Who Comes Up with this Stuff? Interviewing Authors to Understand How They Produce Security Advice

Lorenzo Neil, *North Carolina State University;* Harshini Sri Ramulu, *George Washington University;* Yasemin Acar, *Paderborn University & George Washington University;* Bradley Reaves, *North Carolina State University*

https://www.usenix.org/conference/soups2023/presentation/neil

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

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Who Comes Up with this Stuff? Interviewing Authors to Understand How They Produce Security Advice

Lorenzo Neil
North Carolina State University

Harshini Sri Ramulu
George Washington University

Yasemin Acar
Paderborn University &
George Washington University

Bradley Reaves
North Carolina State University

Abstract

Users have a wealth of available security advice — far too much, according to prior work. Experts and users alike struggle to prioritize and practice advised behaviours, negating both the advice's purpose and potentially their security. While the problem is clear, no rigorous studies have established the root causes of overproduction, lack of prioritization, or other problems with security advice. Without understanding the causes, we cannot hope to remedy their effects.

In this paper, we investigate the processes that authors follow to develop published security advice. In a semi-structured interview study with 21 advice writers, we asked about the authors' backgrounds, advice creation processes in their organizations, the parties involved, and how they decide to review, update, or publish new content. Among the 17 themes we identified from our interviews, we learned that authors seek to cover as much content as possible, leverage multiple diverse external sources for content, typically only review or update content after major security events, and make few if any conscious attempts to deprioritize or curate less essential content. We recommend that researchers develop methods for curating security advice and guidance on messaging for technically diverse user bases and that authors then judiciously identify key messaging ideas and schedule periodic proactive content reviews. If implemented, these actionable recommendations would help authors and users both reduce the burden of advice overproduction while improving compliance with secure computing practices.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

1 Introduction

Most users of technology receive advice from experts to keep themselves and their devices safe. The overarching goal of security advice is to provide reliable and up-to-date security awareness and recommendations to end users so that they can practice secure behaviors. Employees of organizations may receive regular security advice and training from their employers, students may receive security advice from their schools and/or universities, and multiple government organizations including the US Department of State offer security advice to the general public [35]. "Second-hand" security advice abounds, proliferated by media outlets [17,33], websites [22,40,44,48], and peer users [36,39].

End users are thus exposed to a sea of security advice and are unsure which advice is best suitable for them [38,41,44]. Experts also struggle to agree on which security advice should be prioritized. Previous related work demonstrated that experts list a total of 118 studied security behaviors as being the "Top 5" things users should do to protect themselves online [44]. A lack of consensus on the most important security imperatives leaves end users to themselves to prioritize and implement security advice. Authors who write security advice thus have to decide which advice is most important for their target audience, who already struggle to prioritize security advice.

In this paper, we seek to identify ground truth and root causes for why security advice varies in quality and prioritization by going to the source: authors themselves. We report findings from a semi-structured interview study with 21 authors of general security advice where we discussed the full process of advice creation from beginning to end. By "general security advice", we mean security advice just for the general public, or end users with a "general public level knowledge" of security. We investigated authors' backgrounds and motivations, asked about individual and organizational processes surrounding advice, and asked what they felt were the most challenging aspects of advice creation. In reporting the outcomes of these interviews, we present the following key findings:

Content Creation Authors overwhelmingly perceive setting advice scope and technical level as a central challenge. Decisions about scope have major consequences on every other aspect of advice creation. Advice writers also report revising content when novel security threats or events prompt ad hoc additions. These challenges partially explain the overproduction and undercuration of security advice [44].

Internal and External Influences Authors reported input or oversight from a wide variety of stakeholders in their organizations, including technical and operational staff, legal departments, and even C-level executives. Legal regulations and technical standards also heavily influence advice content, with some organizations seeking comprehensive compliance or congruence with multiple sources. Authors consult a wide array of authoritative sources, with little consistency from author to author.

Recommendations Section 5.1 discusses implications of our findings and provides future recommendations. These recommendations include research on sound methodologies for curating and prioritizing advice, research establishing guidance on advice communication for users with varying levels of technical expertise, and for authors to proactively plan advice reviews to improve focus and not just augment advice.

2 Related Work

Security communications towards non-expert computer users comprise of more than just advice style communications. Informal sources of such communications consist of media [17,26,33], stories from peers [39,50], and web pages containing computer security advice [22,40,48]. Formal sources of information that provide general security advice consist of security games [13,47], nudges [4], training programs [24,25,25,47,51], and literature [29,53]. The sources from which users retrieve general security advice impact their security mental models and then ultimately their decision making [7,8,33,38,41,42]. Redmiles et al. suggest that user security decisions can be modeled as a function of past behavior and knowledge of costs, risks, and context of potential security decisions [43]. Understanding the prior work on how security knowledge is communicated to users, we look to investigate a specific but popular medium for end user security communications in security advice.

Since formal security guidance is not as widespread, online general security advice has been crafted to help users practice secure online habits. However, the general public is supplied with an overabundance of security advice and therefore has to prioritize which advice they will follow [21,22,33,40,42]. Prior work has suggested that users typically perform a cost-benefit analysis to determine if the benefits of the advice found are worth the cost of implementing the advice [6,9,10,12,15,20,21,44,45]. Herley et al. analyzed the cost-benefit tradeoff through various forms of security advice to determine much of the available security advice offers a poor cost-benefit tradeoff, therefore prompting users to reject advice [21].

The general public and technical experts have conflicting perceived responsibilities as to who is responsible for security advice implementations [19,23,52]. For example, Haney et al. found that smart home device users have perceived breakdowns in the relationship among who is responsible for the security of their devices between consumers, manufacturers, and relevant third parties such as the government [19]. We build from this prior work to investigate how advice writers determine their perceived set of responsibilities in writing security advice to their intended audience.

In recent years, many researchers have analyzed the quality of security advice for expert [2,3,18] and non-expert [5,30,31,44] computer users. Prior work from Acar et al. evaluated the state of security practices from popular web resources that developers use for programming [2,3]. They found a prevalence of security bugs within current guidance systems, therefore identifying insecure programming practices being advised to developers who seek these web resources [2,3].

The work closest to ours is by Redmiles et al. [44], in which they investigate the quality of security and privacy advice on the web. Their work breaks down the quality evaluation by examining if security advice on the web is comprehensible, actionable, and effective. Their work concludes that the majority of the advice they investigated is perceived as actionable and comprehensible by both users and experts. However, users and experts both failed to come to a consensus as to what specific advice should be prioritized [44]. Not only did experts consider 89% of the 374 identified pieces of advice to be useful, they also struggled with internal consistency and alignment with the latest security guidelines.

The key challenges in addressing the volume and prioritization of security advice, as identified by Redmiles et al. [44], serve as motivations for our work. In this paper, we seek to understand what processes are implemented to write general security advice, as well as what decisions are considered when constructing the advice. We also seek to learn the challenges faced during the advice writing process that impacts the advice content. In doing so, we discover how advice writers gather information to draft advice content, how advice content is prioritized by the writers, and how procedural decision making and responsibilities are perceived by the writers.

