"A five-year-old could understand it" versus "This is way too confusing": Exploring Non-expert Understandings and Perceptions of Cybersecurity Definitions

Lorenzo C. Neil*
North Carolina State University
Raleigh, North Carolina, USA
lcneil@ncsu.edu

Charlotte Healy*
University of Maryland, College Park
College Park, Maryland, USA
chealy@terpmail.umd.edu

Julie Haney*
National Institute of Standards and Technology
Gaithersburg, Maryland, USA
julie.haney@nist.gov

Abstract

Experts struggle with explaining cybersecurity in a language and tone appropriate for non-expert audiences. This communication gap may make it difficult for a broad and diverse audience to fully engage in cybersecurity. Fundamental forms of communication, such as definitions, can be for a means for experts to communicate cybersecurity concepts to non-experts. To explore how non-experts perceive cybersecurity definitions and identify potential areas of misunderstanding and misconception, we performed a semi-structured interview study with 30 non-experts of different generations (ages) and education levels. Our findings reveal that non-experts may have incomplete mental models of cybersecurity, misinterpret terms and concepts commonly used in definitions, and express strong preferences for how cybersecurity is defined. While our study focuses on definitions, our results have broader implications for how cybersecurity should be communicated to a diverse range of individuals.

CCS Concepts

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

Keywords

cybersecurity, definitions, communications

ACM Reference Format:
Lorenzo C. Neil, Charlotte Healy, and Julie Haney. 2025. "A five-year-old could understand it" versus "This is way too confusing": Exploring Non-expert Understandings and Perceptions of Cybersecurity Definitions. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3706598.3713820

1 Introduction

In the midst of dynamic and complex cybersecurity threats targeting all aspects of society, cybersecurity responsibility cannot fall solely to specially-trained cybersecurity experts. One can argue that cybersecurity is ultimately a "collective moral responsibility" consisting of "jointly held, individual moral responsibilities" [40], which are assigned to both experts and non-experts (individuals without specialized cybersecurity expertise). Collective action is, in part, predicated on building common ground – mutual knowledge, beliefs, and assumptions – through communication [14].

Unfortunately, the originators of cybersecurity communications (often cybersecurity experts) may have a difficult time translating highly technical concepts into the language and tone appropriate for non-experts, resulting in a communication gap [26, 48]. While clear communications can help people understand the importance and scope of cybersecurity [50], communications that are vague, use unfamiliar technical language, or are overly complex may alienate, confuse, or frustrate non-experts [61, 74, 76], resulting in less trust and engagement with cybersecurity technologies or practices [23, 51, 61]. Additionally, how a communication frames the relevance of cybersecurity to the audience — for example, as a workplace duty vs. an essential part of daily life -– has potential to impact people's motivation to learn more about particular cybersecurity risks (e.g., ransomware) or enact specific cybersecurity practices (e.g., multi-factor authentication) [23, 27, 61].

Cybersecurity definitions – as simple, yet fundamental forms of communication– likewise have the potential to influence cybersecurity perceptions and behaviors. Definitions – statements of "the meaning of a word or word group" [39] – are important for individuals and society as a whole for reducing confusion, creating common ground, establishing concept boundaries, and laying a foundation for further learning [43, 72]. The philosopher Aristotle believed that a definition signifies the *essence*, "the what it is to be," of a thing [15]. Thus, a cybersecurity definition can serve as an efficient means to communicate the essence of cybersecurity.

Today, there are many different definitions of cybersecurity with varying levels of complexity and completeness [23, 47]. Despite the importance of these definitions in forming the basis for how cybersecurity is collectively understood and acted upon in our daily lives, there have been few efforts to explore their suitability for and potential impacts on the broader non-expert audience for which cybersecurity matters [23]. Prior works on the interpretations of cybersecurity definitions have largely focused on technical, legal, or academic audiences [12, 17, 64], with none investigating non-expert

[*] Authors contributed equally to this research.

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713820

perspectives or differences in understandings across age/generation or education groups. Without these insights, the cybersecurity community may unwittingly create an environment of digital exclusion in which some non-experts disengage from cybersecurity and fail to take appropriate protective actions [23, 31].

To gain insights into non-experts' thoughts about and understandings of cybersecurity definitions, we conducted a semi-structured interview study of 30 non-experts from different generations and education levels. Specifically, we aimed to answer the following research questions (RQs):

RQ1: How do cybersecurity non-experts understand and define cybersecurity?

RQ2: How do non-experts understand and perceive published cybersecurity definitions?

- **RQ2a:** How do non-experts assess the definitions in terms of desirable and less desirable attributes?
- **RQ2b:** Which terms and concepts are less understood?
- **RQ2c:** Are there trends in understandings and perceptions across demographic (generation and education) groups?

Our study makes several contributions:

- Through a first-of-its-kind elicitation of non-expert thoughts about cybersecurity definitions, we show that varying interpretations about the meaning of cybersecurity may engender or confirm (sometimes incorrect or incomplete) assumptions about the scope of cybersecurity and its relevance to non-experts. We illustrate ways in which a communication as simple as a definition can act as a boundary object (a translation device between communities [28]) that can inhibit or facilitate establishment of common ground and recognition of collective responsibility for cybersecurity.
- By using definitions as an efficient way to uncover specific communication influences, we extend the literature by revealing non-experts' preferences for how cybersecurity is described at its core, terms and areas of confusion that may benefit from additional explanation or different word choices, and demographic trends related to understandings. Based on our findings, we offer practical suggestions for improvements in cybersecurity definitions and, more broadly, other forms of cybersecurity communications (e.g., training materials, dialogues) towards empowering, motivating, and promoting inclusion of non-experts in cybersecurity.
- Our study provides a foundation for future research efforts, such as investigating non-experts' understanding of other cybersecurity terms and types of cybersecurity communications. Additionally, demographic trends observed in our study can serve as a foundation for future, generalizable research that can aid the cybersecurity community in developing more effective, usable, and actionable communications for a range of individuals.

2 Related Work

We provide a synopsis of relevant literature about non-experts' understanding of cybersecurity, cybersecurity definitions, and the communications gap between experts and non-experts.

2.1 Non-experts and Cybersecurity

Cybersecurity non-experts may have inconsistent understandings of cybersecurity, as they rely on mental models that are inaccurate, incomplete, or contradictory [29, 33, 55, 69]. They may overgeneralize and conflate concepts (e.g., security and privacy), while failing to see the full range of threats [70]. Further, many individuals never receive cybersecurity training [59, 66], with those that do (typically in the workplace) often viewing it as boring and ineffectual [3]. Cognitive biases, time pressures, poor usability, lack of skills and knowledge, and desensitization can lead to development of negative emotions (e.g., fear, insecurity) and psychological states (e.g., frustration, resignation) about cybersecurity [18, 54, 67, 75]. In turn, negativity can result in avoidance and rejection, less motivation to learn, decreased self-efficacy, and insecure behaviors [10, 74].

Past research found demographics influences on cybersecurity understandings and behaviors. Cybersecurity conceptualizations differ across life stages [31]. Older adults are often fearful of cybersecurity risks and challenged to implement countermeasures [42, 56, 58] while younger adults are less likely to rate cybersecurity as a priority [52]. A survey of a U.S.-representative sample confirmed a knowledge gap where individuals of lower socioeconomic status (linked to lower education levels) were less likely to obtain cybersecurity advice from authoritative sources (e.g., the workplace) and less often took protective actions [59].

While the goal of our qualitative study was not generalizability, we purposefully recruited participants include populations underrepresented in studies that have often consisted of mostly younger [29, 33], older [42, 49], or highly educated [11, 29, 33, 69] individuals. We also utilized cybersecurity definitions as a way to elicit participant understandings about cybersecurity.

2.2 Communicating Cybersecurity Concepts

2.2.1 Cybersecurity Definitions. Cybersecurity definitions vary widely in the terms they include, their complexity, and their structure [8, 17, 35, 47]. While some argue there is benefit in using different terminology for different contexts [23, 43], others caution against the lack of standardization [12, 17, 64]. More so, issues arise when definitions are not consistent in communicating scope or purpose, interpreted differently by different audiences, or not accessible to those without deep knowledge of the topic [43, 72]. These inconsistencies could potentially result in non-experts being confused or limited in their thinking about what cybersecurity involves, who is responsible, what cybersecurity is protecting, and how cybersecurity impacts them personally [23, 47].

Towards standardization, several researchers proposed their own definitions based on analysis of existing definitions in standards and policies [17, 64] or expert input [12]. However, since these analyses were targeted at cybersecurity professionals, policy makers, or academics, it is unclear as to whether those would be meaningful and appropriate to non-experts. Our study addresses this shortfall by using definitions likely to be found in an internet search (rather than those in less-accessible standards and policies) and investigating how definitions are received and understood by non-experts.

2.2.2 Communications Gap. Cybersecurity professionals may suffer from a "curse of knowledge" in which they struggle to effectively communicate technical information to non-experts [48, 71]. They may use terms not well-understood by non-experts or hold incorrect assumptions about the knowledge levels of their audience. Scientific or technical jargon, in particular, can negatively impact non-experts' ability to process information and reduce support for emerging technologies [9, 65].

Research on the general public's understanding of cybersecurity blogs [76], advice [46, 48, 60, 61], and warnings [7, 30, 41] illustrate the communications shortfall. Issues include: the use of unfamiliar technical terms [7, 30, 41, 76]; lack of completeness [46]; and text being at reading levels above the recommended for the average reader [60]. To cope with unclear communications, individuals may gravitate towards explanations that are easier to understand, making them susceptible to information that is inaccurate, exaggerated, or oversimplified [23]. Further, communication gaps can impede non-experts' ability and willingness to take protective actions and engage in cybersecurity [23, 26, 50, 61]. Our study is motivated by these disconnects and extends prior work by taking a targeted look at how the language used in cybersecurity definitions contributes to or bridges the communication disconnect between expert and non-expert communities.

3 Methods

In July–August 2023, we conducted 30 semi-structured interviews to explore how non-experts' understand and react to different cybersecurity definitions.

3.1 Study Design

We selected a semi-structured interview methodology as it afforded a richness of data, the ability to ask follow-up questions to explore responses, and the opportunity for participants to add other relevant information [16].

3.1.1 Definition Selection. We opted to use cybersecurity definitions, rather than longer descriptions, to elicit participant reactions and thoughts. This minimized the amount participants had to read and allowed a more granular focus on terms routinely used in cybersecurity. Further, cybersecurity definitions are sometimes provided without additional context [47], so our approach may reflect the level of detail internet search results might provide.

