Replication: Stories as Informal Lessons about Security

Katharina Pfeffer and Alexandra Mai, *SBA Research;*
Edgar Weippl, *University of Vienna;* Emilee Rader, *Michigan State University;*
Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

https://www.usenix.org/conference/soups2022/presentation/pfeffer

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

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

Replication: Stories as Informal Lessons about Security

Katharina Pfeffer
SBA Research

Alexandra Mai
SBA Research

Edgar Weippl
University of Vienna

Emilee Rader
Michigan State University

Katharina Krombholz
CISPA Helmholtz Center for Information Security

Abstract

Anecdotal stories about security threats told to non-experts by friends, peers, or the media have been shown to be important in forming mental models and secure behaviors. In 2012, Rader et al. conducted a survey (*n=301*) of security stories with a student sample to determine factors that influence security perceptions and behavior. We replicated this survey with a more diverse sample (*n=299*), including different age groups and educational backgrounds. We were able to confirm many of the original findings, providing further evidence that certain characteristics of stories increase the likelihood of learning and retelling. Moreover, we contribute new insights into how people learn from stories, such as that younger and higher educated people are less likely to change their thinking or be emotionally influenced by stories. We (re)discovered all of the threat themes found by Rader et al., suggesting that these threats have not been eliminated in the last decade, and found new ones such as ransomware and data breaches. Our findings help to improve the design of security advise and education for non-experts.

1 Introduction

Today, computers, mobile devices, and IoT devices permeate almost every aspect of our daily lives, forcing all users (including those with little to no security background) to make critical decisions about their IT security and privacy. These range from whether to click on a link or update software, to which password, antivirus software, or messaging service to choose. Although the usability of the devices has improved and security measures have been automated to a certain extent, the complexity of the decisions people have to make has continued to grow.

Several studies [16, 30, 31] have shown that people often make decisions based on incorrect or inaccurate mental models and misperceptions of security threats that expose them and others to security risks. In general, it is difficult for people to develop accurate mental models of cyber security threats since they typically cannot experience them themselves (i.e., we often do not directly experience security threats, nor can we observe others doing so since they are usually subtle or invisible). Redmiles et al. [26] found that people often reject security advice because they have not yet had a related negative experience themselves. They also found that people are generally overwhelmed with security advice from many different sources, such as newspapers, social media, movies, IT professionals, friends and family. In addition, their results suggested that people find it difficult to trust advice that comes from institutions that are obviously guided by marketing ideas.

As a possible solution to the lack of direct personal experience with security threats, it was found that in addition to security advice from IT professionals or security training, which is often ignored, negative experience stories from friends, family, or the media have a major impact on security decision making. We define negative experience stories as statements people have heard or read that relate to cyber security threats that happened to someone else. Rader et al. [25] were the first to examine how stories influence people's thinking and behavior. They conducted a survey in 2012 (hereafter referred to as the *Rader study*) in which they asked 301 undergraduate students open- and closed-ended questions about security advice they had heard from others. Using qualitative and quantitative methods, they determined the characteristics of these stories that lead to changes in thinking and behavior. The Rader study focused on undergraduate students and hence allows to only draw conclusions for this specific population. Also, their study was conducted a decade ago, and since then technology usage and the nature of security threats has fundamentally changed. Later, Fennell et al. [13] conducted another

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

user study examining how security stories may affect people's willingness to adopt two-factor authentication. Although they were able to demonstrate that stories increase adoption, they were unable to determine exactly what aspects of the stories might have convinced people to do so.

We seek to understand if the results from the Rader study are replicable ten years after the original study was conducted. We furthermore examine the generalizability to a broader population. We anticipated differences within our diverse sample, since prior work found evidence that demographics influence mental models, security behavior, and the processing of security advice [5, 26, 31]. A more nuanced understanding of which stories are remembered and which lead to changes in thinking and behavior is an important step towards making security advice better and more personalized. We thus replicated the Rader study with the following modifications:

- We recruited a more diverse sample with different age groups, educational backgrounds, and employment statuses.
- We applied a different recruiting strategy using quotas for age and gender to obtain a sample representative of the U.S. population.
- We examined the changed threat landscape reported in our stories and the changed media usage during the last decade.
- We applied inductive (instead of deductive) coding for the full stories, resulting in more in-depth themes grounded in our data.

Our found threat themes are similar to those of the Rader study, but ransomware and data breaches emerged as two new themes. We were able to confirm many of the original findings, such as that stories with a lesson affect our participant's behavior, while stories with serious threats affect thinking and the likelihood of retelling. Our results also confirm that stories that elicit fear or anger affect both thinking and behavior. In contrast to the Rader study, we found that stories told in a work environment are more likely to lead to behavior change than those told in casual contexts such as at home or in a coffee shop. We also report additional findings, which have not been examined in the Rader study, e.g. that younger and higher educated participants are less likely to report a change in their thinking.

2 Related work

Security advice and stories: Redmiles et al. [27] conducted semi-structured interviews to investigate from where people get security advice and found that a primary source is negative events they have experienced themselves or that have been passed on by peers, family, or the media. They also conducted a quantitative survey [26] to examine how people's security beliefs, knowledge, and demographics correlate with their choice of security advice sources and their security behavior. Their findings suggest possible differences based on people's age and social status. In both studies, the trustworthiness of the advice source and the content of the advice play an important role in whether advice is accepted or rejected. In contrast to Redmiles et al., we do not ask how people decide which security advice to follow, but rather what effect stories have on people's thinking and behavior.

Fagan et al. [12] found that people decide to (not) follow security advice by weighting the benefits of following and the risks and costs of not following (balancing security and convenience). With our study, we investigate how stories can impact people's risk perception and security decisions. Ion et al. [19] compared the security practices of non-experts and security experts and found differences in the tools they use and their security behaviors. In this paper, we have a closer look at how stories impact the security tool usage and behavior of non-experts.

Rader et al. [25] were the first to study how security stories told by non-experts influence thinking and behavior. We replicate their study in this paper with a more diverse sample and some additional and modified survey questions. Rader et al. [24] conducted another study comparing three sources of security advice: news articles, web pages with security advice, and stories from friends or family (using the sample from the study described above). They found that personal stories often focused on who was carrying out the attacks, rather than how they were carried out or what the consequences were. Fennell et al. [13] showed that stories do indeed increase the people's willingness to adopt two-factor authentication. They hypothesized that focusing on negative consequences might work better than focusing on benefits. We investigate their hypothesis for our participants' security stories.

Mental models and risk perception: Mental models of the internet and security risks influence people's security behavior and decision making. Wash [30] identified eight non-expert mental models of security threats. Wash and Rader [31] quantified these mental models in a large-scale survey and found correlations between weak or incorrect mental models and insecure behavior. Asgharpour et al. [4] showed that risk communication often fails since it does not take the mental models of non-experts into account.

Kang et al. [20] examined experts' and non-experts' mental models of the internet and discovered that they often affect privacy and security decisions. Specifically, they found that a better understanding of risks can lead to a more secure behavior. Fulton et al. [16] showed that entertainment media, such as movies or series, can affect people's mental models by allowing them to learn from the actors' experiences (which, however, do not always correspond to reality). In this paper, we assume that security stories have an influence on people's mental models that must be considered alongside the influence of entertainment media, observation, and personal experience.

Nurse et al. [23] showed that in cyber security risk communication, characteristics of the message source (e.g., intent, reputation), the message (e.g., specificity, credibility), and the message recipient (e.g., beliefs, expertise) affect the effectiveness of the communication. In this paper, we investigate how characteristics of the storyteller, the story, and the recipient affect the likelihood of thinking and behavior change.

