce that security conversations are rarely neutral; they are shaped by interpersonal trust, relational expectations, and individuals' perceptions of their own and others' vulnerability. Our findings extend prior research in demonstrating how emotions interact with relational roles. While earlier work notes that users may hesitate to offer unsolicited advice out of fear of seeming intrusive [12], our participants described a broader spectrum of relational tensions: fear about family members who might fall for scams or pride in those who successfully avoided them.

Our results emphasize that social roles influence both the tone and outcomes of conversations. Authority figures often limited dialogue to compliance, whereas peer exchanges and family guidance facilitated exploration, negotiation, and learning. This finding resonates with Das et al.'s work on social triggers for behavior change [11], but our analysis highlights more nuanced relational dynamics, such as generational gaps or partner negotiation, that shape how advice is received and acted upon. Our insights also align with recent work by Preuschen et al. [39], which demonstrated that emotional states play a central role in how individuals engage with cybersecurity guidance.

The relational configurations in our study reveal a stronger sense of obligation toward close others – especially partners, siblings, and friends. These dynamics shaped not only whether advice was shared but also how guidance, reassurance, or negotiation unfolded. An important implication is that trust and relational positioning can either amplify or dampen the effectiveness of security talk. For

example, the same advice may be ignored if framed as top-down instruction but embraced if offered by a trusted peer. This suggests that designing for social learning in security must account not only for the *content* of advice but also for the *relationship* through which it is delivered.

RQ4: Follow-up Actions of Cybersecurity Conversations have been explored by Das et al. [11, 12], and our results both echo and extend their findings. Participants described adopting more secure practices, such as enabling two-factor authentication, updating passwords, or adopting new security tools, following discussions with trusted peers or family members. These examples are consistent with research showing that peer recommendations can provide both motivation and actionable guidance. However, our findings also show that not all conversations lead to concrete behavior change. Many interactions served other important functions: offering emotional reassurance, reducing uncertainty, or helping people interpret ambiguous events. This diverges somewhat from prior studies that tend to emphasize measurable behavioral outcomes. Our findings suggest that conversations can also stabilize existing practices, reduce anxiety, or help individuals feel more in control – effects that are less visible in conventional security metrics but may nonetheless be consequential for long-term security engagement. One interesting finding is that a small number of conversations reinforced misconceptions or even discouraged security behaviors, challenging the assumption that all social interactions are beneficial. Our findings highlight that conversations shape security behavior not only through direct influence but through subtler processes of emotional regulation, reassurance, and shared risk assessment.

5.1 Implications for Human-Centered Security

Our findings point toward four central implications for the design of awareness and education strategies in human-centered security. Together, they suggest that informal conversations represent an underutilized but powerful vector for strengthening secure practices.

(1) Designing for Situational Awareness. By identifying when and where security conversations naturally occur, our study provides a situational map of everyday security talk. We observed that conversations are most often embedded in routine domestic and professional contexts, frequently prompted by personal incidents. This suggests that awareness efforts could be more effective if they are situated within people's daily environments rather than delivered exclusively through formal channels. For instance, security prompts in household devices or workplace tools could be designed not only to guide individual action, but also to seed conversations within small groups, encouraging collaborative sensemaking and peer validation.

This observation aligns with prior work about *Cybersecurity Guardians* [27], which showed that security advice and support often circulate through trusted community relationships, particularly among older adults. Our findings extend this understanding to a broader, cross-generational audience, emphasizing that everyday domestic and workplace settings remain important sites of informal peer learning. Similarly, the *Cyber Advocates framework* [18] highlights how certain individuals act as informal ambassadors of security knowledge – a pattern echoed in our participants who assumed advisory roles among colleagues, partners, and family members. Recognizing and supporting these informal advocates could help amplify the reach of awareness interventions within existing social networks.

> **Implication 1: Situational Embedding** Awareness efforts should be embedded into routine domestic and workplace contexts to activate and sustain naturally occurring cybersecurity conversations.

(2) Supporting Triggers and Topics through the Conversation Lifecycle. We derive a conversation lifecycle (see Figure 10) of everyday security conversations, highlighting common contexts, social settings, and triggers. This model offers a structured lens for understanding how discussions begin (e.g., through incidents or media exposure), what they center on (e.g., phishing, privacy, AI concerns), and how they are embedded in relationships (e.g., family guidance, peer negotiation, authority reminders). Such a lifecycle can guide future interventions by identifying which triggers are most likely to spark meaningful dialogue and which topics are currently under-discussed.

Our analysis reveals that cybersecurity conversations typically unfold across five interrelated stages. First, they emerge within familiar contexts, most often at home, at work, or within academic environments, where social trust enables open exchange. Second, they are set in motion by specific triggers, most frequently personal experiences (51%) or exposure to news and social-media content (27%), which transform abstract risks into personally relevant concerns. Third, participants focus on recurring topics such as incidents, phishing, or password management, while emerging domains like AI systems or device personalization are mentioned less often. Fourth, the conversations evolve through distinct social dynamics: family members teach and reassure one another, peers validate or negotiate advice, and workplace hierarchies can constrain what is shared. Finally, they produce diverse outcomes – from heightened awareness and small behavior changes to lingering uncertainty or misconceptions.

Viewing these stages together as a lifecycle provides a practical map for designing awareness interventions. Triggers such as personal incidents or media stories could be intentionally leveraged to initiate reflection at opportune moments, while interventions might support the transition from curiosity to confident action through timely feedback or social reinforcement. Identifying underrepresented topics, for example, AI-related privacy or data-sharing practices, points to concrete gaps where educational materials or public campaigns could introduce new conversation prompts. In HCI and usable-security design, this perspective underscores the potential of everyday talk as a continuous and social mechanism that accounts for both situational and emotional dimensions.