As a basis for definition selection, we obtained a raw dataset of 167 unique cybersecurity definitions from a prior systematic search and analysis [47]. For each definition, the dataset contained the definition text, source link, Google search results page (if applicable), source type (e.g., government, industry, education), and number of times the same definition was found (repeated) in the systematic search. We then scoped the dataset to only include definitions with working URLs and those non-experts would be able to readily access and read, for example, collected via an internet search, not behind a publication paywall, and not translated into English (given our U.S. sample). We further filtered for definitions from sources with a vested interest in informing the public about cybersecurity and which would reasonably have credibility and expertise in cybersecurity (e.g., government agencies with a cybersecurity focus, cybersecurity vendors, cybersecurity education and training programs, dictionaries), as recommended in [57]. The filtered dataset consisted of 134 definitions (dataset available in Supplemental Materials).

We then performed deductive, qualitative coding on each definition using the codes from [47], which represent the range of components found in the definition corpus. In this process, two research team members independently coded an initial set of 25 definitions, then met to discuss code application and resolve coding conflicts. We achieved a Cohen's Kappa inter-rater reliability score of 0.95, indicating almost perfect agreement [37]. The remaining definitions were then divided among the two researchers and coded. See Table 1 for the codes, examples, and number of definitions per code.

The same two researchers then met to decide upon criteria for selecting a subset of definitions for use in the interview study. This agreed-upon criteria included the following considerations meant to reflect both the variability and commonalities of the definition corpus:

- Source type - definitions provided by industry, general reference/dictionary, and authoritative government institutions
- Component inclusion - definitions containing different combinations of coded components
- Commonly-used terms - definitions containing technical jargon common within the cybersecurity field and identified as potentially problematic for non-experts (informed by [7, 47, 61, 64, 76])
- Length - both shorter and longer definitions
- Search results page - if found via Google search, definitions appearing earlier in the search page results
- Number of repeated definitions - as indicated in the raw data set, definitions identified as being repeatedly found in a Google search

The researchers proceeded to independently select a subset of definitions they felt would encompass the criteria (note that definitions did not need to meet all of the criteria to be considered). The two then met to compare, discuss, and ultimately come to a mutual decision on eight definitions to be used in the interview protocol. Of the eight, we took special care in the selection of the two step-through definitions to ensure 1) at least one was from an authoritative institution (e.g., government agency) widely known for its cybersecurity expertise and 2) the definitions were of sufficient length with multiple components to allow for a rich discussion with participants. A third researcher reviewed and concurred with the definitions and justifications for selection. See Table 2 for the final eight selected definitions. [1] Appendix B contains additional details on the reasons each definition was selected.

3.1.2 Interview Protocol Development. Two definitions (D1 and D2) were used to conduct in-depth step-throughs with participants. Six definitions (SA - SF) were used in a sorting/characterization exercise. As a visual aid, we developed presentation slides showing the definitions for real-time sharing with participants via the virtual meeting platform. The following describes the interview procedure:

(1) **Introduction** and review of participant rights
(2) **General questions about cybersecurity**, including: participant's familiarity with and self-assessed knowledge of cybersecurity; their personal cybersecurity practices; any negative cybersecurity experiences they experienced; how they would

[1] URLs in the table last accessed December 5, 2024, with exception of SC (August, 2024) which is no longer available on the web page as of Dec. 2024.

Table 1: Definition codes (components)

Code/ Component	Description	Examples	Number Definitions
Action	answers question of what cybersecurity does in general	"protect" "defends"	130
How/What	the thing(s) that cybersecurity is composed of	"policy, technology, and education" "set of principles and practices"	99
Objects	what the action is taken on	"networks, devices, programs, and data" "hardware, software, or electronic data"	125
Security principles	the tenets of cybersecurity	"confidentiality, integrity, and availability" "availability, integrity, authentication, confidentiality, and nonrepudiation"	19
Threats	mentions of actors involved in cyber attacks, cyber risks, or means by which cybersecurity can be compromised	"cyber threats" "being stolen, compromised, or attacked"	114
Who	the actor(s) responsible for cybersecurity practices	"individuals and organizations" "an enterprise"	9

describe cybersecurity to a friend; and their own definition of cybersecurity

(3) **Step-throughs** of two cybersecurity definitions (D1 and D2) to glean participant's understanding of and thoughts about each definition, whether they would recommend the definition to a friend or family member, and which of the two definitions they preferred. The researcher began sharing the presentation at the beginning of the step-throughs.
(4) **Sorting exercise** involving six cybersecurity definitions (SA - SF) to glean the participant's opinions about definition characteristics (their favorites, which they think are easy to understand, comprehensive, and useful to them). The researcher continued to share the screen, demonstrated an example sort, then moved definitions to the characteristic boxes (favorites, easy to understand, etc.) according to participant selections.
(5) **Sorting definitions source reveal** to get participant's reactions on how/if their original definition impressions change once the source is revealed. The researcher stopped screen sharing after the source reveal discussion ends.
(6) **Final questions** about how the interview impacted the participant's understanding of cybersecurity.

Two experts reviewed the interview protocol to check for alignment between interview and research questions, use of plain language, and the appropriateness of interview procedures. One expert reviewer had over 20 years of research experience in usability and survey design. The second expert was a cybersecurity practitioner with over 15 years of experience that included the standardization of cybersecurity definitions and the translation of cybersecurity guidance for small businesses lacking cybersecurity expertise. This reviewer also checked definition correctness. After the reviews, we made minor modifications to the protocol.

We conducted three pilot interviews with non-experts representative of the age groups in our target population: one man in their 20s/30s, one woman in their 40s/50s, and one woman in their 60s/70s. During the pilots, we assessed interview logistics and whether interview questions resulted in expected types of answers. At the conclusion of each pilot, we asked each participant about question clarity and interview flow. While there was no feedback that necessitated changes to the questions, we made minor logistical adjustments. The full interview protocol is in the Supplemental Materials.

3.2 Recruitment and Participants

To be eligible for the study, participants had to be adults (18+ years of age) living in the U.S. who had never formally studied or worked in a field related to information technology (IT) or cybersecurity. We employed a consumer research firm to recruit participants from a nationwide panel[2] of individuals who had agreed to be contacted about research opportunities.

To determine eligibility, prospective participants completed an online screening survey (see Supplemental Materials) to collect basic demographic data and prior IT/cybersecurity experience. They also had to confirm they could fulfill the technology requirements: 1) ability to do the interview from a computer to ensure a larger screen for reading slides and 2) their computer could support virtual meetings.

After reviewing the screening responses, we selected 30 participants with a focus on diversity of generation (as defined by Pew Research Center [19]), and education level. A sample size of 30 allowed us to include participants representing each demographic group. This number also considered advice of research methodologists for minimum number of in-depth interviews (ranging from 12 [24] to 25-30 [21]) to ensure there were enough to afford "richness, complexity and detail" [4]. We achieved both inductive thematic saturation (emergence of new codes/themes) and data saturation [63] with P18, but completed additional interviews to ensure demographic groups were well-represented.

[2] https://www.prodege.com/

Table 2: Definitions used in the interviews

ID	Definition	Source Organization	Source Type	Web Page Title and URL
D1	the process of limiting malicious attacks through good security processes, training, and securing computer networks, systems, devices and any other digital applications	Amplify Intelligence	Cybersecurity service provider	*What is cybersecurity?* https://www.amplifyintelligence.com/cyber-security
D2	an approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems	National Institute of Standards and Technology	U.S. Government	*Small Business Cybersecurity Corner Glossary* https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary#C
SA	the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access	Digital Guardian	Cybersecurity vendor	*What is Cyber Security? Definition, Best Practices, Examples* https://digitalguardian.com/blog/what-cyber-security
SB	the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this	Oxford Dictionary	Online dictionary	*Cybersecurity* https://languages.oup.com/google-dictionary-en/
SC	the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation	Cybersecurity and Infrastructure Security Agency	U.S. Government	*Explore Terms: A Glossary of Common Cybersecurity Words and Phrases* https://niccs.cisa.gov/cybersecurity-career-resources/glossary#letter-c
SD	the means by which individuals and organizations reduce the risk of being affected by cyber crime	National Cyber Security Centre	UK Government	*Information for Individuals and Families* https://www.ncsc.gov.uk/section/information-for/individuals-families
SE	the collective methods, technologies, and processes to help protect the confidentiality, integrity, and availability of computer systems, networks and data, against cyber-attacks or unauthorized access	Synopsys (now Black Duck)	Technology design and testing service provider	*Cyber Security* https://www.blackduck.com/glossary/what-is-cyber-security.html
SF	the protection of internet-connected systems such as hardware, software and data from cyberthreats	TechTarget	Technology marketing and sales service provider	*Definition cybersecurity* https://www.techtarget.com/searchsecurity/definitions

Table 3 summarizes participant demographics. Of the 30 participants, 16 were female and 12 were male. Demographics per individual participant and education level are in Appendix A. Beyond demographics, participants assessed their own level of cybersecurity knowledge as little, moderate, or expert. Sixteen rated themselves as having little or little-moderate knowledge, with the others saying they had moderate or moderate-expert knowledge.

Table 3: Summary of participant demographics (N = 30)

Demographic	Subcategory	n	%
Generation	Gen Z (born 1997 or later)	7	23.3%
	Millennials (born 1981-1996)	9	30.0%
	Gen X (born 1965-1980)	4	13.3%
	Boomers (born 1946-1964)	10	33.3%
Education level	High school/equivalent	8	26.7%
	Some college/2-year degree	12	40.0%
	Bachelor's/Grad degree	10	33.3%
Self-reported cybersecurity knowledge	Little	14	46.7%
	Little-Moderate	2	6.7%
	Moderate	13	43.3%
	Moderate-Expert	1	3.3%

3.3 Data Collection and Analysis

We conducted interviews using the Microsoft Teams virtual meeting platform. Two researchers participated in each interview: one as the interviewer and one who advanced the slide presentation and managed the recording. We saved a separate slide presentation with sorting exercise results for each participant and recorded and transcribed the interviews, which averaged 50 minutes.

We performed a thematic analysis of the transcripts, utilizing both deductive and inductive coding. We first developed an *a priori* code list based on the research questions and interview protocol. Using this initial list, each of the three research team members coded a subset of three interviews (136 minutes of audio), then met to discuss code application, suggest emergent codes, and develop a codebook. We performed a second round of coding on the same transcripts, meeting to discuss and refine the codebook.