3 Methods

We conducted 21 semi-structured interviews with authors of online security advice between September 2021 and March 2022 to understand the processes and decision-making that go into writing general security advice. We obtained written transcripts of audio interview recordings and analyzed the transcripts through deductive and inductive coding. Written transcripts were de-identified by replacing personally identifiable information (participant names, organizational names) with pseudonyms such as F001 for freelance workers, I002 for industry workers, and U007 for university IT and security workers. Participants were informed of the research goals and how their information would be protected in our screening survey consent forms. Our study protocol was approved by our University's Institutional Review Board (IRB).

3.1 Participant Recruitment

This project focuses on a specific expert population: authors of general security advice. We define such authors as those with professional experience in drafting content for general security advice. We recruit participants through purposive sampling of those who qualify through various recruitment channels, namely personal and professional contacts, social media advertising, recruitment on the freelancer platform Upwork, and directly emailing those who manage university security advice websites. We first directly recruited qualifying personal and professional contacts, then we posted messages on professional social media (Twitter, LinkedIn, and industry mailing lists) to solicit potential participants. We also advertised our study on the popular freelancer website Upwork [49] to recruit freelancers with professional experience in writing general security advice. After every interview, we asked participants if they knew other individuals that might qualify for our interview study. Finally, we reached out to IT help desks and information security or technology departments from U.S. universities found through a top national universities rankings website [32]. Here, we contacted 109 universities that provided both general security advice on their website and an email contact to either their IT help desk, information technology department, or security department. We contacted all potential participants with a recruitment email, linking to our public website which presented a study overview, supplementary information, and a link to the screening survey consent form.

Once we identified a potential participant and they replied with interest, we sent them a screening survey and informed consent form through Qualtrics [37]. The screening survey described our research goals at a high level, asked for consent to be video and/or audio recorded for the interview, and requested basic demographic information from the participant [37]. The survey also acted as a qualifier to ensure that the participant had prior professional experience with writing general security advice. Our screening survey asked participants to report on their security experience, such as how long they had been writing security advice, for what companies, and how they learned to write advice. Once eligible participants filled out the screening survey, we scheduled a one-hour interview with them. Participants were compensated with $30 per half hour for their participation in the interviews.

We concluded recruitment when we reached theoretical saturation; i.e., we discovered that participant responses were not presenting new information beyond data we had already collected [46]. Of the 21 participants, 12 were freelance workers, 6 were university security department staff, and 3 were industry workers. 9 of the freelancer workers wrote general security advice for external organizations, similar to a consulting role. 3 of the freelancer workers and 1 of the industry workers wrote general security advice for entities within their own organization or subsidiary organizations. The remaining 2 industry workers and 6 university employees wrote general security advice for the public consumer associated with their networks. Participants of different roles held different levels of involvement for specifically prioritizing the advice content. Awareness experts are communication specialists who reported "translating" advice from security employees to the general public, where security experts, technical experts, and analysts reported researching, brainstorming, or reviewing the audience's environment to formulate ideas for content. Demographic information on gender, advice generation role, and the organization type is presented in Table 1.

Table 1: Participant Demographics.

Gender	
Men: 13 (61.9%)	Women: 8 (38.1%)
Target Audience	
University Members: 6 (28.6%)	External Consulting: 9 (42.9%)
Public Consumers: 2 (9.5%)	Internal Consulting: 4 (19.0%)
Advice Generation Role	
Analyst: 3 (14.3%)	Security Expert: 14 (66.7%)
Awareness Expert: 3 (14.3%)	Technical Expert: 1 (4.8%)
Organization	
University: 6 (28.6%)	Industry: 4 (19.0%)
Defense Organization: 1 (4.8%)	Internet Provider: 2 (9.5%)
Government Office: 1 (4.8%)	Security Provider: 7 (33.3%)
Participant Group	
Freelance Workers: 12 (57.1%)	Industry Workers: 3 (14.3%)
University IT/Sec.: 6 (28.6%)	

3.2 Instrument Creation

Our goal in this study was to investigate the processes, decision-making, and challenges that play a role in the creation of general security advice. Based on our research questions, we drafted an initial set of high level questions. Using this draft, we then conducted two practice interviews and one pilot interview; our pilot was with a researcher who has experience writing general security advice. Based on these interviews, we revised our interview guide into three background questions and nine high level questions corresponding to our research questions, each with sub-question-level prompts.

Our interview guide contains questions about processes, decision-making, and challenges, such as *"Can you tell me about how security advice gets made and distributed at your organization?"*, *"Are there particular areas that are prioritized or discussed more in depth within the general security advice?"*, and *"Are there any tasks completed during general security advice creation/revisions that are challenging or time* *consuming?"* The high-level version of our interview guide can be found in Appendix 7; we provide the full version with prompts in our replication package [1].

3.3 Interview Process

Choosing semi-structured qualitative interviews as our research method allowed us to ask broad questions about advice writing and then follow up with more specific questions where appropriate. Once we met participants virtually to be interviewed, we confirmed that they had read and understood the consent form and began recording. We reminded participants of the options to skip questions or terminate the interview, and we gave them a choice of audio or video recording. All interviews were conducted and recorded remotely via Zoom. Recordings were backed up with Open Broadcaster Software (OBS) [34]. All interviews were conducted in English and lasted between 30 minutes to an hour.

3.4 Data Protection

We took multiple steps to protect participants' privacy and data security. First, all participants were pseudonymized. Once interviews were completed, we saved audio recordings of the interviews and had them transcribed by a GDPR-compliant transcription service. Within each transcript, we thoroughly removed all personally identifiable participant data such as names, organizations, and demographic information. We also did not request identifying, confidential, or private information about our participants or their employers in our interviews. We used end-to-end encrypted tools in all of our study communications and data storage components.

3.5 Data Analysis

Data analysis was performed through inductive and deductive qualitative coding. We use coding not as a means to an end, but as a strategy to make sense of our data [14]. Codebook creation, coding, and discussion of disagreements helped us understand the data, formulate the themes that we describe in our results, and describe advice creation. We created our qualitative codebook based on our research questions, then expanded it with additional codes that emerged through open-coding the transcripts. The codebook was iterated over through weekly discussions with the team and through discussing and resolving disagreements between the first and second coder. The high-level version of our codebook can be found in the Appendix 8. The detailed operationalized codebook is included in our replication package. During the codebook development process, the coders independently double-coded 5 transcripts, with good inter-rater reliability at Krippendorff's alpha $>$ 0.75, and resolved all conflicts through discussion [16], after which the primary coder coded the remaining transcripts. With Krippendorff's alpha $>$ 0.75 for all transcripts, we are confident that our codebook is stable, represents our data well, and that our coding strategy was sound [28]. Altogether, the coders coded 21 and 5 transcripts, respectively.

