Negative Effects of Social Triggers on User Security and Privacy Behaviors

Lachlan Moore, *Waseda University and NICT;*
Tatsuya Mori, *Waseda University, NICT, and RIKEN AIP;* Ayako A. Hasegawa, *NICT*

https://www.usenix.org/conference/soups2024/presentation/moore

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings of the Twentieth Symposium on Usable Privacy and Security is sponsored by USENIX.

Negative Effects of Social Triggers on User Security and Privacy Behaviors

Lachlan Moore
Waseda University / NICT

Tatsuya Mori
Waseda University / NICT / RIKEN AIP

Ayako A. Hasegawa
NICT

Abstract

People make decisions while being influenced by those around them. Previous studies have shown that users often adopt security practices on the basis of advice from others and have proposed collaborative and community-based approaches to enhance user security behaviors. In this paper, we focused on the *negative* effects of social triggers and investigated whether risky user behaviors are socially triggered. We conducted an online survey to understand the triggers for risky user behaviors and the practices of sharing the behaviors. We found that a non-negligible percentage of participants experienced social triggers before engaging in risky behaviors. We also show that socially triggered risky behaviors are more likely to be socially shared, i.e., there are negative chains of risky behaviors. Our findings suggest that more efforts are needed to reduce negative social effects, and we propose specific approaches to accomplish this.

1 Introduction

Human beings are intrinsically social. In the usable privacy and security field, researchers have found plenty of evidence that users are socially influenced when they make security and privacy (S&P) decisions [11, 12, 32, 40, 45, 48, 58]. For example, non-expert users learn lessons from S&P advice and stories from others such as family, friends, and colleagues [11, 45, 48, 49]. In such small social groups, people sometimes both receive and give S&P tech care to each other [31]. Furthermore, users can be influenced not only by people they are close with but also by strangers online. Users sometimes ask strangers for S&P advice on forums and question-and-answer sites [23, 41].

While researchers have focused on and attempted to take advantage of the positive aspects of social effects, we should not turn away from the *negative* aspects. Negative social effects include the possibility that non-expert users may be encouraged by others to engage in risky or insecure behaviors. In the context of teenagers' health, having friends who smoke or drink, and invitations to partake in these activities from friends are the dominant factors to smoking and drinking in teenagers [34]. Does the same kind of negative chain occur in the context of digital S&P risks? Not enough systematic research has been done on the negative aspects of social effects in the S&P decision-making of non-expert users.

A popular model in behavioral psychology suggests that human behavior is a product of motivation, ability, and trigger, and *trigger* is defined as something that prompts action [21]. In 2019, Das et al. showed that social triggers were more common than proactive and forced triggers when it came to users' S&P behaviors [11]. They also showed the potential of positive social chains, where socially triggered S&P behaviors are more likely to be shared with others. In this paper, we expand their work to understand social triggers for *risky* behaviors. We examine whether researchers need to work on reducing the negative aspects of social triggers in addition to activating the positive aspects. Specifically, we address the following research questions:

RQ1 How frequent are the social triggers for *risky* user behaviors?

RQ2 By whom are users triggered to engage in *risky* behaviors?

RQ3 What are the factors of the social triggers for *risky* user behaviors?

RQ4 How often and why do users share their *risky* behaviors with others?

To address these research questions, we conducted an online survey ($N = 417$) in which we asked participants about the practices and contexts of risky behaviors. Specifically,

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

we asked participants to select risky behaviors that they had engaged in over the past 6 months, and we then asked them about the behavioral triggers that preceded their behavior, the person associated with the triggers, and whether they shared their behavior with others. The risky behaviors we asked about were related to passwords, account and update management, internet connections, content downloads, and social media posts. We then analyzed the frequency of the triggers for risky behaviors and practices of sharing the behaviors, as well as whether they vary by individual demographics and type of risky behavior.

We found that participants sometimes engaged in the risky behavior due to social triggers; approximately 20–50% of participants observed others engaging in risky behavior or were advised to do so before engaging in the behavior. For example, of the participants who reported having downloaded illegal or unofficial software/applications and media, 48.7% had observed others doing it. Participants observed risky behaviors not only of friends, family, and colleagues but also of online strangers. We also found that the type of risky behavior significantly affected the likelihood of social triggers (observation of others and/or advice from others). Specifically, account sharing and illegal downloading were more likely to be caused by social triggers than other risky behaviors. Importantly, we showed that participants were more likely to share their risky behavior with others when their behavior had been socially triggered. This means that there are negative chains of risky user behaviors. Users share their risky behaviors primarily because they want others to get a benefit. On the basis of our findings, we propose specific approaches to reducing the negative effects of social triggers. Our recommendations include the interventions for posts on online platforms regarding risky behaviors and security education with emphasis on risky behaviors susceptible to negative social chains and the risks.

This study makes the following contributions.

- In contrast to previous studies, we focused on negative social effects on user security and privacy. We show that users are socially triggered to engage in risky behavior. Our results suggest that more efforts are needed to reduce these effects.
- We identified the factors and sources of social triggers for risky user behaviors and the factors and reasons behind the practices of sharing them. This allowed us to discover clues to reducing the negative social effects and propose specific approaches to reducing them.

2 Related Work

We first review studies that investigated risky or insecure behaviors of non-expert users. Then, we go over studies that focused on the social effects on user S&P behaviors.

2.1 Risky User Behaviors

Contrary to security researchers' and experts' expectations, non-expert users sometimes fail to implement adequate security measures or take risky actions. Ion et al. [26] and Busse et al. [9] found that security practices that experts followed and recommended were not employed by non-expert users. Specifically, many non-expert users did not use a password manager, keep their system up-to-date, or use two-factor authentication. In terms of online data privacy, although concern about data collection and misuse is growing in general [27], most users do not read privacy policies [43], and almost half of internet users share their information publicly [30].

Researchers have studied the reasons why non-expert users engage in risky behaviors, fail to implement security measures, or fail to follow security advice. For example, Milne et al. [42] demonstrated that male, younger users, and users with low self-efficacy were more likely to adopt risky behaviors. Zou et al. found that people who are female, have relatively lower levels of education, and lack prior negative experiences and technical background were less likely to adopt security practices [61]. Additionally, Fagan et al. demonstrated that users who disregard security advice perceived the benefits of compliance and the risks of non-compliance to be lower than those who adhere to the advice [19]. Users abandoned security practices when they were perceived as low-value, inconvenient, or when users overrode them through subjective judgment [61]. Moreover, users have misconceptions about S&P technologies [3, 54, 56], and Abu-Salma et al. suggested that specific misconceptions limit user motivation to adopt secure tools [3].

2.2 Social Effects on User Behaviors

Positive aspects. Studies on sources of security advice have showed that non-expert users take security advice informally from family, friends, and colleagues, as well as from formal sources such as technical support [11, 45, 48, 49]. Rader et al. [48] and Pfeffer et al. [45] found that most users have learned lessons from stories about security incidents informally from family and friends and that these stories impact the way users think about security and their subsequent behavior. Other than people that they are close with, users sometimes ask strangers for S&P advice on forums and question-and-answer sites [23, 41].

In 2019, Das et al. [11] systematically typified the triggers that lead to S&P behavior changes. They revealed that "social triggers," where users interacted with or observed others, were most common, followed by proactive triggers, where users acted absent of an external stimulus, and last by forced triggers, where users were forced to act. They also found that participants were four times more likely to share their own S&P behaviors with others when their behaviors were socially triggered. This result suggests the possibility of a

positive feedback loop.

Kropczynski et al. [31] studied the phenomenon of "Tech Caregiving" among small social groups comprised of friends, family members, and/or colleagues. They found that tech caregiving was a fluid role, where some users both gave and received tech care, and older adults and emerging adults tended to be caregivees rather than caregivers.

Note that a digital divide of security advice exists. Specifically, Redmiles et al. found that while higher skilled users, who tend to be socioeconomically advantaged, were significantly more likely to take advice from their workplace, those who were less skilled tended to take advice from family and friends [49].

On the basis of the above interactions among users, some researchers have proposed collaborative and community-based approaches to enhance user S&P behaviors [12, 18, 32, 36, 40, 58]. For example, Das et al. confirmed the effectiveness of social-proof based interventions that encourage users to incline to explore security features by showing them that their friends use security features [12]. Krsek et al. [32] demonstrated that participants who were shown suggested S&P settings from experts and the public were significantly more likely to adhere to those suggested settings than those who saw the default Facebook settings. They did not observe a significant difference in the effectiveness of social suggestions from experts and the public. Wash and Cooper [58] conducted a field experiment involving phishing training that incorporated social stories. They demonstrated that traditional facts-and-advice are more effective when provided by security experts, but stories are more effective when told by people perceived as "like me."

