Be Prepared: How US Government Experts Think About Cybersecurity

Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman and Simson Garfinkel
National Institute of Standards and Technology
firstname.lastname@nist.gov

***Abstract*—Online security experiences, perceptions, and behaviors are key to understanding users security practices. Users express that they are concerned about online security, but they also express frustration in navigating the often confusing and mentally taxing cybersecurity world. This paper examines the differences in cybersecurity perception and behavior between cybersecurity experts in the US Government as contrasted with non-experts. The experts represent a very select group within United States Government Agencies who are directly responsible for cybersecurity guidance for the Federal Government. We used a semi-structured interview protocol to collect data from 23 experts and 21 non-experts. Interview questions addressed experiences, beliefs, and behaviors with respect to online security. Qualitative data techniques were used to code and analyze the data identifying themes related to the similarities and differences in expert and non-expert perceptions of and experiences with cybersecurity. The experts as a group don't trust, develop plans and are proactive in their approach to online security and see security as a personal challenge rather than a risky and potentially disrupting experience. In contrast, our non-experts trust too much, don't develop plans, and experience security with anxiety and fear.**

I. Introduction

In their seminal 1975 paper on computer security, Jerome H. Saltzer and Michael D. Schroder defined the principle of *psychological acceptability* with respect to usability: "It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized" [31]. Since this definition of psychological acceptability relies on mental models and users' goals, part of the challenge of cybersecurity has long been understanding the ways in which different groups of people think about and interact with cybersecurity.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

USEC '17, 26 February 2017, San Diego, CA, USA
 ISBN 1-891562-47-9
http://dx.doi.org/10.14722/usec.2017.23006

While a great deal has changed since 1975, the ever increasing complexity only compounds the challenge as Bishop noted when he revisited psychological acceptability [9]; Herley echoed the theme that more and increasingly complex security mechanisms and advice only serve to increase the chance of errors, decreasing the ability of users to maintain and manage their cybersecurity [20]. Focusing attention on general users certainly seems necessary. But also relevant is understanding what experts in the field know, believe, and do. Examining similarities and differences between the experts and non-experts may provide insights into how to help non-experts understand and protect themselves online.

Researchers in usable security have long been aware of the need to understand users' behavior and the critical role users play in meeting cybersecurity goals [2]. Through programs such as the National Initiative for Cyber Education (NICE), universities and websites are attempting to raise cybersecurity awareness and provide advice to users. It is only recently (September of 2016) that the Commission on Enhancing National Cybersecurity received public comments on the relationship of human behavior as a factor in strengthening cybersecurity for consideration in a report to be delivered to President Obama. The Executive Director of the Commission stated in *Federal Communication Weekly*, "It's this sense that this is not a technology problem—we have to get at where the human behavior plays into it" [12].

Previous work has examined differences in mental models between experts and non-experts [4], [5], differences in perceptions and understanding of security warnings [10], and differences in the security practices followed by experts and non-experts [21]. An emerging theme is the importance of contextualizing the beliefs and understanding that different kinds of users have about cybersecurity, as a way of improving the security of their actions. For example, security experts and non-experts seem to operate with a different set of assumptions about online security. As a result, what might seem routine, obvious, or common-sense to an expert may not be that way at all for non-experts [21]. Exploring where the beliefs and behaviors of experts and non-experts converge and/or diverge may help us find ways to provide each user with what they need to protect themselves while online. This does not mean that all users must become security experts, or that the knowledge and experiences of experts should be used as the norm to educate non-experts. Instead, it recognizes we need to learn from both experts and non-experts, and that we must meet users where they are in order to provide them with cybersecurity tools that they can understand and use.

In this paper, we report on the results of a study which

examines how different groups of users describe their experiences with and perceptions of security and privacy in their own words. In particular, we were interested in identifying what characteristics influenced their attitudes and behaviors. From our previous studies of the general public's security practices [16] [28] [34], it became clear that it was necessary to expand our investigations beyond non-experts. To this end, we conducted in-depth interviews with both security experts and non-experts. We recognize that both these categories are socially constructed and are often thought of as a dichotomy rather than as a continuum of knowledge and experience. Experts are typically defined by qualifications and experience, and what they do with those [14]. By contrast, non-experts are considered to have less qualifications and experience. We were not out to explore the social processes that construct expert and non-expert status, but rather to identify the experiences and beliefs that these two groups have with and about cybersecurity recognizing that participants may fall anywhere along the continuum from expert to non-expert.