Psychology of Behavior Change: One theory commonly used to explain the adoption of secure behavior is the *Motivation-Ability-Trigger model* [14]. This says that a behavior only gets adopted if a person has the motivation, the ability, and is triggered to do so. We think that stories can affect all of these three properties, as people can share ideas to motivate and make each other aware, pass on strategies how to change a behavior, and trigger the behavior change by (re-)telling negative experiences to be avoided. Das et al. [9] showed that social processes often act as trigger to adapt secure behavior and were effective at raising security sensitivity.

The *Extended Parallel Process Model (EPPM)* [32] explains the role of fear-inducing communication in triggering behavior change. It states that although fear determines the intensity of the response, it is only effective if the person is also provided with a viable solution to the threat.

Another frequently cited theory is the *theory of planned behavior* [3], which was extended by Ng et al. [22]. Ng et al. stated that behavior change is affected by (i) perceived behavior control (over the ability to practice computer security), (ii) subjective norm (social pressure to perform an action), and (iii) attitude (influenced by the perceived usefulness). For (ii), the influence of peers, family, the mass media, as well as the work environment is important. In this study, we examine the influence of stories on the subjective norm, i.e. the social pressure to adopt a behavior. Along these lines, Ruoti et al. [29] developed a four-stage process for the adoption of security measures: learning, evaluation of risks, estimation of impact, and weighing trade-offs to different coping strategies.

Generally, it has been shown that *social proof and personal examples* have an impact on secure behavior and decision making. Das et al. [11] demonstrated that when showing people the usage of security features of friends, they were more likely to be adopted. Das et al. also showed in a retrospective interview study [10] that social influence, especially the observability of security feature usage, can affect people's thinking and behavior. Similar, Harbach et al. [17] revealed that risk communication with personalized examples (i.e. which information is at risk when installing an app) can foster secure behavior. With our work we further examine how security stories, much like personal examples, can affect people's thinking and behavior, serving as substitute for the lack of observability of security feature usage.

3 Methodology

We replicated the study design from the Rader study with a few changes. The authors of the original study shared their anonymized data with us for statistical comparison. In this section, we explain the modifications we did to the original questionnaire, our prestudy, how we recruited a diverse sample, and how we analyzed our survey data.

3.1 Questionnaire

Rader's study questionnaire started with an introduction text explaining the goal of the survey. Afterwards, participants answered four open questions where they had to name cyber security threats, protection measures, and stories they had heard related to security threats. These questions were used to help participants remember any stories they might have heard or read. Finally, they had to choose one story they could most easily recall details about and answer the subsequent questions in regards to that story. Most of the following questions were multiple choice. In the last part of the survey, after the participants had thought about the story for a while, they were asked to write down the story as if they would tell it to a friend using as many details as possible. In total, the survey consisted of 7 open-ended questions and 38 closed (multiple choice or checkbox) questions.

For the replication study, we changed the wording of the original questionnaire in the introduction text and in several questions to explicitly include mobile threats (see Appendix 9.1). Moreover, we changed and shortened the original web use skill measure where respondents had to rate their knowledge of technical terms such as phishing, meme, or cache on a Likert scale. We updated the terms to be up to date and included more highly understood terms since our audience mainly consisted of non-experts. According to Hargittai et al. [18], adjusting web-skill measures based on the characteristics of the targeted population helps to reduce non-responses (i.e., non-experts might quit the survey when faced with numerous lesser known items due to frustration).

We also included a bogus term (filtibly), which served as a attention check question. We discarded all responses that rated their knowledge of this term as "good" or "full". We considered the rating "little" still acceptable, since we assumed that the participants might remember having seen a word kind of like "Filtibly" before. We shortened the questions where participants had to rate emotions the story made them feel on a Likert scale, to shorten the time and concentration needed to complete the survey. We added an additional question asking whether the participants received formal training in IT security since we expected differences based on this characteristic. However, we did not find any significant correlations in participants with or without formal training in any of our regression models. Since we wanted to compare the participants' own negative experiences with their reported stories, we included a

Table 1: Demographics

		Sample	Quotas [6]
Gender	Female	53%	51%
	Male	45%	49%
	Prefer not to say	2%	-
Age	18-34	28%	27%
	35-44	18%	17%
	45-59	26%	26%
	>59	28%	30%
Education	High school	8%	
	Technical, vocational school	5%	
	Some college	25%	
	Bachelor degree	36%	
	Master degree	19%	
	Doctoral degree	4%	
	Other	2%	
	None	<1%	
Employment	Employed full time	54%	
	Employed part time	12%	
	Retired	16%	
	Unemployed	9%	
	Student and empl. part-time	1%	
	Student	3%	
	Disabled	2%	
	Other	3%	

question asking about cyber security threats they experienced themselves. We placed this question after they told the story they have heard or read, in order to not confuse them or prime them towards thinking about their own experiences instead of stories they have heard.

We conducted a prestudy (*n=16*) to test the comprehensibility of our questionnaire. At the end of the prestudy, we included a question to ask participants about survey parts that were unclear to them and to make improvement suggestions. We found that responses to the question about the moral of the story and learnings from the story were redundant, thus we merged this questions. Otherwise, no problems arose.

3.2 Recruitment and Participants

We hosted our survey on SurveyMonkey [1] and used their participant pool for recruitment, which allowed us to put quotas on age and gender to ensure that our sample largely matched these quotas of the U.S. population as published by the United States Census Bureau [6] (see Table 1). However, our sample is not representative of culturally different regions. Completing the survey took an average 13 minutes. We compensated each participant with US$5 for their time and effort.

We started our study paying for 350 participants, assuming that we will have to exclude about 15% invalid responses, similar to the Rader study. However, it turned out that about half of our responses did not meet our criteria (see below). After consulting with SurveyMonkey, they relaunched our survey free of charge until we had collected enough responses that matched our original quotas and criteria. For both launches, we received in total 622 responses, from which we excluded:

- 239 since they were unusable (participants did not remember a story, wrote a story not related to cyber security, or answered inconsistently),
- 19 since they failed the attention check question, i.e. rated their understanding of "Filtibly" as "good" or "full" (we accepted 28 ratings as "little"),
- 52 since they wrote a story about themselves,
- 13 since they gave an advice instead of writing a story.

This left us with 299 usable responses.

3.3 Analysis

We used a combination of (i) qualitative coding to account for the subtleties of the stories told, and (ii) quantitative statistical analyses to calculate differences between demographic groups and compare our results with those of the Rader study.

Qualitative Coding: To code the full stories and the responses to the open-ended questions, we used inductive thematic coding [7]. Our goal was to find repeating patterns in the data and use them to build theories. The Rader study used (i) deductive thematic coding with a pre-defined codebook consisting of story themes to code the full stories and (ii) inductive thematic coding to code the open-ended questions, creating the codebook by grouping recurring themes into higher-level themes and sub-themes.

We applied the second approach, i.e. inductive thematic coding, to both the full stories and the open-ended questions, aiming at grounding our analysis as close as possible in the meaning of the data. This allowed us to gain more in-depth results including meta reflections from the full stories. We created a codebook (see Appendix 9.2 for the final version) based on recurring patterns in the full stories and the open-ended questions. First, two independent researchers open-coded all full stories and open-ended questions to create an initial codebook of themes and sub-themes. One of the researchers had not previously read Rader's study, and the second researcher also attempted to look at the emerging categories in an unbiased manner.

Second, both researchers discussed the emerging themes and jointly created a joint version of the codebook. Although reading the Rader study may have influenced one researcher's coding process, we are confident that we also included an unbiased view by jointly creating the codebook. Besides, since our goal was to compare our findings with those of the original study, we do not see it as problematic that our codebook may have been influenced by the codes of the Rader study.