Negative aspects. While usable privacy and security researchers have focused on the positive aspects of social effects, relatively few studies have focused on the negative aspects. Several researchers have discussed the potential of these aspects [13, 60]. For example, Das et al. suggested that social proof may have a negative effect on the adoption of security features for users with only a few friends who adopt the features [13]. Recently, Rader [47] featured a norm-based phenomenon called pluralistic ignorance where people engage in a behavior that they privately do not believe in or approve of because they believe that everyone else approves of it. In addition, Rader showed that social expectations influence user choices to use potentially privacy-invasive technologies. This suggests that sharing information about others' behavior is likely to backfire in a pluralistic ignorance situation.

Other researchers have analyzed risky and insecure advice on social media [4, 8, 59]. For example, Akgul et al. analyzed VPN ad videos on YouTube and found that these videos include vague and potentially misleading statements about the capabilities of VPNs and internet threats [4]. Despite the prevalence of risky and insecure advice on social media, the extent to which users who see it adopt it has not been sufficiently investigated.

In this study, we also focus on the *negative* aspects of social effects. In particular, by incorporating our concerns with these aspects into the methodology of the study by Das et al. [11] that systematically investigated the social triggers for S&P behaviors (i.e., the positive aspects), we systematically investigate the social triggers for *risky* user behaviors (i.e., the negative effects).

3 Methodology

We conducted an online survey to quantitatively and systematically investigate the impact of social triggers for *risky* behaviors. We explain the survey design, recruitment, participants, ethics, and limitations.

3.1 Survey Design

We arranged Das et al.'s questionnaire [11] that investigated triggers for user S&P behaviors to understand triggers for *risky* user behaviors. Our questionnaire consisted of six parts: instruction, risky behavior practices, behavioral triggers, sharing practices, risky behaviors of others, and demographics. The full questionnaire is provided in Appendix A.

Part–1: Instruction. At the beginning, we explained to participants the study purpose, the compensation amount and expected time for completion, and how their data would be handled. Only those who agreed to participate proceeded to the survey. Since our study focused on risky user behaviors, we needed to reduce social desirability bias. We followed the approach of previous work [50] that investigated user lies for protecting their privacy (called "privacy lies"), which can be expected to be influenced by social desirability bias as well as risky user behaviors. Specifically, we told participants that we did not consider engaging in risky behaviors to be bad or uncommon and that we were interested in them as researchers. We then asked participants to answer honestly and accurately.

Part–2: Risky Behavior Practices. First, we asked participants which of the following six behaviors they did in the past 6 months (if any):

- Connecting to an unknown, potentially unsecured public Wi-Fi and then engaging in sensitive data exchanges, such as transmitting credit card or password details through this connection,
- Reusing the same or similar passwords for different accounts,
- Downloading illegal or unofficial software/applications and media (e.g., videos, music, and games),
- Ignoring or delaying software/application updates,

- Sharing sensitive personal information online (e.g., location-based information, real-time activities, and pictures of yourself/others) to strangers on social media,
- Sharing accounts with family, friends or others.

We selected these risky behaviors on the basis of the previous work we reviewed in Section 2.1 and our discussions. Specifically, we selected risky behaviors that could occur on a daily basis and that could apply to all users, regardless of the device they own or the service they use. While these behaviors *potentially* expose users to S&P harms and are considered representative of risky behaviors that are expected to be prevalent among users, it is important to note that these risky behaviors do *not always* pose an S&P threat to users. The riskiness of each behavior is described below.

- Connecting to public Wi-Fi poses significant risks due to the potential for sensitive personal information to be collected and leaked [5]. Unsecured networks can be exploited by attackers through man-in-the-middle attacks or malware distribution. However, these risks can be mitigated by using a VPN or accessing the network through a virtual machine.
- Reusing passwords across multiple accounts increases vulnerability to cross-site password guessing attacks [10], potentially granting attackers access to sensitive information. However, this risk is minimized when password reuse is limited to inconsequential "throwaway" accounts with no sensitive data.
- Downloading illegal or unofficial software, applications, and media often introduces malware, viruses, or spyware that can compromise device security and functionality, and it may also result in legal penalties. However, these risks can be mitigated by using virtual machines or sandboxes and by downloading from reputable open-source communities or platforms.
- Neglecting or delaying software updates enables attackers to exploit known vulnerabilities [37]. While not all updates enhance security (e.g., UI updates), many do address newly discovered vulnerabilities. Additionally, vendors sometimes provide insufficient explanations in their release notes (e.g., fixing a vulnerability without explicitly stating it) [15]. Therefore, delayed updates can result in security risks, such as information leakage.
- Sharing personal information online can lead to harassment, stalking, identity theft, and physical crimes if it reveals that the user is not home [28,46]. However, these risks are reduced when information is shared within trusted groups and privacy settings are properly configured on social media.
- Sharing accounts with family, friends, or others increases the risk of compromised security due to poor practices by other users [39]. However, some platforms mitigate this risk by offering features such as one-time login passwords, eliminating the need to share permanent credentials.

Part–3: Behavioral triggers. For each risky behavior that participants reported engaging in, we next asked them to select the event that preceded their behavior (if any). The options were "I observed/heard about other people doing this," "Other people advised to do this," "My organization required me to do this," "Other (please specify)," and "Nothing in particular happened." Although participants could select more than one option, we considered only "Nothing in particular happened" to be an exclusive option (i.e., they could not select this option and other options at the same time).

We selected the above 5 options that can be applied to triggers for risky behaviors from the 13 options of Das et al.'s study [11] (i.e., triggers for S&P behaviors). We categorized the triggers into three higher level categories of triggers: social ("I observed/heard about other people ..." and "Other people advised ..."), organizational ("My organization required me ..."), and voluntary ("Nothing in particular happened"). Some participants selected "other" and provided text, all of which was related to voluntary decisions, such as decision-making for convenience, and was not related to social and organizational triggers. Therefore, we counted these as voluntary triggers.

If participants selected social triggers, we asked the participants about their relationship to the person whose risky behavior they had observed/heard about or who had advised them. The options included friend, family, colleague, online stranger, and media. If participants received advice from others, we also asked them if the person told them about the risks of the behavior.

Part–4: Sharing practices. For each reported risky behavior, we asked participants whether they shared their behavior with others. If they did share, we asked them to specify with whom (friend, family, colleague, online discussion, and/or other) and why. The options for the reasons for sharing include "I wanted them to get the benefits" and "I wanted them to know that I have knowledge." Participants could select multiple relationships and reasons. We also asked participants who did not share their behaviors why.

Part–5: Risky behaviors of others. We also asked participants about what percentage of the public they thought engaged in each behavior. Participants could specify a number from 0 to 100 using a slider bar.

Part–6: Security attitudes and demographics. While Das et al. [11] modeled user S&P behaviors using SeBIS (the security behavioral intention scale) [16], we adopted SA-6 (the security attitude scale) [20], which was proposed after SeBIS. We believe that attitudinal indicators are more appropriate than behavioral intention indicators for modeling

risky user behaviors. We then asked a series of demographic questions redarding their age, identified gender, education, IT knowledge, and country of residence. We included a simple attention check (a check that does not contain a trap question but simply specifies the option that participants must select) in the middle of the questionnaire.

At the end of the survey, we asked participants if they answered honestly, following the previous studies [7, 35]. We told participants that they would not be penalized/rejected if they indicated dishonesty.

3.2 Recruitment and Participants

We recruited participants through Prolific in January 2024. We advertised our survey as "a study on online behaviors" without using S&P-related terms to avoid self-selection bias related to S&P on the task-list screen. Participants were required to reside in the U.S. and be 18 or older. We used Prolific's representative-sample tool to increase the diversity of our participants. Prolific's representative sample provides a balanced sample in terms of gender, age, and ethnicity based on U.S. Census data. Prior to main data collection, we conducted pilot surveys with 31 Prolific workers to evaluate our survey design and estimate the time required for completion.

We excluded 29 participants who failed the attention check, completed the survey in less than 90 seconds, selected "no" to the honesty-check question, and/or provided incoherent responses. We finally obtained a total of 417 valid survey responses. Participants who completed the survey were compensated with $1.75, and the median completion time was 314 seconds ($20.1/hour; this amount is sufficiently higher than the U.S. minimum wage).