We then coded the remaining interviews using the codebook (see Supplemental Materials), with each transcript coded by two researchers. Each pair met to discuss and resolve differences in code application. Aligned with the recommendation of methodologists regarding analysis of in-depth, interview data [5, 36], in our discussions, we focused not just on agreement but also on how and why disagreements arose. This approach was beneficial in identifying alternate data interpretations given the diverse perspectives of our team (see 3.5). For disagreements, each coding pair engaged in discussion and reached a consensus. Throughout analysis, we wrote analytic memos and regularly met to discuss relationships and patterns among the codes.

For the sorting exercise, we calculated summary statistics, for example, definitions selected as favorites.

3.4 Ethics

The study was approved by our research protections office. Participants returned an informed consent prior to their interviews, signifying agreement to participate in the study and be recorded. To protect confidentiality, we labeled all data with anonymous participant identifiers (e.g., P18). Participants received a $75 gift card as compensation.

To reduce the chance that participants would look up cybersecurity terminology before the interview, in the study invitation and informed consent, we presented the study's purpose as "to discover how people understand descriptions of computers and technology." At the start of the interview, we informed participants that the study focused on cybersecurity terminology and asked them not to look up definitions.

3.5 Positionality

In qualitative research, in which the researcher is the primary instrument of data collection and analysis [38], it is important to note authors' positionality. The first author is a computer scientist and researcher focused on the usability of cybersecurity advice and documentation. A second research team member is a qualitative researcher focusing on education policy, a former teacher, and a cybersecurity non-expert. The third author is a usable cybersecurity researcher with prior experience as a cybersecurity practitioner. These diverse positionalities can improve research quality by enabling stronger study design and encouraging richer analysis [6]. Any potential undue influences of the positionalities were mitigated by a rigorous methodological process and regular meetings during which we identified and discussed individual assumptions as they surfaced.

3.6 Limitations

Our study has several limitations. With a smaller sample size common in qualitative research, we cannot generalize our findings, nor definitively determine demographic differences. Also, the views of our U.S. English-speaking non-experts may not reflect those of individuals in other regions given potential differences in cross-cultural security and privacy perceptions [2]. However, our results can serve as the basis for future investigations with larger sample sizes in other regions. Additionally, we did not counterbalance the order in which definitions were presented. Therefore, there is the potential of an order effect in which the sequence may have influenced participant responses. We also acknowledge that participants' definition preferences may not align with complete definitions. Yet, we see the expression of preferences as an opportunity to identify attributes of communications that could engage or repel non-experts.

Another limitation is due to the challenge of choosing a small subset of definitions that adequately represented a diversely-worded corpus of 130+ definitions. While we took a systematic, purposeful approach that involved discussions and consensus-building among multiple team members, because we did not randomly select the definitions, we acknowledge that there is the potential that researcher bias was introduced.

Finally, social desirability bias may have been a factor in that participants might have hesitated to express their true thoughts or admit ignorance. To counter potential embarrassment, we made a concerted effort to assure participants they were not being tested on their cybersecurity knowledge; rather, we were interested in their honest and immediate thoughts about the definitions towards helping us understand how to describe cybersecurity to all kinds of people. We further emphasized that cybersecurity has been defined in many ways and that the definitions in the interview were not necessarily the best.

4 Findings

We report findings about participants' general understanding of cybersecurity as well as evidence of how cybersecurity definitions are received both positively and negatively. If not explicitly stated, when attributing example quotes, we include the definition ID after the participant ID, for example, *(P16, SD)*. Counts are provided in some instances to illustrate weight, not with intent to distill our qualitative data to quantitative results.

4.1 Understandings of Cybersecurity

Before discussing definitions, we first asked questions to identify participants' conceptualizations and own definitions of cybersecurity.

4.1.1 Conceptualizations of Cybersecurity. Participants often described cybersecurity as protection of information or technology from threats. Twenty participants referenced information broadly or specific types of information such as "financial accounts" (P04). A few mentioned privacy or "private information" (P03). Nine referenced technologies like computers or devices as things that cybersecurity protects.

About one-third of participants related cybersecurity to a program or software one acquires for protection. Most commonly, these programs were antivirus or malware protection software. Several participants described how these programs protect:

> "*It's a program that you can put on any of your devices that you use,... and it kind of works in the background, but it would alert you if anyone takes your credit card information, bank information, or pretty much anything that could kind of hurt you.*" (P05)

One-third described cybersecurity as a set of practices. P02 provided a broad description: "You're trying to secure and protect your technology and those sorts of assets, whether it's your software or your hardware, it's how you're protecting your technology." P07 was more prescriptive: "Have secure passwords...Make sure that your internet connection is secure and private."

Twenty participants described at least one cyber threat, most commonly hackers, malware, and social engineering. Some used language to describe unwanted intrusions or outside actors compromising their information. P19 said, "All I think of when I hear cybersecurity is that individuals can access information that they normally shouldn't be privy to." P08 spoke metaphorically, describing cybersecurity as protecting against the "boogeyman. And they're [cybersecurity professionals] out there to get them for you. You don't have to look for it under the bed because they're doing it for you."

4.1.2 Emotions. Participants occasionally referenced negative emotions during discussions about the role of cybersecurity in their lives. A few were pessimistic: "[there is] just nothing you can do about it. There's always going to be somebody that's going to find a way through cybersecurity" (P11). P10 talked about desensitization to data breaches: "It's just getting worse because even the big companies,...they're getting hit all the time. And they just notify us, 'Sorry, you got hit again.' Okay. It's like no big deal anymore" (P10).

Half of participants had been victims of an account compromise, identity theft, or company data breach, which sometimes resulted in fear or concern. P06 recounted someone using their shopping app "to order themselves some stuff and ship it to themselves. So, I worry about things like that."

Lastly, a few participants expressed annoyance related to implementing cybersecurity or recovering from a negative experience. P04 mentioned the burden of remediating their hacked streaming account. P21 was annoyed by password requirements, which were "a real bugaboo of mine because we have to update them so often that we can't remember them."

4.1.3 Definitions of Cybersecurity. Participants provided their own definition of cybersecurity in the form of short sentences or phrases. Half defined cybersecurity as something that protects or keeps safe their information, technology, or the internet. For example, P27 defined cybersecurity as "Internet protection and computer protection," P17 as "the ways that you protect yourself online," and P03 as "protecting your privacy and information." Several mentioned a combination of things that cybersecurity protects: "Cybersecurity is *[sic]* tools that you can use to protect your identity in the cyberspace, protect your devices, protect all of your confidential and important information" (P30).

Over half of participants mentioned threats in their definitions, which included hackers, malware, scammers, criminals, and vulnerabilities. For example, P03 defined cybersecurity as protection against "malware, protecting against viruses, hackers." P15 more generally said that cybersecurity is "a way to keep the internet safe from threats and vulnerability."

4.2 Definition Exercises

Interview definition exercises — step-throughs and a sorting exercise of definitions in Table 2 — yielded insights into participants' understandings of definition terminology, thoughts about definition attributes, and views on how cybersecurity is relevant to them, reported in sections 4.4, 4.3, and 4.5, respectively. In this section, we first provide an overview of the exercise results.

4.2.1 Step-Throughs. **Definition 1 (D1).** Some participants described D1 using positive attributes, including clear, concise, thorough, and eloquent, with 16 saying they would recommend it to a family member or friend: "It's basic information I think a person could process and retain" (P01). A few remarked that D1 expressed or improved upon their own definition or mental model of cybersecurity: "It's kind of what I was thinking of trying to say at the beginning...like policemen, but online" (P28). Other participants described the definition in more negative terms, including vague, complex, and too long. Six said they would not recommend D1 to family or friends, mostly because the language was too technical or vague: "I would use it for someone who is more experienced in the field" (P03). Eight participants said their recommendation depended on the person and "their knowledge of tech terminology" (P07).

Definition 2 (D2). Participants who were positive about D2 said it was detailed and definitive, with 19 recommending it for family or friends: "It goes more into depth about cybersecurity...So, you understand it better" (P28). Several thought the definition was closer to their own understanding of cybersecurity: "When I think about cybersecurity, this is what I think of, that it is some type of prevention" (P19). Other participants negatively described D2 as wordy, confusing, and convoluted. Eight would not recommend it, largely because of its complexity: "It's like if you put a legal document in front of me" (P02). For similar reasons, three said their recommendation would depend on the audience: "I would recommend it to someone that I know to be more technically-minded,...but it's not for everyone" (P22).

D1 - D2 Comparison. After the step-throughs, we asked participants which of the two definitions they preferred. Responses were split: 15 preferred D1, 14 D2, and P17 said they would recommend D1 for work but D2 for personal use. Reasons for D1 preference included conciseness, ease of understanding, and, because it had fewer technical terms, it was "not as frightening" (P10) to people. Conversely, others preferred D2 because of its comprehensiveness. Interestingly, D2's language, while critiqued by those preferring D1, was cited multiple times as a reason *for* selecting D2: "This one is better for the lower-level user because it doesn't use as much jargon and breaks things down" (P21). There were a few demographic differences in definition preferences. Over half of men, participants with a high school education, and the two younger generations more often preferred D1. Over half of women, those with some college education, and the two older generations preferred D2 (see Table 8, Appendix C).

4.2.2 *Sorting Exercise.*

While we asked participants to select one or two definitions that were their favorites, we allowed participants to select more if desired (5 participants did). For the other characteristics, participants were encouraged to select as few (including none) or as many definitions as they thought fit that characteristic. All participants chose at least one definition for each characterization. Table 4 shows the percentage of participants selecting each definition for each of the sorting characteristics. Overall, only SA was chosen by over half of participants as a favorite, easy to understand, comprehensive, and useful. About 35% of the time, favorite definitions were also selected for the other three characteristics (e.g., if SA was selected by a participant as a favorite, it was also selected by the participant for the other characteristics).

Favorites. Participants often selected definitions as their favorites because of simplicity and detail. For example, one participant chose SF as one of their favorites because of its conciseness: "F is when you are on the elevator and you only have like 30 seconds to explain what it is. I like that one because it's short and to the point" (P01). Over half of participants chose SA as a favorite, describing it as both comprehensive and concise. For example, P03 described SA as giving "specific information about what cybersecurity would entail...And I think it sums it up pretty well."