> **Implication 2: Leveraging the Lifecycle** Awareness strategies should use natural triggers and under-discussed topics to introduce timely prompts that initiate and deepen meaningful security dialogue.

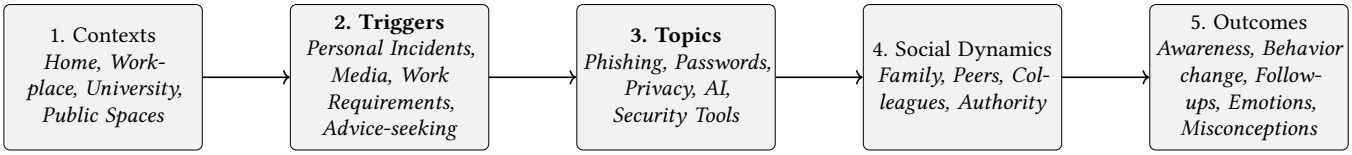


Figure 10: Conversation lifecycle of everyday cybersecurity talk: Conversations arise in specific *contexts*, are initiated by particular *triggers*, center on recurring *topics*, unfold within distinct *social dynamics*, and lead to a range of *outcomes*.

(3) Fostering Sustained Dialogue. Although many conversations were experienced as constructive, less than a half resulted in behavioral change or follow-up discussions. This indicates that informal exchanges alone may not guarantee long-term impact. Human-centered security research could therefore focus on mechanisms that bridge the gap between conversation and action. Systems might provide lightweight follow-up prompts (e.g., reminders to review settings after an incident) or resources that help individuals return to a topic with their peers. Interfaces that enable reflection, continuity, and onward diffusion of advice may help transform short-lived exchanges into sustained practices, fostering a culture of collective vigilance rather than one-off reactions.

Our findings also showed that confidence was strongly correlated with willingness to advise others, suggesting that emotional assurance rather than fear may be the key to sustaining dialogue. Designing interventions that cultivate this confidence – for instance, by providing positive feedback when users discuss or share cybersecurity advice could strengthen the long-term social diffusion of secure practices.

> **Implication 3: Sustaining Dialogue** Awareness initiatives should incorporate light follow-ups and confidence-building elements that help informal conversations develop into ongoing security practices.

(4) Capturing Implicit and Informal Security Talk. Because our study relies on participants' retrospective accounts, it captures only conversations that were memorable or consciously reflected upon. This methodological constraint means that we primarily observe explicit forms of cybersecurity learning, i.e., those moments that participants can describe, explain, and situate in a narrative. Yet everyday social interaction often involves more implicit forms of communication that do not register as "conversations" when recalled later. Much of everyday security talk likely unfolds through brief remarks, shared observations, or subtle cues that are easily forgotten but may still influence how people notice risks or decide to act. These micro-interactions can reinforce norms, prompt small adjustments, or signal concern, even if participants do not remember them as security-related episodes. Thus, relying solely on recall may obscure an important layer of social influence that helps shape behavior over time.

In design terms, interventions should aim not only to support explicit discussions but also to scaffold subtle social cues – for instance, by providing visual feedback on shared device security actions or by surfacing socially legible indicators when shared settings change, in line with the principle of *social translucence* [16]. By attending to these implicit layers of communication, security interventions can align more closely with the natural rhythms of everyday talk instead of interrupting them.

> **Implication 4: Designing for Subtle Social Cues** Awareness approaches should account for subtle, often unspoken interactions through which people share cybersecurity knowledge – for example, by providing contextual reminders, shared feedback, or socially legible cues that can trigger brief, informal exchanges.

5.2 Opportunities and Challenges

Our study highlights both opportunities and challenges in leveraging everyday conversations for cybersecurity. On the opportunity side, informal talk reaches into private and professional domains often untouched by formal training, diffuses best practices across households and peer groups, and creates openings for collaborative problem-solving. These micro-level exchanges illustrate how awareness can emerge organically within trusted networks, suggesting that interventions should strengthen – rather than replace – these grassroots mechanisms. The emotional richness of these exchanges, ranging from anxiety to curiosity to responsibility, suggests that conversations are not only cognitive but also motivational, providing a potential lever for engagement. Future awareness strategies could draw on these emotions – for instance, transforming anxiety into reassurance or curiosity into proactive protection – by offering timely validation or low-effort opportunities for joint action.

At the same time, everyday security conversations present clear challenges. They are unevenly distributed, shaped by trust and authority, and occasionally propagate misconceptions or incomplete advice. Relational hierarchies, especially in workplace settings, may inhibit open exchange or reinforce compliance over understanding. Moreover, because participants reported memorable rather than routine interactions, our findings may not fully capture subtle or implicit forms of influence, underscoring the need for methods that observe conversational dynamics as they unfold. Addressing these challenges requires interventions that amplify constructive dynamics while mitigating risks. For instance, systems could support peer-to-peer explanations with accurate resources or context-sensitive guidance, reducing the spread of misinformation. More broadly, empowering users who possess accurate knowledge with the confidence and language to communicate it – while providing mechanisms to validate or cross-check advice – may help transform fleeting exchanges into ongoing collective learning.

Interpreting our findings requires attention to the nature of the data: participants described a cybersecurity conversation they could recall, which offers insight into interactions perceived as meaningful or confusing but does not capture the full spectrum of routine or

implicit exchanges. By asking whether the conversation influenced behavior, prompted reflection, evoked emotions, or led to anticipated follow-ups, our survey shows how individuals assess the relevance of such interactions for their own practices. The focus on remembered conversations thus reveals not only what users retain but also what fails to register as actionable, pointing to areas where security topics may need stronger cues or support. Given the lack of unobtrusive methods to capture everyday cybersecurity conversations as they naturally occur, retrospective accounts remain a practical and ecologically grounded approach. The patterns in what people report – and omit – offer important directions for future interventions aiming to support more frequent, accurate, and confidence-building security dialogue.