3.6 Limitations

As with any interview study or self-reporting study, participant responses may be biased (e.g., self-reporting bias, social-desirability bias) or incomplete [27]. Specifically, some participants were not able to answer all questions we asked due to either a lack of access to that knowledge or a lack of experience.

Over half of our participants were freelancers (57.1%) who all reported writing advice for company employees in some consultation role. We also do not have detailed data on the audiences beyond what authors reported, though we feel it reasonable to assume only relatively large organizations have employees dedicated to this task. Some freelancers specialize in security advice, while others work on technical writing more broadly. Authors wrote for employees, university students, customers, or users, but in all cases, the authors assumed readers have a "general public level knowledge."

In theory, it is possible that paid participants would fraudulently participate in interviews. However, for participants recruited from advice websites, we are reasonably certain that they were genuine. For UpWork recruits, we specifically reached out to those who listed relevant expertise on their resumes; since writing is not UpWork's main focus, there is little incentive to fraudulently report this expertise. Participant pre-survey data and interview behavior also matched up. We are therefore reasonably sure that our participants were genuine.

Lastly, any study involving qualitative coding is subject to author biases and different coding strategies among coders. We address these biases in our investigation by first establishing a list of high level coding categories a priori that represented the high level questions that we developed in the creation of the interview, as mentioned in Section 3.2. A second research team member double coded five of the transcripts to ensure that the codebook was able to capture data that reflected our research questions, regardless of the coder.

4 Results

In this section, we present our qualitative findings from analyzing the in-depth perspectives of advice writers during general security advice creation. We use participant quotes to represent in their own words how participants answer our interview questions, and ultimately our research questions. We present exploratory findings for understanding the processes, decision making, and challenges encountered by the authors who write general security advice. Such volunteered information includes the company, target audience, and advice

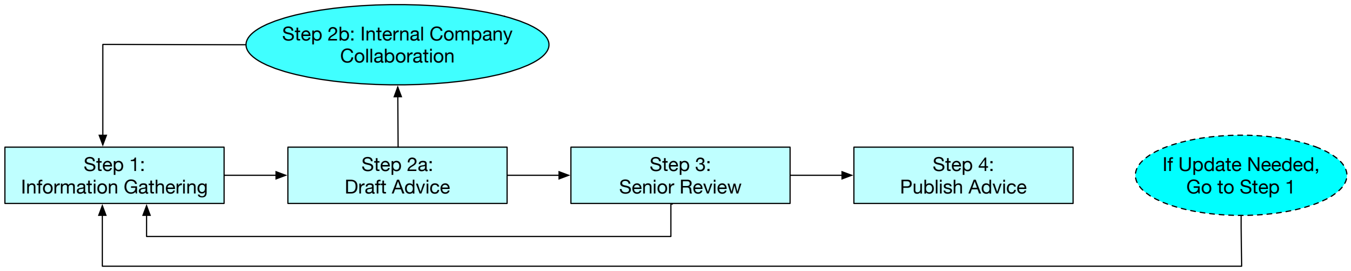
Step 2b: Internal Company Collaboration
Step 1: Information Gathering
Step 2a: Draft Advice
Step 3: Senior Review
Step 4: Publish Advice
If Update Needed, Go to Step 1

Figure 1: How experts write general security advice.

generation role they assumed while writing general security advice.

We find that participants followed a common advice creation for advice writing, found in Figure 1. This four-step process reflects advice-writers gathering information, drafting advice, sending the advice for review, and then publishing the advice, with options for iteration and further information gathering and collaboration in each stage. We also find that authors primarily prioritize and revise their advice content based either on current security trends or in response to security incidents. We organize the remainder of our results around this process. In Section 4.1, we describe how participants gather information for their advice content. Next is Section 4.2, where we explain the decision making that advice authors make when drafting and revising the advice. Section 4.3 details how advice authors collaborate with different internal company departments on the drafted advice before it is reviewed by senior-level employees and the company's legal department, in the case the legal department was involved. Lastly, Section 4.4 reports challenges participants mentioned for writing general security advice and also what improvements they stated could help general security advice writing.

4.1 Information Gathering

Here we explore findings from the first phase of advice writing, and information gathering. In this phase, authors are simultaneously gathering specific pieces of information (e.g., "prefer long passphrases") and establishing the scope of the advice more generally (e.g., "we should discuss password strength").

Theme 1: Advice writers research their environment to scope their advice. Some participants indicated that clients or stakeholders had already defined the scope of their advice documents. In the majority of cases, though, participants were left to figure out what advice was needed based on their own research of the client environment or what would be compliant with the organization. In these situations, authors develop a conceptual model that identifies what issues need to be addressed within the advice. This model is based on the organization, technology, and problems an organization currently faces (e.g. what areas where they are weak in security).Two broad approaches emerged from the interviews: holistic review and gap analysis. The primary difference between them is whether the advice is being written "from scratch" or to supplement existing advice.

As an example of holistic review, F020 explained they begin by determining "what are the devices, connected devices, the architecture and design of the network as well. How the company or how the devices are connected to each other and how the information is being transferred and sent between all the devices." From there, security advice is drafted for the elements of the system. In a gap analysis process, authors compare their architecture and operational environment to the advice available, and where advice is not present for an area that motivates additional material:

> "*Honestly, I report directly to the CISO. We meet every week for an hour at least, and we try to stay in lockstep about where the gaps are with what our incident response and governance compliance, and all those other teams are doing that can be addressed through getting educational materials out there in front of people.*" — U019

Theme 2: Advice writers base their own writing on multiple distinct external sources. 20 out of 21 participants stated they refer to an external source for sample information to include in their advice. These external sources may be regulations, technical standards, or industry or government agency documentation. Participants reported using multiple types of source for their content. 12/21 participants refer to legal regulations, specifically privacy regulations like GDPR(7/21 participants) and HIPAA(4/21 participants). One participant said about regulations they refer to:

> "*I would even say GDPR, where it clearly mentioned 'portal', 'what is personal data', 'what kind of controls', 'how consent should look.' Because, so easily, every company after the Internet boom — every website — was collecting data randomly from users without their consent.*" — F008

Participants specifically mentioned reviewing ISO standards (10/21), NIST publications (9/21), and PCI-DSS (8/21). In some cases, participants' employers may suggest that the advice they publish should comply with regulations or standards the company adheres to. In others, the participants rely on these documents primarily to influence content:

> "*Normally, most of the companies we experienced are starting, and for certain companies, we normally recommend starting with NIST and ISO; they are well known, and their resources are well known, and they are well used.*" — F006

Authors also seek out external sources because the target audience may need to understand how to use specific software or how to mitigate a specific security issue. Sample advice in online web postings from government agencies was also referenced by participants as additional guidance for the advice they write, as one participant states:

> "*I use also some additional resources, such as NCES.ED.gov. This is the link that I also found on some extra information about security agreements, about some templates, for example.*" — F020

In aggregate, our participants cited a total of *20 distinct external sources* for their own work. Overall, these sources tended to be authoritative, so the content is likely correct. However, if these "upstream" standards documents were not properly scoped or written solely for technical experts, those issues may propagate "downstream" to general advice.