We conducted in-depth interviews with a unique sample of US Government cybersecurity experts—a group that has not yet been the subject of study. We interviewed 23 cybersecurity experts who are responsible for developing cybersecurity guidance for the entire US Federal Government. These are the people who inform everyone in the Federal Government how to stay secure. These experts were recruited from the Department of Homeland Security (DHS), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST). DHS is responsible for providing advice and tools on operational cybersecurity and provides assistance to owners and operators of critical infrastructure. NSA is responsible for security of national security systems and national security information. NIST is responsible for providing cybersecurity guidance and standards to the non-national security systems.

We also interviewed 21 non-experts (these were members of the general public who use the internet and spend time online) in order to gain an understanding about cybersecurity beliefs and experiences of those who are not experts in the field. This data allowed us to explore what non-experts know and do, and to identify characteristics that influence their attitudes and behaviors.

Our results show that these U.S. Government cybersecurity experts tend to be proactive in their online security practices: they generally believe they have a plan, or plans, to mitigate or recover from any security problems that might occur. Thus the government experts are prepared. Non-experts, on the other hand, are not prepared. Non-experts are not proactive in their approach to online security. They do not put in place plans or practices in advance to protect themselves or to be able to recover in the event of a problem. In addition, they think differently about what cybersecurity means; their mental models are different, resulting in different approaches to it.

II. Relevant Literature

There are a variety of recent studies examining the differences between what experts and non-experts believe and do related to cybersecurity. Asgharpour *et al.* [5] found that experts and non-experts utilize different mental models when they think about computer and security risks. For example, non-experts relate the use of passwords to the realm of physical security, while experts see them as corresponding to a criminal model. The result is that non-experts conceptualize the compromise of a password as similar to the loss of a key, while experts see it as resulting from explicitly malicious activity. These differences have implications for the best way to communicate effectively with users, as well as how best to motivate appropriate behaviors, with respect to online security and risks. Other work on the mental models of users also demonstrates the ways in which incomplete, oversimplified, and multiple models guide the thinking and behaviors of non-experts related to cybersecurity [11], [28], [36].

The difference in mental models between experts and non-experts is one reason the two groups respond differently to security warnings. Work by Bravo-Lillo, *et al.* found that experts and non-experts took different actions that resulted in different outcomes because they observed different cues and therefore came to different conclusions about the potential risk they might face [10, p. 23]. Novice users also considered fewer options and did less to protect themselves online.

Stewart and Lacey [35] argue that many of the issues related to cybersecurity are presumed to be caused by a lack of facts on the part of users and that the cybersecurity field believes it is necessary to increase awareness through the broadcasting of facts in order to improve security behaviors. This results in a "technocratic" approach to risk communication where technical experts tell people what they need to know. They argue this approach is "fundamentally flawed" [35, p. 29] and posit that risk communication needs to be contextualized based on user beliefs and constraints related to online security. For example, experts and non-experts have different levels of understanding related to the vocabulary and language utilized in cybersecurity information and advice. "The risk is that the choice of words used in awareness communications invokes the wrong mental model in the audience" [35, p. 33]. Stewart and Lacey believe a more contextualized and multifaceted approach is needed, where risk communication meets a variety of user needs utilizing a variety of different tools.

Others have examined why users even with increased awareness and good security advice have difficulties following through. Acquisti and Grossklags argue that bounded rationality limits our ability to acquire and then apply information in the online privacy and security space. Even if individuals had complete information they may still not make rational decisions because they are "influenced by motivational limitations and misrepresentations of personal utility" [1, p. 25].

According to Beautement *et al.* employees engage in a cost-benefit analysis where they weigh the advantages and disadvantages of compliance within a "compliance budget" [8]. Once their compliance limit is reached, people choose not to comply or find ways to work around the compliance; their willingness to comply stops as they are confronted with additional security policies and requirements. Adams and Sasse [2] argue that in fact many security policies promote an adversarial relationship with users, putting them in what Herley calls an "impossible compliance regime" [19, p. 8].