We found observable differences in the selection of definition favorites among demographic groups (see Table 9, Appendix C). The two older generations (combined) more often selected definition SC as a favorite (50%) and less often selected SE (29%) compared to the two younger generations (31% and 50%, respectively). Considering education level, we observed substantial differences for all definitions. For example, 90% of participants with at least a bachelor's degree selected SA as a favorite, with much fewer for those with a high school (38%) and some college (50%) education. Additionally, no participants with a bachelor's degree selected SC as a favorite, in contrast to 75% of those with some college education.

Easy to understand. Participants selected definitions as easy to understand that were short, simple, and written in language they and other non-experts could understand. They selected SD and SF most often. P23 chose these two as easy to understand because "They have the least amount of words." Another remarked that, while they could understand all the definitions, they found SB and SD to be written in "the most simple language to convey the idea" (P20).

Comprehensive. Participants described definitions as comprehensive when they were detailed and covered the breadth of cybersecurity. They selected SA, SC, and SE most frequently. P28 said SA and SE were comprehensive: "They go a little bit more into detail. So it gives you more time to think about what the definition is and understand it more." Another participant chose SA and SC as comprehensive because these definitions clearly conveyed several components of cybersecurity: "The description explains what they're doing, the usage, and the security, the protection...It makes it clear who they're working against and who they're protecting you from" (P08).

Table 4: Percentage of participants (rounded) selecting each definition during the sorting exercises

	Favorites	Easy to Understand	Comprehensive	Useful
SA	60%	67%	77%	57%
SB	33%	67%	23%	33%
SC	40%	13%	77%	40%
SD	23%	77%	13%	30%
SE	43%	33%	70%	63%
SF	40%	73%	23%	33%

Useful. Participants most frequently selected SA and SE as useful to them. They often thought definitions were useful for the same reasons they selected favorites, for example, being simple and quickly understandable. P04 explained their reasoning for choosing SD: "It would be an easy way for me to describe it to somebody if I was telling them what it is. They would understand that quite quickly." (P04) Several explained that the definitions they identified as useful were informative. For example, P22 selected SC as useful because, even though they did not find SC particularly easy to understand, they had not previously considered how modification is a threat related to cybersecurity.

Source reactions. After definition sources were revealed, participants discussed how a definition met or did not meet the tone or purpose of the source. For example, when SB's source was revealed as a dictionary, participants thought the definition's simple, yet formal language aligned with their expectations of a dictionary definition. In another case, many participants were surprised that SD was from a government source because it was not very detailed, especially when compared to another government institution's definition (SC). However, they did not know that SD was targeted to individuals and families.

Cross-definition comparisons. Several participants compared definitions to highlight differences. Many discussed how SA, SC, SE, or a combination of those three, were longer and more detailed and comprehensive than SD and SF, which they often described as shorter, simplistic, and incomplete. For example, P19 explained, "I feel like they basically say the same thing: C, A, and E. I have to choose the same ones, which are C, A, and E because they provide more detail and clarity as to what cybersecurity is."

4.3 Definition Attributes

Throughout the interviews, participants expressed both positive and negative opinions related to attributes of cybersecurity definitions. This section summarizes attributes mentioned by at least three participants, with the number of participants in parenthesis. Note that, since we wanted to see which definition attributes participants personally liked or did not like, when coding for attributes, we excluded responses from the step-throughs and sorting exercises unless the participant made a positive or negative judgment. For example, we did not code "they are simplistic" (P01) from the "easy to understand" sorting exercise under an attribute code but did code "It's...the easiest one to understand. However. . . that's why I didn't choose this as one of my favorites, because it doesn't really cover that much" (P29, SD).

Understandability/clarity (29). Positively, participants used terms such as easy to understand, simple, clear, and self-explanatory. When describing why SA and SB were their favorites, P15 said, "For me, simplicity is important. Otherwise, I just get glazed over." Lack of understandability was expressed in terms such as confusing, complex, and vague: "It sounds really complicated...It's confusing" (P29, D2). Participants also remarked that definitions that are not easy to understand are "annoying" (P04, SC) and turn people off: "Most people, instead of taking the time to go through it and understand that, they would just go away" (P10, SC). Interestingly, we often found differing opinions for the same definitions. For example, many participants viewed definition SD as simple, therefore easily understood; yet, simplicity was not always positive, as expressed by several participants who thought SD was "oversimplified" (P19).

Length (29). With some exceptions (e.g., SD), participants thought positively of definitions described as shorter in length, concise, or succinct: "I like that one because it's short and to the point" (P01, SF). Negative views were expressed in terms such as wordy, convoluted, long, and redundant. P06 thought that SC and SE were "so wordy...it's hard to focus on what they're saying." Longer definitions were often associated with less understandability: "It's really long and very pause-heavy, and I think that does get in the way of understandability" (P22, D2).

Appropriateness for general audience (28). Participants voiced opinions about the appropriateness of definitions for cybersecurity non-experts. These thoughts were often positively associated with ease of understanding and use of plain language, for example, "This is cybersecurity 101" (P25, D1) and "This definition breaks it down even further to laymen's terms...A five-year-old could understand it" (P01, D2). In contrast, P24 thought D2 was "just way too confusing. And the language is just too advanced," and P20 thought D1 was "designed by somebody very, very fluent in cybersecurity not really focused language-wise on the people that need it the most." Several thought negatively of definitions using terms "not normally used in conversations" (P18, SC and SE). For example, four participants did not like the word "exploitation" in SC: "I immediately think of sex or something" (P18). Another commented that the word *cyber* is "this amorphous thing that I think is very hard for someone to understand" (P20, SD and SF).

Definition appraisal often depended on the target audience and context. For example, P17 had divergent opinions on whether they would recommend D1: "For your job, maybe...For your personal stuff, probably not." When explaining why SA and SD were favorites, P14 described attributes of a definition for the average person:

> "*If the point is...just to kind of have the concept embedded in your mind so...you're more willing to put up with the inconveniences that it presents, and you're just more open-minded to take reasonable steps to do it,... then a definition that is fairly simple and fairly engaging and also fairly informative is a good definition.*"

There was little consensus on what was most appropriate. P15 reflected on the difficulty of composing a universal definition:

> "*If you're using it for tech companies, I think the definition should be more technical and encompass more...The general public,... it just depends on the person...Some people like more detail. Others don't. It's really hard to say what definitions should be put out there.*"

Completeness/detail (27). Participants often preferred complete or comprehensive definitions with adequate detail compared to definitions viewed as generic: "I do like that one. It gives a breakdown of exactly what the cybersecurity is going to do" (P01, SC). Negatively, several discussed how various definition aspects or terms may be too limiting or incomplete. For example, several thought the threats mentioned in some definitions (e.g., *cybercrime* in SD and *criminal and unauthorized use* in SB) did not reflect the full scope of threats.

Components (26). Participants discussed how specific information about what cybersecurity entails, who engages in cybersecurity, what is being protected, and threats (i.e., definition "components" [47]) positively contribute to completeness and understandability. P30 thought D1 was a good definition because "It explains exactly what you're protecting and why you're protecting it, and how you're protecting it." However, while several participants appreciated that cybersecurity was presented as encompassing multiple approaches (e.g., *body of* in SA and *collective methods* in SE), others flagged those descriptors as problematic: "body of technologies...That's like the one thing that rubs me the wrong way" (P18, SA). Interestingly, SD, the only definition to explicitly mention *who* is responsible for cybersecurity, evoked differing opinions. P06 thought SD was useful because it "helps me understand that it's both individuals and...organizations." Conversely, P21 was confused: "you're not saving individuals or organizations. It's about networks and data. It's not people."

Facilitation of learning (17). Participants commented about whether definitions taught them something. As a positive example, when reading D2, several remarked that they did not realize that cybersecurity also included restoration of information and systems: "I was thinking about it generally as a preventative sense of a set of practices, but it's always going to be more than that because this system is highly probable to fail at some point" (P22, D2). When talking about *modification* in SC, P22 said, "It's a unique kind of attack that I hadn't considered." Conversely, other participants criticized definitions that did not provide them useful information: "It doesn't really cover that much"(P29, SD).

Tone (14). Several thought negatively of definitions having a scary tone due to use of words like *malicious*: "What is so bad that it has to use that wording?... It sounds evil" (P12, D1). Further, some definitions were seen as less reassuring. For example, when discussing D1, a participant critiqued, "process of limiting malicious attack. I would say, eliminating, not limiting...It just kind of doesn't give me much sense of security" (P29). On a positive note, other participants remarked that some definitions garnered attention to emphasize the importance of cybersecurity: "damage, unauthorized access, exploitation. Those are good keywords for a definition because that gets your attention" (P07, D2).

Structure (7). A few participants noted how grammar and sentence structure impacted their opinions. Two preferred definitions, like SA and SE, that mentioned concepts in groups of three: "People really like the threes in a lot of things" (P22). From a negative perspective, others thought awkward grammar was a detractor: "too many prepositions...I also don't like the hyphenated statement" (P22, D2).

Trustworthiness (3). Three participants mentioned perceived trustworthiness of definitions, mostly after definition sources were revealed at the end of the sorting exercise. P19 was most comfortable with definition SC because "it comes from a government agency that actually regulates and monitors this type of activity." Two others questioned whether cybersecurity vendors were trustworthy sources: "The fact that they're a provider of marketing sales service,...that's not a definition that I would think is the most accurate or the more trusted one" (P19, SF).

4.4 Understanding of Definition Terms

We describe instances of participant understanding or misunderstanding of terms and phrases used in the definitions, categorized by cybersecurity threats, what cybersecurity protects, how cybersecurity is achieved, and cybersecurity principles (confidentiality, integrity, availability). Note that, unlike the step-throughs, we did not explicitly ask participants to explain parts of the sorting definitions. Therefore, we only capture instances in which participants explicitly expressed uncertainties.

4.4.1 Threats. **Malicious attacks (D1).** All but one participant (P06) were able to offer reasonable explanations or examples for this phrase. They often expressed that *malicious* signifies an intent to harm for some gain, usually financial. A virus was the most common example of a malicious attack (11 participants). Other examples included social engineering, account hacking, and information attacks such as identity theft. Participants also revealed their mental models of malicious attacks, with P28 picturing malicious attacks lying in wait "until the person who has created it decides to start looking through your computer." P15 equated malicious attacks with criminality: "I just picture a criminal trying to hack into the system, maybe get people's personal data or maybe somehow stop the whole process of a company."