Some sources (e.g., GDPR, NIST publications) saw wide usage by a plurality of participants. However, of the total 20 cited external sources, only 5 were cited by 6 or more of participants.

4.2 Advice Drafting and Decision-Making

In the second step, advice writers draft advice based on gathered information and specific decision-making. Decision-making that impacts the advice content includes considering what areas of advice to prioritize, perceived responsibility authors held in advice writing, and addressing the usability of the advice.

Theme 3: Advice writers prioritize content in response to specific incidents or current trends. 13 participants indicated that specific security incidents or current industry trends were key prioritization factors. These participants form half of the participants in each of our four advice generation roles and form the majority of participants in each of the six organization groups. F006 describes how remote access became important during the COVID-19 pandemic:

> "*From my experience, most of the companies right now have employed remote work for their employees...They have a higher risk of having their data breached or compromised. So for me, what I would say, the remote access policy is the most important in this area, and we have to look into that because it's easy to compromise and very hard to detect what has happened.*" — F006

One participant described how incidents at other organizations led to advice creation:

> "*Sometimes if they give advice, it's based on something that's going on. For example, in a ransomware attack, they say, "Okay, universities are confronted with this type of attack, we should be careful with this.""* — I002

Advice creation may also correspond to events within the organization.

> "*I would say anything time critical is going to be prioritized, so if a change is happening and there's a deadline by which a user is going to need to make a change in accordance with whatever it is that's occurring, or people need to know about this change before it occurs, something like that is certainly going to be a priority.*" — U007

Theme 4: Advice writers most commonly cover online fraud and password security. While prioritizing advice on current trends or incidents was common, several specific areas were highlighted by participants. 10 participants indicated a priority on online fraud (e.g., phishing, social engineering, identity theft, email scams). On online fraud, U018 said:

> "*I've seen a lot of advice that we've been putting out regarding job scams or email scams. Phishing is a big one that we've put out a lot of general guidance on. Those are the only big ones that really come to mind is the job scams and the phishing.*" — U018

Five participants mentioned password security and authentication. On authentication, I002 said:

> "*And then, of course, password security is also a very important topic on everything that has to do with password security, like use of password managers, multi-factor authentication.*" — I002

Theme 5: Advice updates are reactive. 16 participants reported updating advice after new security trends or incidents become prominent. This theme of revising advice to reflect current trends or security incidents was also mentioned by at least half of participants within all six organization groups. A theme that indicates prioritizing content over novel or recurring advice topics. A majority of participants within the analyst, awareness expert, and security expert advice generation roles responded similarly. On reacting to new security incidents, U018 said:

> "*Any new information that we find we like to provide to the community so that they're aware of the new ways that these scammers or the phishers or the bad actors are trying to get to them.*" — U018

Theme 6: Advice writers cover a wide variety of less-common topics. Outside of online fraud and password security, participants mentioned prioritizing 12 other areas of advice, but no more than 4 participants mentioned any particular topic. Participants mentioned areas like remote access policy management, frameworks, organizational policies, incident response, and risk assessment. These trends concur with prior work that indicated a lack of consensus on advice prioritization [44].

A potential explanation may be that organizations have different advice needs, and our interviews support that interpretation. While fraud advice was the highest mentioned prioritized advice, it was only mentioned by half of the participants within only three different company types, respectively. Every participant representing either a defense company or internet provider mentioned prioritizing fraud advice, and five out of six total university workers mentioned prioritizing fraud advice. The rest of the advice areas are sparsely mentioned among the different participant sub-groups. This finding may also be caused by our Theme 5 findings in that new advice topics are constantly being addressed, given whatever security incident or trend is current.

Theme 7: Advice writers rarely curate advice by intentionally deprioritizing topics. Most participants did not provide significant responses when asked what areas of security advice were *not* prioritized or why. Four participants said advice for obsolete or deprecated technology would be removed or deprioritized. When asked, F016 replied: "*There's a lot of old depreciated functionality in Microsoft Windows.*" (F016). Others mentioned deprioritizing impractical or overly technical advice, though in at least one case this deprioritization was reluctant. For example, I003 mentioned encryption advice as a topic to deprioritize given being "too technical" for general security advice.

.

Theme 8: Advice writers consider usability, but without a consistent or systematic methodology. 20/21 participants mentioned an attempt to make their general security advice usable. However, participants mentioned 9 different methods to address usability, none of which were mentioned by more than 8 participants. 8 participants stated they simplify the technical language of the advice so that the general public can understand the advice. Participants also mentioned using visualizations and graphics to enhance usability:

> "*Our job is to translate this to something less technical and comprehensible for a broad public. Make it sometimes also a bit more visual — more attractive for users.*" — I002

Six participants determined if advice was usable by considering how they themselves would follow the advice.

> "*One of the things that we look at as we're writing the advice, how would we implement it? If we can't figure out how to implement our own recommendations within our own teams... how could we possibly expect people to be able to implement this?*" — I004.

Some participants considered usability but without a specific method for writing or evaluating advice usability.

> "*It's not really a process per se that is implemented. It's just something that we keep in mind to make it as user-friendly as possible.*"" — U018

Theme 9: Help desks are considered a backstop for unclear advice. 20 participants stated their organization had a team (such as a help desk) that could address users' security questions. U007 noted that they assumed that if advice is unclear, the help desk would correct the issue.

> "*Our expectation in every case is if the user is looking at instructional pages and they're confused about what they mean, or basically confused about anything that they see on the central IT website, that they would contact the help desk.*" — U007

We believe that this perspective may be optimistic about users' likelihood of asking questions before engaging in an unsafe action, and in any case this would be an interesting perspective for future work. On the other hand, if help desks receive the same questions frequently, it may be an indicator to authors that they should update advice on a topic.

Theme 10: Advice writers claim a wide range of responsibilities when writing general security advice. Prior work established a mismatch between users' and manufacturers' expectations of each other in smart homes [19]. Inspired by this effect, we asked participants about how much responsibility they or their company bear in advising users of secure practices. Overall, participants gave answers ranging from high levels of responsibility to virtually no responsibility. We also noticed that responses differed between the participants' roles, though we do not claim a literal correlation because this is an initial qualitative study. One of the university participants noted they take extreme ownership of their users' security education, and they stated their team's goal is to: "*help them, guide them, and educate them, and basically be a partner with them*" (U018). On the other hand, a freelancer gave a different perspective on perceived responsibility:

> "*Well, we give advice for the sake of advice. We want to be sure that we are not promoting what we do or represent. We are not trying to sell, like force you to patronize or do business with us*" — F011.