Table 1 shows the demographics of our participants (N = 417). Our participants were 18 to 83 years old (mean 45.5, SD 15.6), 51.3% of them identified as female, and 1.9% selected "non-binary/third gender" or "prefer not to say." In terms of knowledge in IT or related fields, 55.9% rated themselves as "strongly agree" or "somewhat agree" and 19.4% as "neither agree nor disagree." Figure 1 indicates the distribution of the SA-6 score of our participants. The mean score was 20.2 (SD 5.1).

3.3 Ethical Considerations

We carefully designed our survey design, and it was approved by the Institutional Review Board (IRB). Except for the Prolific IDs, which were necessary for compensating the participants, we did not collect any personally identifiable information. We handled all data confidentially. Participants could drop out at any time. All participants who completed the survey were compensated regardless of the quality of their response.

Table 1: Participant demographics (N = 417).

		N	%
Age	18–29	92	22.1%
	30–39	69	16.5%
	40–49	71	17.0%
	50–59	81	19.4%
	60–69	86	20.6%
	70+	18	4.3%
Gender	Male	195	46.8%
	Female	214	51.3%
	Other / Prefer not to say	8	1.9%
Education	High school	131	31.4%
	College	51	12.2%
	Undergraduate	150	36.0%
	Post-graduate	76	18.2%
	Other / Prefer not to say	9	2.2%
IT knowledge	Yes*	233	55.9%
	No	184	44.1%

*For simplicity, we show the percentage of participants who selected "strongly agree" or "somewhat agree" on a 5-point Likert scale in this table.

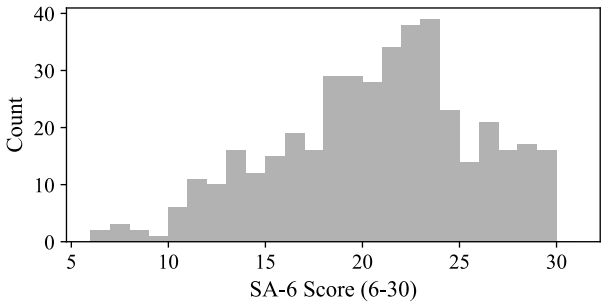

Figure 1: Distribution of SA-6 score of our participants.

3.4 Limitations

Measurement of behavioral triggers. Our study has several limitations in common with Das et al.'s study [11] in investigating behavioral triggers. In the same way as their study, we asked participants what happened before they engaged in the behavior, rather than what triggers influenced their behavior. We focused on the triggers that users perceived in the moment. Other long-term triggers, such as social norms and cultural attitudes, may influence users. Additionally, although multiple triggers may affect users, we did not ask participants which one affected them the most in consideration of recall bias. Therefore, it was not possible to quantify the strength of the impact of each trigger. Furthermore, we analyzed participants' self-reported behaviors and triggers.

Measurement of triggers for *risky* behaviors. Our study also has unique limitations in terms of measuring the behavioral triggers for *risky* behaviors. First, risky behaviors are

considered to be heavily influenced by personal motivations (e.g., the desire to take the easy way out and the desire to watch illegal content), and it is not easy to encompass the behavioral triggers that lead to risky behaviors. In fact, we initially conducted a pilot survey to typify behavioral triggers for risky behaviors, but most of the responses were about such personal motivations. Therefore, as a first step, we focused on understanding the prevalence of the two key social triggers (observations of others and advice from others) rather than on encompassing and typifying the triggers. Future work should explore a variety of behavioral triggers for risky behaviors through observation and in-depth interviews. Additionally, we asked participants about the representative risky behaviors that would be expected to be prevalent among users. It is important to note that the risky behaviors we asked about do not always pose a security and privacy threat to users. In the future, we need to explore the triggers according to the risk levels of risky behaviors.

Second, people may generally be reluctant to report that they have engaged in risky behaviors, and thus, responses are subject to social desirability bias. To reduce this bias, we told the participants at the beginning of the survey that we did not consider engaging in risky behaviors to be bad or uncommon and requested honest and accurate responses.

Recruitment of participants. Because Prolific workers have more technology knowledge than the general U.S. population [2, 55], the percentage of users who engage in risky behavior may be higher than the results of this study.

While Das et. al [11] recruited participants mainly from the U.S. and India and found cultural differences (people from India were significant more likely to report social triggers for S&P behaviors), we decided to recruit participants only in the U.S. We initially considered conducting this study in Japan, which has the lowest SeBIS score [51]. We recruited Japanese participants through Lancers [33], a popular crowdsourcing platform in Japan. We found that the percentage of Japanese participants who reported engaging in risky behavior was much lower than that of the U.S. participants (e.g., public Wi-Fi: 3.2% in Japan, 16.3% in the U.S.). Because Lancers, unlike Prolific, is not academic-specific and is used for a variety of tasks including data analysis, it might have more technically skilled workers than Prolific. Researchers can reach Indian workers through MTurk, but the data quality is generally lower than Prolific [38, 55]. Another reason we did not compare the U.S. to other countries is that the U.S. has been treated as an individualistic country in the past, but the most recent Hofstede's individualism score of the U.S. is much lower than it used to be (from 91 to 60, updated in October 2023) [24]. In the future, we will need to compare a country with a much higher individualism score than the U.S. with a country with a much lower score.

4 Results

We present the survey results to address our research questions: the frequency of social triggers for the risky behaviors (RQ1), the source of social triggers (RQ2), the factors of the social triggers (RQ3), and user practices in sharing the risky behaviors (RQ4).

4.1 RQ1: Frequency of Social Triggers

Table 2 shows the percentage of participants who engaged in each risky behavior and the frequency of behavioral triggers that led to each behavior.

Risky behaviors. The frequently reported risky behaviors were password reuse and delayed update, with 71.2% (297/417) of our participants reporting having reused the same or similar passwords and 61.2% (255/417) reporting having ignored or delayed software/application updates in the 6 months preceding the survey. Additionally, 32.4% (135/417) reported having shared an account with others, 18.2% (76/417) reported having downloaded illegal or unofficial content, 18.2% (76/417) reported having shared their sensitive personal information online, and 16.3% (68/417) reported having connected to public Wi-Fi. Overall, 90.9% (379/417) of our participants reported having engaged in at least one of the six risky behaviors. This result suggests that risky behaviors are common among users and that S&P researchers should work to reduce such user practices.

Behavioral triggers. As shown in Table 2, 23.8% of the participants had observed/heard about others engaging in risky behavior before engaging in the behavior on average. On the other hand, fewer participants had experienced advice from others or coercion from an organization; 6.8% had been advised and 3.4% had been required to engage in risky behavior. The majority (70.0%) of the participants had not experienced any of the three triggers above.

We found that the frequency of the triggers, especially social vs. voluntary triggers, varied depending on the type of risky behaviors. While many participants had voluntarily reused passwords and delayed updates, about half of participants observed others or received advice from others who downloaded illegal content and shared accounts. We explain statistical differences in the frequency of social triggers among risky behaviors in Section 4.3.

Although the majority of participants engaged in risky behaviors solely of their own volition, we cannot ignore the fact that about one third of participants were influenced by social triggers to reduce risky user behaviors. We cannot measure which of the user voluntary volition or social triggers had a greater impact on participants' decisions to engage in risky behaviors as discussed in Section 3.4, but the approach of reducing negative social effects could be helpful in reducing risky user behaviors.

Table 2: Frequency of behavioral triggers for risky behaviors.

Behavioral triggers		Public Wi-Fi	Pwd Reuse	Illegal DL	Delayed Update	Sensitive Post	Account Sharing	All
		N=68 (16.3%)	*N*=297 (71.2%)	*N*=76 (18.2%)	*N*=255 (61.2%)	*N*=76 (18.2%)	*N*=135 (32.4%)	
Social	Observation	33.8%	17.5%	48.7%	14.1%	26.3%	35.6%	23.8%
	Advice	4.4%	1.3%	13.2%	5.5%	10.5%	17.0%	6.8%
Organizational		8.8%	3.0%	1.3%	2.7%	6.6%	2.2%	3.4%
Voluntary		61.8%	79.8%	47.4%	78.8%	63.2%	52.6%	70.0%

We show the percentage of the participants who had experienced each trigger (observation of others' behavior, advice from others, or organizational enforcement) among the participants who reported having engaged in each risky behavior. Participants could select more than one trigger. Therefore, the sum of each column exceeds 100%. On the other hand, a voluntary trigger means the participant had not experienced any of the three triggers above (i.e., an exclusive option).

Table 3: Person engaging in risky behaviors that participants had observed/heard about.