Experts say that cybersecurity can also protect against non-malicious user (in)actions (e.g., human error [73]). Therefore, we asked participants if there are issues that cybersecurity addresses that may not be considered malicious. The responses provided additional insights into participant interpretations and their perceptions of the scope of cybersecurity. Just one participant (P02) said they did not know, with 10 saying they did not think that there were non-malicious issues. Even though we deliberately used the word *issues* in our question, seven participants referred back to the word *attacks* in the definition: "I can't think of any attack that wouldn't be malicious. Even though some people do things and they say they were just goofing off or just testing it, it's still malicious if it hurts the other person and you did it deliberately" (P16). Three participants noted that there could be accidental exposure, for example, "data accidentally leaked...through an email...There could just have not been a good process in place" (P15). Others recognized a gray area in which a malicious attack could be unintentionally propagated, for example, when someone unwittingly forwards a virus-laden email to a friend. Seven participants linked cybersecurity to privacy, mentioning that cybersecurity could protect against unwanted and "invasive" (P19) use of personal information for tracking or marketing purposes: "It also can be useful for simply protecting your privacy in general" (P21).

Seven evaluated maliciousness against their own perceptions of consequence severity, rather than intent. P06 said, "The majority of attacks are not malicious. They're just selfish or unwanted or even just childish behavior, not really necessarily trying to harm anyone." Two thought Facebook account hacking or impersonation were not malicious because of what they believed were low-stake consequences: "They find out how old you are, if you're in a relationship, and look at some pictures" (P08).

Risk of damage to, unauthorized use of, exploitation of (D2). Participants' overall interpretation largely centered on hackers stealing sensitive information, whether that be for less-harmful purposes (e.g., targeted advertising), or more harmful (e.g., financial theft, data destruction, or doxxing). Eighteen described *damage*, often attributing it to viruses and other malware impacting digital assets, for example, "having files be deleted" (P03). A few mentioned damage to hardware or other physical systems: "destroying actual hardware by feeding parameters intended to make systems fail in the physical world" (P22). Others talked about damage in terms of reputation harm: "there's a lot of risk involved if people get a hold of the wrong types of pictures. It can really ruin people's reputation" (P04). All 20 participants who described *unauthorized use* had a fair understanding of the term, linking it to permission: "it's going into the hands of the people who are not allowed to use it or to use it for other reasons other than what it's intended for" (P19). Nine participants talked about *exploitation*, associating it with inappropriately using someone's information for some nefarious benefit: "Hacking into somebody's computer or mobile phone in an attempt to steal their information and use it for malicious purposes" (P30). Conversely, a few did not know how to differentiate exploitation from damage or unauthorized use: "They're synonymous" (P10).

Terms beginning with cyber (SD, SE, SF). Several participants were less familiar with cybercrime in SD (6 participants), cyberthreats in SF (5), and cyber-attacks in SE (3). P28 said, "I feel like I would probably need to contact IT or something and ask, like, okay, what is cyber attacks?" These terms may be especially problematic for those without a firm grasp on what cyber means: "If you want a definition of cybersecurity, cyberthreats is too similar to have in the same definition" (P24, SF).

4.4.2 What Is Protected. **Computer networks, systems, devices, digital applications (D1).** While some participants discussed this phrase in its entirety, most commented on individual words. Twenty described *networks* as Wi-Fi, internet, or VPN connections. Understandings of *systems* were less clear for five participants: "I don't really know what the difference is between a network and a system" (P15). *Systems* included operating systems, laptops, and computers. Examples of *devices* were often similar to systems, but more focused on those for personal use, for example, laptops, tablets, and phones. Six included less-conventional devices, such as smart home devices and gaming systems. Participants generally classified *digital applications* as downloadable, internet-connected, able to access information, and synonymous with mobile apps. However, three participants were unsure about this term: "I don't know if it means websites" (P01).

Interestingly, P6 compartmentalized certain concepts into either organizational (e.g., work, school) or personal/home contexts: "Networks and systems makes me think more like a workplace or college campus sort of situation and then devices and digital applications, more just your phone and tablets and the apps and stuff on...your personal devices." Conversely, P20 recognized these could be found in both environments: "Most people, I think they would think about businesses like a network of business computers in an office. But it's also going to be considered your computer network at your home."

Electronic information and communication systems, and the information they contain (D2). All but three participants easily provided examples of information they considered worthy of protection, such as address, financial information, location, photos, emails, text messages, passwords, contacts, web browsing history, and files. *Electronic information and communication systems* were often grouped together and included phones, computers, tablets, and other devices that allow for "emails, private messages, cloud sharing, file sharing, storage" (P03). However, four participants were unsure or offered incorrect interpretations of these systems: "I'm like picturing those old school computer rooms with huge processors everywhere...I don't know what [they] are" (P06).

4.4.3 How Cybersecurity Is Achieved. **Good security processes and securing (D1).** While P23 thought *good security processes* was subjective ("good could be something for you,...and for me, it's a different meaning"), all but four (three in the Boomer generation) could articulate at least one example of a "good" process. Examples included: authentication mechanisms (e.g., passwords, two-factor authentication); security software (e.g., anti-virus, anti-spyware); physical security (e.g., locking computers); VPNs; safe web browsing; firewalls; limiting/protecting sensitive information; not clicking on suspicious emails; securing the network; and, more vaguely, personal practices like "taking good, proactive steps to make sure that you remain safe while you're online" (P05). Despite the extensive list reported across all participants, 13 participants (9 having education less than a Bachelor's degree) included only one example, perhaps indicating a limited understanding of the scope of security processes. For example, P27 only mentioned "virus protection software," and P28 conceptualized processes simply as "different checkpoints to make sure that the person who's logging in is the actual person."

We also asked how networks, systems, etc. are secured (the *securing* phrase in D1). Twenty-seven provided an answer, with most referring to their previous response on security processes or listing similar items (e.g., security software, authentication). We observed that this question particularly spurred participants to admit their limited knowledge. For example, P07 said, "For my phone, I don't really know what goes on." In contrast, P21 took the opportunity to showcase their knowledge to debunk the popular recommendation to change passwords every 90 days: "I've actually read that studies have shown that that does not increase security. All it does is cause people to write down their passwords."

Training (D1). Seven participants (6/7 in the younger two generations and 6/7 without a Bachelor's degree) were unsure or incorrect about the meaning of *training*. Four questioned, "Who's being trained?" (P04). P29 remarked, "That's kind of confusing. Am I going to be trained on how to use them? Or is it training in general?" Three thought training was for devices and systems: "Testing bugs or anti-viruses and testing its effectiveness against malware or malicious attacks" (P03).

The other participants had at least a partial understanding, relating training to learning about cyber risks and countermeasures: "getting information on what types of behaviors online could lead to attacks or hacking or make you vulnerable or training on how to use security systems" (P06). Seven provided examples of training modalities like "videos or tutorials" (P24) and "phishing resistance training" (P21).

4.4.4 Cybersecurity Principles. The principles of **confidentiality, integrity, and availability** (the CIA Triad) were included in D2 and SE. Twenty-eight participants could articulate at least, in part, what is meant by *confidentiality*, often referencing the concept of privacy: "it means keeping certain information private. Only certain people can access it, people that are given permission to access it or use that information" (P15). However, the terms integrity and availability were less understood. Only four participants — all with a Bachelor's degree or above — had at least a partial understanding of *integrity* [45], for example, "the information is correct and not tampered with" (P17). Participants often knew what integrity meant in other contexts but not for cybersecurity: "a form of trust" (P27), "Done the right way. And done with honor" (P08), and "honest and pure...I know what it means, but I don't know what it means in this sense" (P01). Sixteen participants had a general understanding of *availability* [44], with no trends across demographic groups. Incorrect responses included "instead of one of your devices, it's on all your devices" (P05) and "It means not allowing your information to be readily available for anybody to just obtain" (P30).

4.5 Personal Relevance

The definition exercises elicited participants' thoughts about the relevance of cybersecurity in their own lives.

4.5.1 Personal Involvement. Throughout the interviews, we saw evidence of participants taking personal responsibility for cybersecurity. Many provided examples implying their own or general public involvement, using words like *my*, *I*, or *we*. For example, P24 explained that SB was useful because it includes *measures*: "That's personally what I use,...like VPNs." P20 described good security processes as "Our personal ways that we go about things."

In contrast, others viewed cybersecurity as something that organizations, experts, or other people do. For example, when opining on SE, P16 talked about what others are doing: "They're doing not just one thing to protect you."

Participants particularly struggled to see how *training* in D1 related to them or the general public. Six thought that training is only for cybersecurity professionals: "I don't think this is for the consumer. I think it's just that the back office people all know what they're doing, the people that are working on cybersecurity. I don't think you can train the public" (P11). Further, four participants viewed cybersecurity training as only relevant within a work context, often part of "yearly training" (P17), which few participants mentioned applied to them. Two questioned how people might be trained if not at work: "I don't know that there is a good accessible way for people to learn about security if they're not getting that annual refresh employee training" (P02).

4.5.2 Personal Connections. Sixteen participants often made connections to their own experiences, especially when describing what cybersecurity protects (e.g., systems, information). When discussing the term *networks* in D1, P01 said, "The job that I do, I have to be careful what network I'm on because I don't want someone to gain the financial information to use to harm other people." Commenting that they would not recommend D1 to family and friends, P20 drew on their own experience with their spouse: "I've learned that the second two words come out of my mouth that relate to anything technology, her eyes gloss over...The goal...is to be able to have somebody like that understand it, and these words don't do that."

During definition discussions, seven participants provided examples of their own negative experiences. When talking about *unauthorized access*, P21 mentioned that their fast food app account was compromised: "They were placing...large [restaurant] orders. And since I foolishly had saved my credit card on the account, they were being charged to me." Referring to the *risk of damage* phrase in D2, P01 remembered a time they were impacted by ransomware, "My old computer got hacked and they told me that I couldn't use the computer unless I did X, Y, Z."

Eight (six Boomers) used analogies and metaphors to personally connect with the definitions. When commenting on *good processes* in D1, P08 described security professionals as "the watchdog." P07 gave a health analogy, describing the restoration aspect of cybersecurity as being "Like a doctor. A doctor's supposed to prevent the illness first, but then if you do get sick, then they're also there to help you get better." P09, who worked for the government, likened authorized access to a "room that you go into to look at classified documents and you have to be authorized."