An industry worker mentioned assuming varying levels of responsibility depending on the content:

> "*It depends on what we're writing and why. If I'm writing the security advice or scoping the payment card industry data security standards audits, I'm just going to lean towards every time writing advice that would limit the scope of our environment because obviously, that makes it easier for us to pass the audit. If I am writing advice for, say, being ready to do something with data privacy, for instance, marking data as highly confidential things like that. I'm going to be as broad as I can be because I want everything protected*" — I004.

Overall, we recorded seven different categories of responsibility suggested by participants, though none were mentioned by more than six participants. Other levels of perceived responsibility included writing advice to comply with standards, motivating changes in security behavior, or going beyond documents to offer security workshops.

4.3 Collaboration and Review

In step two of the writing process, advice writers collaborate with internal company departments who review the advice. Then, in step three, the advice is sent to senior-level employees for final review and approval. In both steps, advice writers revise until the requested revisions are approved by the relevant stakeholder. Otherwise, the advice is approved and then published in step four.

Theme 11: Advice writing is distributed and collaborative. 16 participants stated there were multiple writers who worked on content, and they stressed the importance of multiple writers to lessen workload and include multiple perspectives:

> "*Currently, I tend to get most of the cybersecurity writing assignments in our group. I wouldn't necessarily say all, because we do have a focus on trying to develop bench strength, and within our group there are also people who are responsible for the communication regarding specific IT services offered by departments.*" — U010

18 participants mentioned collaborating with internal company departments. Security (12/21), marketing and communications (7/21), and human resources (HR) (3/21) were the most mentioned departments for advice collaboration. Participants noted that the mix of security experts and non-experts helped create content that is technically accurate and understandable to a broad audience:

> "*The central IT communications group (none of them have been members of the information security group) [works] closely with information security. So if they're writing about something that's a security issue, they're going to be corresponding with one or more people within information security making sure that they have the details right in their write-up. Or they may start with a couple of paragraphs that someone in information security supplied, and then they'll write their page around that to make sure that they're getting the technical details right.*" — U007

Theme 12: Advice is routinely reviewed by senior personnel. 17 participants mentioned submitting proposed general security advice to senior level employees (management or advisory board) for review, feedback, and approval. The university employees and industry workers we interviewed keep their advice within their own group before it is sent to their own management who then approves the advice. Freelancers writing for other organizations submit their advice to the management of their client company for review and approval. For example, participant F014 mentioned review by C-level executives.

Theme 13: In-house legal counsel can be heavily involved in advice creation. We reasoned at the beginning of the study that one cause of the overall lack of prioritization of security advice might be organizations writing comprehensively to limit liability rather than focus on the most likely issues. Therefore, we specifically ask about the involvement of counsel.

7 participants confirmed that their legal department was involved to ensure that the advice met certain legal standards and was up-to-date with the current law. As F011 explains:

> "*We believed that being a good lawyer does not mean being a good security expert, ... so [lawyers] just review. If they feel something should be removed on legal grounds, they advise us. nd if they feel that we need to include some things based on legal grounds, they let us know. We include those things and then send that back to them for review, and then we go back and forth until they are satisfied with the documents.*" — F011

Another seven participants stated their legal was occasionally involved depending on the content or intended audience:

> " *If it comes to data protection specifically or a GDPR specifically, yes [legal is involved], because they would be the experts. For the rest, no.*" — I003.

The remaining seven participants indicated that they were either uncertain of the role of legal counsel or were certain that legal counsel was not involved. While legal counsel indeed influences content, we conclude that the extent of their influence does not explain the breadth and variety of security advice reported in the literature.

4.4 Reported Challenges and Improvements

Theme 14: Advice writers struggle to scope advice for broad audiences who lack fundamental security knowledge. 12 participants specifically mentioned difficulty in identifying not just the necessary topics for their intended audience, but also explaining relevant solutions for diverse technical settings. Simplifying advice content was recorded in responses by participants who mentioned it as a possible method to improve future general security advice. Throughout the study, participants gave examples of how both the intended audiences and teammates they worked with during advice writing came from different backgrounds and therefore all have different levels of security awareness. Therefore, it is important that general security advice be simplified for all intended audiences:

> "*I think not underestimating your audience, trying to empathize, trying to put things in terms where they understand that what we're helping them with is really the thing that they want the most.*" — U019

This challenge is especially seen in advice for employees who need to use software but lack necessary security awareness. Specifically, writing advice content that accounts for accurate assumptions about the intended user's security knowledge. One participant stated it is easier to advise more experienced clients who have security knowledge than those who are less experienced. Another participant mentioned that

> "*The problem internally was I think mostly that our IT teams supposed that everyone knew that we had a password manager, and they knew how to use it. But basically, this wasn't the case because a lot of people — I think also a lot of new people working for the organization — didn't know that it existed*" — I002

Theme 15: Advice writers value direct security training, despite its costs. Participants perceived that rectifying gaps in fundamental security knowledge is difficult:

> "*The most time-consuming task is when a company needs to train their employees, which takes a little time to train and give awareness to the employees.*" — F006

They also still recommend direct training.

> "*We believe in constant improvement. We believe in trainings. We believe in our teleconferences. We believe in individual investments in their whole training. So we encourage our team members to learn more. As a company, we try to find where we can get the kinds of trainings, conferences, events and all of that so that we can get updated on the current trends and security.*" — F011

One participant noted an alternative approach to traditional trainings:

> "*During the Cybersecurity Awareness Month we have games (particularly online, given the COVID). I'm astounded at how many people reach out and want to play these games for $25–$50 gift cards. So provide more games to attract people and use that to ask them questions. Perhaps one game session focuses on multi-factor, and another game focuses on strong passwords.* " — U009

Theme 16: Participants recognize the need for proactive updates. Participants also desired to revise or audit published advice on a regular basis, as opposed to strictly reactively as discussed earlier.

> "*Somebody needs to be looking through the pages and making sure that they're still relevant and that they still have current information, and I think that's an area that we're not really that good at.*" — U007

Theme 17: Collaboration and review leads to delay in publishing advice. We previously discussed how authors credited collaboration and review with leading to more readable and appropriate advice. Participants mentioned that collaborators who either are not consistent in their practices or do not meet important guidelines when writing the advice are challenging to work with. 6 participants mentioned that collaboration leads to delay because it requires the time of multiple busy parties. Time from senior stakeholders is even more difficult:

> "*A lot of times, those stakeholders are upper management. It's hard to get on their schedules. So there's always room for improvement in that. Sometimes the process takes too long because you're literally waiting for a day when you can get four people in a room together, and it's two weeks out. So there would be room for improvement there. Maybe that's top-down buy-in where they say this is more important than anything else; make time for it, which only happens after a breach. I would say those are two areas that would make things easier.*" — I004

5 Discussion

In this section, we contextualize our results with prior literature on advice prioritization, procedural decision making, and perceived responsibility in end user security. We then discuss how these findings can promote better practices for curating general security advice with methodological recommendations for both advice writers and their organizations.