Third, both coded all responses independently. Fourth, they discussed the differences and decided to merge certain subthemes of the codebook that were too similar and therefore resulted in different code assignments. For example, the second codebook had a "ransomware" topic with "enterprise" and "public entity" sub-themes, which were merged. For the remaining differences, we calculated the inter-coder-agreement

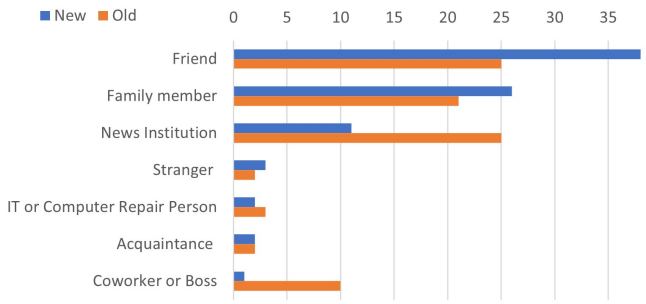

Figure 1: Source of hearing/reading the story (percentages).

with a Cohen's Kappa κ [8] of 0.89, which shows a good level of agreement. Finally, both researchers met and reached agreement on all code assignments.

Quantitative Analysis/ Statistical Tests: We used logistic regression for binary dependent variables and OLS regression for interval scaled dependent variables. We calculated models for the same factors as the Rader study to make the results comparable. Additionally, we created models with different demographics (e.g., age, education level) as factors.

4 Results: Descriptive Statistics

Most of our participants chose a story told by friends or family members (see Figure 1), which is similar to the findings of the Rader study. However, we discovered that fewer stories in our sample came from news institutions. We also found that a lower percentage of stories (34% in our sample versus 55% in the Rader study) were told face-to-face, as more people used social networks, instant messaging, or the phone. We attribute this to either changes in technology use over the past decade or to the global pandemic. The majority of our participants (64%) heard the story within the last year.

In line with the Rader study, we found that 96% of our participants believed that the story was true (see Table 2). Almost half of the stories (48%) were retold, most (57%) within a day and almost all within a week (90%). 59% of the stories were autobiographical, meaning that the protagonist was the person telling the story. Our results and the Rader study show that most of the stories contain a lesson about something you should always do or never do, or both.

Our participants had to rate the seriousness of the threat described in their chosen story on a Likert scale of 1-5. We report a mean score of 4.05, indicating very high severity, which is higher than the more moderate mean score of 3.5 in the Rader study. Possible reasons for this are discussed in Section 6. The average story had a moderate effect (M=3.1) on participants' thinking and influenced their behavior in half of the cases in both studies.

Table 2: Facts about stories

	New	Old
Believed story to be true	96%	95%
Retold Story	48%	45%
Autobiographical	59%	51%
Contains lesson	71%	72%
Change of behavior	52%	52%
Change of thinking (mean, 1-5 scale)	3.1	2.9
Seriousness of threat (mean, 1-5 scale)	4.1	3.7

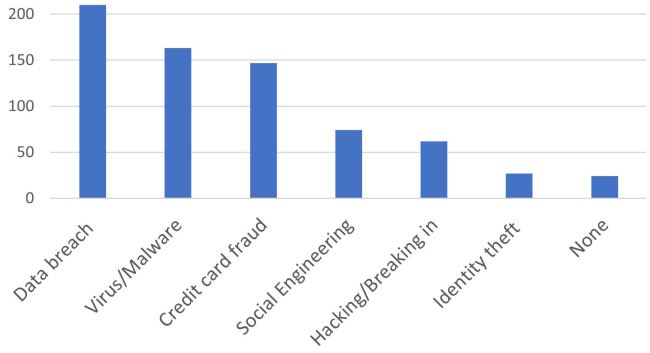

Figure 2: Threats that happened to participants (counts).

Stories told by our participants affected single or multiple individuals, companies, governmental or educational institutions, or society as a whole. The reported threats resulted in the loss of money, time, data, reputation, or the availability of critical infrastructure such as a gas pipeline, electricity, or the healthcare system. We asked our participants which threats happened to them personally (see Figure 2). We found that more than two thirds had already fallen victim to a data breach. Many also experienced credit card fraud or having a virus or malware. Fewer participants reported that hacking or social engineering such as phishing had happened to them.

5 Qualitative Results

In this section, we report and discuss our qualitative findings in comparison to the Rader study. Note that although we report numbers for both studies, they are not directly comparable since many themes overlap (e.g., "Hacking/Breaking In", "Virus/Malware", and "Social Engineering"). For all themes, multiple assignments are possible for one story.

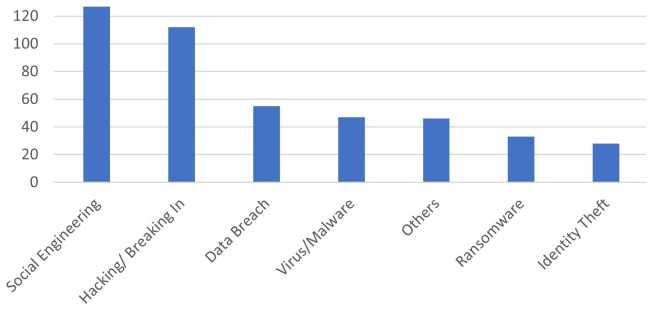

Figure 3: Threat categories of reported stories (counts).

5.1 Full Stories

For the full stories, we constructed sub-themes to each threat category, in contrast to the Rader study, where only the top-level themes were coded. Figure 3 shows the distribution of emerged threats of the reported stories.

Since we asked participants to report on only *one* story they remember most vividly, these numbers do not claim to be representative of security story themes in general. However, we use them to show trends in such themes.

Comparing the threats found in the stories with the threats experienced personally by the participants (see Figure 2), it seems that incidents related to hacking or social engineering are mentioned much more often in the stories than they were experienced personally. Note that we did not introduce a specific category for ransomware in our questionnaire, thus these threats may have been reported as hacking or viruses/malware in Figure 2.

Social Engineering The largest fraction of stories were related to social engineering threats (127), which were often coded together with the categories "Virus/Malware" (47) and "Hacking/Breaking In" (112). Social engineering threats include phishing messages (71), where people are tricked into clicking on fraudulent links or attachments, and fraudulent messages or calls (25), where attackers take false identities and tell fraudulent stories to steal valuable information or money. These threats occurred via social media, email, or via the phone. Moreover, participants were told about fraudulent websites (15), apps (4), or USB sticks (2) tricking people into giving away sensitive information. We identified several pretexts under which these social engineering attacks are usually carried out. Many participants shared stories of using fake friend requests or messages on social media platforms to gain trust and subsequently steal information. Some stories were about sophisticated threats where the attacker went through multiple stages:

> *"Someone pretend to be his high school classmate [and] requested friend connection. [They] chatted and exchanged email addresses. Tom shared [his] work email. Tom received [an] email from Facebook (fake, phishing). Tom clicked [on the] email content and [his] computer got infected by a virus. The virus infected Tom's company network and the hacker stole company data."*

In many cases, the attacker posed as a friend or relative in need of money, a representative of the bank or tax office, or a co-worker or boss. Some stories also claimed that the victim had won money or an item.

> *"The incident had occurred after my friend had sent personal information to another Instagram user who had claimed they would send them money via cash app."*

Several stories were about a fraudulent pop-ups or IT help desk numbers (8).

> *"He came across an old man whose computer was infected and was asking to call a support number to fix it. The person called the support number which was actually a hacker."*

Comparison Rader study: They also found many stories related to phishing (53) using similar tricks as reported in our study. In line with our findings, they reported that phishing messages ranged from emails pretending to be from a bank to more sophisticated attempts, where someone started a chat with the victim via Facebook or an online game. Unfortunately, this shows that phishing is a persistent problem that has not been solved in the last decade.