Our work is most similar to Ion *et al.*, who examined the attitudes and practices of experts and non-experts related to online security mechanisms [21] by asking a single question,

"What are the top three pieces of advice you would give to a non-tech-savvy user to protect their security online?" They found that the two groups utilized different tools and methods to protect themselves online. Security experts were more likely to install software updates, use two-factor authentication, and utilize a password manager in their efforts to stay safe online. In contrast, non-experts used antivirus software, visited only known websites, and changed their passwords frequently as ways to stay safe online. The authors argue that recognizing these differences can inform the ways we approach security advice and design campaigns aimed at improving security education and practice.

However, there are key differences between our work and Ion *et al.*'s: We did not ask our experts to provide a single actionable recommendation on how users can improve their security, because we were trying to understand the mental models of both groups of users - experts and non-experts. Ion *et al.* interviewed 40 experts during interviews at the Black Hat security conference; interviews lasted 8 minutes on average. We interviewed 23 experts in the field who were involved in setting cybersecurity practice and policy at high levels within the U.S. Government; our interviews lasted 32 minutes on average. Ion *et al.*'s experts were generally younger and less experienced than our experts, and had "a vast range of job titles," unlike our experts who were focused on defining cybersecurity practice for large organizations.

We add to the existing body of knowledge an analysis of user behavior, perceptions, and beliefs as described by users in their own words. We compare experts with a unique set of responsibilities for providing cybersecurity guidance for the U.S. Federal Government and non-experts and identify behavioral models that characterize their differing approaches to security.

III. Methods

This qualitative study draws on data generated as part of a larger study that examines the perceptions and experiences of two different user groups within cybersecurity: cybersecurity experts (defined as U.S. Federal employees responsible for providing cybersecurity guidance for the U.S. Federal Government and); non-experts, or general public (defined as anyone who does not work in cybersecurity who uses the internet).

A. Research Questions

These research questions guided the study:

1. How do participants talk about their experiences with and perceptions about online privacy and security?
2. If and what mental models guide participants' understandings, beliefs, and behaviors regarding online privacy and security?

B. Development of the Interview Protocol

The interdisciplinary research team, comprised of researchers from Computer Science, Human Factors, and Sociology/Education collaboratively developed a semi-structured interview protocol. The protocol was designed to elicit participant beliefs, perceptions, and experiences related to online security and privacy, in order to see if and how participants articulated a mental model(s) related to cybersecurity. For example, we asked participants how they would explain computer privacy and cybersecurity to a child, which often helped the experts to articulate the mental model(s) that guided their thinking. We also asked questions about the emotions they felt about these topics, stories about times they felt at risk, and how they would describe their relationship with the internet. The protocol varied slightly for each of the interview groups, primarily to address how the experts came to work in cybersecurity and their current work in the area (See Appendices A and B).

In order to insure that all of the goals of the study and the categories associated with them were addressed in the interviews, we created an alignment matrix (see Table I for the General Public Alignment Matrix) that identified research goals and categories of investigation and then linked them to the interview questions that aligned with them. Since interview questions may address a variety of goals and categories, they may appear in several places on the matrix. An alignment matrix is one way to provide consistency, logic, and transparency in the research process [26], by linking the objectives, categories, and interview items. Often used in survey research, an alignment matrix is also used in qualitative research to insure that research goals and categories for analysis are represented in the interview protocol. We then piloted the protocol with a small group of participants in each category to assess the face validity of questions and language appropriateness. We reviewed this data and adjusted the instrument based on feedback from the pilot and our review of the data it generated. The protocol began with a questionnaire, which included demographic questions, questions about time spent online and tasks engaged in while online, and a self-assessment of their knowledge of computer security and privacy. Interviews were transcribed verbatim, and these transcripts form the corpus of data for analysis, along with field notes from the interviews.

C. Interviews

In total, we interviewed 23 experts and 21 non-experts. These numbers reflect our goal as qualitative researchers "to build a convincing analytical narrative based on 'richness, complexity and detail' rather than on statistical logic" [6] Our data collection, coding, and analysis were iterative and recursive, allowing us to recognize when we reached saturation, the place where no new properties or dimensions emerged from the coding process [13].