5.1 Identifying Lack of Consensus

Advice Prioritization Participants prioritized their advice to reflect current security trends or respond to security incidents during advice construction and revision. Prioritized advice topics experience variable attention over time and may undergo fluctuating cycles of prioritization. Similarly, advice revisions exhibit a reactive manner in an attempt to constantly keep up with the latest security incidents and trends. While it may seem appropriate to prioritize content like this, it leads to a possible overproduction of advice on numerous security topics. We see this in Theme 6 as participants mention a total of 14 topics they prioritize in their advice writing.

Differences in prioritized advice topics among our study population may also be likely contributed by the differences in specific target audiences, roles, and organizations. However, even participants among the same groups sparsely agreed on which specific topics of advice they should prioritize. Rather, they instead looked to whatever novel security threat they determined they needed to cover. Relying on the latest threats and trends for advice writing also makes it more difficult to determine which security advice should *not* be prioritized. Outside of not covering obsolete or impractical advice, advice writers rarely provided significant responses to how they would deprioritize security advice.

We believe the reluctance to curate or deprioritize content partially explains the advice prioritization crisis documented in prior work. To borrow a common expression, "if everything is a priority, nothing is." Practitioners recognize that the attack surface for modern computing is vast and ever-changing. However, they may fail to account for the effort and opportunity cost to users caused by comprehensive advice. Our findings on the curation of security advice from advice writers add context to a continued theme from prior work indicating a lack of consensus on which general security advice should be prioritized [44]. Our results show that content covered in security advice is not curated to cover perennial topics, rather it is curated to cover many novel topics. Focusing on novel threats instead of perennial threats for security advice may contribute to overwhelming end-users with security advice they do not need. This implies that much general security advice found online may either be outdated or less relevant than when it was first written. Users of varying levels of security experience are left on their own to distinguish which security advice they actually need or is still important. While security experts are better equipped to make these important choices, end users lacking proper security awareness are less likely to understand the distinction between outdated and relevant security advice. This increases the number of security topics that end-users have to read through in advice and determine which advice they should prioritize. We make recommendations for a more proactive approach to advice and improving the lack of consensus for prioritizing general security advice in Section 5.2.

Procedural Decision Making A lack of consensus in procedural decision making was also prevalent in our findings. This is first observed among our Theme 1 and 2 findings which describe how information is gathered for their advice. We discovered that advice writers experience challenges in identifying key aspects of the scope of the advice they are tasked to write for their intended audience. This is a critical challenge given that most participants in our study state that information gathering is their first task in writing advice and sets the foundation for the scope of the content. If advice writers then make decisions on prioritization given an insufficient foundation, their advice will experience variable prioritization, given their inability to consistently define a scope for their advice. P009 stated they would prefer their advice to "target messages to students. It's a challenge. What we create is available to them, but how it's delivered and where it's delivered should be better targeted." Participants among all of the recruited groups experienced this challenge regardless of their organization or intended audience. General security advice affects end users in universities, organizational employees, and many other types of audiences who lack adequate general security awareness. A lack of consistency in properly identifying how general security advice should be written leads to a lack of consensus in advice prioritization from experts, which then trickles down to the lack of advice prioritization among general users.

Advice writers also refer to multiple distinct sources of sample advice that include any legal regulations, technical standards, or other organizational entities. In total, we identified 20 different external sources that participants mentioned they use to influence their general security advice. Of the 20 different external sources mentioned, only four were mentioned by at least 30% of participants. Similar to how this work and prior work [44] demonstrate a lack of advice content prioritization, there is also a lack of consensus among organizations and advice writers on which external sources to pull sample advice from. We see this lack of consensus among participants of the same recruitment group and also between participants of different recruitment groups. Specifically, we observe differences in external sources cited for influencing advice content even among participants who share both the same intended audience and the type of organization they worked for. An upstream usage of distinct external sources and an inconsistent foundation for gathering information for advice add more clarity as to why security experts differ in security advice prioritization. As suggested in prior related work [19], we discuss the importance of both advice authors and organizations to formulate standards to consistently curate perennial topics for security advice in Section 5.2.

Lastly, it is evident there is no consensus on agreed-upon methods in which advice authors consider the usability of their general security advice. Also, it is unclear if participants are performing appropriate usability checks in their advice for their intended audience. This lack of consensus for methods in considering the usability of general security advice construction may be due to the lack of experience or knowledge about usability from both the authors and organizations. Another possible factor could be the pressure to release advice for a client within a specific time frame, a challenge that is seen more often for industry or freelancer workers. This increased pressure to meet deadlines to produce content may come at the expense of thoroughly considering the usability of general security advice. Regardless, a lack of consensus on which usability methods to implement to write general security advice can create advice of variable degrees of usability. Prior work has shown that end users follow or reject advice based on perceived cost and benefit analyses of the advice [6, 10, 15, 21]. This adds another burden that end users have to consider when deciding what general security advice they should prioritize. On top of deciding if advice presented to them is relevant to their needs, they also have to consider if that advice is worth implementing given the opportunity costs of implementing the advice. We recommend that specific usability tactics should become standards agreed upon by experts and authors of general security advice in order to lessen this burden. We explain this in further detail in Section 5.2

Perceptions on Security Responsibilities Previous work by Haney et al. [19] identified an interdependent relationship within user perceptions of the responsibility of smart home device privacy and security between three actors, namely the smart home device end users themselves, device manufacturers, and third parties such as government or regulatory bodies. In that paper, it was reported that users based their actions on that perceived interdependent relationship and therefore would not consider themselves the sole protector of the security of their smart home devices. However, manufacturers and regulatory third parties do not always act on this interdependent relationship, thus there exist gaps in understanding of the responsibilities for each party. In our work, we discovered several different responses for how authors of general security advice assess their perceived responsibility in advice writing. Some participants only wrote advice to comply with standards or requirements their organization enforces whereas other participants emphasized a need to educate their intended audience to develop better security decision making habits. Overall, there is no agreed upon consensus for what levels of responsibility that authors of general security advice or their organizations should assume in assisting their target audience. Our findings support results from previous work and highlight gaps in responsibility assumed not just between the general public and entities providing content, but also between the parties responsible for generating general security advice for users. Gaps in perceptions of shared responsibilities among the experts and end users fall further than just for smart home users, but also for both the general public and organizations who seek assistance with general security. A lack of agreed upon consensus on perceived responsibilities is apparent within both end users and the experts. This leads to increased confusion about which parties should be responsible for mitigating what issues or making security decisions for end-user software and technology. In Section 5.2, we add onto recommendations from previous related work [19] and make suggestions for explicit responsibility establishment for future general security advice creation.

5.2 Methodological Improvements for Advice Writing

We identify areas of improvement for general security advice construction by analyzing the current state of advice construction from the lens of the writers. We suggest methodological improvements for general security advice construction based on our current findings and findings from previous related work [11, 19, 44].