Hacking/Breaking In The majority of stories in this category were about hacked bank, email, or social media accounts (91), which usually included a hacked password. As a result of the hacked account, various threats occurred, such as attackers sending spam emails or messages, or making transactions. Some incidents were more serious than others, such as:

> *"Someone hacked the email of a vendor and provided fraudulent wire details to pay for an invoice."*

Several stories dealt with the hacking of (public) WiFis (2), cameras (16), or celebrities (3).

> *"A stranger hacked into the camera and was spying on the child and started speaking to the child through the security camera."*

Comparison Rader study: They also reported 59 stories in the category "Breaking In". In this category, our results are very similar to the Rader study, as many incidents of hacked computers, systems and accounts were also reported there. Their participants also often talked about negative affects of the "hacking", such as altered accounts or profile information, or sending fraudulent messages. This shows that such hacking incidents are a long-term challenge that has not yet been solved.

Data Breach We found many stories of data breaches affecting banks, credit institutes, shops, retailers, or institutions (49) and the governmental (2), educational (1), or healthcare (3) sector. These stories described personal data such as social security numbers or credit card information being stolen, and affected customers often being informed of the incident via email.

Comparison Rader study: They describe theft (75) only in the context of stealing personal information or money through unauthorized credit card use, fraudulent websites, or as part of a phishing scam. They did not report stories about data breaches, which our participants frequently described. For this reason, and in line with the cyber security report [2], we assume that the frequency of data breaches has mainly increased in recent years.

Virus/Malware We found many generic stories related to a virus or malware attacking the victims' computers or phones (22). From those that described the viruses in more detail, seven mentioned that screens behaved differently (e.g., turned blue or blinked), nine that devices slowed down or crashed, and five that people were logged off. Three stories involved link redirects, where the victim was always redirected to a site chosen by the attacker, independent from the URL that was entered into the browser.

> *"Everytime my friend opened up his web browser, it would go to a fake looking Google search engine site. A virus was planted from someone so that it forced him to use that site to search with."*

One participant also mentioned that the virus or malware was stealing data, which was associated with phishing.

Comparison Rader study: They describe similar stories to the ones we found and grouped them under the category of PC effects (95). Their participants also frequently reported that their computers behaved differently than usual due to a virus or malware, such as freezing, being slow, or losing information. In comparison to the Rader study, we found a decrease in stories about viruses, possibly due to the increasing importance of newly emerging threats such as data breaches or ransomware. Still, 23% of our respondents said they had already been a victim of a virus or malware (see Figure 2) showing that these threats are still prevalent.

Ransomware A large percentage of the stories were about ransomware that affected both individuals (13) and companies/public institutions (20). For instance, stories were told about ransomware affecting critical public infrastructure such as oil pipeline companies or hospitals. These stories describe attacks that locked computers or encrypted data and asked the owner to pay a ransom in order to regain data access. Various reasons have been cited as the source of the ransomware, including viruses, clicking on fraudulent links, attachments or pop-ups, or connecting fraudulent external devices. The amount of requested ransom ranged from four hundred to several millions of dollars. Of these stories that mentioned whether the ransom was paid or not, 76% (13) did pay the ransom. In most stories, data access was returned after the ransom was paid. However, in some stories this was not the case.

> *"My friends computer was locked. She got a message [that] there was a virus and she had to call a number. She did and they needed $500. She paid and it did not resolve the problem. She had to take it in and pay more."*

> *"He paid the requested ransom but he still lost all his files."*

Those who did not pay the ransom either found a way to remove the ransomware themselves, had backups of their data, or faced serious consequences.

> *"My brother-in-law's small real estate company received a ransom notice. They were told that unless they paid $100,000 all their files would be destroyed. He thought it was a joke at first. It was not. Luckily they had an off-site backup that saved the day."*

Comparison Rader study: Ransomware was not reported because this type of cyber threat, although it already existed, was very rare in 2012.

Identity Theft Although this theme often appears along with others, we decided to code it as a separate theme, as it was re-occurring. This category includes stories about people whose identities were stolen so that the attacker could open up credit card accounts, conduct fraudulent transactions, or purchase houses and other expensive items in the victim's name. As a result, the victims' credit scores or reputations were often ruined. In some cases, it took them a long time to resolve the problem. Some stories report the usage of fraudulent websites or hacking as the source of identity theft, while most claim not to know why this happened.

Comparison Rader study: They also report on identity theft as part of their category "Theft" (see above) and give the example of identity theft by a fraudulent website that their participant claimed had been "hacked."

Others This category includes various themes that appeared more frequently but could not be assigned to an overarching theme. Two stories were about whistle-blowing and six about that Facebook generally steals data and is not respecting people's privacy. Two other stories were about cyber bullying that led to serious psychological consequences for the victim. Three stories described a person catching a scammer to prevent the scam or to set an example. Two stories mentioned software vulnerabilities leading to security attacks.

5.2 Retelling Stories

When asking our participants with whom they shared the story and why they did so, three main themes emerged:

The majority of participants (64) explained that the story contains a general risk which has to be shared with everybody, while thirty-one participants reported that they shared the story only with impacted people. Impacted people ranged from those who potentially fell victim to a data breach or hack to those who might open spam messages from a specific person.

> *"My friend's Facebook account got hacked. Watch out for links from him."*

Six participants explicitly mentioned that they shared the story with others who they assume to not be knowledgeable (e.g., elderly people) or who they assume to be highly knowledgeable and therefore, interested in their story.

Our participants mentioned a variety of emotions as reasons for retelling the story, which were scary/dangerous (10), unexpected/unbelievable/crazy (7), relevant/informative (10), interesting (8), funny/entertaining (2), and frustrating/sad (3).

The most common reason for retelling (97) was to create awareness and knowledge to protect others from falling for the same threat. Fourteen participants described that an action was required such as changing the provider, reacting to a shutdown due to ransomware, or reacting to a shutdown of computers in a work environment. Six participants answered that the story fitted the conversation, two aimed at getting other opinions, and two simply wanted to spread gossip.

Comparison Rader study: They did not report qualitative findings on why people retell stories.

5.3 Learnings and Behavior Changes

The themes for participants' learnings and behavior changes overlapped since learning and behavior is often intertwined, so we coded them together. Five main themes emerged:

Behavior Most of our participants (215) expressed that they learned some kind of security awareness or caution from the story. While many expressed these in general phrases, e.g. "To be very careful online" or "Security is important", others were specific about their behavior change. Fifty participants reported to have changed their password security practices and usage as a result of the story heard, such as *"keep different passwords for different accounts"* or *"always update passwords"*. Another fifteen updated their software or changed to a more secure version. Twelve participants started to monitor their accounts or credit card charges more carefully. Another six participants did back-ups of their data, mostly as a response to stories about ransomware. Two participants stopped connecting to insecure WiFis and one changed their privacy settings. Five participants mentioned that they communicated with others about their security concerns. Four even took such radical actions as to quit using Facebook or using credit cards.

Comparison Rader study: In line with our findings, the Rader study found that many participants described their behavior change on a very generic level which means that they seemed to not have taken actionable advice from the stories, but but rather vague learnings. As an exception their findings indicated that participants explicitly mentioned to have changed their password habits as well as using antivirus (see paragraph "Tools/Services"), which we can also confirm with our study. When it comes to specific fields in which participants learned something or reported behavior change, the Rader study reported similar findings regarding caution when clicking on links, downloads and shady websites, where participants learned actionable lessons. We also confirm findings from the Rader study of participants being more keen to update software and monitoring their accounts. One theme which we found in our data was not reported in the Rader study: Backing-up data, which was often reported along with ransomware.