Although many participants reported positive emotions and confidence when discussing cybersecurity, this does not imply a sample dominated by experts. Only 22% of the analytic sample worked in IT-related fields, and most disagreed with the statement *I often give cybersecurity advice to others*. The combination of moderate confidence with limited formal expertise suggests that people feel comfortable engaging in security talk even without professional knowledge – and that their interpretations of such interactions provide a valuable window into how security topics surface in everyday life.

The contexts in which conversations occurred again reveal both opportunities and challenges. A substantial share of conversations took place at home (42%) and at work (34%), indicating that cybersecurity talk spans both personal and professional spheres and can be supported at multiple everyday touchpoints. At the same time, contextual variability complicates the creation of universal support strategies: conversations triggered at home among friends or family may require different forms of guidance than those arising within workplace interactions.

Summary. Our study shows that informal conversations are not peripheral to cybersecurity but central to how individuals perceive, interpret, and sometimes act upon digital risks. By documenting their situational characteristics, common triggers, relational dynamics, and occasional misconceptions, we derive a lifecycle of everyday security conversations and identify implications for strengthening cybersecurity awareness in everyday life. For HCI, this means reimagining security not only as a matter of individual decision-making but as an ongoing, socially embedded process that technologies can support, scaffold, and amplify.

5.3 Future Work

Our study opens several avenues for future research. First, combining retrospective surveys with in-situ or longitudinal approaches, could enable the capture of both salient and more subliminal conversational dynamics. This could help observe how conversations evolve over time, offering insights into the persistence of informal security knowledge sharing beyond single encounters. Second, focusing the sample by restricting the participant pool to a specific subgroup – such as cybersecurity experts or non-expert users, or those within (non-)organizational settings – may provide a clearer understanding of whether and how conversational patterns differ under more uniform conditions. Third, future research could further explore cross-cultural variations in cybersecurity conversations. Comparative studies across regions with different social norms, media landscapes, and regulatory frameworks could help identify how cultural context shapes when, where, and with whom people discuss security topics. Finally, building on our insights, future work could explore intervention design, particularly the development of practical strategies that encourage constructive security talk, especially among non-expert users.

6 Conclusion

In this paper, we investigated everyday conversations about cybersecurity through an online survey of 215 participants. By combining quantitative and qualitative analysis, we documented when, where, and with whom such discussions occur, what typically prompts them, and how participants describe their emotional responses and behavioral outcomes. Our analysis produced a conversation lifecycle that maps how security talk unfolds, from its context and triggers, through the topics and social dynamics it involves, to the outcomes it produces. A key insight is that many conversations emerged spontaneously in private settings, often triggered by personal experiences, and were emotionally rich, ranging from curiosity and confidence to anxiety and frustration. While some exchanges fostered increased awareness or concrete practice changes, others primarily served as reassurance or collaborative sensemaking. Importantly, we also observed a small number of conversations in which misconceptions or misleading advice were shared. While these cases were rare, it is worth noting that everyday talk does not always lead to accurate or constructive outcomes and may occasionally reinforce incomplete mental models of security. Taken together, this paper underscores that cybersecurity is not only a technical or individual challenge but also a socially embedded process shaped by emotions, relationships, and routine interactions. Rather than treating everyday conversations as peripheral, our results show that they are key moments in which security norms are negotiated, reinforced, or questioned. For HCI and human-centered security, this perspective suggests opportunities to strengthen awareness by supporting constructive dialogue, providing clear reference points that counter misconceptions, and acknowledging the relational contexts in which people discuss digital risks. More broadly, recognizing the role of everyday talk can help foster a more resilient security culture, one that grows not only through formal instruction but also through the informal exchanges that shape how people understand and navigate digital threats.

Acknowledgments

This research is part of the *Voice of Wisdom* project and received funding from dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

Acknowledgment of AI Use. GPT-5 was used to paraphrase, reword and shorten text, improve writing style, and perform grammar and spelling checks to improve the overall text quality.

References

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. doi:10.1145/322796.322806

[2] Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro. 2024. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications* 2 (2024), 100031. doi:10.1016/j.csa.2023.100031

[3] Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, Sumanth Kunisetty, Yaxing Yao, and Nikita Soni. 2024. Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces. 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 983, 12 pages. doi:10.1145/3613904.3641962

[4] Rawan A. Alsharida, Bander Ali Saleh Al-rimy, Mostafa Al-Emran, and Anazida Zainal. 2023. A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society* 73 (2023), 102258. doi:10.1016/j.techsoc.2023.102258

[5] Eytan Bakshy, Itamar Rosenn, Cameron Marlow, and Lada Adamic. 2012. The role of social networks in information diffusion. In *Proceedings of the 21st International Conference on World Wide Web* (Lyon, France) *(WWW '12)*. Association for Computing Machinery, New York, NY, USA, 519–528. doi:10.1145/2187836.2187907

[6] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative Hci Research: Going Behind the Scenes*. Morgan & Claypool Publishers.