All participants received a copy of the information sheet, which researchers reviewed with them prior to the interviews. Non-federal employee interviewees received $50.00 in compensation for their participation (Federal employees may not be paid for their participation in federally sponsored testing). Interviews for experts and the general public ranged from an outlier of approximately 12 minutes to 60 minutes per interview, which generated 331 pages of transcripts. These were true in-depth interviews where participants spoke at length and in detail about their beliefs, perceptions, and experiences.

1) Expert Interviews (N=23): Expert interviews were conducted from August 2015 to August 2016 in the Washington D.C. metropolitan area with 13 experts who work at NIST

and 10 experts who work for other DHS and NSA. We were interested in speaking with experts "in" the field, in their work environment whenever possible (or close to it in some cases where it was impossible to visit and/or record in those spaces). Interviewing *in situ*, in their actual work environments, positioned them as the experts and provided a situation where they controlled the space and felt comfortable while at the same time providing us with a view of them in their natural work environment (which created a level of trustworthiness related to their position as experts). Recruitment began with an email request to previously identified experts in each of the agencies, which resulted in a convenience and snowball sample. Expert interviews began by asking how they got into the field, what they were working on currently, and why they think this work is important. After these introductory questions, the expert protocol followed the same format as the general public protocol until the end when we asked: "As an expert, what kind of advice would you give someone who is not an expert in the field?" This was followed by: "Do you follow your own advice?" Expert interviews ranged from 17 to 55 minutes, with the average expert interview lasting 32 minutes.

Expert participants included 15 men and eight women. Seven were 21–29 years old; seven were 30–39 years old; and nine were 40–49 years old. Eleven of the experts had a Bachelor's degree, 10 had a Master's degree, and two had PhDs. The self-assessment of knowledge about online and computer privacy and security asked participants to rate themselves using the following categories: Very Little; Little; Moderate; High; and Expert. One expert rated him/herself as having Little knowledge, four rated themselves as having Moderate knowledge; 12 rated themselves as having High knowledge; and six rated themselves as having Expert knowledge. We note that while many of these experts did not rate themselves as such, they are indeed a highly specialized group that represents some of the top experts in cybersecurity. We also observed that this group of experts was extremely humble with respect to their stature in the field and their accomplishments.

2) Non-Expert Interviews (N=21): Non-expert interviews were conducted from August 2015 to January 2016 in the Washington D.C. metropolitan area and the Midwest, with participants from urban, suburban, and rural areas. Recruiting for general public participants occurred through social media venues, postings at local libraries, researcher contacts, and word of mouth. It was a random sample in that anyone who responded and met the criteria was interviewed, but it also included a level of snowball sampling since several participants recommended others for the project. General public interviews followed a process similar to that for the experts and included questions asking for definitions of online privacy and security, how they would explain these to a child, and experiences they had related to them. These interviews ranged from 12 to 50 minutes with a mean time of approximately 25 minutes. Younger participants, in general, had less to say and their interviews tended to be shorter than those with older participants.

General public participants included 11 participants from the D.C. metropolitan area and 10 participants from the Midwest. Nine were men and 12 were women. Three were 18–20 years old; seven were 21–29 years old; four were 30–39 years old; two were 40–49 years old; two were 50–59 years old; and three were 60 or older. One had a high school degree, five had some college, 12 had a Bachelor's degree, and three had a Master's degree. Three self-rated themselves as having Very Little knowledge, five as having Little knowledge, eight as having Moderate knowledge, and five as having High knowledge.