	Public Wi-Fi (*N*=23)	Pwd Reuse (*N*=52)	Illegal DL (*N*=37)	Delayed Update (*N*=36)	Sensitive Post (*N*=20)	Account Sharing (*N*=48)	All
Friend	**65.2%**	**65.4%**	**70.3%**	47.2%	**80.0%**	**64.6%**	**64.4%**
Family	39.1%	**55.8%**	16.2%	38.9%	**55.0%**	**77.1%**	49.1%
Stranger/Online posts	30.4%	34.6%	**67.6%**	36.1%	40.0%	25.0%	38.4%
Colleague	**52.2%**	26.9%	18.9%	27.8%	20.0%	20.8%	26.4%
Media (e.g., news and TV programs)	21.7%	13.5%	10.8%	11.1%	15.0%	12.5%	13.4%
Influencer	13.0%	5.8%	10.8%	8.3%	25.0%	8.3%	10.2%
Teacher/Mentor	4.3%	3.8%	2.7%	0.0%	5.0%	4.2%	3.2%

The first row shows the number of the participants who had observed others engaging in each risky behavior before engaging in the behavior. The sum of the percentages for each behavior exceeds 100% because the participants could select more than one type of relationship. Bold numbers highlight items greater than 50%.

4.2 RQ2: Source of Social Triggers

Existing studies have showed that non-expert users have various sources of security advice, such as family, friends, colleagues, and technical support [11, 45, 48, 49]. We were interested in from whom users learn about *risky* behaviors.

Table 3 shows the person engaging in risky behaviors that participants had observed/heard about. For the five risky behaviors other than delayed update, more than 60% of participants had observed/heard about their friend engaging in the behavior. In particular, 80.0% of participants had observed/heard about their friend sharing sensitive personal information online to strangers on social media. Family was the second most common, with an average of about half (49.1%) of participants having observed/heard about risky behaviors of their family members and especially 77.1% having observed/heard about account sharing.

We found that participants had observed/heard about the risky behaviors of online strangers relatively frequently. In particular, 67.6% of participants had encountered strangers downloading illegal or unofficial content. The result indicates that the social triggers for risky behaviors occur both offline and online.

More than half (52.2%) of participants had seen or heard about their colleague connecting to public Wi-Fi. Some participants had observed/heard about risky behaviors from media (e.g., news websites and TV programs) and influencers, while few participants had observed/heard about teachers or mentors.

We show who advised the participants to engage in risky behaviors in Table 9 of Appendix B. Please note that the number of others advising the participants was less than the number of others being observed by the participants.

We were interested in whether the person by whom users are triggered differs by user demographics. Table 4 shows which relationships led to socially-triggered risky behaviors by participant demographics. We performed Fisher's exact tests to test whether the proportions differed by user group (p-values were adjusted using the Bonferroni method). We found that, for friends, family, and colleagues, there were no significant differences in the proportions across user groups. On the other hand, there were significant differences in the proportion of risky behaviors triggered by online strangers across the age groups of the participants. Specifically, younger participants' socially-triggered risky behaviors were more likely to be triggered by online strangers ($p < 0.001$ for the 18–34 age group (45.3%) vs. the 60+ age group (13.3%);

Table 4: Relationships between participant demographics and those who influenced them.

		Friend	Family	Stranger	Colleague
Age	18–34	71.6%	50.5%	**45.3%**	30.5%
	35–59	51.6%	42.2%	**39.1%**	23.4%
	≥ 60	64.4%	57.8%	**13.3%**	24.4%
Male		62.9%	47.4%	37.9%	31.9%
Female		64.8%	52.3%	34.1%	20.5%
SA-6	6–14	60.9%	52.2%	52.2%	13.0%
	15–24	63.2%	54.4%	36.0%	28.8%
	25–30	66.1%	37.5%	30.4%	28.6%

We show the proportions of risky behaviors triggered by a particular relationship to those triggered by others for each user group. Note that this does not show how each user group relates to the likelihood of risky behaviors or the likelihood of social triggers (which we show in Table 5). Bold text indicates that there was a significant difference in the proportions.

Table 5: Logistic regressions for risky behaviors and social triggers (coefficients and p-values).

	Social Triggers		Risky Behaviors	
Age	−0.001		−0.050	***
Male (vs. Female)	0.334		0.420	*
SA-6	0.068	*	−0.099	***
DL (vs. Pwd)	2.503	***		
Account (vs. Pwd)	2.139	***		
Update (vs. DL)	−2.424	***		
Account (vs. Update)	2.060	***		

The middle column shows the results of a logistic regression explaining whether social triggers had occurred before participants engaged in risky behaviors. Of the fifteen pairwise comparisons of risky behaviors, only those pairs with a significant difference are shown in this table. The right column shows the results of an ordinal logistic regression explaining the number of risky behaviors reported by participants. Significance levels: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$.

p =0.014 for the 35–59 age group (39.1%) vs. the 60+ age group (13.3%)). Given that young people generally spend more time online [53], it is perhaps not surprising that they are more likely to observe risky behaviors of online strangers.

4.3 RQ3: Factors of Social Triggers

To understand the factors of social triggers for risky user behaviors, we performed a logistic regression. Specifically, we modeled how likely a participant would be to report a social trigger given their age, gender, SA-6, and the type of risky behavior they reported having engaged in. We used random intercepts for each participant to consider repeated observations. We calculated fifteen pairwise comparisons between the six different risky behaviors using R's multcomp package [25]. We corrected the significance levels due to the multiple comparisons using the Bonferroni method [1]. In addition, we ran an ordinal logistic regression to understand the demographics of users who are generally more likely to engage in risky behaviors, regardless of the trigger type. The dependent variable was the number of risky behaviors that a participant reported engaging in. Table 5 shows the results of the two logistic regressions. A positive coefficient implies that the independent variable has a positive effect on the dependent variable, while a negative coefficient implies the opposite. Coefficients imply the expected change in log odds of having the outcome per unit change in the independent variable. More specifically, the odds ratio (OR) indicates the change in the odds of the outcome (e.g., odds of how likely participants report a social trigger) for a 1-unit increase in the continuous independent variable (e.g., 1-score increase of participants' SA-6) or compared with a reference categorical independent variable (e.g., male participants compared with female participants).

Individual demographics. We found that while individual demographics were significantly correlated with risky behaviors, they were less correlated with whether the risky behaviors were socially triggered.

In terms of age and gender, younger participants were significantly more likely to engage in the risky behaviors we examined in this study ($coeff = -0.050$, $OR = 0.951$, $p < 0.001$) and male participants were significantly more likely to engage in the risky behaviors ($coeff = 0.420$, $OR = 1.522$, $p = 0.020$). These results are consistent with the study by Milne et al. [42], which concluded that younger and male online shoppers in the U.S. were more likely to adopt risky behaviors. On the other hand, we found no significant correlations between age and the likelihood of social triggers ($coeff = -0.001$, $OR = 0.999$, $p = 0.917$) and between gender and the likelihood of social triggers ($coeff = 0.334$, $OR = 1.396$, $p = 0.292$). Das et al. [11] found that younger people were more likely to report social triggers for S&P behaviors, but gender was not correlated with this, and then suggested that some level of age-based personalization may be needed to trigger user S&P behaviors. Such age-based personalization may be effective in socially promoting S&P behaviors but may be less effective in reducing socially triggered risky behaviors.

In terms of security attitude (SA-6), we found that participants with a lower SA-6 score were significantly more likely to engage in the risky behaviors we examined in this study ($coeff = -0.099$, $OR = 0.906$, $p < 0.001$), which is consistent with our intuition. On the other hand, participants with a higher SA-6 score were significantly more likely to report social triggers ($coeff = 0.068$, $OR = 1.071$, $p = 0.030$). It may be possible that users with high security attitudes are less likely to engage in risky behaviors for voluntary motivations such as convenience, but they may think it would be okay to engage in the behaviors if they observe others engaging in them. Note, however, that we did not collect the data to conclude that users with high security attitudes had not observed

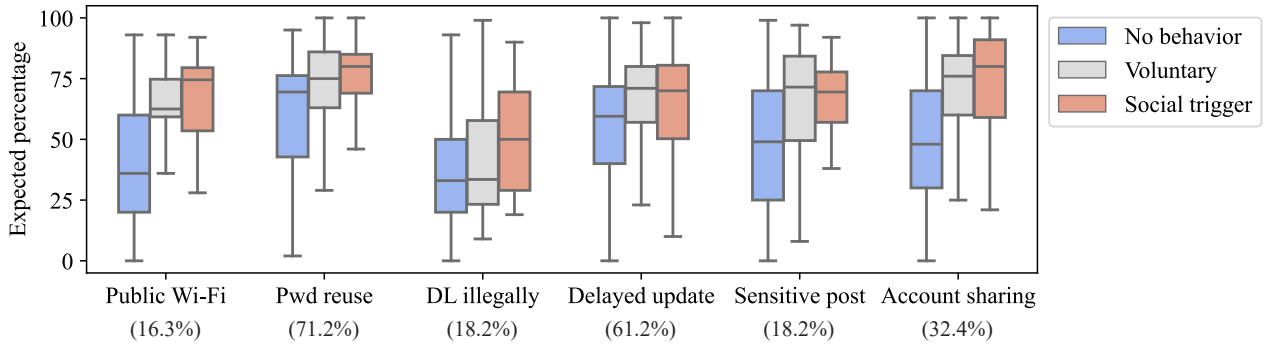

Figure 2: Expected percentages of public engaging in risky behavior.
The numbers in parentheses indicate the percentage of the participants who reported engaging in the behavior.

risky behaviors of others when they decided not to engage in the behaviors, and thus, we need further investigation.