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. doi:10.1191/1478088706qp063oa arXiv:https://doi.org/10.1191/1478088706qp063oa

[8] L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and society magazine* 28, 3 (2009), 37–46. doi:10.1109/MTS.2009.934142

[9] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. 2014. Defining cybersecurity. *Technology Innovation Management Review* 4, 10 (2014), 13–21. doi:10.22215/timreview/835

[10] Lorrie Faith Cranor. 2008. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (San Francisco, California) *(UPSEC'08)*. USENIX Association, USA, Article 1, 15 pages. https://www.usenix.org/legacy/events/upsec08/tech/full_papers/cranor/cranor.pdf

[11] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 97–115. https://www.usenix.org/conference/soups2019/presentation/das

[12] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The effect of social influence on security sensitivity. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (Menlo Park, CA) *(SOUPS '14)*. USENIX Association, USA, 143–157. https://www.usenix.org/conference/soups2014/proceedings/presentation/das

[13] Nigel Davies, Sarah Clinch, and Florian Alt. 2014. *Pervasive Displays: Understanding the Future of Digital Signage* (1st ed.). Morgan & Claypool Publishers. doi:10.2200/S00558ED1V01Y201312MPC011

[14] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1065–1074. doi:10.1145/1357054.1357219

[15] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 4254–4265. doi:10.1145/3025453.3025636

[16] Thomas Erickson and Wendy A. Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM Trans. Comput.-Hum. Interact.* 7, 1 (March 2000), 59–83. doi:10.1145/344949.345004

[17] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2893–2902. doi:10.1145/2702123.2702442

[18] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 411–425. https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

[19] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (Oxford, United Kingdom) *(NSPW '09)*. Association for Computing Machinery, New York, NY, USA, 133–144. doi:10.1145/1719030.1719050

[20] Wilson Cheong Hin Hong, ChunYang Chi, Jia Liu, YunFeng Zhang, Vivian Ngan-Lin Lei, and XiaoShu Xu. 2022. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies* 28, 1 (June 2022), 439–470. doi:10.1007/s10639-022-11121-5

[21] Eve Jenkins, Dinislam Abdulgalimov, Pamela Briggs, Patrick Olivier, and James Nicholson. 2025. Using Anonymous Discussion Platforms to Support Open Conversations about Cybersecurity in Organisations. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 924, 14 pages. doi:10.1145/3706598.3713290

[22] 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

[23] Kalam Khadka and Abu Barkat Ullah. 2025. Human factors in cybersecurity: an interdisciplinary review and framework proposal: Human factors in cybersecurity: an interdisciplinary review and framework proposal. *Int. J. Inf. Secur.* 24, 3 (April 2025), 13 pages. doi:10.1007/s10207-025-01032-0

[24] Samreen Mahmood, Mehmood Chadhar, and Selena Firmin. 2024. Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Applied Sciences* 14, 24 (2024). doi:10.3390/app142411610

[25] Benjamin S. Meyers, Nuthan Munaiah, Andrew Meneely, and Emily Prud'hommeaux. 2019. Pragmatic characteristics of security conversations: an exploratory linguistic analysis. In *Proceedings of the 12th International Workshop on Cooperative and Human Aspects of Software Engineering* (Montreal, Quebec, Canada) *(CHASE '19)*. IEEE Press, 79–82. doi:10.1109/CHASE.2019.00026

[26] Eyitemi Moju-Igbene, Hanan Abdi, Alan Lu, and Sauvik Das. 2022. "How Do You Not Lose Friends?": Synthesizing a Design Space of Social Controls for Securing Shared Digital Resources Via Participatory Design Jams. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 881–898. https://www.usenix.org/conference/usenixsecurity22/presentation/moju-igbene

[27] 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

[28] Simon Parkin, Simon Arnell, and Jeremy Ward. 2022. Change that Respects Business Expertise: Stories as Prompts for a Conversation about Organisation Security. In *Proceedings of the 2021 New Security Paradigms Workshop* (Virtual Event, USA) *(NSPW '21)*. Association for Computing Machinery, New York, NY, USA, 28–42. doi:10.1145/3498891.3498895

[29] Peter Peltonen, Esko Kurvinen, Antti Salovaara, Giulio Jacucci, Tommi Ilmonen, John Evans, Antti Oulasvirta, and Petri Saarikko. 2008. It's Mine, Don't Touch! interactions at a large multi-touch display in a city centre. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1285–1294. doi:10.1145/1357054.1357255

[30] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. 2022. Replication: stories as informal lessons about security. In *Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security* (Boston, MA, USA) *(SOUPS'22)*. USENIX Association, USA, Article 1, 18 pages. doi:10.5555/3563609.3563610

[31] Sarah Prange, Lukas Mecke, Michael Stadler, Maximilian Balluff, Mohamed Khamis, and Florian Alt. 2019. Securing personal items in public space: stories of attacks and threats. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (Pisa, Italy) *(MUM '19)*. Association for Computing Machinery, New York, NY, USA, Article 27, 8 pages. doi:10.1145/3365610.3365628

[32] Sarah Prange, Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. 2022. "I saw your partner naked": Exploring Privacy Challenges During Video-based Online Meetings. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 71–82. doi:10.1145/3568444.3568468

[33] Farzana Quayyum. 2025. Co-designing cybersecurity-related stories with children: Perceptions on cybersecurity risks and parental involvement. *Entertainment Computing* 52 (2025), 100753. doi:10.1016/j.entcom.2024.100753

[34] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 6, 17 pages. doi:10.1145/2335356.2335364

[35] Elissa M. Redmiles. 2019. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. 920–934. doi:10.1109/SP.2019.00059

[36] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 666–677. doi:10.1145/2976749.2978307

[37] Qiurong Song, Renkai Ma, Yubo Kou, and Xinning Gui. 2024. Collective Privacy Sensemaking on Social Media about Period and Fertility Tracking post Roe v. Wade. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 161 (April 2024), 35 pages. doi:10.1145/3641000

[38] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying wolf: an empirical study of SSL warning effectiveness. In *Proceedings of the 18th Conference on USENIX Security Symposium* (Montreal, Canada) *(SSYM'09)*. USENIX Association, USA, 399–416. doi:10.5555/1855768.1855793

[39] Alexandra von Preuschen, Carolin Benda, Monika Christine Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 1091, 24 pages. doi:10.1145/3706598.3713538

[40] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. doi:10.1145/1837110.1837125