D. Data Analysis

Data analysis for each of the groups began with the development of an *a priori* codelist (informed by the literature and our knowledge of the field) constructed by the research team. While there was some overlap in the in initial codelists for experts and non-experts, there were also differences reflecting some of our early ideas about what the data might look like. For each group, we operationalized all codes and then each worked with the same subset of four interviews to insure that our use of codes was consistent and coherent [3], [32]. We decided early on as a team not to calculate a measure of inter-rater reliability (such as Cohen's) since we believe that "the degree of concordance between researchers is not really important; what is ultimately of value is the content of disagreements and the insights that discussion can provide for refining coding frames. The greatest potential of multiple coding lies in its capacity to furnish alternative interpretations" [7, p.116]. We utilized these team coding discussions to explore how and where we saw things differently which allowed us to go back and examine our use of codes and their appropriateness for the data. They also provided a space to explore emergent codes. These discussions often resulted in revisions to the coding schema and additional insights into the data. Once we reached agreement on the codes and their operationalization, we continued to code interviews independently, with each interview being coded by at least two researchers. In this process we used both descriptive and values coding [30]. We continued to meet regularly as a team to discuss our coding, to identify emergent codes, and to revise the code list as needed until we reached saturation. Saturation in this instance refers to the point at which no new codes emerged [17]. At this point, we shifted from coding to analysis, to discuss the relationships we saw in the data and amongst the codes. We wrote memos and shared ideas related to our interpretation of the data and codes, all of which became part of the data set to be coded [13], [30]. This iterative and recursive analytic process provided opportunities for interdisciplinary discussions and the development of alternative interpretations.

E. Validity and Reliability

Validity and reliability are often referred to as trustworthiness, rigor, and quality in qualitative research [18], [23], [24]. In many ways it is about the "truth value" of the findings—the ways in which they accurately represent the data. Trustworthiness is provided in this study by a variety of measures, including the use of: well-established research methods (such as in-depth interviews and observation field notes); triangulation (the use of multiple and different sources of information to search for convergence of information); tactics to insure honest responses from participants (such as informing them they can voluntarily withdraw or refuse to answer a question at any time); iterative questioning (to insure

Objective/Goal	Category	Category Definition	Question
To identify definitions of online privacy and security in the different user groups	Definitions of online privacy and security	How participants understand the concepts of online privacy and security	Demographics Question 11 List the first several words that come to mind when you hear "online privacy" (& security) Q1 How would you describe your relationship to the internet? Q2 How would you explain online privacy to a child—what about computer security? Q3 What about security? Q4 What do you think is the difference between online privacy and security? Q5 How would you explain online privacy to a child? What about computer security?
To identify experiences with online privacy and security in the different user groups	Experiences with online privacy and security	What participants do or have done related to online privacy and security; their behaviors related to online privacy and security	Demographics Questions 6–9 Hours online and activities engage in Q11 Tell me about a time when you felt at risk. Q11a Why or when is it you feel at risk? Q11b What triggers alarm bells? Q12 Describe what makes you feel safe? Q12a What do you do to feel safe?
To identify beliefs about online privacy and security in the different user groups	Beliefs bout online privacy and security	Participants ideas about the goals, meanings, consequences, and/or usefulness of online privacy and security	Q1 How would you describe your relationship to the internet? Q2 We give information...what do you think privacy means in that setting? Q3 What about security?

TABLE I. GENERAL PUBLIC ALIGNMENT MATRIX.

consistent data from participants); frequent debriefing sessions amongst researchers (to explore gaps in the process and insure exploration of varied and alternative ideas); and experienced investigators who are knowledgeable about the content and the population [33]. The use of an interdisciplinary, iterative analytic process that explores similarities and differences in accounts and interpretations provides a level of trustworthiness in the analysis. Trustworthiness in qualitative research also extends to the presentation of results. The use of participants' own words is one indicator of trustworthiness in the presentation of results (rather than a reliance on researchers' words and descriptions), and the ability to link this data back to a particular participant provides readers with the knowledge that the researchers know their data and the context around it.

Reliability in quantitative work demonstrates that similar results would be obtained if the research was repeated in the same context, utilizing the same methods, and with the same participants. In qualitative research, this is provided by insuring transparency and consistency in the research process and providing detail about all research processes. This creates a model of the research that others can utilize as a "prototype" to conduct a similar study. In this paper, we provide specific, detailed descriptions of our research design, interview protocols, data collection, and data analysis processes. Copies of code lists, and other study-related documents are available upon request. In this way, the study can be replicated in the future, by other researchers and with other populations. The use of consistent and transparent processes also helps insure that other researchers would arrive at similar findings if they were to undertake the study.