Risky behaviors. In contrast to individual demographics, the type of risky behaviors was significantly correlated with whether the risky behaviors were socially triggered, i.e., several risky behaviors were more likely to be socially triggered. Our regression analysis revealed significant differences across risky behaviors controlling for age, gender, and SA-6, as shown in Table 5. Of the fifteen pairwise of comparisons of risky behaviors, we found significant differences in four as follows. Illegal downloading was significantly more likely to have reported social triggers than password reuse ($coeff$ = 2.503, OR = 12.221, $p < 0.001$). Delayed update was significantly less likely to have reported social triggers than illegal downloading ($coeff$ = −2.424, OR = 0.089, $p < 0.001$). Account sharing was significantly more likely to have reported social triggers than password reuse ($coeff$ = 2.139, OR = 8.493, $p < 0.001$) and delayed update ($coeff$ = 2.060, OR = 7.843, $p < 0.001$). In summary, illegal downloading and account sharing are more likely to be socially triggered, as opposed to password reuse and delayed update.

Risk information. We asked participants having engaged in risky behaviors due to advice from others whether they had been told about the risks of the behavior by the person. We found that they were not always told about the risks; of the reported risky behaviors that were triggered by advice from others, 59.6% of the behaviors occurred when the participants had not been told about the risks.

Expected risky behaviors of others. We were also interested in what the participants who had engaged in the risky behavior, especially those who had experienced social triggers (i.e., observations of others or advice from others), expected the percentage of the public who engaged in risky behavior to be. This could provide insights into how users generalize that they have observed risky behaviors of their friends and family and how they generalize their own risky behavior. Note that our data would only show correlation, not causation, i.e., we cannot conclude that users engage in risky behaviors as a result of their expectations that most of the public engage in the behaviors.

Figure 2 shows box plots indicating the expected percentage of the public who engage in each risky behavior among three groups: the participants who did not engage in the behavior, those who voluntarily engaged in the behavior, and those who experienced social triggers. Due to the non-normal distribution, we compared the three groups by using Kruskal-Wallis tests and then compared each pair by using post-hoc Steel-Dwass tests. The significance levels were corrected using the Bonferroni method for multiple comparisons [1]. For all risky behaviors, the median of the no-behavior group was lower than that of the other two groups, and the differences were significant for all pairs except for the voluntary group for illegal downloading. In other words, those who engaged in risky behaviors tended to expect more of the public to engage in the behavior than those who did not. On the other hand, there was no significant difference between the voluntary and social-trigger groups, possibly due to the small sample size of the social-trigger group. This does not mean differences do not exist but rather that they might be too slight to detect at smaller sample sizes. When considering the medians instead of just p-values, we found that the social-trigger group had a higher median than the voluntary group for 4 out of the 6 risky behaviors.

We also found that all of the medians of the expected percentages were higher than the percentage of our participants who reported engaging in the risky behaviors (e.g., 16.3% of our participants connected to public Wi-Fi), except for the non-behavior group for illegal downloading. This may be somewhat natural given that participants from Prolific have more technology knowledge than the general U.S. population [2, 55]

The fact that users engaging in risky behaviors tend to expect more of the public to engage in the behaviors may contribute to the users continuing practices of the risky behaviors, even if the expectation may not be their initial motivation.

Table 6: Participants' sharing practices and person with whom they shared.

	Public Wi-Fi (*N*=68)	Pwd Reuse (*N*=297)	Illegal DL (*N*=76)	Delayed Update (*N*=255)	Sensitive Post (*N*=76)	Account Sharing (*N*=135)	All
Overall shared	26.5%	24.2%	52.6%	27.2%	46.1%	80.7%	37.8%
Family	**55.6%**	**70.8%**	40.0%	**53.6%**	48.6%	**86.2%**	**65.6%**
Friend	50.0%	45.8%	**77.5%**	39.1%	**51.4%**	47.7%	49.6%
Colleague	38.9%	6.9%	5.0%	21.7%	11.4%	7.3%	12.0%
Online discussion	11.1%	2.8%	10.0%	11.6%	28.6%	1.8%	8.2%

The first row indicates the number of participants who reported engaging in each risky behavior, and the second row indicates the percentage of participants who shared the behavior with others among those who reported engaging in the behavior. The third and subsequent rows indicate the percentage of participants who shared the risky behavior with a specific person among those who shared the behavior. The sum of the percentages for each behavior exceeds 100% because the participants could select more than one type of relationship. Bold numbers highlight items greater than 50%.

Therefore, efforts to change user expectations that most of the public engages in risky behaviors may be promising.

4.4 RQ4: Sharing Practices

Frequency of sharing. Das et al. [11] found that 32% of S&P behaviors were shared with others. This suggests a promising phenomenon of stories about S&P practices being widespread among users. We show the frequency of sharing *risky* behaviors in Table 6. On average, 37.8% of risky behaviors were shared with others, although the frequency of sharing varied considerably by behavior type (see Table 8 for the regression analysis). This means that stories about risky behaviors are spreading among users as much or more than stories about S&P practices.

Table 6 also shows the person with whom participants shared their risky behaviors. Just as participants often observed their friends and family members engaging in risky behaviors (as shown in Table 3), they often shared their risky behaviors with family and friends. On the other hand, it is interesting to note that while participants often observed online strangers engaging in risky behaviors, they seldom shared their risky behaviors with strangers on online discussion sites. This asymmetry suggests a large impact relative to the number of people sharing risky behaviors online, i.e., one person's post about risky behaviors could be seen by many users.

Reasons for sharing. Table 7 shows the reasons why participants shared their risky behaviors with others. The most common reason was "I wanted them to get the benefits." Naturally, users do not share their risky behaviors with others for malicious purposes; rather, they simply want others to get the benefits, such as convenience. The second most common reason was "I just wanted to talk about my recent behavior," which Das et al. [11] found to be the most common reason for sharing S&P behaviors. The third most common reason, "I wanted them to know about other options, regardless of risk," also indicates that the participants valued other objectives, such as convenience, more than the risk of the behavior. The participants who selected "They noticed my change" may not have initially had a clear intention to share their risky behaviors.

The reasons given by participants in open-ended form as "other" include "to share a complaint" (e.g., a participant answered "I complained that I am sick of these forced <OS name> updates so frequently so I put them off") and "Others confided in me first" (e.g., "They told me they do this").

We also asked participants who reported engaging in risky behaviors but did not share their behaviors about their reasons for doing so. The primary reasons were "I just didn't want to talk about this with anyone" (54.3%) and "I assumed everyone did this" (33.3%).

Factors of sharing. To understand the factors of sharing practices, we performed a logistic regression modeling how likely a participant was to share their risky behavior given their age, gender, SA-6, the type of risky behaviors, and whether their behavior was socially triggered. In the same way as Table 5, we used random intercepts for each participant to consider repeated observations and calculated the fifteen pairwise comparisons between the six different risky behaviors using R's multcomp package [25]. We corrected the significance levels using the Bonferroni method [1]. Table 8 shows the result.

Das et al. [11] found no significant correlations between user sharing practices of S&P behaviors and individual demographics (age, gender, and SeBIS). We also found no significant correlation between user sharing practices of *risky* behaviors and individual demographics (age, gender, and SA-6).

On the other hand, we found significant correlations between user sharing practices and the type of risky behaviors. Specifically, as shown in Table 8, all pairwise differences between the likelihood of sharing practices of account sharing and each of the other behaviors were significant. From the results of Table 6, next to account sharing, illegal downloading was likely to be shared, followed by sensitive posts.

Importantly, we also found a significant correlation between user sharing practices and whether their behavior was

Table 7: Reasons for sharing risky behaviors with others.