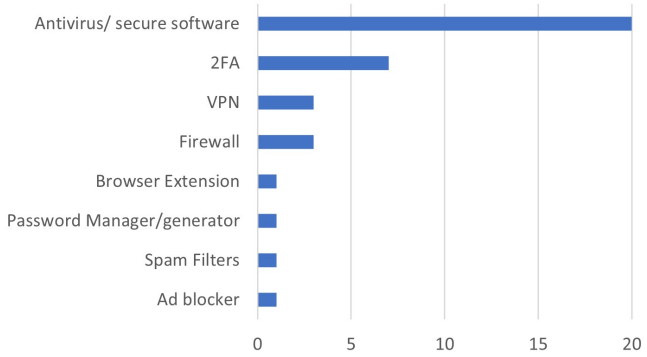

Figure 4: Reported tools/services participants started using after hearing the story (counts).

Distrust Thirty-one participants mentioned a general distrust in data protection online as well as in security applied by companies or institutions. For example,

> *"Even though you think your data is undoubtedly secure, there is always a chance it could be compromised."*

Five mentioned a distrust in a specific technology such as email (4), credit cards (1), or apps. One participant wrote,

> *"Just because Android apps are in the Google Play store does not necessarily mean that they do not contain malware."*

Comparison Rader study: They also found a theme describing that the internet is generally a dangerous place and that their participants often distrusted companies as well strangers in the internet. This is an interesting finding, as it speaks for an experienced helplessness without the participant having learned anything that could improve their situation.

Tools/Services Many participants stated that they started to use a new tool or service after hearing the story (see Figure 4), where the most prominent tool was antivirus software, followed by 2FA, VPNs and firewalls.

Comparison Rader study: They also found that the most participants reported to start using antivirus and keeping it up-to-date. However, they did not report on participants mentioning 2FA or VPNs. This is likely because these tools have grown in popularity over the last decade.

Education Another theme that emerged was that many participants (18) said that they started to educate themselves more about possible threats online as well as prevention mechanisms, such as:

> *"I ended up reading more about scams as well as watching videos on the topic."*

Some mentioned to also educate their employees or vulnerable people (i.e., elderly). This is in line with the theme we

created for why participants retold stories, where we found that sharing them with elderly people who might not be as tech-savvy was often mentioned.

Comparison Rader study: No such theme was reported.

Others 20 participants said they had learned that everyone can be impacted, which was a belief that was not as present for them before they heard the story. Examples are attacks on close individuals which made it clear to participants that such threats are not only discussed in the media but happen in reality, as well as data breaches or ransom attacks on big companies which were considered to have security in place.

> *"It shows how a big company can be hacked and required to pay despite having security software."*

Three participants described that their views were re-enforced.

6 Quantitative Results

In this section, we report our quantitative findings in comparison to those of the Rader study. Note that although the change in behavior and thinking is self-reported as a causal relationship by our participants, we cannot infer causality from our survey, only correlations. For all logistic regression models, calculated for binary dependent variables such as change in behavior (yes/no), retelling (yes/no), we report odds ratios. For the OLS regressions, calculated for interval scaled variables such as change in thinking (1-5), angry/anxious (1-5), seriousness of threat (1-5), we report estimates to interpret our results.

6.1 Stories' influence on thinking and behavior

In line with the Rader study, we found that specific properties of a story change the thinking and behavior of our participants. There were two types of properties, related to the content and the source. We built two respective regression models, which we can directly compare to the results of the Rader study.

Content influences: Table 3 shows that when a story *contains a lesson*, i.e., claims something which one should always or never do, then the odds that the participant reported they had changed their behavior are about twice as high as for stories without a lesson. This replicates the results of the Rader study. For the influence of stories with lessons on thinking, we found a positive but non-significant correlation, in contrast to the Rader study which found a significant correlation between stories containing a lesson and reported change in thinking. This shows that lessons directly affect behavior, but there was inconsistency in perceived change in thinking.

The *seriousness of the threat* described in the story significantly impacts the change in behavior and change in thinking. We found that the odds of a reported change in behavior are 31% higher when the seriousness of the threat increases by one, while the Rader study did not find statistically significant results. Moreover, we found a strong influence of serious threats on the change in thinking, which is in line with the Rader study. We hypothesize that the seriousness of threats is an influential property of the story, as people usually have a *negativity bias* [28]. This means that people tend to give more weight to negative events than to positive ones. Therefore, negative stories are more likely to be present in people's minds and to influence their thinking and behavior.

Whether a story is *autobiographical*, i.e. the protagonist is the same person as the one telling the story, seems to have some influence on thinking and behavior. However, it is unclear which of the two are influenced more, since we found a significant correlation between autobiographical stories and thinking, whereas the Rader study found a correlation with behavior change. This only shows that, since thinking and behavior are so deeply intertwined, a distinction might not always be possible. We cannot be sure why this correlation exists. It might be that autobiographical stories are perceived as more credible or easier for people to identify with.

Source influences: Where and from whom a story is heard also influences the thinking and behavior, as shown in Table 4. When the story is heard in a *casual context* such as at a friend's or relative's house, at a coffee shop, or at home, then our results show that the odds are 41% lower that participants reported they had changed their behavior. This is in contrast to the Rader study where the odds were 95% higher for that casual context changes the behavior. We compared casual context to a more formal context such as at work, in class, or in the library, which seems to have increased the odds for changing the thinking of our participants. Due to these conflicting results, we searched for other variables (e.g. demographic differences) in our data that could explain the difference. We found that participants of age > 60 are more likely to hear the story in a casual context (presumably since they are often retired), as well as participants from 18-29 years

Table 3: Content influences on thinking and behavior

	Change in Behavior		*Change in Thinking*	
	New	Old	**New**	Old
(Intercept)	**0.19**	0.27	**1.66**	2.27
Contains a lesson	**2.02 ****	2.33 **	**0.18**	0.26 .
Seriousness of threat	**1.31 ***	1.14	**0.27 *****	0.15 **
Autobiographical	**1.42**	1.79 *	**0.43 ****	0.15

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Table 4: Source influences on thinking and behavior

	Change in Behavior		*Change in Thinking*	
	New	Old	**New**	Old
(Intercept)	**1.11**	0.21	**3.30**	2.50
Casual Context	**0.59 .**	1.95 .	**0.27 .**	0.28
Knowledgeable Source	**1.12**	1.40 **	**0.32 *****	0.11

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Casual context: compared to "Home context" as baseline.

old. However, we did not find a significant influence of the age group on the change of thinking or behavior, which is why we excluded it from our source influence regression model. When it comes to the change in thinking, we found a positive correlation with the reported change in thinking. This finding is also statistically significant, in contrast to the Rader study. Basically, our results suggest that a formal context more likely influences perceived change in behavior, while the casual context more likely influences a change in thinking. We suspect that people might feel more pressured at work to behave in a certain expected way after hearing a story (e.g., from a coworker or boss). However, since we found different results in comparison to the Rader study, this hypothesis should be taken with a grain of salt.

We found that stories from a *knowledgeable source* (expertise of the source rated on a 1-5 Likert scale) significantly increase the change of thinking. Although we also found a positive correlation for behavior change, this result is not statistically significant. However, since the Rader study found the same correlation with statistical significance, we hypothesize that an effect of source expertise on both change in thinking and behavior exists. Sources with greater knowledge may be perceived as more trustworthy.

Table 5: Influence of emotions on thinking and behavior

	Change in Behavior		*Change in Thinking*	
	New	Old	**New**	Old
(Intercept)	**0.16**	0.27	**1.79**	1.83
Happy	**1.22**	0.91	**0.04**	0.07
Sad	**0.95**	0.64 .	**0.05**	0.15
Anxious	**1.46 ***	1.88 *	**0.33 *****	0.24 *
Anger	**1.44***	1.84 **	**0.14 .**	0.19 *

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Influence of emotions: We asked our participants to what extent (on a 1-5 Likert scale) they experienced the emotions listed in Table 5 after hearing the story. In line with the Rader study, we found a significant impact of feeling *anxious* or *angry* about a story on both thinking and behavior, and negative odds (although not statistically significant) for the influence of feeling *sad* on the change in behavior. This could again be explained with the negativity bias [28], saying that negative events are more impactful than positive ones, and with the EPPM model [32], stating that fear can induce behavior change. Moreover, our results and the Rader study have shown that stories involving serious threats influence reported changes in thinking and behavior, and we hypothesize that such stories are more likely to make participants anxious and angry.

