IEICE TRANS. INF. & SYST., VOL.E106–D, NO.9 SEPTEMBER 2023

PAPER *Special Section on Information and Communication System Security*

Analysis of Non-Experts' Security- and Privacy-Related Questions on a Q&A Site*

Ayako A. HASEGAWA[†a)], **Mitsuaki AKIYAMA**[††], ***Members***, **Naomi YAMASHITA**[††,†††], ***Nonmember***, **Daisuke INOUE**[†], ***and*** **Tatsuya MORI**[†,††††,†††††], ***Members***

SUMMARY Although security and privacy technologies are incorporated into every device and service, the complexity of these concepts confuses non-expert users. Prior research has shown that non-expert users ask strangers for advice about digital media use online. In this study, to clarify the security and privacy concerns of non-expert users in their daily lives, we investigated security- and privacy-related question posts on a Question-and-Answer (Q&A) site for non-expert users. We conducted a thematic analysis of 445 question posts. We identified seven themes among the questions and found that users asked about cyberattacks the most, followed by authentication and security software. We also found that there was a strong demand for answers, especially for questions related to privacy abuse and account/device management. Our findings provide key insights into what non-experts are struggling with when it comes to privacy and security and will help service providers and researchers make improvements to address these concerns.

key words: *usable security and privacy, user concerns, Q&A sites*

1. Introduction

Because security and privacy technologies are currently incorporated into every device and service, non-expert users are often compelled to make decisions on security and privacy in their daily lives [2], [3]. For example, they need to decide whether to permit apps to access their personal data [4] and whether to proceed against browser warnings [5]. However, security and privacy technologies are generally difficult for non-experts to understand and use owing to the complexity of these concepts [6]. Researchers have actually demonstrated that misconceptions regarding security and privacy technologies are ingrained and pervasive in non-expert users [7], [8].

According to a study that investigated the advice sources of non-expert users pertaining to digital media use, 43% of young adults ask strangers online as well as family and friends for advice [9]. Hence, we can expect that Question-and-Answer (Q&A) sites for non-expert users contain many security- and privacy-related questions that non-expert users have in their daily lives. In the security and privacy research community, researchers have successfully identified the security and privacy concerns of developers during their development work by analyzing questions posted on Stack Overflow, a Q&A site for developers and programmers [10]–[13]. However, little is known about security- and privacy-related questions posted on Q&A sites for non-expert users. By analyzing such questions, we can identify the issues these users face in their daily lives and provide insights to help stakeholders (e.g., service providers and security researchers) address these problems.

In this study, to clarify the security and privacy concerns of non-expert users in their daily lives, we investigated questions posted on Yahoo! Chiebukuro (Yahoo! 知恵袋) [14], the largest Q&A site for non-experts in Japan. We chose a Japanese Q&A site because a previous survey revealed that among Arabic, French, Japanese, Chinese, Korean, and Russian participants, the Japanese participants exhibited the least secure behaviors [15]. Thus, we speculated that a Japanese Q&A site would contain the questions commonly asked by those with less knowledge of security and privacy. To support such users effectively, it is essential to identify frequent, serious, and sensitive question topics. Given these observations, we address the following research questions in this work.

RQ1 What types of security and privacy topics do non-expert users post questions about on the Q&A site?

RQ2 Among these topics, which do they perceive as more serious or sensitive?

We analyzed 445 questions that were posted in security categories or that contained security- and privacy-related words in the question texts. For RQ1, we qualitatively coded topics for each question post and identified seven themes. We found that many non-expert users posted questions to determine whether they had been victimized/abused, to learn about response strategies for errors/damages, and to understand the necessity of security and privacy technologies. We also found that some users faced privacy abuse. For RQ2, for evaluating question seriousness, we measured the averages of coder-rated seriousness and the percentage of questions with rewards. We also measured the percentage of anonymous posts for evaluating question sensitivity. We found that the average of the coder-rated seriousness of questions in "privacy abuse" and "account/device manage-

Manuscript received October 14, 2022.
Manuscript revised April 2, 2023.
Manuscript publicized May 25, 2023.
[†]The authors are with NICT, Koganei-shi, 184–8795 Japan.
[††]The authors are with NTT, Musashino-shi, 180–8585 Japan.
[†††]The author is with Kyoto University, Kyoto-shi, 606–8501 Japan.
[††††]The author is with Waseda University, Tokyo, 169–8555 Japan.
[†††††]The author is with RIKEN AIP, Tokyo, 103–0027 Japan.
*This paper is the extended version of the paper presented at SOUPS'22 [1].
a) E-mail: aya.h.research@gmail.com
DOI: 10.1587/transinf.2022ICP0006

ment" was significantly higher than that of other themes. We also found that those who seek answers are likely to use a strategy of either appealing linguistically or offering rewards. On the other hand, we found no statistically significant difference in question sensitivity among the question themes.

This study makes the following contributions.

- To the best of our knowledge, this is the first qualitative security and privacy study of a Q&A site for non-expert users to demonstrate that a Q&A-site analysis can provide insights into what non-expert users are struggling with when it comes to security and privacy in their daily lives. We identified frequently asked question themes ("cyberattack," "authentication," and "security software") and question themes that askers perceived as more serious ("privacy abuse" and "account/device management"). We also demonstrated that some of the concerns of non-expert users have not been sufficiently investigated in previous studies.
- We assessed the effectiveness of potential indicators of question seriousness and sensitivity to help researchers better understand and prioritize the concerns of non-expert users. The results suggest that researchers should complementarily incorporate multiple indicators.
- We provide design implications for Q&A sites to help non-expert users judge what and how much information they should reveal in their questions.

2. Related Work

In this section, we present a review of the literature closely related to this study. We first discuss studies that investigated non-expert users' advice sources for security and privacy issues, and the contents and quality of the advice. Next, we go over previous studies on HCI and security/privacy that explored the posts and users (i.e., askers and responders) of Q&A sites. Finally, we identify the gaps in the previous studies and clarify how our study addresses these gaps.

2.1 Security and Privacy Advice

Many researchers have assessed the contents and quality of security and privacy advice given by experts to non-expert users or advice available on the web [16]–[21]. Redmiles et al. showed that the majority of advice on the web was at least somewhat actionable and somewhat comprehensible [16]. Mossano et al. identified various issues such as contradictory or abstract advice [19]. Redmiles et al. also investigated non-expert users' reactions to security advice and found that they determined whether to accept digital security advice based on the trustworthiness of the advice source [22]. Fagan et al. surveyed users who followed security advice and found that they rated the benefits of following, the risks of not following, and the costs of not following higher that those who did not follow the advice [23].

Other researchers have focused on advice sources [3], [9], [22], [24]–[27] and found that these include both informal (e.g., family and friends) and formal (e.g., technical support) sources, as well as both offline and online sources. Micheli et al. [9] investigated the advice sources of young adults for digital media use in 2016 and found that 43% of participants asked questions to strangers online. They also reported that males with higher Internet skills were significantly more likely to ask questions to strangers online.

2.2 Asking Questions on Q&A Sites

Q&A sites such as Yahoo! Answers offer people the opportunity to obtain desired information rapidly and efficiently online. Thus, Q&A sites have become an interesting and promising subject of research in computer science [28], [29].

User motivations. Askers post questions for various reasons, such as to obtain specific information, to obtain non-popular information, to gather diverse opinions and experiences, and to satisfy curiosity [30], [31]. Previous studies examining the motivation of responders commonly concluded that the primary motivation was altruism (e.g., to feel like they were helping someone) [32], [33].

Question topics and types. Researchers have examined Q&A sites to clarify people's concerns (i.e., question topics) about specific issues, such as eating disorders [34] or cancer [35]. Other researchers have classified the types of questions posted on Q&A sites [32], [36]–[40]. For example, Choi et al. categorized question types as information-, advice-, opinion-, and non-information-seeking questions and found that advice- and opinion-seeking questions were the most popular on Yahoo! Answers [32], [36]. A key finding of these studies is that the frequency of question types differs among categories and Q&A sites.

Anonymity and sensitivity of posts. One of the most unique features of Q&A sites is anonymous posts. When users create accounts, some sites (e.g., Yahoo! Answers) allow pseudonyms, whereas with others (e.g., Quora[†] [41]), real names are mandatory. When users post questions, both types of sites typically offer anonymity. Researchers consider anonymity to be related to the sensitivity of a post [42], [43]. Naturally, the questions that are rated highly sensitive by coders are more likely to be asked anonymously [42]. Peddinti et al. [43] identified some of the question categories for which users are more likely to answer anonymously as religion, drugs, and sexual orientation.

Askers' strategies and question answerability. Although posting questions on Q&A sites has many benefits, these sites do not always work as expected because not all questions receive answers, and the quality of received answers is not always high. Therefore, askers utilize strategies such as specifying, clarifying, and signaling to ensure a higher

[†]Quora initially required users to register their real names, but it has allowed users to use pseudonyms since 2021.

chance of a response [30], [31]. Many studies have examined the answerability of questions on Q&A sites [29], [42], [44]–[48]. For example, Harper et al. [44] explored the variables that affect answer outcomes (such as number, length, effort, and quality of answers) and found that question topics, question types, levels of reward, and the site itself significantly affected one or more of these outcomes. Another study showed that the topics, uniqueness, and urgency of questions significantly affected the possibility of receiving answers [45]. As for allowing anonymity, it had no significant effect on the answer quality [42].

2.3 Security and Privacy Posts by Developers

Stack Overflow [49] is unique in that its target users are developers and programmers, and it has become the most popular information source for developers [50]. Many researchers have studied question topics on Stack Overflow to clarify developers' concerns and challenges related to security and privacy [10]–[13]. For example, Tahaei et al. performed qualitative analysis to determine what developers ask about privacy-related issues on Stack Overflow and found that they often asked questions about privacy policies, privacy concerns, access control, and version changes [10]. Patnaik et al. identified the usability issues of cryptography libraries by qualitatively reviewing the questions on Stack Overflow [11]. Yang et al. conducted a large-scale study of questions with tags related to security on Stack Overflow and found that they covered a wide range of topics mainly belonging to five categories: web security, mobile security, cryptography, software security, and system security [12]. They also revealed that questions about passwords and signatures were posted frequently, but were less likely to be answered.