	Public Wi-Fi (*N*=18)	Pwd Reuse (*N*=72)	Illegal DL (*N*=40)	Delayed Update (*N*=69)	Sensitive Post (*N*=35)	Account Sharing (*N*=109)	All
I wanted them to get the benefits	50.0%	28.8%	45.0%	10.0%	25.7%	**73.4%**	41.7%
I just wanted to talk about my recent behavior	33.3%	45.2%	42.5%	45.7%	**57.1%**	14.7%	35.9%
I wanted them to know about other options	5.6%	16.4%	42.5%	15.7%	5.7%	5.5%	14.2%
They noticed my change	27.8%	11.0%	0.0%	12.9%	17.1%	11.9%	11.9%
I wanted them to know about my knowledge	22.2%	2.7%	2.5%	2.9%	5.7%	1.8%	3.8%
Other	5.6%	12.3%	12.5%	15.7%	11.4%	5.5%	10.4%

The first row indicates the number of participants who shared their risky behavior with others. The sum of the percentages for each behavior exceeds 100% because the participants could select more than one reason. Bold numbers highlight items greater than 50%.

Table 8: Logistic regression for sharing practices.

	Coeff	*p*-value	
Age	0.004	0.553	
Male (vs. Female)	−0.231	0.327	
SA-6	0.024	0.289	
Account (vs. Wi-Fi)	2.794	< 0.001	***
Account (vs. Pwd)	2.833	< 0.001	***
Account (vs. DL)	1.684	0.011	*
Account (vs. Update)	2.696	< 0.001	***
Account (vs. Post)	1.997	0.001	**
Social Trigger	2.062	< 0.001	***

Of the fifteen pairwise comparisons of risky behaviors, only those pairs with a significant difference are shown in this table. Significance levels: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$.

socially triggered (*coeff* = 2.062, *OR* = 7.862, $p < 0.001$). In other words, if a participant engaged in risky behavior due to social triggers, they were more likely to share it with others. Specifically, while 25.9% of the risky behaviors caused by other triggers (organizational or voluntary) were shared with others, 70.7% of the risky behaviors caused by social triggers were shared (i.e., 2.7 times more frequently).

5 Discussions

5.1 Summary of Findings

- Social triggers can lead users to engage in risky behaviors. Specifically, approximately 20–50% of the participants observed others engaging in risky behavior or were advised to do so before engaging in the risky behavior. (RQ1)
- Risky user behaviors are primarily triggered by friends, family, and online strangers. (RQ2)
- The likelihood of social triggers is significantly correlated with the type of risky behavior. In other words, certain behaviors (account sharing and illegal downloading) are often caused by social triggers. (RQ3)
- Risky behaviors caused by social triggers are more likely to be shared with others (i.e., negative social chains). Users share their risky behaviors primarily because they want others to get the benefit. (RQ4)

5.2 Recommendations

We showed that participants engaged in risky behaviors following observations of others and/or advice from others. Researchers should work to reduce such negative effects of social triggers, but this issue is not so straightforward. In extreme cases, preventing users from having social connections would protect them from negative social effects, but this is an impractical measure. Most importantly, social triggers also have positive effects. As Das et al.'s study [11] and the other previous studies we mentioned in Section 2.2 demonstrated, users often engage in S&P behaviors due to social triggers, such as receiving security advice from others. Therefore, researchers need to work simultaneously on activating the positive aspects of social triggers and reducing the negative aspects.

It is also important to note that it is essential for researchers to work to reduce the number of users engaging in risky behaviors voluntarily, as our results show that the majority of participants engaged in risky behaviors voluntarily. For this purpose, basic security education and the interventions that have been proposed in the usable privacy and security field, such as nudges and warnings [14], would be effective.

In the following, we suggest approaches to reducing the *negative* aspects of social triggers (i.e., triggering *risky* user behaviors).

Interventions on online platforms. We found that participants were triggered to engage in risky behaviors not only by offline social connections, such as friends, family, and colleagues, but also by online strangers and influencers. In particular, downloading of illegal or unofficial content was often triggered by online strangers. This suggests the need for interventions to combat the negative chains of risky behaviors that occur online. Online intervention is important because a single post about risky behaviors can be seen by

multiple users, meaning that negative social chains can be easily amplified. Online intervention would be less difficult than eliminating of offline negative chains. Specifically, we recommend that online platforms formulate or strengthen their guidelines regarding posts encouraging risky behaviors and reporting risky behaviors, detect such posts, and present warnings for such posts. Our work would help online platforms identify the risky behaviors for which they should implement the above interventions. In the field of dis/misinformation research, researchers have evaluated the effective design of warnings to prevent the spread of dis/misinformation [22, 29]. The findings of those studies may also be useful in preventing the spread of risky behaviors online. In addition to direct interventions by online platforms, we suggest that online platforms provide features for S&P experts or the public to intervene, such as reporting or correction features. The above efforts should be made not only for posts encouraging illegal downloading (at the request of the copyright owners of the original content) but for any risky behavior susceptible to negative social chains.

Security education with emphasis on risky behaviors susceptible to negative social chains and the risks. We show that the type of risky behaviors is more likely to influence the likelihood of social triggers for risky behaviors and practices of sharing risky behaviors than individual demographics. This suggests the need for countermeasures specific to risky behaviors that are prone to negative social chains, rather than personalized countermeasures tailored to individual demographics. Incorporating such risky behaviors into security education materials or conducting activities to publicize the risks of such risky behaviors would be an effective way to combat negative social chains. In addition, we showed that participants shared their risky behaviors with others because they wanted others to get the benefits or to know about other options, regardless of the risks. In other words, users share their risky behaviors in favor of benefits (e.g., convenience) rather than risks. On the basis of this fact, we recommend that security education not only introduce non-recommended risky behaviors but also convey the risks together. Risk information should be conveyed in an impressive way that is easy for users to understand and remember, such as by quantifying the degree of risks and showing the risks in a graphic or video presentation. For example, graphic cigarette packages that depict the risks of smoking have successfully reduced the demand for cigarettes [57]. For another example, exposure to a drama that focused on the aversive consequences of traffic accidents successfully raised people's awareness of the potentially negative consequences of traffic accidents [44]. In the S&P field, researchers have already worked on visualizations of specific types of risks (e.g., unsafety of URLs [6] and data collection by IoT devices [17]), but it would be desirable to propose and evaluate designs for visualizing the risks of diverse risky behaviors.

Removal of expectation that most of public engages in risky behaviors. We found that participants engaging in a risky behavior expected a higher percentage of the public to engage in the risky behavior than those who did not and that it is possible that participants engaging in a risky behavior due to social triggers expected an even higher percentage. We cannot conclude that such expectations are a cause of risky user behaviors, but dispelling such expectations would be effective in preventing users from continuing to engage in risky behaviors. Interventions that present the percentage of security experts who would not engage in a risky behavior before a user engages in the behavior may be effective in dispelling such user expectations. As related interventions, interventions for dispelling user expectations of others with respect to the phenomenon of pluralistic ignorance (i.e., users do not really want to do something but do it because they think everyone else is doing it) have been proposed and discussed [47, 52]. For example, holding discussions to learn about the true beliefs of others was effective in dispelling user expectations of others [52]. However, it may be impractical to apply those interventions for dispelling user expectations of the risky behaviors of others because risky behaviors often bring users benefits.

6 Conclusion and Future Work

To improve user security and privacy behaviors, researchers need to not only focus on the attitudes and behaviors of individual users but also understand the relationship between each user and society. We analyzed the effects of social triggers for risky behaviors and found that participants sometimes engaged in risky behaviors after observing others or getting advice from others. Participants shared their risky behaviors with others primarily to let others get the benefits.

Future work should examine behavioral triggers for more diverse risky behaviors in multiple countries/cultures, especially individualistic and collectivistic countries. In addition, we need to implement interventions to reduce the negative social effects and evaluate their effectiveness in the future.

References

[1] Hervé Abdi. Bonferonni and šidák corrections for multiple comparisons. *Encyclopedia of measurement and statistics*, 3(01), 2007.

[2] Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L. Mazurek. Comparing security and privacy attitudes among U.S. users of different smartphone and smart-speaker platforms. In *Proceedings of the 17th Symposium on Usable Privacy and Security*, SOUPS'21, 2021.

[3] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy*, S&P'17, 2017.

[4] Omer Akgul, Richard Roberts, Moses Namara, Dave Levin, and Michelle L. Mazurek. Investigating influencer vpn ads on youtube. In *Proceedings of the 2022 IEEE Symposium on Security and Privacy*, S&P'22, 2022.