5.2.1 Develop the Domain of General Security Advising

A lack of consensus across multiple areas in the general security advice writing process indicates that its domain is not fully developed. We describe six domains of focus for professionals to consider when writing general security advice.

Resources/Technology: The biggest challenge participants mentioned when writing general security advice was defining the scope of advice content and how the advice can be broadly applied to all intended targeted audiences. P004 and P021 both advocated for the creation of an open source based repository to act as a research forum for advice writers. Both participants recommended that such a system should contain organized information about current general security questions or issues and that this system can be queried or allow open discussion between advice writers. Such a tool could be used by advice writers to both better discover what security topics need advice on and collaborate with other advice writers to come up with implementable solutions to communicate with their target audiences. While this is one idea of tool creation, future research may investigate the creation of new tools to help authors of general security advice identify advice content. Advice writers then would not have to rely on waiting for an incident to happen or a new trend to become popular in order to generate ideas for general security advice.

Relationships: Multiple parties are involved in discussing and reviewing general security advice before it is published. Understanding differences in viewpoints and requirements among organizational parties has been studied at a broader scope for internal corporate communications [11]. Critical challenges described in such work emphasized the importance of addressing communication related management problems between management and communications practitioners. Similarly, we recommend that advice writing parties each receive clear definitions on their responsibilities and roles during advice writing to reduce confusion among everyone involved.

Participants also mentioned that meeting with every party involved in the writing process can be time consuming since different parties (e.g., marketing, communications, security) have different schedules and duties to adhere to. Authors of general security advice should consider adopting a formal schedule and process that is agreed upon by all collaborating parties. This may help decrease the amount of time waiting for collaborating parties to meet and discuss advice content and how it should be implemented.

General Security Focus: Improving the security culture of both the intended audience and parties who write general security advice was recommended by participants as a means of improvement. Security awareness games, workshops, and other events to keep authors of general security updated on security trends help them stay connected to what issues are affecting their target audience. Providing the same programs for general users is also helpful for them to learn general security advice in a non-conventional way and should be considered by experts who write general security advice.

Content Improvement Metrics: Agreeing to a set of usability practices to make general security advice more usable can consist of the following: advice visualizations (e.g., diagrams, images, media, etc), and simplifications of overly technical words or phrases or templates to organize the advice content.

Community Support for Advice Writing: Establishing a community for advice writers to collaborate on ways to address common security threats through advice would greatly help writers in earlier stages of advice writing. Such a community can communicate by sharing best practices, sample advice from experts, or even recommendations for non advice-based approaches (e.g. games, workshops). Methods to evaluate the effectiveness of published advice over time can also be agreed upon by a community of advice writers. Academic researchers should also be involved in community collaboration in advice writing.

Human-Centered Engagement in Earlier Writing Stages: Advice writers in our study rarely mentioned user interaction with their intended audience as a means to generate content. Earlier stages in the writing process would benefit greatly from engaging directly with their intended audience to learn about security problems they may encounter. These direct interactions can help inform writers on which topics to prioritize, as well as how understandable or actionable their advice is. Writers should also gauge their users on whether the volume of advice is too high.

5.2.2 Proactive Advice Updates and Curation

Proactive Advice Updates: Implementing a proactive manner of updating or reviewing general security advice better ensures the advice is up to date. Participants mentioned performing more frequent check ups or audits of general security advice helps maintain the relevancy of the advice. Without consistent content audits, there increases the chances of advice becoming stagnant or not reflective of the current environment. Therefore, adopting a proactive approach to reviewing general security advice on a timely basis prevents the presence of outdated advice.

Establish a Set of Agreed Upon Standards for Advice Curation: We advocate there be a consistent standard to determine perennial areas of general security advice to cover. We say a set of standards since no one standard can be broadly applied to all advice of all intended audiences. Therefore, we suggest advice authors and industries communicate both what advice should be perennial and what advice should not be prioritized. Also, we suggest the research community investigate further what security advice end-users actually claim they need and if they are receiving that advice now.

6 Conclusion

In a semi-structured interview study with 21 authors of general security advice, we analyze the processes, decision making, and challenges that experts face when writing general security advice. We corroborate the lack of consensus on security advice as well as responsibility assignment from prior work. Our contribution gives insights into the context and reasons for this lack of consensus: advice writers struggle to define the advice scope and prioritize the information necessary to write advice, and must prioritize time-sensitive events over curating perennial advice. Based on our findings, we provide recommendations for how general security advice authors can better develop the domain of general security advice writing, implement proactive approaches towards writing and revising general security advice, and establish a set of agreed-upon standards for advice writers to reference when curating general security to end users. Addressing the lack of agreement on how general security should be advised from both the end user and advice writer side may improve the relationship between both parties in general security advice prioritization and perceived responsibilities.

References

[1] Anonymized replication package. https://advice22.netlify.app/.

[2] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek, and Christian Stransky. You get where you're looking for: The impact of information sources on code security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 289–305. IEEE, 2016.

[3] Yasemin Acar, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L Mazurek, and Sascha Fahl. Developers need support, too: A survey of security advice for software developers. In *2017 IEEE Cybersecurity Development (SecDev)*, pages 22–26. IEEE, 2017.

[4] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017.

[5] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Washington, D.C., August 2013. USENIX Association.

[6] Adam Beautement, M Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*, pages 47–58, 2008.

[7] Maia J Boyd, Jamar L Sullivan Jr, Marshini Chetty, and Blase Ur. Understanding the security and privacy advice given to black lives matter protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2021.

[8] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[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 *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 117–136, 2019.

[10] Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags. It's all about the benjamins: An empirical study on incentivizing users to ignore security advice. In *International Conference on Financial Cryptography and Data Security*, pages 16–30. Springer, 2011.

[11] Joep P Cornelissen. Corporate communication: A guide to theory and practice. *Corporate Communication*, pages 1–336, 2020.

[12] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. Why employees share information security advice? exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67:196–206, 2017.

[13] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 915–928, 2013.

[14] Victoria Elliott. Thinking about the coding process in qualitative data analysis. *The Qualitative Report*, 23(11):2850–2861, 2018.

[15] 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.

[16] Deen Freelon. *ReCal2: Reliability for 2 Coders*.

[17] 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, Santa Clara, CA, August 2019. USENIX Association.

[18] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Möller, Yasemin Acar, and Sascha Fahl. Developers deserve security warnings, too: On the effect of integrated security advice on cryptographic {API} misuse. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 265–281, 2018.

[19] Julie Haney, Yasemin Acar, and Susanne Furman. " it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 411–428, 2021.

[20] Julie M Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. " we make it a big deal in the company": Security mindsets in organizations that develop cryptographic products. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 357–373, 2018.

[21] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, pages 133–144, 2009.

[22] Cormac Herley. More is not the answer. *IEEE Security & Privacy*, 12(1):14–19, 2013.