2.4 Research Gaps in Previous Studies

As mentioned in Sect. 2.1, nearly half of young adult users ask questions regarding digital media use to strangers online. Hence, in this study, we analyzed security- and privacy-related questions posted on a Q&A site. Although many researchers in the security and privacy community have investigated questions posted on Q&A sites for developers (as mentioned in Sect. 2.3), little is known about the questions posted by non-expert users. To clarify the security- and privacy-related questions posted by non-experts, we generally adopted the same analysis approaches and findings as previous Q&A site studies (see Sects. 2.2 and 2.3), which we explain in detail in Sect. 3.3.

3. Methodology

We collected and analyzed security- and privacy-related questions posted on Yahoo! Chiebukuro (Yahoo! 知恵袋) [14], a site that was chosen because of its popularity and the wealth of features available to users (e.g., rewards for best answers, anonymous posts). In this section, we first present the mechanism of posting questions and receiving answers on Yahoo! Chiebukuro and then explain our data collection and analysis method.

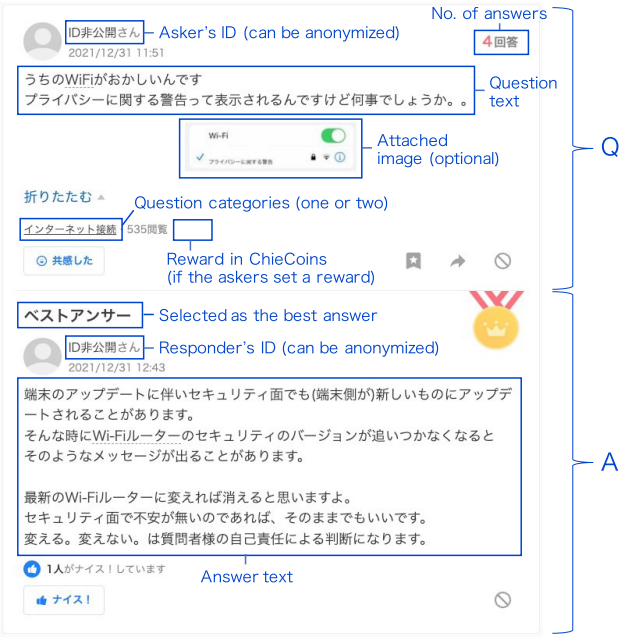

Fig. 1 Interface of a question in Yahoo! Chiebukuro.

3.1 Descriptions of the Target Q&A Site

Yahoo! Chiebukuro (Yahoo! 知恵袋) [14], where users share their knowledge and wisdom by answering questions, is the most popular Q&A site in Japan†. The meaning of the Japanese word "Chiebukuro" is "bag of knowledge." It is provided only in Japanese and is available on the web and as an app (iOS and Android). Yahoo! Chiebukuro is generic, which means the site is not dedicated to a specific demographic of people (e.g., people with specific professions), and open, which means it is not invitation-only but is available to everyone. Anyone with a Yahoo! ID can post a question and answer for free. Yahoo! does not recommend that users include their real names in their Yahoo! IDs, and users can set random or favorite strings. Thus, we consider Yahoo IDs to be pseudonyms. Yahoo! Chiebukuro has various question categories spanning entertainment, romance, health, politics, technology, and more. It received approximately 4.5 million posts per month as of March 2021 [51].

Figure 1 shows a screenshot of the interface of a question on the Yahoo! Chiebukuro website. Herein, we present the mechanism of Yahoo! Chiebukuro in accordance with the four steps of a Q&A lifecycle: 1) an asker posts a question, 2) potential responders view the question, 3) responders post answers, and 4) the question is closed either man-

†Yahoo! Answers, which is the global version of Yahoo! Chiebukuro, was closed in May 2021. The closure did not affect Yahoo! Chiebukuro because it is run by a different operating company.

ually by the asker or automatically by the system.

1) Posting a question. An asker inputs the question text and, if necessary, attaches an image file (e.g., screenshot). The asker then selects one or two categories either manually or from a list of automatically recommended categories based on the question text. The categories are structured in a three-tier hierarchy (e.g., *Computer technology > Security > Network security*), and the Yahoo! ID of the asker is not anonymous by default. When posting a question using the Yahoo! Chiebukuro app, askers can opt to make their Yahoo! ID anonymous for free. When posting a question via the website, they can make their Yahoo! ID anonymous by paying with ChieCoins, which are used only on Yahoo! Chiebukuro and have no real-world value. Users can receive ChieCoins from the service by performing various actions such as registering, logging in, posting a question, posting an answer, and selecting the best answer; in addition, they receive ChieCoins if their answer is selected as the best answer. An asker can offer rewards for the best answer (25, 50, 100, 250, or 500 ChieCoins) to increase the probability of receiving answers. Each question has only the question text without any title or tag.

2) Viewing a question. A potential responder finds questions by selecting a category of interest or searching for a specific word. On an index page of each category/word, a potential responder can explore the questions by status (i.e., open or resolved) and sort them by newness, number of answers received at that time, or reward amount. On the index page, a potential responder can see the beginning of the question text (about 40 Japanese characters), the main question category, the number of answers received at that time, an attached image (optional), any additional rewards (optional), and an anonymous-posts flag (optional) for each question.

3) Posting an answer. A responder inputs the answer text and if necessary, attaches an image file.

4) Closing a question. Each question is open for responders to answer for seven days by default. If a question does not receive any answers within this period, it is automatically deleted. If a question receives one or more answers, the asker can select the "best answer" from among them. When the asker selects the best answer, the question is marked as "resolved", and no further answers will be accepted. A question that has received one or more answers and has been live for more than seven days is marked as "closed and waiting for the asker's vote" until the asker selects the best answer.

3.2 Data Collection

As shown in Fig. 2, we created a dataset consisting of three subsets of questions collected in different ways: questions from security-related categories (Subset–1), questions containing the words "security" and/or "privacy" (Subset–2), and questions containing some words related to security and privacy (Subset–3). This merged dataset was created to cover a wide variety of security- and privacy-related questions.

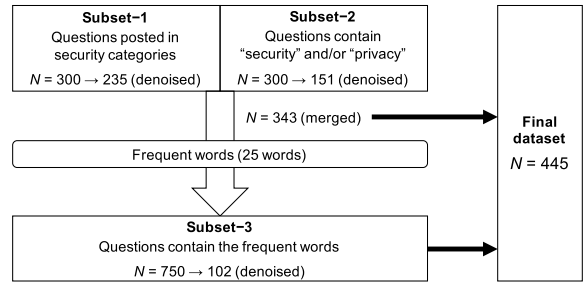

Fig. 2 Data collection flow in this study.

Subset–1: Collected in security-related categories. Yahoo! Chiebukuro has three categories that are directly related to security: "*Computer technology > Security > Network security,*" "*Computer technology > Security > Cryptography and authentication*," and "*Internet > Internet services > Computer virus measures and security practices*." There are no categories that are directly related to privacy. We collected all question posts (comprising the question text, attached image, and some metadata) from these three categories. Note that we collected all posted questions regardless of whether they had received answers, even though a question with no answers is removed from the service later. We started collecting question posts in December 2021 and continued for seven days until we had obtained 300 without random sampling. Then, two authors (security and privacy researchers) independently reviewed all the question posts to exclude any that satisfied any of the following conditions: (1) questions that were not related to computer security or privacy, (2) questions that were too vague, and (3) questions that the askers seemed to be using for an exam or homework. The discrepancies between the two coders were resolved by discussion and we finally obtained 235 question posts.

Subset–2: Collected with "security" and/or "privacy". Although Yahoo! Chiebukuro has three categories directly related to security, askers may post security-related questions in categories besides these. For example, when an asker who wants to know about the security and privacy of smartphones posts a question, the automatic category recommendation system might recommend a category related to smartphones. Therefore, we collected question posts that contained the word "security" and/or "privacy" in the question text from all categories. We collected 300 question posts in the same way and period as Subset–1, and after performing the same exclusion, we obtained 151 question posts.

Subset–3: Collected with related words. Users might post security- and privacy-related questions that do not actually include the words "security" or "privacy," e.g., "What does this warning mean?" with an attached image file. Therefore, we collected questions that contain specific words that appear frequently in security- and privacy-related topics in the question text from all categories. After merging Subsets–1 and –2 without overlapping (N = 343), we extracted fre-

quent nouns in the question texts using MeCab [52] and mecab-ipadic-NEologd [53], which are Japanese morphological analyzers. The top 25 most frequent nouns were as follows: site, account, virus, setting, information, password, app, login, PC, software, screen, email, code, smartphone, authentication, (tele)phone, fraud, iPhone, Google, infection, connection, file, Internet, registration, and deletion. We believe these nouns are a representative, though not comprehensive, set of frequently used keywords related to the research theme of usable security and privacy [2]. We started collecting posts in all categories that included the above 25 nouns in the question text in January 2022. It took only one day to collect 30 question posts for each word (a total of 750 posts) without random sampling. After performing the same exclusion as Subsets–1 and –2, we obtained 102 question posts.

Final dataset. After merging Subsets–1, –2, and –3 without overlapping, we obtained a final dataset consisting of 445 question posts. Our sample size (N = 445) was sufficiently larger than that of a recent representative study (N = 315) in which privacy-related posts on a developer Q&A site were qualitatively reviewed [10]. In our dataset, the average text length was 168.6 Japanese characters (Med. 132), which is regarded as equivalent to 86.5 English words (Med. 67.7) [54]. Of the 445 question posts, 73 (16.4%) had an attached image. After the period for receiving answers, 353 (79.3%) posts had received one or more answers ("resolved": 43.1% and "closed and waiting for the asker's vote": 36.2%), and the remaining 92 (20.6%) posts received no answers ("deleted").

3.3 Data Analysis

Analysis approach. To determine the question topics of non-expert users, we adopted a qualitative analysis approach (i.e., manual coding) rather than quantitative. A previous study that analyzed question posts on a Q&A site [10] demonstrated that the topic modeling yielded high-level results similar to the results of manual coding. We did not utilize topic modeling in this study because our preliminary investigation revealed that Yahoo! Chiebukuro users often post questions by attaching images instead of explaining their situation in detail using only words. In contrast to topic modeling, which lacks syntax and semantics, manual qualitative coding can provide deeper insights: for example, we can identify whether an asker was trying to preserve their privacy or abuse someone else's privacy.

Coding procedure. Two authors (security and privacy researchers) reviewed the question texts and attached images using inductive thematic analysis [55]. For each question post, we coded the question topics (RQ1) and the askers' perceived seriousness (RQ2). The two coders independently coded 100 randomly selected question posts and developed a codebook over the course of many discussions, which was then used to independently code all the collected question posts.