[41] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. 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, 1–12. doi:10.1145/3313831.3376605

[42] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Franziska Roesner, and Kurt Thomas. 2023. "There's so much responsibility on users right now:" Expert Advice for Staying Safer From Hate and Harassment. 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 190, 17 pages. doi:10.1145/3544548.3581229

[43] Maximiliane Windl, Verena Winterhalter, Albrecht Schmidt, and Sven Mayer. 2023. Understanding and Mitigating Technology-Facilitated Privacy Violations in the Physical World. 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 585, 16 pages. doi:10.1145/3544548.3580909

[44] Yuxi Wu, W. Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*. 1863–1879. doi:10.1109/SP46214.2022.9833757

[45] Leah Zhang-Kennedy, Michaela Valiquette, An Bella Chen, Hilda Hadan, and Sangho Suh. 2025. Folk Tales of IoT: Understanding the Impact of Stories on Users' Positive and Negative Perceptions of Smart Home IoT Devices. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 941, 18 pages. doi:10.1145/3706598.3713712

A Survey

1. **Do you remember having a conversation about any cybersecurity topic?**
   Examples of cybersecurity topics may include discussions about the Bundestag hack, a ransomware attack on a municipality or university, how to choose a secure password, whether or not to start using a password manager, and more.
   ○ Yes (1)
   ○ No (2)
   ○ I do not know (3)
   Skip to: Demographics; if Q1 ≠ Yes
2. **Please describe, in as much detail as possible, the last time you talked about cybersecurity.**
   Consider:
   - Who was involved?
   - Where did the conversation take place?
   - What did you talk about?
   - What triggered the conversation?
   - How long did it last?
   - Anything else you remember?

   _____
   _____
   _____
   _____
3. **How many people were involved, apart from you?**
   _____
4. **What was your relationship to the person/people you talked to? (Check all that apply)**
   □ Friend (1)
   □ Colleague (2)
   □ Acquaintance (3)
   □ Stranger (4)
   □ Other (please specify) (5) _____
5. **Who started the conversation?**
   ○ Myself (1)
   ○ Other (2)
   ○ I do not know (3)
6. **Did anybody else join the conversation after you started?**
   ○ Yes, somebody I know (1)
   ○ Yes, a stranger (2)
   ○ No (3)
   ○ I don't know (4)
7. **Where did this conversation happen?**
   ○ At home (1)
   ○ Workplace/University (2)
   ○ Public space (e.g., café, train) (3)
   ○ Other (please specify) (4) _____
8. **What led to the topic of cybersecurity coming up? (Check all that apply)**
   □ Personal experience (e.g., cybersecurity incident) (1)
   □ News story or social media post (2)
   □ Work/school-related requirement (3)
   □ Someone asked for advice (4)
   □ Other (please specify) (5) _____
9. **What specific cybersecurity issue(s) did you discuss? (Check all that apply)**
   □ Application areas (web browsing, smartphone, social media etc.) (1)
   □ Identity theft or fraud (2)
   □ Incidents (ransomware attack, data breach, leak, device theft etc.) (3)
   □ Phishing or scams (4)
   □ Privacy tools (permission manager, cookie banners etc.) (5)
   □ Security behavior (choice of passwords, updating software etc.) (6)
   □ Security tools (password managers, antivirus, VPN etc.) (7)
   □ Surveillance or data collection (government, companies etc.) (8)
   □ Other (please specify) (9) _____
10. **I felt confident talking about the topic.**

1 (Strongly disagree)	2	3	4	5 (Strongly agree)
○	○	○	○	○

11. **How did you feel during the conversation? (Check all that apply)**
    □ Interested/curious (1)
    □ Worried/anxious (2)
    □ Confident/informed (3)

- ☐ Annoyed (4)
- ☐ Helpful/responsible (5)
- ☐ Indifferent (6)
- ☐ Other (please describe) (7) _____

12. **Why did you feel this way during the conversation?**

_____
_____
_____
_____
_____

13. **How do you think the other person felt during the conversation? (Check all that apply)**
    - ☐ Interested/curious (1)
    - ☐ Worried/anxious (2)
    - ☐ Confident/informed (3)
    - ☐ Annoyed (4)
    - ☐ Helpful/responsible (5)
    - ☐ Indifferent (6)
    - ☐ Other (please describe) (7) _____
14. **Why do you think the other person felt this way during the conversation?**

_____
_____
_____
_____
_____

15. **Did this conversation lead to any changes (for you or others) regarding cybersecurity practices?**
    - ○ Yes (1)
    - ○ No (2)
    - ○ I do not know (3)

    Display if Q15 = Yes
16. **Describe the changes regarding cybersecurity practices.**

_____
_____
_____
_____
_____

17. **Did you have, or do you plan to have, a follow-up conversation regarding the situation you described?**
    - ○ Yes, I had (How many?) (1) _____
    - ○ No, but I plan to have one in the future (2)
    - ○ No, I do not plan to have one (3)
    - ○ I do not know (4)
18. **Would you like to describe another, different in-person conversation you had about a cybersecurity topic?**
    (This should be a separate conversation from the one you just described.)
    - ○ Yes, I'd like to describe another conversation (1)
    - ○ No (2)

    Skip to: Demographics; if Q18 = No
    Repeat Q2–Q18; if Q18 = Yes, I'd like to describe another conversation

Demographics

19. **What is your age?**

_____

20. **What is your gender?**
    - ○ Male (1)
    - ○ Female (2)
    - ○ Non-binary (3)
    - ○ Other (please specify) (4) _____
    - ○ Prefer not to answer (5)
21. **What is your country of residence?**