6.2 Story Retelling

While the Rader study found that whether a story *contains a lesson* does significantly increase the odds of retelling this story, this correlation was not statistically significant in our data, although we also found a positive correlation (see Table 6). However, in line with the Rader study, our regression model for content properties shows a 46% increased chance of the influence of the *seriousness of the threat* on the retelling. Hence, the seriousness of threat seems to be a pivotal property of a story, which significantly influences our participants' thinking, behavior, and retelling.

Table 6: Content influence on retelling

	Retelling	
	New	Old
(Intercept)	**0.13**	0.17
Contains a lesson	**1.51**	2.30 **
Seriousness of Threat	**1.46 ****	1.30 *
Autobiographical	**1.28**	1.07

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Table 7: Source influences on retelling

	Retelling	
	New	Old
(Intercept)	**0.65**	0.29
Casual Context	**0.91**	0.88
Knowledgeable Source	**1.14**	1.41 **

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Casual context: compared to "Home context" as baseline.

We did not find statistically significant effects for *autobiographical* stories, nor for any of the source properties (see Table 7) on whether a story is retold or not. This means, we could not replicate the correlation between a knowledgeable source and retelling a story in the Rader study.

Table 8: Influence of emotions on retelling

	Retelling	
	New	Old (Re-calculated)
(Intercept)	**0.14**	0.28
Happy	**1.21**	1.47.
Sad	**0.95**	0.89
Anxious	**1.40** *	1.10
Anger	**1.47** **	1.24

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

For the influence of emotions on retelling (see Table 8), we found a strong correlation between stories that made participants *anxious* (40% increase in the odds of retelling) or *angry* (40% increase in the odds of retelling). This correlation was statistically significant, in contrast to the Rader study. Similar to the influence of these feelings on thinking and behavior, we think that this correlation can be explained by that more exciting stories are more likely retold. This also matches with our qualitative results regarding participant's answers on why they retold the story (see Section 5.2).

6.3 Demographics' influence

We fitted various regression models to investigate the influence of demographics on variables of our interest such as

change in thinking and behavior, emotions, and factors that have been shown to influence perceptions and behavior in the Rader study (e.g., seriousness of threat or context). In this section, we only report those models where we found statistically significant correlations.

Table 9: Influence of demographics on seriousness of threat and change of thinking

	Seriousness of Threat	*Change in Thinking*
(Intercept)	4.25	3.61
Age		
18-29	-0.72 ***	-0.32
30-44	-0.20	0.07
45-60	0.05	0.09
Education		
Some college	0.10	-0.48
Techn., voc. school	-0.04	-0.53
Bachelor Degree	-0.11	-0.70 *
Master degree	-0.13	-0.66 *
Doctoral Degree	0.04	-0.67

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Age: ">60" as baseline; Education: "High school" as baseline.

Table 9 shows that younger participants between 18-29 perceive the seriousness of threat statistically significantly lower than other age groups and are slightly less likely to report a change of thinking after hearing a story, which is however not a significant results (p>0.1). For participants with higher education, we found a statistically significantly lower likeliness of changing their thinking.

Table 10: Influence of demographics on emotions

	Angry	*Anxious*
(Intercept)	3.30	2.57
Age		
18-29	-0.48 *	0.17
30-44	-0.13	0.04
45-60	0.27	0.17
Education		
Some college	-0.34	-0.33 .
Tech., voc. school	-0.70 *	-0.71 *
Bachelor Degree	-0.59 **	-0.48 *
Master degree	-0.55 *	-0.48 *
Doctoral Degree	-1.25 ***	-0.87 **

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Age: ">60" as baseline; Education: "High school" as baseline.

Table 10 shows, that participants age 18-29 and with higher education also reported feeling angry about a story less often. Hence, younger and higher educated participants are less likely emotionally affected by stories and assess their seriousness lower. This might explain why they are less likely to change their thinking, which we found to have a positive correlation with the perceived seriousness of the threat and feeling anxious or angry (see Table 3). We did not find differences in the influence of participant's demographics on the reported behavior change or chance of retelling a story.

7 Discussion

Comparison Rader study: The results of our replication study confirm many of the original findings. We found that neither the topics of the stories nor the ways in which participants learn best from stories have changed much across time and demographics. The threat landscape we discovered in our full stories is very similar to that of the Rader study with the exception of the newly found categories of "Ransomware" and "Data Breaches." This is in line with the Accenture Cyber Threat Intelligence Report of 2021 [2], stating that ransomware as well as infostealing were active problems in 2021. Other threats such as social engineering, hacking, viruses, and identity theft have been an unsolved problem for over a decade. Although we changed the introductory text and some questions to explicitly include mobile threats in addition to computer threats, we did not find neither more stories of mobile threats than the Rader study, nor did we find new story themes related to mobile threats. This shows that the results of the Rader study are still largely valid today, across age and educational differences.

Similar to the Rader study we found that behavioral changes based on stories can help both prevent security threats and respond to them after they occur. Stories often conveyed strategies for responding to threats, such as advice on whether or not to pay ransom, or awareness of data breaches. Our results also suggest that participants often learn distrust through stories, which in many cases was only described on a general level and was unhelpful. Only in some cases distrust led to secure behavior, such as frequent monitoring of accounts. Consistent with the EPPM model [32], we hypothesize that this may be the case since effective responses to fear are only possible if viable solutions to threats are offered. Another interesting finding was that stories can encourage participants to educate themselves about certain security-related topics. We can confirm that the stories were mainly related to what happened rather than why. We suspect that this is due to the fact that security threats often cannot be traced back to their source and are only noticed when they occur.

Stories and psychology of behavior change: Our findings suggest that the threats in the commonly told stories differ from those that participants had experienced themselves. This means that stories can broaden the range of threat awareness. In addition, we found evidence that stories can influence security risk perception, as participants often reported learning that anyone can be affected by security threats after hearing a story that happened to a close relative or a company they previously considered secure. Moreover, our results confirm that stories can influence participants' thinking, which in turn can change their motivation and capabilities and serve as a trigger for adopting secure behavior.

Our qualitative and quantitative survey results suggest that our participants' thinking and behavior are intertwined. For

the seriousness of the threat and the emotions of anger and anxiety, we found a correlation with thinking, behavior, and retelling. Although our results suggest that some factors only affect behavior (such as containing a lesson) and others only thinking (such as autobiographical stories and knowledgeable sources), we argue that the two are difficult to separate. If changes in behavior only, but not in thinking, are reported for one factor, this could also be because people's mental models are often tacit [21] and people may not be aware that they are changing. Behavioral changes tend to be more obvious and therefore easier for participants to recognize and report. Likewise, if participants reported a change of thinking without a change in behavior, altered mental models could affect their security decisions without them being aware.

Advice based on stories: Surprisingly, we found that it made no significant difference whether stories came from the media or from friends or family. It would be interesting to see whether this finding holds in the future as the media landscape continues to change. We argue that our results can be used to better design media articles on security threats, advice, and security training. We suggest that those should focus on stories containing lessons with concrete actions and serious threats to the individual. This is in line with Nurse et al. [23], suggesting that clear actions increase the effectiveness of risk communication, and with the EPPM model [32], stating that fear can encourage behavior change if a concrete solution is presented. One idea could be to create an online platform, e.g. on social media, where people can share security incidents, since we found that autobiographical stories positively effect learning. This platform could serve as a story pool for media articles or security training, which could pass on the most relevant or often occurring stories. When a knowledgeable person leads the training or writes the media article, this could further increase the impact of the stories told.