Question topics (RQ1). We represented question topics using themes and sub-themes. Following a previous study that analyzed question topics posted by developers on Stack Overflow [12], we categorized the themes in our study on the basis of security and privacy technologies and threats (e.g., theme: "authentication"). Sub-themes were categorized to describe the question topics in more detail and to cover the concepts of question types (i.e., whether the askers sought information or advice), question drivers (what prompted the askers to post questions), and phase of security and privacy practice (e.g., prevention or response). For each question post, we assigned one theme and one or two sub-themes, as askers sometimes asked two questions within the same post. For example, they might ask whether their devices have been infected, and if so, what they should do (e.g., theme: "cyberattack," and sub-themes: "have I been hacked?" and "how to handle this?"). Our final codebook consisted of seven themes and 19 sub-themes (excluding "other"). Of the 445 question posts, 416 were assigned one sub-theme, and the remaining 29 were assigned two sub-themes. We calculated the inter-rater reliability of the two coders' theme assignment for all question posts and found that the Cohen's Kappa coefficient was 0.87, indicating high agreement.

Question seriousness (RQ2). According to Hsieh and Counts, a serious question can be defined as a one that you believe the question asker really wanted an answer for [40]. We adopt their definition in this study and utilize two evaluation measurements that may act complementarily.

The first measurement is the coder-rated seriousness of the question text. The coders manually reviewed the seriousness of each question text based on the above definition using a 5-point Likert scale, where 1 is not serious, 3 is moderately serious, and 5 is very serious [40]. The coders considered posts to have higher seriousness when the askers expressed certain signals such as expressions of urgency, anxiety, or a call for help. They judged based only on the question text, i.e., without looking at the metadata such as reward amount or anonymity. We provide some examples of question posts and the value of coder-rated seriousness in Table A· 1 of Appendix Appendix. The correlation coefficient between the ratings of the two coders was r = .773, indicating adequate reliability. We calculated the average ratings of the two coders for each question topic.

The second measurement was the rewards (ChieCoins) for the best answer. Yahoo! Chiebukuro recommends that users who want to increase the probability of receiving answers should offer rewards for the best answer [56]. For each question topic, we calculated the percentage of question posts for which the askers offered rewards. Note that we did not report the average number of ChieCoins that askers offered. On Yahoo! Chiebukuro, askers must set rewards from either 25, 50, 100, 250, or 500 ChieCoins, so we cannot be certain that the level of seriousness perceived by askers exactly matches the reward amount.

The coder-rated seriousness is intended to capture the linguistic expressions of the askers, and the percentage of

reward is indicative of the askers' behaviors when requesting answers. In this study, we judged a question as serious when either or both of these measurements were high.

Question sensitivity (RQ2). For measuring question sensitivity, we calculated the frequency of anonymous posts for each question topic. It is well known that anonymity can be used as a metric that captures the sensitivity of questions [43], i.e., askers tend to post sensitive questions anonymously [42].

3.4 Ethical Consideration

We followed the ethical principles laid out in the Menlo Report [57] and the ethical methods of studying online communities [58]–[60]. We also abided by Yahoo! Chiebukuro's Terms of Service. Our crawler sent requests with intervals of more than 15 seconds. We did not collect any personally identifiable information or the Yahoo! IDs of the askers. To investigate whether the posts were anonymous, we collected only the flag metadata that indicated whether the posts were anonymous or non-anonymous. In this paper, we present only the aggregated data or the translated and abstracted contents of the original question posts (i.e., we avoid direct quotes) so that readers will not be able to identify the original question posts or askers. For the example shown in Fig. 1, we selected a post in which both the asker and responder were anonymous. Our study design was approved by our Institutional Review Board (IRB).

4. Results

4.1 RQ1: Question Topics

The final codebook for question topics consisted of seven themes and 19 sub-themes, excluding "Other." Table 1 gives an overview of the themes and their frequencies, and Table 2 lists the frequent nouns included in each theme.

4.1.1 Cyberattack (40.7%)

The most frequent question theme was cyberattacks, including online fraud, phishing, malware, and account hijacking, as evidenced by the frequent occurrence of the terms "virus," "fraud," and "infection" (see Table 2). Askers posted questions regarding the prevention of such cyberattacks, incident identification, and responses to these incidents. Askers reported that they input their information onto suspicious websites; thus, the terms "password," "information," and "phone number" exhibited high occurrences in this theme. Note that we did not split the theme code into different attack types because in some cases, the description of the question was not clear, making it difficult to perform such classification.

Is this malicious? / Have I been hacked? (24.0%) Various triggers can make users anxious that they are facing a cyberattack. Examples of such triggers include suspicious messages (email, SMS, or popup), mistakenly accessing an unintended webpage, notifications from security software, suspicious activity logs that the user does not recognize, reduced operation speed of the device, and rapid draining of the device battery. Among cyberattacks, a frequently encountered event was one that we suspect to be a technical-support fraud: "*I received a warning that my computer has been infected with Trojan Horse and I need to call Microsoft Support Center. Is this a fraud or has my computer actually been infected?*" Moreover, we found that many users reported receiving suspicious messages after signing up for the Sweepstakes campaign spread through social media. In some questions, the users copied and pasted the received messages into the questions and asked if these messages were fraudulent. Most of the messages received by the users were spoofed with URLs or sender email addresses using typical techniques such as typosquatting (e.g., `AppleSupp0rt`) or using an email address of a well-known free mail service (e.g., a message disguised as Google by using a Gmail address). As Reynolds et al. revealed, non-expert users are not even aware of the typical fraud techniques [61], so it is difficult for them to detect fraud on their own.

We found that users who noticed that a site was a fraud before they completely entered their personal information were worried about being victimized by attacks: "*[...] After entering my real name, I finally calmed down and closed the browser without entering my credit card information. Was my device already infected with a virus at the moment I accessed the URL?*"

Some users asked about the safety of websites by providing names or URLs of the websites. Users seemed to experience difficulty in judging safety by themselves, particularly in the case of international websites that are not offered in their native languages (i.e., Japanese).

How to handle this? (11.9%) Many users seemed to have no idea what to do when they perceived that they had been subjected to a cyberattack: "*When I was browsing web sites, a message saying 'Your device is infected with 39 computer viruses' was suddenly displayed. What should I do? I've never seen this message before, and I'm very worried. Please help me deal with this!*" In cases where users have already undertaken the basic security measures, they may be looking for additional actions: "*I accessed a phishing URL posing as Amazon and input my personal information, prepaid card number, and Amazon login information. Now I have changed my Amazon and prepaid card service passwords. Is there any other action I should take?*" According to prior studies that analyzed the advice on anti-phishing and anti-account-compromise on the web, a minority of the websites provided complete advice for remediation [19], [20]. Hence, users may be unable to complete the necessary measures against online fraud.

Is there any possibility of being hacked? (4.7%) Users were worried about the types of situation in which they could be at risk of cyberattacks, as indicated by questions such as "*Are smartwatches also at risk of being infected by*

Table 1 Results of question topics and the askers' perceived seriousness and sensitivity.

Theme	Sub-theme	Frequency*		Seriousness (RQ2)				Sensitivity (RQ2)	
				Ave. rating**		% Reward **		% Anonymous**	
Cyberattack (e.g., online fraud, phishing, malware, and account hijacking)	Is this malicious? / Have I been hacked?	40.7%	24.0%	3.6	3.8	29.3	29.9	48.1	50.5
	How to handle this?		11.9%		4.1		41.5		50.9
	Is there any possibility of being hacked?		4.7%		3.0		23.8		52.4
	How to prevent it?		3.4%		3.1		26.7		46.7
	Other		2.5%		2.5		9.1		36.4
Authentication	How to handle this?	16.2%	14.6%	3.6	3.7	29.2	26.2	36.1	36.9
	Is it necessary/effective/trustworthy?		1.1%		–		–		–
	Other		0.4%		–		–		–
Security software	How to use it?	13.0%	6.7%	3.1	3.3	41.4	40.0	31.0	26.7
	Which product do you recommend?		3.1%		2.9		35.7		28.6
	Is it necessary/effective/trustworthy?		2.2%		3.1		40.0		40.0
	Other		0.9%		–		–		–
Privacy abuse (e.g., IPA, cyberstalking, parental control, and voyeurism)	How to escape from surveillance?	7.9%	2.9%	4.0	4.3	25.7	23.1	42.9	38.5
	Am I under surveillance?		2.2%		4.0		30.0		50.0
	Is this privacy abuse?		1.8%		–		–		–
	How to surveil a target?		0.7%		–		–		–
	Other		0.7%		–		–		–
Account and device management	How to handle this?	7.0%	5.6%	3.9	4.0	45.2	44.0	48.4	48.0
	What should I (not) do?		1.1%		–		–		–
	Other		0.2%		–		–		–
Secure connection (e.g., Wi-Fi and VPN)	How to use it?	6.5%	4.9%	3.2	3.4	27.6	31.8	48.3	36.4
	Is it necessary/effective/trustworthy?		1.1%		–		–		–
	Other		0.4%		–		–		–
Privacy setting	How to set it?	5.6%	3.1%	3.7	3.8	36.0	35.7	44.0	42.9
	Are my data disclosed?		2.2%		3.9		50.0		40.0
	Other		0.4%		–		–		–
Other		3.1%		2.9		14.3		35.7	

* For each question post, we assigned one theme and one or two sub-themes, as askers sometimes ask two questions within the same post.
** '–' indicates that the sub-theme accounts for less than 2.0% of all question posts. These sub-themes are potentially influenced by an outlier.

Table 2 Top 10 frequent nouns included in question texts of each theme.

Theme	Nouns
Cyberattack	website, virus, password, fraud, information, email, account, infection, phone number, smartphone
Authentication	login, authentication, password, account, phone number, Google, iPhone, code, screen, two-step
Security software	security, computer, website, Windows, Norton, Virus Buster, smartphone, software, screen, McAfee
Privacy abuse	smartphone, friend, account, LINE*, information, privacy, password, history, Twitter, Instagram
Account and device management	account, iPhone, password, device, login, setting, factory reset, email address, data, iCloud
Secure connection	connection, VPN, security, setting, port, router, encryption, key, Wi-Fi, IP address
Privacy setting	setting, information, location, iPhone, privacy, accept, consent, website, restriction, company

Note that the original question texts were in Japanese. We extracted the frequent Japanese nouns and then translated them into English.
* LINE is a messaging app that is commonly used in Japan and other Asian countries.

viruses?" and "*If a smartphone belonging to a member of my family gets infected by a virus, is it possible that devices of other family members will get infected by the virus via Wi-Fi or other means?*" A few users believed in unscientific conspiracy theories (e.g., the coronavirus containing malware code inside it) and were concerned about unrealistic cyberattacks (e.g., eavesdropping on thoughts).