_____

22. **What is your occupation/field of study?**

_____

23. **I often give cybersecurity advice to others.**

1 (Strongly disagree)	2	3	4	5 (Strongly agree)
○	○	○	○	○

Honesty

24. **I have answered all questions honestly.**

1 (Strongly disagree)	2	3	4	5 (Strongly agree)
○	○	○	○	○

B Codebook

Category 1	Code	Frequency
advise		35
advise	antivirus software	2
advise	child to parent cybersecurity advise	3
advise	enablling 2FA for all important services	3
advise	how to choose/generate passwords	12
advise	how to setup up a new password manger	3
advise	parent to child cybersecurity advise	4
advise	receiving cybersecurity advice	1
advise	recommending post-attack steps	3
advise	risks of public wi-fi - VPN recommended	2
advise	sharing anti-phishing/anti-scam tips	3

Category 2	Code	Frequency
behaviour change		79
behaviour change	adopting 2FA/MFA	5
behaviour change	better protection of personal data	11
behaviour change	changing password practices	22
behaviour change	changing phishing-related practices	10
behaviour change	did not shop online after the attack	1
behaviour change	do not trust anyone at first - ask the attacker a "security question" for verification	3
behaviour change	enhanced security literacy	3
behaviour change	inform the company about the issue	1
behaviour change	more awareness at work	9
behaviour change	no longer worrying about it	1
behaviour change	pay close attention to potential deep fakes	1
behaviour change	person pays more attention to info they reveal in chats	2
behaviour change	proactive device protection	5
behaviour change	raised awareness	6
behaviour change	use more strict security checks	9

Category 3	Code	Frequency
feeling other		216
feeling other	annoyed - because they were feeling vulnerable and scared	2
feeling other	annoyed - by the situation	9
feeling other	annoyed - data is being used without consent	1
feeling other	annoyed - due to actions of others	3
feeling other	annoyed - measures associated with loss of comfort	4
feeling other	annoyed – due to perceived indifference of others	1
feeling other	ashamed - because they had caused a problem by falling for phishing	1
feeling other	concerned - as they were personally affected by the email hack	2
feeling other	concerned - lost of trust due to attacks	1
feeling other	confident/informed - how data is processed in such situations	1
feeling other	confident/informed - is always able to help with anything they ask on the topic	1
feeling other	confident/informed - knew it was a phishing email	3
feeling other	confident/informed - knew what to do after the conversation	7
feeling other	confident/informed - more info and increased self-efficacy	21
feeling other	confident/informed - other colleagues had no questions indicating they are confident with the topic	2
feeling other	confident/informed - overconfidence (acting as a know-it-all)	2
feeling other	confident/informed - they have prior experience with the topic	11
feeling other	excited - about new tools	1
feeling other	helpful/responsible - always wanted to help with situations	2
feeling other	helpful/responsible - because they were leading on fixing the problem	2
feeling other	helpful/responsible - gave advise about secure measures	8
feeling other	helpful/responsible - had knowledge on the topic so they steered the conversation	2
feeling other	indifferent - confirmed restricted access to some websites and services on company internet	1
feeling other	indifferent - does not use online services	1
feeling other	indifferent - initially did not see a problem clicking on links	1
feeling other	indifferent - problems sought in others (poor self-awareness)	2
feeling other	indifferent - they do not care about security	5
feeling other	indifferent - topic not interesting	2
feeling other	insecure - why the other person felt that way	1
feeling other	interested/curious - about how the company will react to the flaw	2
feeling other	interested/curious - concerned after being a victim of the cyber incident, in order to be able to prevent it next times	1
feeling other	interested/curious - engaged to find solutions	9
feeling other	interested/curious - experienced in the field	6
feeling other	interested/curious - has area knowledge	6
feeling other	interested/curious - interested in the topic	23
feeling other	interested/curious - learned from the conversation	8
feeling other	interested/curious - less knowledgeable on tech	8
feeling other	interested/curious - more attention to problem	8
feeling other	interested/curious - not ready to protect country from cyber attacks	1
feeling other	interested/curious - some people believe that if you use a smartphone you have to agree that your data will be used	2
feeling other	lazy - to explain best practices to older people	1
feeling other	proud - of having acted securely	1
feeling other	surprised - about not doing what the majority does	1
feeling other	worried/anxious - about companies snooping on users	4
feeling other	worried/anxious - about impacts of M&S breach	1
feeling other	worried/anxious - as head of security worried that new employees might not take the security issues seriously enough	1
feeling other	worried/anxious - concern about own accounts	3
feeling other	worried/anxious - due to lack of knowledge	11
feeling other	worried/anxious - electricity shutdown that lasted a day made them feel anxious	1
feeling other	worried/anxious - failed to detect the phishing email	11
feeling other	worried/anxious - future effects on society	5
feeling other	worried/anxious - hard to assess data security	9
feeling other	worried/anxious - learnt new ways to get exposed	1
feeling other	worried/anxious - paranoid as a personality trait	4
feeling other	worried/anxious - personally affected	5
feeling other	worried/anxious - sharing credit card details	1
feeling other	worried/anxious - that they need to change their passwords	1
feeling other	worried/anxious – financial loss	4
feeling other	worried/anxious – personally affected	6