[23] Sri Lakshmi Kanniah and Mohd Naz'ri Mahrin. A review on factors influencing implementation of secure software development practices. *International Journal of Computer and Systems Engineering*, 10(8):3032–3039, 2016.

[24] Ponnurangam Kumaraguru. *Phishguru: a system for educating users about semantic attacks*. Carnegie Mellon University, 2009.

[25] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[26] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):1–31, 2010.

[27] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[28] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[29] Christine Mekhail, Leah Zhang-Kennedy, and Sonia Chiasson. Visualizations to teach about mobile online privacy. In *Persuasive Technology Conference (poster)*, 2014.

[30] Lorenzo Neil, Yasemin Acar, and Bradley Reaves. Investigating Web Service Account Remediation Advice. In *Who Are You?! Adventures in Authentication Workshop*, WAY '20, pages 1–6, Virtual Conference, August 2020.

[31] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. Investigating web service account remediation advice. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 359–376. USENIX Association, August 2021.

[32] U.S. News. Best national university rankings. https://www.usnews.com/best-colleges/rankings/national-universities?_mode=table. [Online; accessed February 23, 2022].

[33] James Nicholson, Lynne Coventry, and Pamela Briggs. " if it's important it will be a headline" cybersecurity information seeking in older adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2019.

[34] OBS. Open broadcaster software. https://obsproject.com/wiki/OBS-Studio-Overview. [Online; accessed February 23, 2022].

[35] U.S. Department of State. *Fraud Warning*. https://travel.state.gov/content/travel/en/us-visas.html/.

[36] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 1–18, 2022.

[37] Qualtrics. qualtrics. https://www.qualtrics.com/. [Online; accessed February 23, 2022].

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

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

[40] 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.

[41] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 931–936, 2017.

[42] 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.

[43] Elissa M Redmiles, Michelle L Mazurek, and John P Dickerson. Dancing pigs or externalities? measuring the rationality of security decisions. In *Proceedings of the 2018 ACM Conference on Economics and Computation*, pages 215–232, 2018.

[44] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 89–108, 2020.

[45] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[46] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52(4):1893–1907, 2018.

[47] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99, 2007.

[48] Sarah Turner, Jason Nurse, and Shujun Li. When googling it doesn't work: The challenge of finding security advice for smart home devices. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 115–126. Springer, 2021.

[49] Upwork. Upwork. https://www.upwork.com/. [Online; accessed February 23, 2022].

[50] 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*, pages 1–12, 2018.

[51] Laurie Williams, Andrew Meneely, and Grant Shipley. Protection poker: The new software security" game". *IEEE Security & Privacy*, 8(3):14–20, 2010.

[52] Jing Xie, Heather Richter Lipford, and Bill Chu. Why do programmers make security errors? In *2011 IEEE symposium on visual languages and human-centric computing (VL/HCC)*, pages 161–164. IEEE, 2011.

[53] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257, 2016.

7 Interview Guide

1. Ice Breaker Questions:
   (a) When and where did you learn to write general security advice?
   (b) What is your current occupation?
   (c) Can you describe the type of company you worked for when you wrote general security advice?
2. Can you tell me about how security advice gets made and distributed at your organization?
   (a) Is there a decision making model for the creation of security advice?
   (b) Are there any external sources used to provide sample advice that gets posted?
3. Can you tell me about the people or roles involved in the process?
   (a) Does a chain of command or hierarchy exist within the parties?
   (b) Are all of these parties involved with the company or external?
   (c) What is typically the experience or knowledge of parties in regards to computer security?"
4. Are there particular areas that are prioritized or discussed more in depth within the general security advice?
   (a) If so, what is the reason for this prioritization or focus into this area?
   (b) Are there any areas that are intentionally excluded from being covered in the security advice?
   (c) If so, what is the reason for not writing advice for this specific area?
5. Is the general security advice regularly updated or reviewed?
   (a) If so, what systems or procedures are in place to update/review the advice?
   (b) Were these systems/procedures always in place, or did an event or policy create them?
   (c) If possible to comment, are there legal practices or regulations that prompt the creation and/or regulation of the advice?
6. Is your company's legal department involved in the creation or even discussion of the general security advice?
   (a) If so and you are able to comment, are they able to edit or create any parts of the advice, or even recommend certain areas be covered?
7. If possible, can you comment on how much responsibility your organization claims in assisting in general security?
   (a) How much of the advice is well-meant, or meant to limit the reliability/responsibility of the service in security matters with general security?
8. Does your company have a team or group of individuals that handle general security internally?
   (a) Are they external workers?
   (b) Do they have expert experience in computer security?
9. When creating the general security advice, is there a thought process as to how actionable or practical the advice may be for the typical user?
10. These last questions are more so geared to your own experiences when creating the advice.
    (a) Are there any tasks completed during general security advice creation/revisions that are challenging or time consuming?
    (b) Have you ever thought about how general security advice for your company, or overall can be improved?

8 Codebook

High Level Codes

Codes	**Code Explanations**
1a. Learn to write Advice	How the participant first learned to write general security advice.
1b. Occupational Role	Occupations for participants during the time they wrote general security advice.
1c. Companies	Places where the participant worked for and wrote the advice.
2a. Formal Writing Process	Any formal or structured process (Gap Analysis, SLA, defining scope, etc) used for writing advice.
2b. Informal Writing Process	Advice writing that is not dependent on any formal process. Rather, it is written in an informal or non-structured writing process.
2c. Legal or Non Legal Guidelines	Mandates, regulations, laws, or frameworks that were used to influence the advice. These are not solely or specifically technical, but apply to a wider range of compliance standards.
2d. Technical,Security Standards	Advice content is influenced by technical and/or security standards.
2e. External Entities	External entities (organization, group, company, etc) that authors seek for guidance on advice writing.
3a. Background,Experience	Backgrounds of fellow workers/teammates of advice authors.
3b. External Company Party Collaboration	Parties outside the primary advice construction group that collaborate in the advice writing process (outside or external to the company).
3c. Internal Company Party Collaboration	Parties outside the primary advice construction group that collaborate in the advice writing process (within the company).
3d. Writers	The number of people specified by the participant who helps physically write the advice.
4a. Most Prioritized Advice	Most common/prioritized topics of advice written.
4b. Least Prioritized Advice	Least common/prioritized topics of general security advice.
4c. Reasons Advice is Prioritized	Reasons or events that would cause the creation of general security advice.
4d. Reasons Advice is not Prioritized	Reasons certain advice has not been covered as much or prioritized.
5a. Revision Process	Processes and reasons to revise advice.
6. Company's legal department	Company's legal department involvement within the advice writing process.
7. Responsibilities	Responsibilities claimed by participant companies when creating the advice.
8. Internal Support	Support for clients that is internal or technical (not advice).
9. Advice Usability Thought Process	Though process or methods of improving actionability/usability of the advice.
10a. Challenges	Challenges with writing the advice.
10b. Improvements	Authors' opinions of how the advice writing process could be improved.