How to prevent it? (3.4%) Some users were proactively contemplating prevention methods against cyberattacks, as indicated by the following questions: "*How can I keep my computer and smartphone secure?*" and "*Is it better to log out every time after I use a Google account?*" The prevention methods mentioned by users were not always effective or usable: "*I heard someone's <service name> account had been hijacked on the news. To prevent account hijacking, what should I do? I have installed shopping apps on my smartphone. Is it effective to uninstall them after every time I use them?*" A self-identified non-expert user who wanted to browse the Dark Web out of curiosity asked for a way to browse it without being exposed to any risk.

4.1.2 Authentication (16.2%)

Authentication is a security technique that most users encounter whenever they access services. Most of the questions in this question theme were posted when the users' authentication had failed. Consequently, the terms that indicate authentication itself (e.g., "login" and "authentication") and authenticator (e.g., "password" and "code") occurred frequently in this theme as shown in Table 2.

How to handle this? (14.6%) We found that many users failed to receive security codes for multi-factor authentication because of discarded authenticator devices or fake email addresses registered for email verification: "*I can't log in to*

my <service name>'s account, where I set up a two-factor authentication with my phone number. Some days ago, I changed my phone number. How do I log in to the account again?" A user who was unable to log in to a service where they had registered a fake phone number faced difficulty in canceling a paid subscription service: "*I registered a temporary phone number that wasn't my own, which I had received from an app that provides temporary phone numbers, to <dating app's name>. After that, I accidentally logged out of <dating app's name> and cannot log in again. Is there any way to cancel <dating app's name>'s paid subscription other than by canceling my credit card?*" Lies that users tell to protect their privacy are called "privacy lies." Sannon et al. found that most users had lied [62].

Some users had trouble using multi-factor authentication because of an implementation issue with the service or its app: "*I confirmed the security code in the SMS app. However, when I go back to the original app, the screen for sending the security code is displayed, instead of the screen for inputting the security code. I'm stuck in this loop.*"

When authentication failed, some users tried to contact the service operator. However, they sometimes could not find the contact point: "*I can't log in to <service name>. I can't find the contact form on the website, and the service doesn't have a Twitter account, so I can't contact them. [...] How do I get my account back?*"

Another user was irritated with a smartphone unlock issue that arose because of measures put in place during the COVID-19 pandemic: "*I've been wearing a mask all the time due to COVID-19, and because of that, the Face ID doesn't work. I end up having to input the passcode every time. That is inconvenient. [...] Is there any good way around that?*"

Is it necessary/effective/trustworthy? (1.1%) Service providers and security researchers have stressed to users that two-factor authentication and two-step authentication are important technologies to improve the security of user accounts while maintaining their usability [63]–[66]. Unfortunately, some users are skeptical about the necessity of these technologies: "*I read reviews of a two-step authentication app and found many critical reviews. Do we really need two-step authentication?*"

A few users considered using fingerprint authentication but were concerned about the accuracy: "*I have heard that elderly people have difficulty passing fingerprint authentication. Is that true? An 80-year-old woman that I know cannot remember passcodes, so I am looking for a useful biometric authentication method for her.*"

4.1.3 Security Software (13.0%)

Security software is often bundled with the OS or preinstalled in products, making it the most familiar security tool for most users. However, users did not sufficiently understand how to use it, in addition to its usefulness. As shown in Table 2, users mentioned specific security software names and asked about usage, functions, and necessity.

How to use it? (6.7%) Users struggle to set up security software and understand its features: "*<Anti-virus software's name>'s offline scan did not run. [...] What should I do?*" and "*The message says that silent mode is disabled, and the scheduled scan and detection notification are enabled. What does this mean?*" We observed an unfortunate case in which the message displayed by the security software misled a user, though this issue may be peculiar to Japanese grammar. When the user saw the screen message saying that it was scanning for a Trojan Horse, they misunderstood that it had been detected on their device. Users also struggled to set up exception cases, i.e., legitimate access: "*<Anti-virus software's name> recently blocked my access to <service name>, deeming it a suspicious site. How can I stop the blocking?*" Other users asked about errors that occurred while installing or uninstalling anti-virus software.

Which product do you recommend? (3.1%) It was difficult for users to compare and choose between the technical advantages of various security products, so they sought opinions and recommendations from others: "*What is the best anti-virus software? I currently use <software name>, but I frequently receive fraud emails. I plan to change to another software.*" Users requested recommendations for software that has specific features and a good cost performance. Some users wondered which was better, using OS-bundled anti-virus software or purchasing their own anti-virus software.

Is it necessary/effective/trustworthy? (2.2%) Users, especially those who used their devices only for limited purposes, tended to be skeptical about the effectiveness and necessity of security software: "*I use <anti-virus software's name>, but I don't see the benefits. When it runs in the background, my computer gets hot and the fan gets noisy. I want to uninstall it. I use this computer only for creating documents and surfing popular websites. Please tell me why I should use anti-virus software on my computer.*"

4.1.4 Privacy Abuse (7.9%)

Privacy researchers have been worried about the prevalence of privacy abuse issues such as intimate partner abuse (IPA) [67]–[71], cyberstalking [72], [73], excessive parental control [74]–[76], voyeurism [77], [78], and bugging [77], [78]. In previous studies, privacy abuse has been researched in cooperation with professional organizations by means of closed questionnaires and interviews [68], [70], [71]. Surprisingly, we found a non-negligible number of questions on privacy abuse posted on the open Q&A site. We found questions from both the attackers' and the victims' points of view. Many questions were related to the surveillance of online activities and histories, including social media, as shown in Table 2.

How to escape from surveillance? (2.9%) Users sought

ways to escape surveillance by their partners (or ex-partners), friends, parents, acquaintances, schools, and companies. Users asked about various kinds of surveillance:

> "*When I was married to my ex-husband, I logged into my Instagram account from his Facebook account once. Since then, he seems to be logging into my Instagram account using his Facebook account. I find this very unpleasant, but I don't know his Facebook password. Please tell me how to remove his surveillance.*"

> "*My friend snooped on my smartphone and tried to use it. It has private chat logs and apps containing info on my sexual habits, so I don't want it to be peeked at. [...]*"

> "*I'm a student. My device is restricted by <security software's name> that my parents set. Is there any way I can unlock it without using my parents' devices? [...]*"

Am I under surveillance? (2.2%) We found that some users, presumably children, wanted to know if they were being monitored by parental control features: "*I heard that parents can see children's (browsing) histories with <security software's name>. I remembered that the app had been pre-installed on my smartphone and I checked it. Then it asked me to agree to the privacy policy. It isn't working, is it? My parents haven't seen my history, have they?*" Another user was worried about voyeurism and bugging at the place they were staying: "*I hear something strange from the digital speakers on the ceiling of my hotel room. Is it possible that I'm being a target of voyeurism or being bugged?*"

Is this privacy abuse? (1.8%) Uses asked for objective opinions on whether a certain action by themselves or another person constituted a privacy violation. "*My company asks me to submit a QR code for my private ID of <messaging service's name>. This is a privacy violating action, isn't it?*" and "*Please give me your opinion on children's privacy and rights with conducting parental control. In the case of teenage children, to what extent do you think parents should intervene in their children's smartphones? Specifically, please tell me about each of the following behaviors: keeping an eye on their location with a GPS, limiting the web sites they can visit, viewing their contact information, viewing their browsing histories, viewing incoming and outgoing call histories, and viewing their emails and chats.*"

Further, other users also asked about slander on social media: "*I received a message containing sexual harassment from an acquaintance and told them that I would post it on my social media to give my friends a heads-up. The acquaintance then told me that this would be slander. Is posting a message a form of privacy abuse or slander even when it is meant to alert people?*"

How to surveil a target? (0.7%) Users were curious about the extent to which they could monitor a target using spyware apps: "*I want to know about the features of spyware apps, especially <spyware app's name>. Is it possible to track targets even when they have turned off the GPS on their smartphone? How about when they have switched their smartphone to airplane mode?*" However, not all question posts were necessarily asked by malicious users. One user needed advice on monitoring their children to prevent them from being involved in a crime: "*[...] I found that my daughter created <social media service's names> accounts. On her Twitter profile, she wrote messages asking to go on dates with adult males. I explained the various risks to her, and she agreed and deleted her accounts. However, today, I found that she received an email saying that her <social media service's name> account had been restored. As a countermeasure, I set up her Gmail account so that I can view her emails. Should I take further countermeasures?*"

4.1.5 Account and Device Management (7.0%)

Questions in this theme are associated with security- and privacy-related issues of "account" and "device" management, especially those related to "setting" up new accounts/devices and disposal of old "data" (e.g., "factory reset"), as shown in Table 2.

How to handle this? (5.6%) Users asked for the appropriate account deletion procedure to protect their privacy: "*I want to delete my <service name> account. But I couldn't find the delete option on my profile page. Can someone please tell me how to delete my account?*" Previous studies on the presence of account deletion options on websites reported that not all websites provided such options [79], [80], which can cause confusion to the users. Another user seemed to be confusing the deletion of an account of service with uninstalling the service's app from their device.

What should I (not) do? (1.1%) A small number of users sought general advice on what to do with the apps and local data on their old devices when buying new ones. They also asked about the potential risks of simply discarding their old devices. As Ceci et al. reported, non-expert users are concerned about safe ways to dispose of their devices but seem to lack sufficient knowledge about how to do so [81].

4.1.6 Secure Connection (6.5%)

We found that a certain number of users tried to establish a secure connection encrypted by one or more security protocols. Most of the questions in this theme were about virtual private networks (VPNs) and Wi-Fi. As presented in Table 2, this theme contained relatively numerous technical terms. Users found it difficult to understand technical terms and thus establish a secure connection.