[5] Suzan Ali, Tousif Osman, Mohammad Mannan, and Amr Youssef. On privacy risks of public WiFi captive portals. In *Proceedings of the Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops*, DPM CBT'19, 2019.

[6] Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. I don't need an expert! making url phishing features human comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI'21, 2021.

[7] Daniel V. Bailey, Collins W. Munyendo, Hunter A. Dyer, Miles Grant, Philipp Markert, and Adam J Aviv. "someone definitely used 0000": Strategies, performance, and user perception of novice smartphone-unlock pinguessers. In *Proceedings of the 2023 European Symposium on Usable Security*, EuroUSEC'23, pages 158–174, 2023.

[8] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. "Adulthood is trying each of the same six passwords that you use for everything": The scarcity and ambiguity of security advice on social media. In *Proceedings of the 25th ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW'22, 2022.

[9] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Proceedings of the 15th Symposium on Usable Privacy and Security*, SOUPS'19, 2019.

[10] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *Proceedings of the 2014 Network and Distributed System Security Symposium*, NDSS'14, 2014.

[11] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. A typology of perceived triggers for end-user security and privacy behaviors. In *Proceedings of the 15th Symposium on Usable Privacy and Security*, SOUPS'19, 2019.

[12] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, CCS'14, 2014.

[13] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I Hong. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on Computer Supported Cooperative Work & Social Computing*, CSCW'15, 2015.

[14] Verena Distler, Gabriele Lenzini, Carine Lallemand, and Vincent Koenig. The framework of security-enhancing friction: How ux can help users behave more securely. In *Proceedings of the New Security Paradigms Workshop 2020*, NSPW'20, 2020.

[15] Daniel Domínguez-Álvarez, Daniel Toniuc, and Alessandra Gorla. Rechan: an automated analysis of android app release notes to report inconsistencies. In *Proceedings of the 9th IEEE/ACM International Conference on Mobile Software Engineering and Systems*, MobileSoft'22, 2022.

[16] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, CHI'15, 2015.

[17] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *Proceedings of the 2020 IEEE Symposium on Security and Privacy*, S&P'20, 2020.

[18] Pardis Emami-Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. In *Proceedings of the 21st ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW'18, 2018.

[19] Michael Fagan and Mohammad Maifi Hasan Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Proceedings of the 12th symposium on usable privacy and security*, SOUPS'16, 2016.

[20] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. A self-report measure of end-user security attitudes (SA-6). In *Proceedings of the 15th Symposium on Usable Privacy and Security*, SOUPS'19, 2019.

[21] Brian J. Fogg. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology*, PT'09, 2009.

[22] Katrin Hartwig, Frederic Doell, and Christian Reuter. The landscape of user-centered misinformation interventions–a systematic literature review. *arXiv preprint arXiv:2301.06517*, 2023.

[23] Ayako A. Hasegawa, Naomi Yamashita, Tatsuya Mori, Daisuke Inoue, and Mitsuaki Akiyama. Understanding non-experts security-and privacy-related questions on a Q&A site. In *Proceedings of the 18th Symposium on Usable Privacy and Security*, SOUPS'22, 2022.

[24] Hofstede Insights. Country comparison tool. https://www.hofstede-insights.com/country-comparison-tool, (accessed January 15, 2024).

[25] Torsten Hothorn, Frank Bretz, Peter Westfall, Richard M. Heiberger, Andre Schuetzenmeister, and Susan Scheibe. multcomp: Simultaneous inference in general parametric models. https://cran.r-project.org/web/packages/multcomp/index.html, (accessed February 8, 2024).

[26] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind"': Comparing expert and non-expert security practices. In *Proceedings of the 11th Symposium On Usable Privacy and Security*, SOUPS'15, 2015.

[27] Ipsos. Ipsos global trends report 2023. https://www.ipsos.com/en/global-trends, (accessed December 29, 2023).

[28] Shareen Irshad and Tariq Rahim Soomro. Identity theft and social media. *International Journal of Computer Science and Network Security*, 18(1):43–55, 2018.

[29] Ben Kaiser, Jerry Wei, Eli Lucherini, Kevin Lee, J. Nathan Matias, and Jonathan Mayer. Adapting security warnings to counter online disinformation. In *Proceedings of the 30th USENIX Security Symposium*, SEC'21, pages 1163–1180, 2021.

[30] kaspersky. Stranger danger: the connection between sharing online and losing the data we love. https://www.kaspersky.com/blog/my-precious-data-report-three/16883/, (accessed December 29, 2023).

[31] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J. Godfrey, Heather Lipford, and Pamela J. Wisniewski. Examining collaborative support for privacy and security in the broader context of tech caregiving. In *Proceedings of the 24th ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW'21, 2021.

[32] Isadora Krsek, Kimi Wenzel, Sauvik Das, Jason I. Hong, and Laura Dabbish. To self-persuade or be persuaded: Examining interventions for users' privacy setting selection. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI'22, 2022.

[33] Lancers, Inc. Lancers. https://www.lancers.jp/, (accessed December 12, 2023).

[34] Alice Yuen Loke and Yim-wah Mak. Family process and peer influences on substance use by adolescents. *International journal of environmental research and public health*, 10(9):3868–3885, 2013.

[35] Philipp Markert, Daniel V Bailey, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. On the security of smartphone unlock pins. *ACM Transactions on Privacy and Security (TOPS)*, 24(4):1–36, 2021.

[36] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. Exploring nudge designs to help adolescent sns users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI'20, 2020.

[37] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. "they keep coming back like zombies": Improving software updating interfaces. In *Proceedings of the 12th Symposium on Usable Privacy and Security*, SOUPS'16, 2016.

[38] Tenga Matsuura, Ayako A. Hasegawa, Mitsuaki Akiyama, and Tatsuya Mori. Careless participants are essential for our phishing study: Understanding the impact of screening methods. In *Proceedings of the 2021 European Symposium on Usable Security*, EuroUSEC'21, 2021.

[39] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "she'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI'16, 2016.

[40] Tamir Mendel and Eran Toch. Social support for mobile security: Comparing close connections and community volunteers in a field experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI'23, 2023.

[41] Marina Micheli, Elissa M. Redmiles, and Eszter Hargittai. Help wanted: Young adults' sources of support for questions about digital media. *Information, Communication & Society*, 23(11):1655–1672, 2020.

[42] George R. Milne, Lauren I. Labrecque, and Cory Cromer. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3):449–473, 2009.

[43] Jonathan A. Obar and Anne Oeldorf-Hirsch. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1):128–147, 2020.

[44] G. O'Brien, F. Rooney, Colm Carey, and Ray Fuller. Evaluation of the effectiveness of a dramatic presentation on attitudes to road safety. In *Behavioural Research in Road Safety: Twelfth Seminar*, 2002.

[45] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Proceedings of the 18th Symposium on Usable Privacy and Security*, SOUPS'22, 2022.

[46] Michael L. Pittaro. Cyber stalking: An analysis of online harassment and intimidation. *International journal of cyber criminology*, 1(2):180–197, 2007.

[47] Emilee Rader. Data privacy and pluralistic ignorance. In *Proceedings of the 19th Symposium on Usable Privacy and Security*, SOUPS'23, 2023.

[48] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the 8th Symposium on Usable Privacy and Security*, SOUPS'12, 2012.

[49] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS'16, 2016.

[50] Shruti Sannon, Natalya N. Bazarova, and Dan Cosley. Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, CHI'18, 2018.

[51] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI'17, 2017.

[52] Christine M. Schroeder and Deborah A. Prentice. Exposing pluralistic ignorance to reduce alcohol use among college students 1. *Journal of Applied Social Psychology*, 28(23):2150–2180, 1998.

[53] statista. Average daily time spent using the internet by 3rd quarter 2023, by age and gender. https://www.statista.com/statistics/1378510/daily-time-spent-online-worldwide-by-age-and-gender/, (accessed February 15, 2024).

[54] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. In *Proceedings of the 21st Privacy Enhancing Technologies Symposium*, PETS'21, 2021.

[55] Jenny Tang, Eleanor Birrell, and Ada Lerner. Replication: How well do my results generalize now? the external validity of online privacy and security surveys. In *Proceedings of the 18th symposium on usable privacy and security*, SOUPS'22, 2022.

[56] Jenny Tang, Hannah Shoemaker, Ada Lerner, and Eleanor Birrell. Defining privacy: How users interpret technical terms in privacy policies. In *Proceedings of the 21st Privacy Enhancing Technologies Symposium*, PETS'21, 2021.