Participants often reported that they retold stories since they fitted the conversation, which shows that bringing IT security on people's agenda on its own already improves the likelihood of sharing stories and learning from them. This finding could be used, e.g. in companies, to encourage employees (e.g. in specifically therefore scheduled meetings) to share security incidents. We found a positive correlation of sharing security stories at work and reported behavior changes, so this could help people learning from their colleagues. We hypothesize that the reason stories heard in a work context have a greater influence on behavior than those heard in a casual context may be that they influence the subjective norm, which in the theory of planned behavior is the social pressure to perform an action [3, 22]. However, it is up to future work to investigate this further, as the Rader study found that stories in casual contexts have a greater impact on perceived behavior changes.

We derive from our results that younger and better educated participants are harder to reach with security stories, as they commonly perceive threats as less serious and are less likely to report being emotionally affected by stories and change their thinking. We hypothesize that this is because people growing up with information technology have had more exposure to security reports and therefore, perceive security threats as less shocking. Education possibly increases the chances to have heard about similar security incidents before, thus being less anxious or angry about them, and less likely to change the thinking as a result. Future work to explain these correlations is required. However, we still found that this group is influenced by autobiographical stories from knowledgeable sources, which should be kept in mind when designing security advice. We found that elderly and less educated participants might learn easier from security stories. However, according to Frik et al. [15] they are also at higher security risk due to less knowledge and experience with technology, but do not always perceive threats as more severe. Hence, for elderly people or those retired (who do not have access to training at work-places), it would be especially useful to create a platform for sharing stories in their own words.

Methodological reflections: It was generally straightforward to replicate the original study since all needed material was available. We noticed that our participants' responses were similar to the Rader study in terms of complexity and technical details. In line with the Rader study, we also found that some participants gave superficial and general answers when asked how the story changed their thinking or behavior. It could be that these participants were unable to draw specific conclusions from the stories or that the setting of an online survey did not encourage them to explain details. It would be interesting to explore the impact of different stories on people's thinking and behavior in a qualitative interview study in the future. Because the data in our study and the original study consist only of self-reported stories, future work could examine in a prospective study how different stories affect people's security behaviors in the wild. Although we only asked participants to tell us one story that they remembered most clearly, and thus may have missed others, we believe that the reported stories are the ones that are retold most often and thus have the greatest effect.

8 Conclusion

With our replication study, we confirm most of the Rader study's findings regarding which characteristics of stories lead to changes in thinking, behavior, and retelling. In addition, our diverse sample allowed us to examine differences among participants of various age groups and educational backgrounds. Based on our findings, we provide guidance on how security training or media content on IT security can be better designed. We strongly suggest that security stories should be considered alongside professional training and personal experience as important sources of security advice.

9 Acknowledgments

We thank the anonymous reviewers for their valuable feedback on our work. SBA Research (SBA-K1) is a COMET Center within the framework of COMET – Competence Centers for Excellent Technologies Program and funded by BMK, BMDW, and the province of Vienna. The COMET program is managed by FFG.

References

[1] Surveymonkey. https://www.surveymonkey.com/, accessed: 2022-06-01.

[2] Accenture. Cyber threat intelligence report - vol 2 21. https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf, accessed: 2022-06-01.

[3] Icek Ajzen. The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2):179–211, 1991.

[4] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. Mental models of security risks. In *International conference on financial cryptography and data security*, pages 367–377. Springer, 2007.

[5] Vanessa Boothroyd. *Older Adults' Perceptions of Online Risk*. PhD thesis, Carleton University, 2014.

[6] United States Census Bureau. ACS demographic and housing estimates. https://data.census.gov/cedsci/table?q=DP05&tid=ACSDP5Y2020.DP05, accessed: 2022-06-01.

[7] Victoria Clarke, Virginia Braun, and Nikki Hayfield. Thematic analysis. *Qualitative psychology: A practical guide to research methods*, 222:248, 2015.

[8] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and psychological measurement*, 20(1):37–46, 1960.

[9] Sauvik Das, Laura A Dabbish, and Jason I Hong. A typology of perceived triggers for end-user security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 97–115, 2019.

[10] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, 2014.

[11] Sauvik Das, Adam DI 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*, pages 739–749, 2014.

[12] 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 *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75, 2016.

[13] Chris Fennell and Rick Wash. Do stories help people adopt two-factor authentication? *Studies*, 1(2):3, 2019.

[14] Brian J Fogg. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology*, pages 1–7, 2009.

[15] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019.

[16] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 79–95, 2019.

[17] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2647–2656, 2014.

[18] Eszter Hargittai and Yuli Patrick Hsieh. Succinct survey measures of web-use skills. *Social Science Computer Review*, 30(1):95–107, 2012.

[19] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[20] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, 2015.

[21] Anne R Kearney and Stephen Kaplan. Toward a methodology for the measurement of knowledge structures of ordinary people: the conceptual content cognitive map (3cm). *Environment and behavior*, 29(5):579–617, 1997.

[22] Boon-Yuen Ng and Mohammad Rahim. A socio-behavioral study of home computer users' intention to practice security. *Pacific Asia Conference on Information Systems (PACIS)*, 2005.

[23] Jason RC Nurse, Sadie Creese, Michael Goldsmith, and Koen Lamberts. Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE, 2011.

[24] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 2015.

[25] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012)*, pages 1–17, 2012.

[26] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677, 2016.

[27] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[28] Paul Rozin and Edward B Royzman. Negativity bias, negativity dominance, and contagion. *Personality and social psychology review*, 5(4):296–320, 2001.

[29] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. Weighing context and trade-offs: How suburban adults selected their online security posture. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 211–228, 2017.

[30] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*, pages 1–16, 2010.

[31] Rick Wash and Emilee Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, 2015.

[32] Kim Witte. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4), 1992.

Appendix

9.1 Questionnaire

In this survey, we are interested in things you have heard about or learned through stories from others related to protecting your computer or mobile device and yourself from cyber security threats. We are NOT interested in something that happened to you personally, only in stories about other people you've heard, e.g. from a friend, coworker or acquaintance, social media sites, blogs and newspapers, or any other source you can think of.

Cyber security threats might include things like hackers, viruses, malicious apps, identity theft, shady URLs in spam emails, etc. It can be very hard sometimes to tell when someone is facing a cyber security threat- symptoms might include when someone's computer or mobile device is slow or freezes unexpectedly, when programs won't close, or lock up, unwanted popup windows, spam email, posts appearing in someone's Instagram or Facebook account without their permission or knowledge, or other undesirable computer or mobile device issues. Sometimes people cope with these threats by using tools such as antivirus or firewall software, or by making sure to back up their data, or not clicking links or installing apps from people they don't know or trust.

We will start with 4 longer open questions to help you start to remember stories you have heard or read about cyber security. Afterwards, we will continue with shorter questions, which are mainly multiple choice.