How to use it? (4.9%) Users were confused by the many technical terms and names of security standards and encryption methods that appear on Wi-Fi connection setting screens. "*Which Wi-Fi security mode should I choose among WEP, WPA, WPA2, PSK, and 802.1X/EAP?*" Users also expressed confusion about frequently getting warning messages when they tried to connect to Wi-Fi networks: "*When*

I tried to connect to Wi-Fi using the IEEE802.11b standard, my iPhone screen showed that it was a legacy access point. Does this mean that there is a security problem?" and "*When I use Wi-Fi on my iPhone, I get a 'Privacy Warning' message. Does this happen often? How do you deal with it?*"

Is it necessary/effective/trustworthy? (1.1%) Users seemed interested in the necessity, effectiveness, and trustworthiness of VPNs: "*I was recommended to use a VPN app as a trick to access a web site that my device can't access. Are VPN apps secure?*" and "*Is VPN effective in making public Wi-Fi secure?*"

4.1.7 Privacy Setting (5.6%)

Application or website privacy settings can allow users to control their privacy. Users expressed concerns regarding how their information is processed, especially their location information, as shown in Table 2. Users also expressed concerns related to privacy consent with companies, as evidenced by the high occurrence of the terms "accept" and "consent." However, it is sometimes difficult for users to understand these settings and configure them appropriately.

How to set it? (3.1%) With regard to cookies, there have been numerous discussions about how service providers present users with cookie notifications (e.g., option, framing, and display position designs, as well as default) [82]–[84]. We observed that users suffered from different usability issues regarding cookies: "*When I visited the <service name>'s website, it asked me whether I would allow cookies. I mistakenly hit the allow button. Is it possible to change it to deny permission?*" Another user had difficulty understanding the meaning and mechanism of personalization on the privacy setting page: "*What does 'Personalization based on your inferred identity' on Twitter's privacy setting page mean?*"

Are my data disclosed? (2.2%) Users expressed concern about whether their data were disclosed or shared, especially because of unintended privacy settings: "*I browsed a certain company's websites via Safari with my iPhone's location information turned on. In this case, is my location information disclosed to the company? Is there a difference between using Wi-Fi at home and on a mobile line?*"

In addition, we found that some users were concerned about whether they unintentionally left a footprint by viewing other users' profiles or posts on social media: "*Is there a possibility that someone could find out that I viewed their <social media service's name>'s profile? Can they find out even if my account is private?*" For example, on Instagram, users cannot know the usernames of those who view regular posts, but they can know it for "story" posts [85]. Because the feature of a read mark or footprint on social media and messaging services negatively impacts users' privacy [86], service providers need to assume the responsibility of explicitly explaining its mechanism to the users.

4.2 RQ2: Seriousness and Sensitivity

We examined relatively serious and sensitive question themes to better understand non-experts' expectations and prioritize the themes accordingly. Note that every question theme is already regarded as at least some level of seriousness at the point of posting a question on a Q&A site.

4.2.1 Question Seriousness

For all the collected question posts, the average coder-rated seriousness was 3.5, and 31.5% (140/445) of the questions were posted with rewards for the best answer. The averages of the coder-rated seriousness and the percentage of question posts for which the askers offered rewards are listed in Table 1. We performed an unpaired t-test to compare the coder-rated seriousness score between the question posts of askers who offered rewards and those who did not. Although we found no significant difference ($p = .054$), those who offered rewards seem to express slightly more serious signals in their questions (avg. seriousness = 3.7) than those who did not offer rewards (avg. seriousness = 3.5). This indicates that askers who seek answers are likely to use a strategy of either appealing linguistically or offering rewards.

The average coder-rated seriousness was higher for questions under the themes of "privacy abuse" and "account/device management." We observed that askers frequently expressed their anxiety in question posts under these themes. We performed a Kruskal-Wallis test to compare the coder-rated seriousness across the question themes and found that there was a statistically significant difference ($p < .001$). We then performed post hoc Wilcoxon rank-sum tests in which the p-values were adjusted using the Bonferroni method. We found that the average of coder-rated seriousness in "privacy abuse" and "account/device management" was significantly higher than in "security software" and "secure connection" at the 5% level. At the sub-theme level, the coder-rated seriousness of "*how to*"-type questions was higher than that of other types.

The percentage of question posts in which askers offered rewards was relatively higher under the themes of "account/device management" and "security software." We performed a Fisher's exact test to compare the percentage of question posts with rewards across the question themes and found that while the percentage varied moderately across themes, there was no significant difference ($p = .286$). The lower number of question posts in some question themes may have resulted in a lack of statistical power.

4.2.2 Question Sensitivity

The percentage of anonymous posts among all questions was 42.9% (191/445). While this percentage was relatively higher in "account and device management," "secure connection," and "cyberattack," the Fisher's exact test revealed no significant differences in themes ($p = .361$). As with the

test for rewards, the lower number of question posts in some question themes may have resulted in a lack of statistical power. Researchers have treated "privacy abuse" as a highly sensitive topic, but we found that the percentage of anonymous posts in "privacy abuse" was not much higher than that in other themes. Users perceive the incident identification and responses to "cyberattack" as equally or more sensitive than "privacy abuse" because the incidents may expose their personal and sensitive information more broadly. It is also possible that Yahoo! Chiebukuro's pseudonym-registration policy has an effect here, as users can keep their user IDs pseudonymized even if they do not use the anonymous post feature.

5. Discussion

In this section, we discuss the design implications for Q&A sites for non-expert users, how to leverage the Q&A-site analysis to facilitate usable security research, and the limitations.

5.1 Design Implications

We demonstrated that non-expert users post a variety of security- and privacy-related questions on Yahoo! Chiebukuro, which is a general purpose Q&A site. We believe that general Q&A sites should help non-expert users find a solution to their security- and privacy-related concerns by adopting an approach that both "pulls in" professionals and "hands off" to professionals. However, general Q&A sites may have little business motivation to provide such a support mechanism only for a specific category (including security and privacy) of questions. Having subsidies for such services provided by public agencies could be an effective solution. The call for such subsidies would not be limited to security- and privacy-related questions but would extend to various categories of serious questions that require immediate attention, such as urgent medical conditions, severe violence, and life-threatening disasters. Our specific suggestions regarding cyberattacks and user privacy problems are detailed below.

Supporting users coping with cyberattacks. The most frequent theme of questions was "cyberattack." Many non-expert users experienced issues related to incident identification and response. Non-expert users are vulnerable to attack techniques [61], [87]. Web-based knowledge related to basic attack tactics, symptoms, and advice can be utilized to create quick answers. Because of the low quality of anti-phishing advice on most websites (e.g., contradictory or abstract advice, and lack of suitable guidance) [19], the challenge is to create a usable knowledge base made up of consistent, specific, and actionable advice. We also need to understand that it is not always easy for users to find accurate information because many of the threats target users who are anxious and vulnerable. For example, technical-support fraud uses false alerts [88], and fake-removal-advertisement sites exploit malware-infected users' solution search behavior [89]. Therefore, Q&A sites should collaborate with a knowledge base operated by a trusted organization to present users with appropriate information. Further, non-expert users often have difficulty explaining their issues. In our dataset, 16.4% of the question posts had an image file attached, and among them, screenshots were attached without detailed explanation. For Q&A sites to obtain appropriate information from the aforementioned type of knowledge base, first, it is necessary to obtain accurate information about the users' issues. A possible application to support the use of information in the knowledge base is a security version of an "expert system," which asks users for more information that is missing from their question posts and then presents a relevant solution from the knowledge base.

Helping users facing sensitive privacy problems. Users who asked questions as victims of privacy abuse require careful social support because their own privacy has been or could be severely compromised. Although anonymous online spaces provide a supportive environment for discussing potentially stigmatized sensitive topics [90], such spaces are usually created for communities facing similar issues [91]. Users may hesitate to ask questions about their privacy issues on an open and generic Q&A site, as they may become targets of slander. More than half of the questions about privacy abuse stemmed from the need to properly understand whether or not they were under surveillance or had been abused. To get answers to such questions, users have to reveal a certain amount of private information. However, non-expert users may find it difficult to judge what and how much information they should reveal.

Chatbots could be a useful tool for addressing the users' risks of revealing private information on a public platform, as people tend to disclose their stigmatized experiences (e.g., experiences of failure or abuse, symptoms of depression) more actively to virtual agents than to humans [92], [93]. As with security- and privacy-related questions, users may disclose sensitive content (e.g., privacy abuse) to a chatbot because they do not have to worry about slander or their private information spreading. Additionally, using chatbots allows users to exchange messages interactively and incrementally, which means users only need to disclose a sufficient and necessary amount of information for receiving their answers. In answering users' questions, the chatbots themselves can respond in accordance with the aforementioned knowledge base. However, as pointed out by Zou et al. [71], security issues surrounding sensitive topics are complex, and there may be a variety of unsurfaced issues lurking. Therefore, it is also important to provide users with a feature that refers them to professionals for further advice [71], [94].

5.2 Exploring New Research Topics

As previously reported [10]–[13], analyzing questions on a Q&A site for expert users (e.g., Stack Overflow) has helped researchers to better understand the security and privacy

concerns of developers and programmers when developing systems. In this study, we confirmed that analyzing questions on a Q&A site for non-expert users can also allow researchers to understand the security and privacy concerns that such users are facing daily. Furthermore, our analysis of question seriousness suggests that askers who seek answers are likely to use a strategy of either appealing linguistically or offering rewards. This observation implies that researchers who analyze Q&A sites should complementarily incorporate multiple indicators to understand and prioritize the concerns of non-expert users.

Security and privacy concerns change over time as technology and lifestyles change. For example, in our dataset, the problems caused by lifestyle changes owing to COVID-19 include the inability to use Face ID, fear created by conspiracy theories, and issues with VPN settings stemming from the increase in remote work. As an efficient way to explore the usable security and privacy topics for non-expert users that have not yet been addressed, the research community should cultivate a research ecosystem that regularly extracts and clarifies the current user concerns from Q&A sites and works to resolve them. Among the questions obtained from our dataset, we highlight some usable security topics that need to be studied in more depth.

Support for authentication and account management. The second most common theme was "authentication." We found that many users had difficulty receiving security codes for multi-factor authentication because of discarded authenticator devices or having registered with fake email addresses, not just users who failed to log in because of forgetting their credentials. In addition to an in-depth analysis of the reasons users forget to manage their credentials, researchers should further look for secure and usable ways of implementing account recovery. For example, researchers should investigate whether services (especially non-Western services) have provided their contact points and appropriate support for users who encounter authentication errors. Some users were concerned about security and privacy in account management because they did not know how to properly create, delete, and/or link accounts. Future studies should thus cover a greater number of specific situations and diverse users.