[57] James F. Thrasher, Matthew C. Rousu, David Hammond, Ashley Navarro, and Jay R. Corrigan. Estimating the impact of pictorial health warnings and "plain" cigarette packaging: evidence from experimental auctions among adult smokers in the united states. *Health policy*, 102(1):41–48, 2011.

[58] Rick Wash and Molly M. Cooper. Who provides phishing training? facts, stories, and people like me. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, CHI'18, 2018.

[59] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. Anti-privacy and anti-security advice on TikTok: Case studies of technology-enabled surveillance and control in intimate partner and parent-child relationships. In *Proceedings of the 18th Symposium on Usable Privacy and Security*, SOUPS'22, 2022.

[60] Yuxi Wu, W. Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *Proceedings of the 2022 IEEE Symposium on Security and Privacy*, S&P'22, 2022.

[61] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI'20, 2020.

Appendix

A Questionnaire

A Study on Online Behaviors

We are conducting a study to explore the impact of behavioral triggers on risky cyber behavior. We don't view taking risky behaviors as bad or uncommon. We are interested in it as researchers. Thus, we kindly request that you provide honest and accurate responses. Your input will be crucial in helping us gain insights into this research area.

The survey will consist of multiple-choice and open-ended questions. We once again request that you provide **honest** and **accurate** responses. Rest assured, your answers will remain entirely confidential and will be anonymous. The aggregated data will be published in an academic paper(s) in a form that does not identify individuals.

The estimated duration for completing the survey is 7 minutes. For your time you will be compensated $1.75 for completing the survey. Please note that participation in this research is entirely voluntary, and you reserve the right to withdraw at any point during the survey without any obligation. Should you have any questions, concerns or comments, feel free to contact the Principal Investigator at <email address>.

By clicking the button below, you acknowledge the following:

- Your participation in the study is voluntary.
- You are 18 years of age or older.
- You are aware that you may choose to terminate your participation at any time for any reason.
- You are a resident of United States of America or Japan

Thank you for your participation in advancing our understanding of cyber behavior. Your valuable input contributes significantly to the success of this research.

- ○ I consent to the above and will voluntarily participate in this survey
- ○ I do not consent to the above and will not participate in this survey

Q01. Have you done any of the following in the past 6 months? Please select all that apply.

- ☐ Connecting to an unknown, potentially unsecured public Wi-Fi, and then engaging in sensitive data exchanges, such as transmitting credit card or password details through this connection
- ☐ Reusing same or similar passwords for different accounts
- ☐ Downloading illegal or unofficial software/applications and media (e.g., videos, music, and games)
- ☐ Ignoring or delaying updating software/applications
- ☐ Sharing sensitive personal information online (e.g., location-based information, real-time activities, and pictures of yourself/others) to strangers on social media
- ☐ Sharing accounts with family, friends or others
- ☐ None of these apply to me

Q02. *<Asked for each behavior selected by participants in Q01.>*
Did any of the following happen before you took the behavior? Please select all that apply.

- ☐ I observed / heard about other people doing this
- ☐ Other people advised to do this
- ☐ My organization required me to do this
- ☐ Other (Please Specify):
- ☐ Nothing in particular happened

Q02.1 *<Asked for each participant that selected 'I observed / heard about other people doing this' in Q02.>*
You observed/heard people around you doing this. Who did you observe/hear? Please select all that apply.

- ☐ Friend
- ☐ Family
- ☐ Colleague
- ☐ Teacher / Mentor
- ☐ Stranger
- ☐ Influencer
- ☐ Media (e.g., news websites and TV programs)
- ☐ Other (Please Specify)
- ☐ I don't remember

Q02.2 *<Asked for each participant that selected 'Other people advised to do this' in Q02.>*
Who advised you to take this behavior? Please select all that apply.

- ☐ Friend
- ☐ Family
- ☐ Colleague
- ☐ Teacher / Mentor
- ☐ Stranger / Online posts
- ☐ Influencer
- ☐ Media (e.g., news websites and TV programs)
- ☐ Service provider / Salesperson
- ☐ Other (Please Specify)
- ☐ I don't remember

Q02.3 *<Asked for each participant that selected 'Other people advised to do this' in Q02.>*
Did the person who advised you take this behavior share any risks of the behavior?

- ○ Yes
- ○ No
- ○ I don't remember

Q03. <*Asked for each behavior selected by participants in Q01.*>
When taking this behavior did you talk about it with anyone else? Please select all that apply.

- ☐ Friend
- ☐ Family
- ☐ Colleague
- ☐ Online discussion (e.g., Social media, blog posts, forums)
- ☐ Other (Please Specify)
- ☐ I didn't talk about this with anyone

Q03.1 <*Asked for each participant that only selected 'I didn't talk about this with anyone' in Q03.*>
Why did you decide not to talk about this behavior to anyone? Please select all that apply.

- ☐ I didn't feel comfortable talking about security and privacy
- ☐ I assumed everyone did this
- ☐ I just didn't want to talk about this to anyone
- ☐ I hadn't had the chance to talk with anyone about this yet
- ☐ Other (Please Specify)

Q03.2 <*Asked for each participant that did not select 'I didn't talk about this with anyone' in Q03.*>
What prompted you to talk about this behavior with them? Please select all that apply.

- ☐ They noticed my change
- ☐ I wanted them to get the benefits
- ☐ I just wanted to talk about my recent behavior
- ☐ I wanted them to know that I have knowledge in the hacking field
- ☐ I wanted them to know about other options, regardless of risk
- ☐ Other (Please Specify)

Q04. What percentage of all users do you think engage in the follow behaviors?

- ○ Connecting to an unknown, potentially unsecured public Wi-Fi, and then engaging in sensitive data exchanges, such as transmitting credit card or password details through this connection.
- ○ Reusing same or similar passwords for different accounts
- ○ Downloading illegal or unofficial software/applications and media (e.g., videos, music, and games)
- ○ Ignoring or delaying updating software/applications
- ○ Sharing sensitive personal information online (e.g., location-based information, real-time activities, and pictures of yourself/others) to strangers on social media
- ○ Sharing accounts with family, friends or others

<*Q05–Q10: SA-6 questions. A series of SA-6 questions were asked on a 5-point Likert scale: 'strongly disagree,' 'somewhat disagree,' 'neither agree nor disagree,' 'somewhat agree,' and 'strongly agree.'*>

Q05. I seek out opportunities to learn about security measures that are relevant to me.

Q06. I am extremely motivated to take all the steps needed to keep my online data and accounts safe.

Q07. Generally, I diligently follow a routine about security practices.

Q08. I often am interested in articles about security threats.

Q09. I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.

Q10. I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

Q11. Where do you normally receive your information regarding digital technologies? Please select all that apply.

- ☐ Friends
- ☐ Family
- ☐ School / Teacher
- ☐ Workplace/Colleague
- ☐ News sites / Blogs
- ☐ Service provider / Salesperson
- ☐ Influencers
- ☐ Other (Please Specify)
- ☐ None of the above

Q12. Please select 'Influencers' for this question.

- ☐ Friends
- ☐ Family
- ☐ Colleague
- ☐ Teacher/Mentor
- ☐ Stranger/Online posts
- ☐ Influencers
- ☐ Media (e.g., news websites and TV programs)
- ☐ Service provider/Salesperson
- ☐ Other (Please Specify)
- ☐ I don't remember

Q13. What gender do you identify as?

- ○ Male
- ○ Female
- ○ Non-binary / third gender
- ○ Other (Please Specify)
- ○ Prefer not to say

Q14. How old are you?

Q15. Please select the option which best describes your education level.

- High School or Equivalent
- College diploma
- Undergraduate degree
- Post-graduate education (Masters, Doctorate, Medical/Law School)
- Prefer not to say
- Other (Please Specify)

Q16. Do you consider yourself knowledgeable in Information Technologies or related fields?

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Q17. What nationality do you most identify with?

Q18. What country do you currently reside in?

Q19. Please indicate if you have honestly participated in this survey. You will not be penalized/rejected for indicating 'No' but your data may not be included in the final analysis.

- Yes
- No

B Detailed Results

Table 9: Person who advised participants to engage in risky behaviors.

Relationship	%
Family	56.7%
Friend	50.0%
Stranger/Online posts	25.0%
Colleague	20.0%
Media (e.g., news site and TV programs)	10.0%
Influencer	10.0%
Service provider/Salesperson	3.3%
Teacher/Mentor	1.7%
Other	1.7%

Table 9 indicates from whom the participants were advised to engage in risky behaviors. Participants were primarily influenced by family, friends, online strangers, and colleagues, similar to Table 3 (i.e., observation of others).