4.5.3 Importance. Nine participants reflected on how discussing the definitions either reinforced or awakened their own recognition of the importance of cybersecurity. When discussing how D1 broadened their understanding, P29 remarked, "When it tells you about different devices, to me, that's kind of cool...It expands the horizon and it gives it [cybersecurity] more importance." When given the opportunity to share additional thoughts at the end of the interview, five participants talked about the importance of cybersecurity education for the general public. P20 commented, "People being more understanding of the threats and how they can protect themselves, I think, is critical...It's got to be easier to understand and access" (P20). P25, a Millennial, spoke about populations that need more help:

> "*There's not enough resources for older people or for people with little to no knowledge about it...Some people don't take...using different security measures seriously. Sometimes we look at it as a nuisance more than the intended purpose: they're there for our benefit.*"

P06 was an interesting counterexample. During the D1 step-through, they said, "I don't know if I believe in cybersecurity. I don't know if I believe it works." They often expressed frustration with the definitions because of perceived vagueness or not understanding the terms: "I still don't know what cybersecurity is. I still don't know how it works or what it can do for me." P06 did not see the importance of cybersecurity due to their lack of understanding, so felt that cybersecurity vendors were disingenuous: "It's almost like you're getting conned. Until I understand how I'm being threatened, I don't really understand how you're going to securely protect me."

5 Discussion

> *"Defining a term includes not only coming up with a general way to explain that term to an audience, but it also requires putting a term into a given context." [43]*

As this quote exemplifies, definitions – which are critical in establishing common ground between expert and non-expert communities [43, 72] – should bring a concept to life for a particular audience in the environment in which they apply it. Thus, in this digital age in which cybersecurity is a collective responsibility no longer relegated to specialists, it is imperative to craft cybersecurity definitions that resonate with non-experts – who, historically, are confused about and detached from cybersecurity – in their own context of use.

Through discussions with non-experts about representative cybersecurity definitions, we identified specific examples of attributes and terminology that have the potential to influence individuals' perceptions and behaviors. These findings provide novel insights that could inform the development of definitions and other cybersecurity communications that inform and motivate non-experts. In this section, we situate our findings within existing literature (organized by research question), then provide practical recommendations for cybersecurity communicators.

5.1 RQ1: How Non-experts Understand and Define Cybersecurity

Non-expert participants understood cybersecurity at its most general: it protects. Similar to findings in prior work [29, 55], some participants had a very limited view of cybersecurity (e.g., it is a program or just involves protecting information). Perceptions of cybersecurity were often related to a constrained perception of context, both in the context of the technology they use (e.g., just mentioning smartphones) and where they take cybersecurity actions (e.g., work vs. home). Negative emotions that participants voiced towards cybersecurity often stemmed from past experiences or how they viewed the (sometimes inconvenient) role of cybersecurity in their lives [74]. Thus, many participants came to this study with either incomplete, context-limited, or negative perceptions of cybersecurity, which may have impacted how they understood or reacted to the definitions. In some cases, these perspectives may have been reinforced by the definitions we presented (e.g., as was the case with P06), especially when participants did not understand the terminology, thought the definition was too detailed or irrelevant, or the tone was scary. However, we also saw evidence of how definitions have the power to either positively reinforce or change the participants' initial understanding of cybersecurity. For example, multiple participants commented on how the definitions expanded their knowledge of the breadth of cybersecurity (e.g., to include restoration), called attention to their own role in cybersecurity, or brought attention to the importance. Therefore, even in the limited time we spent with participants, we see how definitions have the potential to impact attitudes and behavior intentions about cybersecurity.

5.2 RQ2: How Non-experts Understand and Perceive Cybersecurity Definitions

Our participants' understandings and perceptions illustrate the way in which cybersecurity definitions can act both positively and negatively at the boundary of expert and non-expert communities, perhaps reflecting deeper attitudes towards cybersecurity. We also comment on the lack of consensus among participants.

5.2.1 Definitions as Boundary Objects. Definitions have potential to impact an audience's expectations of cybersecurity either positively or negatively [43]. While cybersecurity expectations are influenced by myriad factors [66, 69], we see evidence of at least short-term impacts or reflections of these prior-held expectations in our study, finding that definitions can be positive or negative *boundary objects* between experts and non-expert communities of knowledge. *Boundary objects* — abstract or concrete "things" that serve as a translation device between intersecting communities — aim to establish a shared language to represent knowledge but can be received as either positive or negative [1, 13, 28, 68]. Ultimately, boundary objects can be indicators of larger issues: "positive and negative boundary objects are not simply passive vehicles...but elements that encapsulate the broader social meaning of a concept...and the underlying relations that surround its development and adoption" [22].

Positive (facilitative) boundary objects act as "bridges and anchors" between communities [68]. We saw evidence of how definitions established common ground between the expert community creating the definitions and the non-expert community receiving them. Participants reacted positively to definitions that use clear and easy-to-understand language, provide enough detail to show the breadth of cybersecurity, and expand or align with their own understanding. They also made personal connections when definitions were relatable to their own experiences and appreciated definitions that elicited attention and a sense of importance. These insights may have implications for how cybersecurity definitions and other communications impact behaviors. Prior work has found that motivation to perform cybersecurity tasks is in part based on perceived importance or relevance at an emotional level [32]. Further, interest in cybersecurity–as demonstrated by our participants' expression of how the interviews raised their awareness–is associated with a desire to take action [10].

In contrast, negative (inhibitory) boundary objects are viewed as "barricades and mazes" that accentuate social and occupational hierarchies and inhibit uptake or understanding [22, 53]. In our study, while participants critiqued definitions that were too vague and limiting, they also reacted negatively to overly complex and long definitions and those using language inappropriate for a general public audience. Further, they sometimes demonstrated a lack of understanding of common terms used in the definitions. Our results align with prior work that illuminated issues with the use of technical language (e.g., [7, 76]) and readability [59] in cybersecurity communications, while we further provide insights into (mis)understandings of specific terminology.

We also found that the disconnect in understanding could lead to participants separating themselves from cybersecurity, seeing it as: only relevant to an elite group of cybersecurity experts; only mildly consequential; not something they had the desire, opportunity, or capacity to learn; or not even possible to fully achieve. Our findings provide evidence of what other researchers have only hypothesized to be consequences of unclear cybersecurity communications: confusion; limitations in thinking and attraction to overly-simplified, incomplete definitions (e.g., SD); and lack of recognition of personal responsibility and relevance [23, 47]. All of these may demotivate individuals to engage in cybersecurity [20, 27].

Further, participants perceived some definitions as having a negative tone, which could result in associations between cybersecurity and emotions such as fear, annoyance, and anxiety, which were expressed during general discussions of cybersecurity in the interviews and are common in cybersecurity [74, 75]. Negative emotions evoked by cybersecurity boundary objects may be particularly problematic, as they can demotivate long-term, positive learning and behaviors, reduce self-efficacy, or lead to avoidance of responsibilities [10, 62, 66, 74].

While prior work examined how perceptions of cybersecurity can influence attitudes and behaviors, we uniquely pinpoint specific examples of how even simple communications in the form of a short definition might influence. Further, although definitions are limited, our findings highlight general attributes and understandings that can guide the development of longer, more expository types of cybersecurity communications that positively capture non-experts' attention while mitigating negative and dissociative perceptions of cybersecurity.

5.2.2 Lack of Consensus. We found much variability in participants' preferences for definitions. While we observed trends in definition attributes, the attributes could be applied either negatively or positively by different participants for the same definitions. Sorting exercise analysis also suggests inconsistencies in the relationships between selected favorite, easy to understand, comprehensive, and useful definitions. There might be some optimal combination of a definition having just the right amount of content to be useful, while being easy enough to understand that it is not grossly oversimplified. However, this combination, again, may depend on individual preferences.

The lack of consensus supports the observation that non-experts' perceptions of cybersecurity are deeply contextual and intertwined with their own knowledge and lived experiences [34]. We particularly saw the importance of context in participants' statements about how their definition assessments depended on the knowledge of the intended audience and whether the definition would be used for personal or work purposes.

We also uniquely identify potential trends and problematic areas in definitions across demographic groups. For example, generational and education groups sometimes differed in their selection of favorites during the sorting exercise. Additionally, education level appeared to play a role in the understanding of some technical terms (e.g., integrity). It may be that these results extend previously identified generational differences in cybersecurity conceptualizations [31] or even readability levels (linked to education level) of cybersecurity texts [60]. Differences across education groups might also be partially due to exposure to cybersecurity awareness and training opportunities in the professional context afforded to those who are more highly educated [66].

5.2.3 Future Research Opportunities. Our study provides a foundation for future research exploring non-experts' understandings and perceptions of specific cybersecurity terms (e.g., those related to attacks and defenses), since engagement with these lower-level concepts may be impacted by the high-level feelings and biases about cybersecurity identified in our study. Additionally, our findings on definition attributes could inform future investigations into how these attributes, when present in other types of cybersecurity communications, may impact non-experts' perceptions and engagement.

Our results also provide an important first step towards developing cybersecurity definitions that are correct, informative, and relevant to different demographic groups of non-experts. While a deeper understanding of an audience is critical for developing effective communications [26], our demographic findings are preliminary due to sample size. Therefore, we recommend future research with a larger, representative sample to more deeply explore potential demographic influences. Additional research could also sample non-experts living in countries outside the U.S. to identify potential cross-cultural differences [2].

5.3 Practical Recommendations

Towards communicating cybersecurity concepts in a manner that is both meaningful and accessible to audiences of varying contexts and levels of knowledge, we provide suggestions for those who craft cybersecurity definitions, descriptions, or training for non-experts.

Terminology

- The use of technical jargon can result in the development of negative associations, as indicated by our participants in their preference for plain language and terms without a negative tone (4.3). Therefore, avoid or provide additional information for terms not widely understood [76]. "Pilot" the communication before publication to obtain feedback from non-experts representative of the intended audience to ensure understanding.
- Be mindful of using terms with overlapping meaning in different contexts – such as *integrity*, *exploitation*, and *training*, which caused confusion among our participants (4.4) – that may require additional explanation.
- Use context-relevant examples, negation (i.e., does not mean), comparisons, and additional information to clarify terms used within the communication, and prevent non-experts from making incorrect assumptions [43] (e.g., our participants' beliefs that cybersecurity is the responsibility of professionals) (4.5, 4.3).
- Avoid recursive definitions or descriptions that include a reference to part of the term that is being defined. For example, in 4.4, participants noted the use of *cyber* in several *cyber*security definitions as problematic.