Usability issues of security software. Usable security researchers have worked diligently on the various usability issues facing security technologies. However, we showed that many users still do not have a sufficient understanding of information about security technologies, how they work, and the merits of adopting them (see the "Security Software," "Secure Connection," and "Privacy Setting" parts in Sect. 4.1). While some security technologies (e.g., private browsing, Tor, ad-blockers, and firewalls) have been analyzed with respect to user perceptions [7], [95]–[98], we believe that usability issues of security software such as antivirus software and security terminology need to be studied more. In one unique approach, Zhang-Kennedy et al. succeeded in persuading users to update antivirus software by utilizing comic materials [99]. It will be necessary to investigate the usability of the features implemented in actual security software and that of the wording used in them. It will also be important to more extensively explore the user mental models about the effectiveness of the features.

5.3 Limitations

Our study has several limitations, most of which are common to similar types of research.

The first is the demographic bias among the users of Q&A sites. In general, the demographics depend on the type of service. One study that explored the demographics of active askers on Yahoo! Answers indicated that the user group was younger than the average population of web search users [100]. According to another study that explored the advice sources of young adults for digital media use, males with higher Internet skills were significantly more likely to ask questions to strangers on online [9]. Unlike Stack Overflow, which targets expert users (developers and programmers), Yahoo! Chiebukuro targets a wide range of users and is likely to attract many who are not familiar with information technology. Although Yahoo! Chiebukuro has not officially released the statistics of its active users, such demographic biases may also exist in our dataset to some extent.

The second limitation is that we analyzed only a Q&A site provided for a particular language. This means that the only people who ask questions are those who can use the language that the Q&A site supports. For example, we investigated Yahoo! Chiebukuro in this study, which only supports Japanese, and we acknowledge that non-expert users from Japan may have different security and privacy attitudes compared to those from other countries due to differences in cultural factors or security and privacy literacy levels [15], [101]–[104]. However, we believe that our findings identify the potential issues that researchers from other countries also need to resolve because most of the security and privacy technologies and concepts mentioned in our dataset are common to users worldwide.

The third limitation is the lack of profile analysis of the askers. We decided not to conduct such analysis (e.g., exploring the relationships between askers' demographics and question topics) because we found in our preliminary investigation that a non-negligible number of users posted questions anonymously and did not publish their age and gender on their profile pages. In addition, we could not measure the asker's expertise in security and privacy. Although we identified one question post regarding secure coding (classified into "other") and a few question posts containing technical terms (e.g., IPSEC), we considered that almost all of the questions were posted by non-expert users.

Fourth, our metric for question sensitivity (i.e., anonymous posts) may not exactly match askers' perceived sensitivity, although it is a commonly used metric in the literature [42], [43]. Askers tend to post sensitive questions anonymously [42], but not every anonymous post is sensi-

tive; i.e., there may be other reasons askers choose to post anonymously.

Lastly, because of the short sampling period (seven days), we do not claim the generalizability of our results. Instead, as we mentioned in Sect. 5.2, we recommend that the research community establish a research ecosystem that regularly extracts and clarifies the current user concerns from Q&A sites. We have contributed to this endeavor by demonstrating that analyzing Q&A sites for non-expert users can be a useful method for identifying their concerns at any given time.

6. Conclusion and Future Work

Research methodology to understand the concerns of non-expert users related to security and privacy in daily life is becoming increasingly important, as such concerns change over time with the evolution of technology and changes in lifestyles. We conducted an analysis of questions posts on a Q&A site for non-expert users and successfully identified their main concerns about security and privacy. Many users experienced issues related to incident identification and response, appropriate measures after being attacked, and usability of security software. Our analysis of question seriousness suggests that there is a strong demand for answers, especially for questions about privacy abuse and account/device management.

Future work should assess the answers given for the security- and privacy-related questions. We are interested in whether the askers received high-quality answers (i.e., comprehensive, actionable, and effective advice [16]) and whether they were satisfied. In future work, we aim to obtain a deeper understanding of askers and responders so as to design better social support for security and privacy.

References

[1] A.A. Hasegawa, N. Yamashita, T. Mori, D. Inoue, and M. Akiyama, "Understanding non-experts' security- and privacy-related questions on a Q&A site," Proc. 18th Symposium on Usable Privacy and Security, SOUPS'22, 2022.

[2] S. Garfinkel and H.R. Lipford, "Usable security: History, themes, and challenges," Synthesis Lectures on Information Security, Privacy, and Trust, vol.5, no.2, pp.1–124, 2014.

[3] E. Rader and R. Wash, "Identifying patterns in informal sources of security information," J. Cybersecur., vol.1, no.1, pp.121–144, Sept. 2015.

[4] B. Bonné, S.T. Peddinti, I. Bilogrevic, and N. Taft, "Exploring decision making with {Android's} runtime permission dialogs using in-context surveys," Proc. 13th Symposium on Usable Privacy and Security, SOUPS'17, pp.195–210, July 2017.

[5] R.W. Reeder, A.P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman, "An experience sampling study of user reactions to browser warnings in the field," Proc. 2018 CHI Conference on Human Factors in Computing Systems, CHI'18, no.512, pp.1–13, April 2018.

[6] M.A. Sasse and I. Flechais, Usable security: Why do we need it? How do we get it?, O'Reilly, 2005.

[7] P. Story, D. Smullen, Y. Yao, A. Acquisti, L.F. Cranor, N. Sadeh, and F. Schaub, "Awareness, adoption, and misconceptions of web privacy tools," Proc. 21st Privacy Enhancing Technologies Symposium, PETS'21, no.3, pp.308–333, 2021.

[8] J. Tanga, H. Shoemaker, A. Lerner, and E. Birrell, "Defining privacy: How users interpret technical terms in privacy policies," Proc. 21st Privacy Enhancing Technologies Symposium, PETS'21, vol.2021, no.3, pp.70–94, 2021.

[9] M. Micheli, E.M. Redmiles, and E. Hargittai, "Help wanted: Young adults' sources of support for questions about digital media," Information, Communication & Society, vol.23, no.11, pp.1655–1672, 2020.

[10] M. Tahaei, K. Vaniea, and N. Saphra, "Understanding privacy-related questions on Stack Overflow," Proc. 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, pp.1–14, April 2020.

[11] N. Patnaik, J. Hallett, and A. Rashid, "Usability smells: An analysis of developers' struggle with crypto libraries," Proc. 15th Symposium on Usable Privacy and Security, SOUPS'19, pp.245–257, Aug. 2019.

[12] X.L. Yang, D. Lo, X. Xia, Z.Y. Wan, and J.L. Sun, "What security questions do developers ask? A large-scale study of Stack Overflow posts," Comput. Sci. Technol., vol.31, no.5, pp.910–924, Sept. 2016.

[13] T. Lopez, T. Tun, A. Bandara, L. Mark, B. Nuseibeh, and H. Sharp, "An anatomy of security conversations in Stack Overflow," Proc. 41st International Conference on Software Engineering: Software Engineering in Society, ICSE-SEIS'19, 2019.

[14] Yahoo! Japan, "Yahoo! Chiebukuro." https://chiebukuro.yahoo.co.jp/, 2021 (accessed Dec. 28, 2021).

[15] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, "Self-confidence trumps knowledge: A cross-cultural study of security behavior," Proc. 2017 CHI Conference on Human Factors in Computing Systems, CHI'17, pp.2202–2214, May 2017.

[16] E.M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M.L. Mazurek, "A comprehensive quality evaluation of security and privacy advice on the web," Proc. 29th USENIX Security Symposium, SEC'20, Article No.6, pp.89–108, Aug. 2020.

[17] K. Busse, J. Schäfer, and M. Smith, "Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice," Proc. 15th Symposium on Usable Privacy and Security, SOUPS'19, pp.117–136, Aug. 2019.

[18] I. Ion, R. Reeder, and S. Consolvo, """...No one can hack my mind": Comparing expert and non-expert security practices," Proc. 11th Symposium on Usable Privacy and Security, SOUPS'15, pp.327–346, July 2015.

[19] M. Mossano, K. Vaniea, L. Aldag, R. Düzgün, P. Mayer, and M. Volkamer, "Analysis of publicly available anti-phishing webpages: Contradicting information, lack of concrete advice and very narrow attack vector," Proc. 5th European Workshop on Usable Security, EuroUSEC'20, 2020.

[20] L. Neil, E. Bouma-Sims, E. Lafontaine, Y. Acar, and B. Reaves, "Investigating web service account remediation advice," Proc. 17th Symposium on Usable Privacy and Security, SOUPS'21, pp.359–376, 2021.

[21] R.W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," IEEE Security & Privacy, vol.15, no.5, pp.55–64, 2017.

[22] E.M. Redmiles, A.R. Malone, and M.L. Mazurek, "I think they're trying to tell me something: Advice sources and selection for digital security," Proc. 37th IEEE Symposium on Security and Privacy, S&P'16, 2016.

[23] M. Fagan and M.M.H. Khan, "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice," Proc. 12th Symposium on Usable Privacy and Security, SOUPS'16, pp.59–75, June 2016.