Category 4	Code	Frequency
feeling self		233
feeling self	annoyed - bad situation	3
feeling self	annoyed - because they feel exploited	1
feeling self	annoyed - by scams	1
feeling self	annoyed - data is being used without consent	1
feeling self	annoyed - due to perceived indifference of others	8
feeling self	annoyed - due to workload & time constraints	5
feeling self	annoyed - homeless person was being pushy	1
feeling self	annoyed - poor security behaviour	3
feeling self	annoyed - that access to services was restricted on company internet	1
feeling self	annoyed - that other person's account got hacked	1
feeling self	concerned - about family member being a victim	2
feeling self	concerned - about how well the AI was able to interpret all the information into an overall picture about themselves	1
feeling self	concerned - about own data	3
feeling self	concerned - can Microsoft be trusted	0
feeling self	concerned - having the same hardware as the person who was hacked	1
feeling self	confident/informed - confident in others ability ot guide them	1
feeling self	confident/informed - knowledgeable on the topic	32
feeling self	confident/informed - previous experience	15
feeling self	confident/informed - self-confidence	9
feeling self	confident/informed - think ahead and plan responsibly	3
feeling self	confident/informed - thought systems were more complex	1
feeling self	disappointed - because the other person had fallen for such a simple scam	1
feeling self	empathy - for affected person	1
feeling self	frustrated - topic of passwords is frustrating	1
feeling self	helpful/responsible - enjoys interacting with the topic	3
feeling self	helpful/responsible - help family and friends to stay secure	4
feeling self	helpful/responsible - knowledgeable about the topic	13
feeling self	helpful/responsible - significant improvements to company environment since incident	1
feeling self	helpful/responsible - spreading knowledge	9
feeling self	indifferent - personally not interested in cybersecurity	1
feeling self	indifferent - phishing is not a very interesting topic	1
feeling self	indifferent - was expecting to be briefed on cyber security on his first day of work	1
feeling self	indiffrent - knew it was a phishing email	1
feeling self	interested/curious - AI development unpredictable	4
feeling self	interested/curious - concerns about data privacy	2
feeling self	interested/curious - enjoys interacting with the topic	18
feeling self	interested/curious - finds it interesting to learn more about the topic	25
feeling self	interested/curious - had never heard of an incident like that so close by	1
feeling self	interested/curious - little knowledge of subject	8
feeling self	interested/curious - make a career in the field	2
feeling self	interested/curious - personally affected	7
feeling self	interested/curious - raised awareness of secure behaviour	5
feeling self	interested/curious - using new tools	4
feeling self	interested/curious - wants data to be safe	2
feeling self	interested/curious - was curious how people manage to steal a complex currency such as crpyto	1
feeling self	interested/curious - was wondering how the company is planning on tackling phishing	1
feeling self	interested/curious - worried about the incident but curious how it happened and how to prevent this in the future	6
feeling self	overwhelmed - cannot find a solution	1
feeling self	proud - of having acted securely	1
feeling self	socially obligated - to stay engaged	1
feeling self	worried/anxious - about how fragile user data is to data breaches	8
feeling self	worried/anxious - AI can pose threats if it "goes too far"	2
feeling self	worried/anxious - cyberattcks make us vulnerable as society	4
feeling self	worried/anxious - data security not always guaranteed	10
feeling self	worried/anxious - fear of future	10
feeling self	worried/anxious - financial loss	5
feeling self	worried/anxious - fraud in online shopping	2
feeling self	worried/anxious - got viruses on laptop in the past	1
feeling self	worried/anxious - how data is processed from big companies	2
feeling self	worried/anxious - long term effects of the issue	4
feeling self	worried/anxious - personally affected	7
feeling self	worried/anxious - relatives are victims of scam	7
feeling self	worried/anxious - sharing credit card details	1
feeling self	worried/anxious - that other person was not worried about phishing links in the beginning	1
feeling self	worried/anxious - trusts the expertise of the other person	2

Category 5	Code	Frequency
misconception		3
misconception	no one cares about our data	2
misconception	write down password until you know it by heart	1

Category 6	Code	Frequency
mistrust in big tech companies		7

Category 7	Code	Frequency
other		54
other	browser security	1
other	discussed last electricity shutdown in spain	1
other	discussed why Wordfence Plugin was disabled	1
other	effects of software updates in security systems	1
other	founding cybersecurity company	1
other	general cybersecurity topics	2
other	hacker attacks	7
other	low awareness on secure behaviour and its impact	7
other	low compliance with security guidelines	3
other	OS selection	1
other	potential ways to hack cars connected to the internet and the involved risk	1
other	security flaw in commercial services	4
other	social events on cybersecurity	0
other	social media vulnerability issues	4
other	someone plugged in private phone into computer to charge and the other person remarked that outside devices should not be plugged in	1
other	steps we take for cybersecurity as individuals handling security theme	6
other	talked about call centers and how they get your phone number through websites that sell your data	1
other	talked about how secure file sharing platforms like we transwer are	1
other	talked about how to protect the friend's bitcoin	1
other	talked about two factor authentication	1
other	talked about vpns and how they can be used to watch shows only available in other contries	1
other	talked about website to check if file had a virus or not	1
other	technical issues email not working	1
other	vulnerabilities of IT departments' infrastructure	4
other	were briefed about tail gaiting	1
other	were questioning why they have to use two-factor authentication to log into university account	1

Category 8	Code	Frequency
topic_AI		13
topic_AI	AI effects on society	5
topic_AI	AI using/generating crime	1
topic_AI	privacy concerns around AI	3
topic_AI	use of user data for training	3
topic_AI	using AI in schools	1

Category 9	Code	Frequency
topic_cyber attacks		18
topic_cyber attacks	are an ever evolving cycle since the defenses eget better and then there are better attacks and so on	1
topic_cyber attacks	bot spams that influence social media e.g. in Ukraine war	1
topic_cyber attacks	data breach threat - attackers breaking through company security	7
topic_cyber attacks	discussion on russian cyber attacks on polish websites	1
topic_cyber attacks	easily losing data	1
topic_cyber attacks	got hacked via Wi-Fi	1
topic_cyber attacks	how secure are institutions against cyber attacks	1
topic_cyber attacks	nation-state cyber operations	3
topic_cyber attacks	scams, phishing detection	1
topic_cyber attacks	talked about acquitance beeing scammed and how they had to be extrememly careful with cyber security	1