1. First, please make a list of as many different kinds of computer or mobile security problems, or threats that you can think of, using only a couple of words to describe each of them.
Open-ended answer

2. Next, think of all the different ways you can protect yourself and your computer or mobile device from cyber security problems or threats, and make a list of these below.
Open-ended answer

3. Take a moment to think back to times in the past when you remember being told or reading about a story related to computer or mobile security. Please make a list of as many of these stories as you can remember, using only a couple of words to describe each story (you may want to read over your answers to the previous questions to jog your memory).
Open-ended answer

4. Finally, please choose one story for which you can most easily recall details about where you were and what happened when you heard or read the story (You can go back to review your list). In a sentence or two, briefly summarize what happened. You will be answering further questions about this story in the rest of the survey.
Open-ended answer

5. How long ago did you hear or read the story?
Answers: Within the last day/ Within the last week/ Within the last month/ Within the last year/ Longer than one year ago / Don't remember

6. Where were you when you heard or read the story?
Answers: At a coffee shop/ At a friend or relative's house/ At home/ At work/ In a computer lab In class/ Other (please specify)

7. Via what medium did you hear or read the story?
Answers: In person (face-to-face)/ Phone/ Text message/ Chat (instant messaging)/ Video chat/ Email/ Blog post/ Social network site (Instagram, Facebook, Twitter, etc.)/ Print news media (physical newspaper, magazine, etc.)/ Broadcast news media (TV, Radio, etc.)/ Online news media (CNN.com, Yahoo News, etc.)/ Don't remember/ Other (please specify)

8. From what source did you hear or read the story?
Answers: Family member/ Friend/ Acquaintance/ Coworker or Boss/ IT or Computer Repair Person/ Stranger/ News Institution/ Don't Remember/ Other (please specify)

9. How knowledgeable do you think the source you selected above is about cyber security? Please rate the source's knowledge from 1 (Not Knowledgeable) to 5 (Very Knowledgeable).

10. Did you tell, send, post, or otherwise share this story with anybody else?
Answers: Yes/ No/ Don't remember

11. Approximately how many times did you share the story?
Answers: 1/ 2/ 3/ More than 3/ Don't remember

12. With whom did you share the story (select all that apply)?
Answers: Family member/ Friend Acquaintance/ Coworker or Boss/ IT or Computer Repair person/ Stranger/ News Institution/ Follower/ Don't Remember/ Other (please specify)

13. How long after you first heard or read the story did you first share it with others?
Answers: Within one day/ Within one week/ Within one month/ Within one year/ Longer than one year/ Don't Remember/ Other (please specify)

14. Please briefly describe why you shared this story with others.
Open-ended answer

15. Was this story about the same person who told the story to you or who wrote it?
Answers: Yes/ No/ Don't Remember/ Other (please specify)

16. How serious was the threat or problem? Please rate the severity from 1 (Not Serious At All) to 5 (Very Serious).

17. Did the story end well or badly for the main character? Please rate the outcome from 1 (Very Well) to 5 (Very Badly).

18. In general, was the story about something you should ALWAYS do (e.g., wash your hands after using the bathroom), or something you should NEVER do (e.g.,

stick your tongue to a frozen flagpole)?
Answers: Always do/ Never do/ Both/ Neither/ Other (please specify)

19. What did you learn from this story?
Open-ended answer

20. This story made me feel... Sad/ Happy/ Helpless/ Curious/ Angry/ Anxious (Not at all - Somewhat - Mostly - Extremely)

21. Did you start doing anything differently to try to protect yourself from IT security threats or problems after hearing this story?
Answers: Yes/ No/ Other (please specify)

22. Please describe one thing you started doing differently after hearing this story.
Open-ended answer

23. Do you believe this story actually happened?
Answers: Yes/ No/ Don't know

24. How much do you think hearing this story has affected the way you think about cyber security threats? Please rate it from 1 (A Lot) to 5 (Not At All)

You're almost done!

25. You have now answered a number of questions about a story, you remembered being told or reading about, related to a computer or mobile security threat or problem.Below, please write the story as if you were telling it to a friend. Use as much detail as you can, including any thoughts or recollections you might have had about what happened as you were filling out the survey. Use about 4-5 sentences to describe the story.
Open-ended answer

26. Have you ever had one of the following experiences? Select all that apply:
Answers: Fell victim to a phishing email message or other scam email/ Received a notification from a company that your information was involved in a data breach/ Had a virus on your computer or mobile device/ Someone broke in or hacked your computer, mobile device, or account/ Stranger used your credit card number without your knowledge or permission/ Identity theft more extensive than use of your credit card number without permission/ None of the above

27. What is your age in years?
Open-ended answer

28. What gender do you identify as?
*Answers:*Female/ Male/ Prefer not to say/ Other

29. What is your highest completed level of education?
Answers: None/ High school/ Technical, vocational school AFTER high school/ Some college/ Bachelor degree/ Master degree/ Doctoral degree/ Other (please specify)

30. What is your current employment status? *Answers:* Employed full time/ Employed part time/ Unemployed looking for work / Unemployed not looking for work/ Retired/ Student /Student and employed part-time/ Disabled/ Other (please specify)

31. Please rate your understanding of each term below from None (no understanding) to Full (full understanding). Wiki/ Meme/ Phishing/ Bookmark/ Cache/ TLS/ AJAX/ RSS/ Filitbly

32. Have you ever received formal training in computer science, software engineering, IT, computer networks, or a related technical field?
*Answers:*Yes/ No/ I'm not sure

9.2 Codebook

Table 11: Codes and counts for full stories

A Ransomware	33	**B Data Breach**	55	**C Social Engineering**	127
A.1 Company/Public Institution	20	B.1 Shop/Company/Bank	49	C.1 Phishing/Scam messages	71
A.2 Individual	13	B.2 Governmental	2	C.2 Scam Call	25
A.3 Ransom payed: yes	13	B.3 Educational	1	C.3 Fraudulent website	15
A.4 Ransom payed: no	4	B.4 Healthcare	3	C.4 Fraudulent pop-Up	8
				C.5 Fraudulent app	4
				C.6 Revenge	2
				C.7 Fraudulent device	2
D Virus/Malware	47	**E Hacking**	112	**F Others**	74
D.1 General	22	E.1 Account/password/data	91	F.1 Others	31
D.2 Screen different	7	E.2 Device	16	F.2 Whistleblower	2
D.3 Computer slow	2	E.3 WiFi	2	F.3 Cyber bullying	2
D.4 Computer crash	7	E.4 Celebrity	3	F.4 Facebook privacy	6
D.5 Logged out	5			F.5 Catching scammer	3
D.6 Link redirection	3			F.6 Security vulnerabilities	2
D.7 Stealing data	1			F.7 Identity theft/Credit card fraud	28

Table 12: Codes and counts for reported learnings and behavior changes

O Behavior		**P Distrust**		**Q Tools/Services**	
O.1 Security awareness/caution	215	P.1 General/ Company/ Institution	31	Q.1 Firewall	3
O.2 Change settings	1	P.2 Credit cards	1	Q.2 Ad blockers	1
O.3 Credit/ account monitoring/ protection	12	P.3 Email	4	Q.3 VPN	3
O.4 Back ups	6	P.4 Technology/Devices	4	Q.4 2FA	7
O.5 Connect to trusted WiFis	2			Q.5 Spam Filters	1
O.6 Updating/ securing software	15			Q.6 Antivirus/ secure software	20
O.7 Password hygiene/usage	50			Q.7 Password manager/ generator	1
O.8 Exchange with others about security (concerns)	5			Q.8 Browser Extension	1
O.9 Stop using tool/service					
S Education		**T Ransom should be**		**V Other**	
S.1 Employees	4	T.1 paid	2	V.1 Everyone can be impacted	20
S.2 Elderly	3	T.2 not paid	1	V.2 View reinforcement	3
S.3 General/ Self	18			V.3 Stop using credit card	3
				V.4 Stop using Facebook	1
				V.5 Other	27

Table 13: Codes and counts for why stories were retold

K Shared with		**L Incident was**		**M Reason**	
K.1 impacted persons	31	L.1 scary/dangerous	10	M.1 Action required	14
K.2 all/ general risk	64	L.2 unexpected/unbelievable/ crazy	7	M.2 Knowledge/Awareness/ Warning/ Protection	97
K.3 other (not/knowledgeable)	6	L.3 relevant/informative	10	M.3 Fitted conversation	6
		L.4 interesting	8	M.4 Get other opinions	2
		L.5 funny/entertaining	2	M.5 Gossip	2
		L.6 frustrating/ sad	3		