[24] E.M. Redmiles, S. Kross, and M.L. Mazurek, "How well do my

results generalize? Comparing security and privacy survey results from mturk, web, and telephone samples," Proc. 40th IEEE Symposium on Security and Privacy, S&P'19, 2019.
[25] E.M. Redmiles, S. Kross, and M.L. Mazurek, "Where is the digital divide?: A survey of security, privacy, and socioeconomics," Proc. 2017 CHI Conference on Human Factors in Computing Systems, CHI'17, pp.931–936, May 2017.
[26] E.M. Redmiles, S. Kross, and M.L. Mazurek, "How I learned to be secure: A census-representative survey of security advice sources and behavior," Proc. 23rd ACM Conference on Computer and Communications Security, CCS'16, pp.666–677, Oct. 2016.
[27] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," Proc. 8th Symposium on Usable Privacy and Security, SOUPS'12, Article No.6, pp.1–17, July 2012.
[28] I. Srba and M. Bielikova, "A comprehensive survey and classification of approaches for community question answering," ACM Trans. Web, vol.10, no.3, pp.1–63, Article No.18, pp.1–63, Aug. 2016.
[29] A. Baltadzhieva and G. Chrupała, "Question quality in community question answering forums: A survey," ACM SIGKDD Explorations Newsletter, vol.17, no.1, pp.8–13, June 2015.
[30] G.Y. Jeon and S.Y. Rieh, "The value of social search: Seeking collective personal experience in social Q&A," Proc. 76th Association for Information Science and Technology Annual Meeting, ASIST'13, vol.50, no.1, pp.1–10, 2013.
[31] G.Y. Jeon and S.Y. Rieh, "Social search behavior in a social Q&A service: Goals, strategies, and outcomes," Proc. 78th Association for Information Science and Technology Annual Meeting, ASIST'15, vol.52, no.1, pp.1–10, 2015.
[32] C. Shah, V. Kitzie, and E. Choi, "Modalities, motivations, and materials–investigating traditional and social online Q&A services," J. Inf. Sci., vol.40, no.5, pp.669–687, May 2014.
[33] K.K. Nam, M.S. Ackerman, and L.A. Adamic, "Questions in, knowledge in?: A study of Naver's question answering community," Proc. 27th International Conference on Human Factors in Computing Systems, CHI'09, 2009.
[34] L. Bowler, J.S. Oh, D. He, E. Mattern, and W. Jeng, "Eating disorder questions in Yahoo! Answers: Information, conversation, or reflection?," Proc. 75th Association for Information Science and Technology Annual Meeting, ASIST'12, vol.49, no.1, pp.1–11, 2012.
[35] S. Oh, Y. Zhang, and M.S. Park, "Cancer information seeking in social question and answer services: Identifying health-related topics in cancer questions on Yahoo! Answers," Information Research, vol.21, no.3, Sept. 2016.
[36] E. Choi, V. Kitzie, and C. Shah, "Developing a typology of online Q&A models and recommending the right model for each question type," Proc. 75th Association for Information Science and Technology Annual Meeting, ASIST'12, vol.49, no.1, pp.1–4, 2012.
[37] L.A. Adamic, J. Zhang, E. Bakshy, and M.S. Ackerman, "Knowledge sharing and Yahoo Answers: everyone knows something," Proc. 17th International Conference on World Wide Web, WWW'08, pp.665–674, April 2008.
[38] F.M. Harper, J. Weinberg, J. Logie, and J.A. Konstan, "Question types in social Q&A sites," First Monday, vol.15, no.7, 2010.
[39] F.M. Harper, D. Moy, and J.A. Konstan, "Facts or friends?: Distinguishing informational and conversational questions in social Q&A sites," Proc. 27th International Conference on Human Factors in Computing Systems, CHI'09, pp.759–768, April 2009.
[40] G. Hsieh and S. Counts, "mimir: A market-based real-time question and answer service," Proc. 27th International Conference on Human Factors in Computing Systems, CHI'09, pp.769–778, April 2009.
[41] Quora Inc., "Quora." https://www.quora.com, 2022 (accessed Jan. 14, 2022).
[42] C. Guo and K. Caine, "Anonymity, user engagement, quality, and trolling on Q&A sites," Proc. 24th ACM Conference on Computer-Supported Cooperative Work and Social Computing, CSCW'21, vol.5, no.CSCW1, Article No.141, pp.1–27, April 2021.
[43] S.T. Peddinti, A. Korolova, E. Bursztein, and G. Sampemane, "Cloak and swagger: Understanding data sensitivity through the lens of user anonymity," Proc. 35th IEEE Symposium on Security and Privacy, S&P'14, 2014.
[44] F.M. Harper, D. Raban, S. Rafaeli, and J.A. Konstan, "Predictors of answer quality in online Q&A sites," Proc. 26th Annual CHI Conference on Human Factors in Computing Systems, CHI'08, pp.865–874, April 2008.
[45] Z. Liu and B.J. Jansen, "Questioner or question: Predicting the response rate in social question and answering on Sina Weibo," Inf. Process. Manage., vol.54, no.2, pp.159–174, March 2018.
[46] Y. Zhao, L. Wu, J. Zhang, and T. Le, "How question characteristics impact answer outcomes on social question-and-answer websites," J. Glob. Inf. Manag., vol.29, no.6, pp.1–21, 2021.
[47] C. Shah, M.L. Radford, L.S. Connaway, E. Choi, and V. Kitzie, "“How much change do you get from 40$?” - Analyzing and addressing failed questions on social Q&A," Proc. 75th Association for Information Science and Technology Annual Meeting, ASIST'12, vol.49, no.1, pp.1–10, 2012.
[48] E. Choi, V. Kitzie, and C. Shah, "A machine learning-based approach to predicting success of questions on social question-answering," Proc. 2013 iConference, iConference'13, 2013.
[49] Stack Exchange Inc., "Stack Overflow." https://stackoverflow.com/, 2022 (accessed Jan. 14, 2022).
[50] Y. Acar, M. Backes, S. Fahl, D. Kim, M.L. Mazurek, and C. Stransky, "You get where you're looking for: The impact of information sources on code security," Proc. 37th IEEE Symposium on Security and Privacy, S&P'16, 2016.
[51] Y. Japan, "Transparency report." https://about.yahoo.co.jp/common/transparencyreport/, 2022 (accessed Jan. 11, 2022).
[52] T. Kudo, "Mecab: Yet another part-of-speech and morphological analyzer." http://taku910.github.io/mecab, 2022 (accessed Jan. 20, 2022).
[53] T. Sato, "mecab-ipadic-neologd : Neologism dictionary for mecab." https://github.com/neologd/mecab-ipadic-neologd, 2022 (accessed Jan. 20, 2022).
[54] C.G. Wilt, "Japanese-English translation." http://cw-translation.net/e/japanese-english-translation-industry-rates-comparison.html, 2022 (accessed Feb. 12, 2022).
[55] V. Braun and V. Clarke, "Using thematic analysis in psychology," Qualitative research in psychology, vol.3, no.2, pp.77–101, 2006.
[56] Y. Japan, "Yahoo! Chiebukuro Help center." https://support.yahoo-net.jp/PccChiebukuro/s/article/H000008128, 2022 (accessed Feb. 12, 2022).
[57] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan, "The menlo report," IEEE Security & Privacy, vol.10, no.2, pp.71–75, March-April 2012.
[58] L. Sugiura, R. Wiles, and C. Pope, "Ethical challenges in online research: Public/private perceptions," Research Ethics, vol.13, no.3-4, pp.184–199, 2017.
[59] L.D. Roberts, "Ethical issues in conducting qualitative research in online communities," Qualitative Research in Psychology, vol.12, no.3, pp.314–325, 2015.
[60] L. Townsend and C. Wallace, "Social media research: A guide to ethics," University of Aberdeen, vol.1, p.16, 2016.
[61] J. Reynolds, D. Kumar, Z. Ma, R. Subramanian, M. Wu, M. Shelton, J. Mason, E. Stark, and M. Bailey, "Measuring identity confusion with uniform resource locators," Proc. 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, pp.1–12, April 2020.
[62] S. Sannon, N.N. Bazarova, and D. Cosley, "Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts," Proc. 2018 CHI Conference on Human Factors in Computing Systems, CHI'18, pp.1–13, April 2018.
[63] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor,

and N. Christin, " "It's not actually that horrible": Exploring adoption of two-factor authentication at a university," Proc. 2018 CHI Conference on Human Factors in Computing Systems, CHI'18, pp.1–11, 2018.

[64] J. Reynolds, N. Samarin, J. Barnes, T. Judd, J. Mason, M. Bailey, and S. Egelman, "Empirical measurement of systemic 2FA usability," Proc. 29th USENIX Security Symposium, SEC'20, Article No.8, pp.127–143, Aug. 2020.

[65] M. Golla, G. Ho, M. Lohmus, M. Pulluri, and E.M. Redmiles, "Driving 2FA adoption at scale: Optimizing two-factor authentication notification design patterns," Proc. 30th USENIX Security Symposium, SEC'21, 2021.

[66] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," Proc. 15th Symposium on Usable Privacy and Security, SOUPS'19, pp.357–37, Aug. 02019.

[67] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart, "The spyware used in intimate partner violence," Proc. 39th IEEE Symposium on Security and Privacy, S&P'18, 2018.

[68] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, " "A stalker's paradise": How intimate partner abusers exploit technology," Proc. 2018 CHI Conference on Human Factors in Computing Systems, CHI'18, pp.1–13, April 2018.

[69] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J.P. Woelfer, M. Shelton, C. Manthorne, E.F. Churchill, and S. Consolvo, "Stories from survivors: Privacy & security practices when coping with intimate partner abuse," Proc. 2017 CHI Conference on Human Factors in Computing Systems, CHI'17, pp.2189–2201, May 2017.

[70] E. Tseng, D. Freed, K. Engel, T. Ristenpart, and N. Dell, "A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during covid-19," Proc. 2021 CHI Conference on Human Factors in Computing Systems, CHI'21, Article No.71, pp.1–17, May 2021.

[71] Y. Zou, A. McDonald, J. Narakornpichit, N. Dell, T. Ristenpart, K. Roundy, F. Schaub, and A. Tamersoy, "The role of computer security customer support in helping survivors of intimate partner violence," Proc. 30th USENIX Security Symposium, SEC'21, pp.429–446, 2021.

[72] P. Kaur, A. Dhir, A. Tandon, E.A. Alzeiby, and A.A. Abohassan, "A systematic literature review on cyberstalking. An analysis of past achievements and future promises," Technological Forecasting and Social Change, vol.163, Feb. 2021.

[73] R.S. Tokunaga and K.S. Aune, "Cyber-defense: A taxonomy of tactics for managing cyberstalking," J. Interpers. Violence, vol.32, no.10, pp.1451–1475, 2017.

[74] A.K. Ghosh, K. Badillo-Urquiola, S. Guha, J.J. LaViola Jr, and P.J. Wisniewski, "Safety vs. surveillance: What children have to say about mobile apps for parental control," Proc. 2018 CHI Conference on Human Factors in Computing Systems, CHI'18, pp.1–14, April 2018.

[75] P. Wisniewski, A.K. Ghosh, H. Xu, M.B. Rosson, and J.M. Carroll, "Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?," Proc. 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing, CSCW'17, pp.51–69, Feb. 2017.

[76] W. Shin and H. Kang, "Adolescents' privacy concerns and information disclosure online: The role of parents and the internet," Comput. Hum. Behav., vol.54, pp.114–123, Jan. 2016.

[77] Y. Song, Y. Huang, Z. Cai, and J.I. Hong, "I'm all eyes and ears: Exploring effective locators for privacy awareness in iot scenarios," Proc. 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, pp.1–13, April 2020.

[78] S. Mare, F. Roesner, and T. Kohno, "Smart devices in Airbnbs: Considering privacy and security for both guests and hosts," Proceedings on the 20th Privacy Enhancing Technologies Symposium, PETS'20, vol.2020, no.2, pp.436–458, 2020.