Communication attributes

- Considering the demographic trends described in 4.2 and 4.4, tailor to the audience of the communication, including their technical skill, context, and education. Personalize the communication towards motivating positive behaviors [20]. Tailoring could counter our participants' criticism of definitions that used language inappropriate for a general audience (4.3).
- Be cautious of statements that inaccurately constrain the breadth of cybersecurity, for example, as illustrated by participants' noting of the limited scope of cybercrime in 4.3 and 4.2. Include a broader range of what cybersecurity does and protects to counter narrow understandings of cybersecurity, such as many participants' views that cybersecurity only involves information protection (4.1). This comprehensiveness and facilitation of learning was appreciated by our participants (4.2, 4.3).
- Ensure that definitions and descriptions meet non-experts' expectations of being informative, easy to understand, simple (but not overly so), and containing enough details to explain what cybersecurity entails, as evidenced by participants' expressions of preferences for definitions (4.2, 4.4, 4.3).
- To address our participants' emotive reactions (4.1) based on perceived tone or word choice (4.3), be cognizant of how certain framings of cybersecurity or terminology can evoke positive or negative emotions that engage or repel [74].
- To encourage action and avoid instances in which non-experts do not see their responsibility in cybersecurity (4.5), communicate personal relevance (i.e. impacts to individuals). This includes specifying *who* is responsible for cybersecurity (e.g., the *individuals and organizations* clause in SD) (4.3).

Training for non-experts

- Since context plays a role in cybersecurity perceptions and behaviors [34] and individuals may ascribe more importance to work-related interactions (as seen in our participants' focus on employee training in 4.1 and 4.5), within organizational contexts, encourage individuals to form positive cybersecurity habits no matter where they are by making a work-home connection (as recommended in [25]).
- Support efforts to counter misconceptions about cybersecurity (4.1) via cybersecurity awareness and training to the general public. Our participants stressed the importance of cybersecurity education and the dearth of training for the general public (4.5). One way to provide awareness is by engaging non-experts in discussions about cybersecurity, which, as expressed by our participants (4.4, 4.3, 4.5), can be helpful in catalyzing individuals to think about their own role in cybersecurity, facilitating learning, and identifying misconceptions that can then be addressed .

6 Conclusion

We conducted a semi-structured interview study with 30 participants from various generation and education groups to gain novel insight into non-experts' understandings and perceptions of published cybersecurity definitions. Non-experts often held incomplete mental models of cybersecurity, did not always fully understand terms and concepts commonly included in cybersecurity definitions, and expressed differing views on how definitions should be expressed. Further, these findings demonstrate that definitions can act as positive or negative boundary objects between cybersecurity expert and non-expert communities. Our findings can serve as a foundation for developing cybersecurity communications that are more effective, usable, and actionable for a broad range of individuals.

Disclaimer

Certain commercial companies or products are identified to foster understanding, not to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor to imply that these are necessarily the best available for the purpose.

Acknowledgments

This material is based upon work supported by the North Carolina State University NIST Graduate Student Measurement Science and Engineering Fellowship Program under Award Number 70NANB21H090 and the University of Maryland NIST Professional Research Experience Program under Award Number 70NANB18H165.

References

[1] Sanne F. Akkerman and Arthur Bakker. 2011. Boundary crossing and boundary objects. *Review of Educational Research* 81, 2 (2011), 132–169.

[2] Isslam Yousef Alhasan. 2023. *Human Factors in Cybersecurity: A Cross-Cultural Study on Trust.* Doctoral Dissertation. Purdue University.

[3] Maria Bada, M. Angela Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf.

[4] Sarah Baker and Rosalind Edwards. 2012. How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. https://eprints.ncrm.ac.uk/id/eprint/2273/4/how_many_interviews.pdf.

[5] Rosaline S. Barbour. 2001. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *British Medical Journal* 322, 7294 (2001), 1115–1117.

[6] Christine A. Barry, Nicky Britten, Nick Barbera, Colin Bradley, and Fiona Stevenson. 1999. Using reflexivity to optimize teamwork in qualitative research. *Qualitative Health Research* 9, 1 (1999), 26–44.

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

[8] Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, and Sławomir Górniak. 2015. Definition of cybersecurity-gaps and overlaps in standardisation. *Heraklion, ENISA* (2015).

[9] Olivia M. Bullock, Daniel Colon Amill, Hillary C. Shulman, and Graham N. Dixon. 2019. Jargon as a barrier to effective science communication: Evidence from metacognition. *Public Understanding of Science* 28, 7 (2019), 845–853.

[10] A. J. Burns, Tom L. Roberts, Clay Posey, and Paul Benjamin Lowry. 2019. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research* 30, 4 (2019), 1228–1247.

[11] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. 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).* USENIX Association, USA, 117–136.

[12] Mariana G. Cains, Liberty Flora, Danica Taber, Zoe King, and Diane S. Henshel. 2022. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis* 42, 8 (2022), 1643–1669.

[13] Paul R. Carlile. 2002. A pragmatic view of knowledge and boundaries: Boundary objects in new product development. *Organization Science* 13, 4 (2002), 442–455.

[14] Herbert H. Clark and Susan E. Brennan. 1991. Grounding in Communication. In *Perspectives on Socially Shared Cognition*, Lauren B. Resnick, John M. Levine, and Stephanie D. Teasley (Eds.). American Psychological Association, 222–233.

[15] S. Marc Cohen and C. D. C. Reeve. 2021. Aristotle's Metaphysics. In *The Stanford Encyclopedia of Philosophy (Winter 2021 Edition)*, Edward N. Zalta (Ed.). Stanford University.

[16] Juliet Corbin and Anselm Strauss. 2015. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (4th ed.). Sage Publications, Thousand Oaks, CA.

[17] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. 2014. Defining cybersecurity. *Technology Innovation Management Review* 4, 10 (2014).

[18] John D'Arcy and Pei-Lee Teh. 2019. Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management* 56, 7 (2019), 103151.

[19] Michael Dimock. 2019. Defining generations: Where Millennials end and Generation Z begins. https://www.pewresearch.org/short-reads/2019/01/17/where-millennials-end-and-generation-z-begins/.

[20] Cassandra E. Dodge, Nathan Fisk, George W. Burruss, Richard K. Moule Jr, and Chae M. Jaynes. 2023. What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy* 22, 4 (2023), 849–868.

[21] Shari L. Dworkin. 2012. Sample size policy for qualitative studies using in-depth interviews. *Archives of Sexual Behavior* 41 (2012), 1319–1320.

[22] Nick J. Fox. 2011. Boundary objects, social meanings and the success of new technologies. *Sociology* 45, 1 (2011), 70–85.

[23] Steven Furnell and Emily Collins. 2021. Cyber security: What are we talking about? *Computer Fraud & Security* 2021, 7 (2021), 6–11.

[24] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* 18, 1 (2006), 59–82.

[25] Julie Haney and Wayne Lutters. 2020. Security awareness training for the workforce: moving beyond "check-the-box" compliance. *Computer* 53, 10 (2020).

[26] Julie M. Haney and Wayne G. Lutters. 2018. 'It's Scary…It's Confusing…It's Dull': How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *2018 Symposium on Usable Privacy and Security.* USENIX Association, USA, 411–425.

[27] Tejaswini Herath and H. Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (2009), 106–125.

[28] Isto Huvila, Theresa Dirndorfer Anderson, Eva Hourihan Jansen, Pam McKenzie, and Adam Worrall. 2017. Boundary objects in information science. *Journal of the Association for Information Science and Technology* 68, 8 (2017), 1807–1822.

[29] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. '…no one can hack my mind': Comparing expert and non-expert security practices. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015).* USENIX Association, USA, 327–346.

[30] Rebecca Jeong and Sonia Chiasson. 2020. 'Lime', 'Open Lock', and 'Blocked': Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings. In *2020 CHI Conference on Human Factors in Computing Systems.* Association for Computing Machinery, New York, NY, USA, 1–13.

[31] Simon L Jones, Emily IM Collins, Ana Levordashka, Kate Muir, and Adam Joinson. 2019. What is' Cyber Security'? Differential Language of Cyber Security Across the Lifespan. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems.* 1–6.

[32] Hwee-Joo Kam, Philip Menard, Dustin Ormond, and Robert E. Crossler. 2020. Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security* 96 (2020), 101875.

[33] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "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).* USENIX Association, USA.

[34] Nadiya Kostyuk and Carly Wayne. 2021. The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies* 6, 2 (2021), ogz077.

[35] Eric Luiijf, Kim Besseling, and Patrick De Graaf. 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6* 9, 1-2 (2013), 3–31.

[36] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. In *ACM on Human-Computer Interaction.* ACM, New York, NY, USA, 72.

[37] Mary L. McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia Medica* 22, 3 (2012), 276–282.

[38] Sharan B. Merriam and Elizabeth J. Tisdell. 2016. *Qualitative Research: A Guide to Design and Implementation* (4th ed.). John Wiley & Sons, San Francisco, CA.

[39] Merriam-Webster Dictionary. [n. d.]. definition. https://www.merriam-webster.com/dictionary/definition.

[40] Seumas Miller and Terry Bossomaier. 2024. *Cybersecurity, Ethics, and Collective Responsibility.* Oxford University Press.

[41] David Modic and Ross Anderson. 2014. Reading this may harm your computer: The psychology of malware warnings. *Computers in Human Behavior* 41 (2014), 71–79.

[42] Benjamin Morrison, Lynne Coventry, and Pam Briggs. 2021. How do Older Adults feel about engaging with Cyber-Security? *Human Behavior and Emerging Technologies* 3, 5 (2021), 1033–1049.

[43] Brigitte Mussack and Brandi Fuglsby. 2021. Descriptions and Definitions. In *Introduction to Technical and Professional Communication*, Brigitte Mussack (Ed.). University of Minnesota.

[44] National Institute of Standards and Technology. 2024. Glossary: availability. https://csrc.nist.gov/glossary/term/availability.

[45] National Institute of Standards and Technology. 2024. Glossary: integrity. https://csrc.nist.gov/glossary/term/integrity.

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

[47] Lorenzo Neil, Julie M. Haney, Kerrianne Buchanan, and Charlotte Healy. 2023. Analyzing Cybersecurity Definitions for Non-experts. In *International Symposium on Human Aspects of Information Security and Assurance*. USENIX Association, USA, 391–404.