Category 10	Code	Frequency
topic_cybersecurity training at work		4
topic_cybersecurity training at work	data protection, identity theft, and password protection were discussed	1
topic_cybersecurity training at work	security issue at work	1
topic_cybersecurity training at work	talk about cyber security at company	1
topic_cybersecurity training at work	was briefed about triggers/causes of cyber security	1

Category 11	Code	Frequency
topic_cybersecurity career		9
topic_cybersecurity career	experience with appling to the UK Secret Intelligence Service	1
topic_cybersecurity career	having a career in cybersecurity	5
topic_cybersecurity career	obtained a cybersecurity certificate (from Coursera)	2
topic_cybersecurity career	told them about their job	1

Category 12	Code	Frequency
topic_data protection/privacy		28
topic_data protection/privacy	(not)allowing access to third parties	2
topic_data protection/privacy	company restricting access to services due to internal data protection regulation	3
topic_data protection/privacy	concern about providing credit card details	8
topic_data protection/privacy	declining cookies to avoid linking personal and work data	2
topic_data protection/privacy	difference between obfuscating and encrypting	1
topic_data protection/privacy	handling sensitive education data	0
topic_data protection/privacy	internet security	2
topic_data protection/privacy	targeted ads after speaking about a topic	2
topic_data protection/privacy	use and misuse of personal data	8

Category 13	Code	Frequency
topic_incidents_news stories		32
topic_incidents_news stories	biggest data leak in history	2
topic_incidents_news stories	company-related incidents/attacks	16
topic_incidents_news stories	country-related incidents/attacks	5
topic_incidents_news stories	influencer account being hacked	1
topic_incidents_news stories	many news about bank scams	1
topic_incidents_news stories	massive data breach	1
topic_incidents_news stories	memes of german politicians	1
topic_incidents_news stories	news about private person victim of a scam	2
topic_incidents_news stories	news article misplaced paperwork on a train	1
topic_incidents_news stories	talked about crypto investments were hacked	1
topic_incidents_news stories	university cyber attack	1

Category 14	Code	Frequency
topic_incidents_personally affected		35
topic_incidents_personally affected	"grandparent scam"	4
topic_incidents_personally affected	comprimised API keys used for sending scam emails	2
topic_incidents_personally affected	data breach attempt at the place of work (bank)	3
topic_incidents_personally affected	data leak - friend got an email he might be affected by a data breach at ticketmaster	1
topic_incidents_personally affected	fraud/theft	9
topic_incidents_personally affected	lost physical device - risk of data misuse	1
topic_incidents_personally affected	passwords and accounts	5
topic_incidents_personally affected	phishing experience	2
topic_incidents_personally affected	public sector incident, schools/universities being hacked	4
topic_incidents_personally affected	ransonware	1
topic_incidents_personally affected	talked to colleague about a cyber security incident they went through a couple of years ago and what was improved since	1
topic_incidents_personally affected	temporary unavailability of network and cloud services at work due to OneDrive vulnerability	0
topic_incidents_personally affected	unauthorized subscription of a service	1
topic_incidents_personally affected	wife found a webiste with a virus	1

Category 15	Code	Frequency
topic_measures		14
topic_measures	cybersecurity training	3
topic_measures	individual actions taken	6
topic_measures	placing more importance on passwords	3
topic_measures	proposed info event with IT department	2
topic_measures	regular cybersecurity update meetings	1

Category 16	Code	Frequency
topic_passwords		48
topic_passwords	difficulty logging in to different accounts	8
topic_passwords	how to manage passwords and keep accounts safe	13
topic_passwords	password security	17
topic_passwords	questioning the need for passwords on low-sensitivity accounts	2
topic_passwords	reusing passwords	6
topic_passwords	risks of weak passwords	5
topic_passwords	storing passwords	2
topic_passwords	talked to friend about passwords being more secure with more letter, numbers and special characters and to not write them down	1
topic_passwords	the need for using strong passwords to protect a smartphone	1
topic_passwords	website/app that generates unique OTP	1
topic_passwords	what passwords they use for their emails	11

Category 17	Code	Frequency
topic_phishing		43
topic_phishing	attack on London library	1
topic_phishing	be on the llokout when opening and sending mails	1
topic_phishing	detecting potential scam/phishing texts	16
topic_phishing	email hacked and used for phishing	3
topic_phishing	gaining access	2
topic_phishing	older family member (aunt) had asked if a mail was legit	1
topic_phishing	receiving suspicious email/text	13
topic_phishing	surprised how well the phishing email copied the usual supplier invoice	2
topic_phishing	talked about text message from scammer	1
topic_phishing	talked to other person to be more careful when clicking on links	1
topic_phishing	test campagne from IT department	2
topic_phishing	university shared information about phishing mails after hack attack	1
topic_phishing	were briefed about phishing mails and how to spot them	2

Category 18	Code	Frequency
topic_quantum_computing		3
topic_quantum_computing	cybersecurity in the age of quantum computing	3

Category 19	Code	Frequency
topic_social_media_security		5
topic_social_media_security	discussion about disinformation on portals such as x and facebook	1
topic_social_media_security	risk of profile takeover	1
topic_social_media_security	talked about app with suspicious behaviour	1
topic_social_media_security	talked about having to share personal data with facebook in order to receive shorter adds	1
topic_social_media_security	unauthorized login attempts	1

C Distribution of Participants by Country (N=215)

Country	Count	Percentage (%)
United Kingdom	42	19.53
Germany	41	19.07
United States	32	14.88
Poland	20	9.30
Portugal	19	8.84
Spain	16	7.44
Italy	14	6.51
Greece	13	6.05
Netherlands	6	2.79
France	4	1.86
Sweden	3	1.40
Montenegro	1	0.47
Denmark	1	0.47
Ireland	1	0.47
Estonia	1	0.47
Hungary	1	0.47