[79] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L.F. Cranor, N. Sadeh, and F. Schaub, "An empirical analysis of data deletion and opt-out choices on 150 websites," Proc. 15th Symposium on Usable Privacy and Security, SOUPS'19, pp.387–406, Aug. 2019.

[80] A.A. Hasegawa, T. Watanabe, E. Shioji, and M. Akiyama, "I know what you did last login: Inconsistent messages tell existence of a target's account to insiders," Proc. 35th Annual Computer Security Applications Conference, ACSAC'19, pp.732–746, Dec. 2019.

[81] J. Ceci, H. Khan, U. Hengartner, and D. Vogel, "Concerned but ineffective: User perceptions, methods, and challenges when sanitizing old devices for disposal," Proc. 17th Symposium on Usable Privacy and Security, SOUPS'21, pp.455–474, 2021.

[82] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems: A user study of consent dialogs after GDPR," Proc. 20th Privacy Enhancing Technologies Symposium, PETS'20, vol.2020, no.2, pp.481–498, 2020.

[83] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," Proc. 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, pp.1–13, 2020.

[84] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed consent: Studying GDPR consent notices in the field," Proc. 26th ACM Conference on Computer and Communications Security, CCS'19, pp.973–990, Nov. 2019.

[85] Meta, "Help center: How to tell who's seen your instagram story."

[86] R. Hoyle, S. Das, A. Kapadia, A.J. Lee, and K. Vaniea, "Was my message read?: privacy and signaling on facebook messenger," Proc. 2017 CHI Conference on Human Factors in Computing Systems, CHI'17, pp.3838–3842, May 2017.

[87] S. Albakry, K. Vaniea, and M.K. Wolters, "What is this URL's destination? empirical evaluation of users' URL reading," Proc. 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, pp.1–12, April 2020.

[88] N. Miramirkhani, O. Starov, and N. Nikiforakis, "Dial one for scam: A large-scale analysis of technical support scams," Proc. 24th Annual Network and Distributed System Security Symposium, NDSS'17, Feb. 2017.

[89] T. Koide, D. Chiba, M. Akiyama, K. Yoshioka, and T. Matsumoto, "It never rains but it pours: Analyzing and detecting fake removal information advertisement sites," Proc. 17th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA'20, pp.171–191, July 2020.

[90] X. Ma, J. Hancock, and M. Naaman, "Anonymity, intimacy and self-disclosure in social media," Proc. 2016 CHI Conference on Human Factors in Computing Systems, CHI'16, pp.3857–3869, May 2016.

[91] T. Ammari, S. Schoenebeck, and D. Romero, "Self-declared throwaway accounts on reddit: How platform affordances and shared norms enable parenting disclosure and support," Proc. 22nd ACM Conference on Computer-Supported Cooperative Work and Social Computing, CSCW'19, vol.3, no.CSCW, Article No.135, pp.1–30, Nov. 2019.

[92] G.M. Lucas, J. Gratch, A. King, and L.P. Morency, "It's only a computer: Virtual humans increase willingness to disclose," Comput. Hum. Behav., vol.37, pp.94–100, Aug. 2014.

[93] Y.C. Lee, N. Yamashita, Y. Huang, and W. Fu, " "I hear you, I feel you": Encouraging deep self-disclosure through a chatbot," Proc. 2020 CHI Conference on Human Factors in Computing Systems, CHI'20, pp.1–12, April 2020.

[94] Y.C. Lee, N. Yamashita, and Y. Huang, "Exploring the effects of incorporating human experts to deliver journaling guidance through a chatbot," Proc. 24th ACM Conference on Computer-Supported Cooperative Work and Social Computing, CSCW'21, Article No.122, pp.1–27, Article No.122, pp.1–27, April 2021.

[95] A. Mathur, J. Vitak, A. Narayanan, and M. Chetty, "Characterizing the use of browser-based blocking extensions to prevent online

tracking," Proc. 14th Symposium on Usable Privacy and Security, SOUPS'18, pp.103–116, Aug. 2018.
[96] K. Gallagher, S. Patil, and N. Memon, "New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network," Proc. 13th Symposium on Usable Privacy and Security, SOUPS'17, pp.385–398, 2017.
[97] H. Habib, J. Colnago, V. Gopalakrishnan, S. Pearman, J. Thomas, A. Acquisti, N. Christin, and L.F. Cranor, "Away from prying eyes: Analyzing usage and understanding of private browsing," Proc. 14th Symposium on Usable Privacy and Security, SOUPS'18, pp.159–175, Aug. 2018.
[98] A. Voronkov, L.H. Iwaya, L.A. Martucci, and S. Lindskog, "Systematic literature review on usability of firewall configuration," ACM Comput. Surv., vol.50, no.6, Article No. 87, pp.1–35, Dec. 2017.
[99] L. Zhang-Kennedy, S. Chiasson, and R. Biddle, "Stop clicking on "update later": Persuading users they need up-to-date antivirus protection," Proc. 9th International Conference on Persuasive Technology, PERSUASIVE'14, pp.302–322, 2014.
[100] G. Gardelli and I. Weber, "Why do you ask this? Using toolbar data to identify common patterns of Q&A users," Proc. 21st International Conference on World Wide Web, WWW'12, pp.815–822, April 2012.
[101] M. Harbach, A. De Luca, N. Malkin, and S. Egelman, "Keep on lockin' in the free world: A multi-national comparison of smartphone locking," Proc. 2016 CHI Conference on Human Factors in Computing Systems, CHI'16, pp.4823–4827, May 2016.
[102] A.A. Hasegawa, N. Yamashita, M. Akiyama, and T. Mori, "Why they ignore english emails: The challenges of non-native speakers in identifying phishing emails," Proc. 17th Symposium on Usable Privacy and Security, SOUPS'21, 2021.
[103] K. Mori, T. Watanabe, Y. Zhou, A.A. Hasegawa, M. Akiyama, and T. Mori, "Comparative analysis of three language spheres: Are linguistic and cultural differences reflected in password selection habits?," IEICE Trans. Inf. & Syst., vol.103, no.7, pp.1541–1555, July 2020.
[104] M. Mizutani, J. Dorsey, and J.H. Moor, "The internet and japanese conception of privacy," Ethics and Information Technology, vol.6, no.2, pp.121–128, June 2004.

Appendix: Examples of Coder-Rated Seriousness

Table A·1 shows some examples of question posts and the value of coder-rated seriousness reviewed by two coders. These coders manually reviewed the seriousness of each question text using a 5-point Likert scale (1 is not serious; 3 is moderately serious; 5 is very serious), where a serious question can be defined as one that you believe the question asker really wanted an answer for [40].

Table A·1 Examples of question posts and the value of coder-rated seriousness.

Question Texts	Ave.
When I was looking at an adult site, I mistakenly called the number. *I can't sleep because of anxiety.* Will my personal information be leaked due to my call? *I am also worried* that my parents will know about it because I have registered their credit card. *Please help me.*	5.0
URGENT! When I plugged the USB cable connected to my smartphone into the computer that my company owns, the message "Do you want to load images" was displayed. I immediately unplugged it. This doesn't leave any images of my smartphone on the computer, does it? I don't want my images to be leaked. *I'm very anxious.*	5.0
I'm a student. My device is restricted by <security software's name> that my parents set. Is there any way I can unlock it without using my parents' devices? If anyone knows, *please answer*.	4.0
I got this email. This is a fraud email, right?	3.0
In general, are anti-virus apps needed for smartphones?	2.0
Who is making phishing emails that spoof credit card companies?	2.0

Words in italics indicate signals expressed by askers, such as expressions of urgency, anxiety, or a call for help, that would affect the coders' judgement. Note that coders did not rate seriousness based solely on the number of signals but rather did so comprehensively. Questions were originally posted in Japanese.

Ayako A. Hasegawa received her B.S. and M.S. degrees in information science from Ochanomizu University in 2013 and 2015, respectively. She also received her B.S. degree in human science from Musashino University in 2019. She is currently a researcher at NICT. She received the EuroUSEC 2021 Best Paper Award. Her current research interests are mainly on usable security and privacy. She is a member of IPSJ and IEICE.

Mitsuaki Akiyama received his M.E. and Ph.D. in engineering from Nara Institute of Science and Technology in 2007 and 2013. Since joining Nippon Telegraph and Telephone Corporation (NTT) in 2007, he has been engaged in research and development on cybersecurity. He is currently a Senior Distinguished Researcher at NTT Social Informatics Laboratories. He received the Cybersecurity Encouragement Award of the Minister for Internal Affairs and Communications in 2020 and IPSJ/IEEE Computer Society Young Computer Researcher Award in 2022. His research interests include cybersecurity measurement, offensive security, and usable security and privacy. He is a senior member of IPSJ and a member of IEEE, SIGCHI, and IEICE.

Naomi Yamashita is a Distinguished Researcher at NTT Communication Science Laboratories and a visiting professor at Kyoto University. Her current projects focus on the design, development and evaluation of technologies for mindful inclusion in various domains such as global teams and mental healthcare.

Daisuke Inoue received his B.E. and M.E. degrees in electrical and computer engineering and Ph.D. degree in engineering from Yokohama National University in 1998, 2000 and 2003, respectively. He joined Communications Research Laboratory (CRL), in 2003. CRL was relaunched as National Institute of Information and Communications Technology (NICT) in 2004, where he is currently the director general of Cybersecurity Nexus (CYNEX) and the director of Cybersecurity Laboratory. His research interests include practical Cybersecurity technologies, and security visualization. He received several awards including the best paper award at the 2002 Symposium on Cryptography and Information Security, the commendation for science and technology by the minister of MEXT in 2009, the Good Design Award 2013, the Asia-Pacific Information Security Leadership Achievements 2014, the award for contribution to Industry-Academia-Government Collaboration by the minister of MIC in 2016, the Maejima Hisoka Award in 2018, the Distinguished Paper Award at the NDSS 2019, and the 16th information security culture award in 2020.

Tatsuya Mori is currently a professor at Waseda University, Tokyo, Japan. He received B.E. and M.E. degrees in applied physics, and Ph.D. degree in information science from the Waseda University, in 1997, 1999 and 2005, respectively. He joined NTT lab in 1999 and moved to Waseda University in 2013. From Mar 2007 to Mar 2008, he was a visiting researcher at the University of Wisconsin-Madison. He has engaged in the research of network measurement, security, and privacy. He has received many best paper awards including NDSS 2020 and EuroUSEC 2021. Dr. Mori is a member of ACM, IEEE, IEICE, and IPSJ.