[48] Lorenzo Neil, Harshini Sri Ramulu, Yasemin Acar, and Bradley Reaves. 2023. Who comes up with this stuff? interviewing authors to understand how they produce security advice. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, USA, 283–299.

[49] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. '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*. Association for Computing Machinery, New York, NY, USA, 1–11.

[50] Jason RC Nurse. 2013. Effective communication of cyber security risks. In *7th International Scientific Conference on Security and Protection of Information (SPI 2013)*.

[51] Jason RC Nurse, Sadie Creese, Michael Goldsmith, and Koen Lamberts. 2011. Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. 60–68.

[52] Jason R.C. Nurse, Inka Karppinen, Jo Milward, and Joanne Varughese. 2022. Oh behave! The annual cybersecurity attitudes and behaviors report. https://staysafeonline.org/online-safety-privacy-basics/oh-behave/.

[53] Clif Oswick and Maxine Robertson. 2009. Boundary objects reconsidered: From bridges and anchors to barricades and mazes. *Journal of Change Management* 9, 2 (2009), 179–193.

[54] Shari Lawrence Pfleeger and Deanna D. Caputo. 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security* 31, 4 (2012), 597–611.

[55] Sandra Spickard Prettyman, Susanne Furman, Mary Theofanos, and Brian Stanton. 2015. Privacy and security in the brave new world: The use of multiple mental models. In *Intl Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer-Verlag, Berlin, Heidelberg, 260–270.

[56] Anabel Quan-Haase and Isioma Elueze. 2018. Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. In *9th International Conference on Social Media and Society*. Association for Computing Machinery, New York, NY, USA, 150–159.

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

[58] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2019. "Woe is me": Examining Older Adults' Perceptions of Privacy. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–6.

[59] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA.

[60] Elissa M. Redmiles, Miraida Morales, Lisa Maszkiewicz, Rock Stevens, Everest Liu, Dhruv Kuchhal, and Michelle L. Mazurek. 2018. First steps toward measuring the readability of security advice. In *2018 IEEE Security & Privacy Workshop on Technology and Consumer Protection (ConPro)*.

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

[62] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*. 42–56.

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

[64] Daniel Schatz, Rabih Bashroush, and Julie Wall. 2017. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law* 12, 2 (2017), 8.

[65] Hillary C. Shulman, Graham N. Dixon, Olivia M. Bullock, and Daniel Colon Amill. 2020. The effects of jargon on processing fluency, self-perceptions, and scientific engagement. *Journal of Language and Social Psychology* 39, 5-6 (2020), 579–597.

[66] Joëlle Simonet and Stephanie Teufel. 2019. The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference (SEC 2019)*. 194–208.

[67] Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security fatigue. *IT Professional* 18, 5 (2016), 26–32.

[68] Susan Leigh Star and James R. Griesemer. 1989. Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology 1907-39. *Social Studies of Science* 19, 3 (1989), 387–420.

[69] Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman, and Simson Garfinkel. 2017. Be prepared: How US government experts think about cybersecurity. In *Workshop on Usable Security (USEC)*.

[70] Julia D. Thompson, Geoffrey L. Herman, Travis Scheponik, Linda Oliva, Alan Sherman, Ennis Golaszewski, Dhananjay Phatak, and Kostantinos Patsourakos. 2018. Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice* 1 (2018), 5.

[71] Kerry Tomlinson. 2023. The curse of knowledge can damage awareness programmes: Here's how to defeat it. *Cyber Security: A Peer-Reviewed Journal* 6, 4 (2023), 311–319.

[72] Unified Compliance Framework. [n. d.]. The Definitions Book: How to Write Definitions. https://www.unifiedcompliance.com/education/how-to-write-definitions/.

[73] Verizon. 2024. 2024 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/.

[74] Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. 2024. Beyond Fear and Frustration-Towards a Holistic Understanding of Emotions in Cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 623–642.

[75] Alexandra von Preuschen, Verena Zimmermann, and Monika Schuhmacher. 2023. How do you Feel about Cybersecurity? A Literature Review on Emotions in Cybersecurity. In *Proceedings of the International Symposium on Technikpsychologie*. 1–13.

[76] Tingmin Wu, Rongjunchen Zhang, Wanlun Ma, Sheng Wen, Xin Xia, Cecile Paris, Surya Nepal, and Yang Xiang. 2020. What risk? I don't understand. An empirical study on users' understanding of the terms used in security texts. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 248–262.

A Detailed Participant Demographics

Table 5: Individual participant demographics

ID	Generation	Education	U.S. Region	Self-reported Cybersecurity Knowledge
P01	Boomer	Some college or Associate's degree	South	Little
P02	Millennial	Bachelor's degree	South	Little
P03	Gen Z	Bachelor's degree	South	Little
P04	Millennial	High school diploma or equivalent	Northeast	Little
P05	Millennial	High school diploma or equivalent	Midwest	Moderate
P06	Millennial	High school diploma or equivalent	Midwest	Little
P07	Millennial	High school diploma or equivalent	West	Moderate
P08	Boomer	Some college or Associate's degree	South	Little
P09	Boomer	Graduate or professional degree	Northeast	Little-Moderate
P10	Boomer	Graduate or professional degree	South	Moderate
P11	Boomer	Bachelor's degree	South	Moderate
P12	Gen X	High school diploma or equivalent	Midwest	Little
P13	Gen X	High school diploma or equivalent	South	Little
P14	Boomer	Graduate or professional degree	South	Little
P15	Boomer	Bachelor's degree	Midwest	Little
P16	Boomer	Some college or Associate's degree	West	Little
P17	Millennial	Bachelor's degree	South	Moderate
P18	Millennial	Some college or Associate's degree	South	Moderate
P19	Gen X	Some college or Associate's degree	South	Little
P20	Boomer	Some college or Associate's degree	South	Moderate
P21	Boomer	Graduate or professional degree	West	Moderate
P22	Gen Z	Bachelor's degree	South	Little
P23	Gen Z	High school diploma or equivalent	West	Moderate
P24	Gen Z	Some college or Associate's degree	Midwest	Moderate-Expert
P25	Millennial	Some college or Associate's degree	South	Moderate
P26	Gen Z	Some college or Associate's degree	South	Moderate
P27	Gen Z	Some college or Associate's degree	Midwest	Little
P28	Gen Z	High school diploma or equivalent	West	Moderate
P29	Gen X	Some college or Associate's degree	South	Little-Moderate
P30	Millennial	Some college or Associate's degree	Midwest	Moderate

Table 6: Number of participants per education level

Demographic	Sub-category	High School/ equivalent	Some College/ 2-year degree	Bachelor's/ Grad degree	TOTAL
Generation	Gen Z	2	3	2	7
	Millennial	4	3	2	9
	Gen X	2	2	0	4
	Boomer	0	4	6	10
Self-reported knowledge	Little	4	5	5	14
	Little-Moderate	0	1	1	2
	Moderate	4	5	4	13
	Moderate-Expert	0	1	0	1

B Definition Selection Details

Table 7: Reasons for Selection of Interview Definitions

ID	Definition	Reasons for Selection
D1	the process of limiting malicious attacks through good security processes, training, and securing computer networks, systems, devices and any other digital applications	• Components: Action, How/What, Objects, Threats • Terms of interest (jargon, terms common throughout the corpus): digital, malicious, attacks, training, networks, systems, devices • Has multiple phrases/components that can be discussed in-depth
D2	an approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems	• Authoritative source (U.S. Government) • Page 1 of Google search results • Components: Action, How/What, Objects, Security Principles, Threats • Terms of interest: exploitation, confidentiality, integrity, availability, electronic information and communications systems • Has multiple phrases/components that can be discussed in-depth
SA	the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access	• Components: Actions, How/What, Objects, Threats • Page 1 of Google search results • Definition repeated 4 times in initial search and almost identical to another definition that was repeated 5 times • Terms of interest: networks, devices, programs, unauthorized access
SB	the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this	• Dictionary source • Components: Actions, How/What, Objects, Threats, What • Page 1 of Google search results - first definition to appear when searching for "cybersecurity definition" • Like nine other definitions in the corpus, only mentions protection of data (limited to information security) • Terms of interest - criminal, electronic data, unauthorized use
SC	the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation	• Authoritative source (U.S. Government) • Components: Actions, How/What, Objects, • Page 1 of Google search results • Definition repeated 3 times in the initial search • Terms of interest: information and communications systems, damage, unauthorized use, modification, exploitation • Example of longer definition
SD	the means by which individuals and organizations reduce the risk of being affected by cyber crime	• Authoritative source (UK Government) • Components: Actions, How/What,Threats, Who (one of the few) • Targeted specifically to individuals and families (our sample population) • Example of short definition • Terms of interest: "cyber crime"
SE	the collective methods, technologies, and processes to help protect the confidentiality, integrity, and availability of computer systems, networks and data, against cyber-attacks or unauthorized access	• Components: Actions, How/What, Objects, Security principles, Threats • Page 1 of search results • Definition repeated 5 times in initial search • Terms of interest: confidentiality, integrity, and availability, cyber used in cybersecurity definition

Table 7: Reasons for Selection of Interview Definitions

ID	Definition	Reasons for Selection
SF	the protection of internet-connected systems such as hardware, software and data from cyberthreats	• Components: Actions, Objects, Threats • Page 1 of search results • Definition repeated 3 times in initial search • Terms of interest: internet-connected systems, cyberthreats, hardware, software • Example of short definition

C Additional Tables

Table 8: Percentages of participants preferring each step-through definition by demographic

		D1	D2	It Depends
Demographic	Sub-category	(n=15)	(n=14)	(n=1)
Education	High school	63%	37%	0%
	Some college	42%	58%	0%
	Bachelor's +	50%	40%	10%
Generation	Gen Z + Millennial	56%	38%	6%
	Gen X + Boomer	43%	57%	0%

Table 9: Percentage of each demographic group selecting definitions SA - SF as favorites during the sorting exercise

Demographic	Sub-category	SA	SB	SC	SD	SE	SF
Education	High school	38%	25%	38%	25%	38%	75%
	Some college	50%	50%	75%	17%	42%	17%
	Bachelor's +	90%	20%	0%	30%	40%	40%
Generation	Gen Z + Millennial	56%	31%	31%	25%	50%	44%
	Gen X + Boomer	64%	36%	50%	21%	29%	36%