F. Limitations

This study is focused on examining the beliefs and experiences of U.S. Government experts and a group of non-experts related to cybersecurity. The experts we interviewed all worked for the U.S. Government, with an average of 14 years of service (service ranged from 4 to more than 20 years), which is typical of high-level U.S. Government experts. Our results do not make any claims of a causal nature: we did not investigate whether government service has attracted experts of a particular outlook, or if the act of setting cybersecurity policy influenced the way these experts think. However, we recognize that the age and experience levels of this group may vary from other groups of experts. Their work in the U.S. Government may also set them apart from other types of experts. While this may be seen as a limitation, we also believe their unique position in working with and setting federal policy, standards, and practice makes them a particularly interesting and insightful group to examine. In spite of their often humble assessment of their status as cybersecurity experts, many of those we interviewed represent the upper echelon of those working within cybersecurity, at least at a government level. In some ways, they represent one end of the continuum. With our non-expert group, another limitation is that we draw from the DC metropolitan area and the Midwest and not other parts of the country. While the concept of generalizability is often debated in qualitative research, many researchers argue that the goal is to provide explanations for the experiences of others who are in similar situations [22], [25], [27]. Kincheloe [22] in particular argues that the generalizability of a qualitative study rests in the hands of the readers, who use their understandings of a variety of other contexts to determine how generalizable a study is to their particular situation.

Since the experts that we interviewed had on average 14 years of service within the federal government; the proactive security outlook evidenced by our experts may also have been a result of their experience, rather than their government roles.

IV. RESULTS

In this paper, we report on the findings related to experts and non-experts and their understandings of and approaches to cybersecurity. Since qualitative data analysis refines individual

concepts into themes, our results are also organized and reported in this manner [29]. We use the words of participants, the actual data, to present the results of the study.

Quotes from participants are listed with their participant identifier, which begins with the location (FedE for Federal employee Expert; DCGP for DC metropolitan area general public; MWGP for Midwest general public). After the colon is the interview number, which is followed by the time stamp where the data is found. For example MWGP:09–10:40 is Midwest General Public interview number nine at 10 minutes and 40 seconds into the interview. The data presented below to support each of the codes discussed is representative of the data that was coded in each.

We were struck early on in our analysis by three themes that emerged in the expert interviews: 1) the experts did not seem to trust anything (or anyone) in the online environment; 2) the experts had all implemented plans to ward off or recover from risks they might encounter; and 3) because the experts had put plans in place to deal with any potential threat they were not afraid (for themselves or for their information). In addition, the experts believed the general public put too much trust in websites and online entities and did not do enough to protect themselves. As one expert participant noted: "*Security should always be running in the back of your mind, it actually probably should be in the front of your mind, but I don't know how realistic that is to tell a lot of people*" (Fed01–37:16). In the following sections we explore the codes of trust, proactive behavior, and fear in both the expert and non-expert groups.

A. To trust or not to trust

As we coded our data, it became obvious that experts overwhelmingly did not trust anything or anyone in the online environment, and also believed that the general public trusted too much when they were online. Our operational definition for Don't Trust was "the lack of faith in individuals or systems to always act or perform in the expected way." We operationalized Trust Too Much as "the belief that individuals and the general public have too much faith in systems and technology which may put them or the systems at risk."

The lack of trust was expressed often in the expert interviews. One expert noted: "*Given what I know now. Nothing has really made me feel 100% assured that anything is [safe]—whenever I go online I basically have to assume someone's watching all the time*" (FedE:05–34:50). Another expressed a similar sentiment: "*I don't think I ever feel safe online, it's more of accepting risks. But it's not safe because there's so many ways that something can go wrong that are outside of my control"* (FedE:13–20:42). While these experts did not trust, they believed it was this thinking that kept them safe.

While experts expressed no trust in the safety of the Internet or online environment, they also believed the general public trusted too much, which led to them having problems. When asked whether they thought the general public protected themselves adequately, most answered "No" very quickly. "*I think people tend to be gullible. They believe what they see. If you find it on a document on the Internet, it has to be true, right? . . . A lot of people I think, just don't look at where information comes from and so they don't analyze the risk, they don't recognize the risk*." (FedE:06–19:15). Over and over again, experts discussed how non-experts often engaged in behaviors without thinking of the consequences, trusting that the people and sites they interacted with would be safe.

And in fact, non-experts often expressed ideas that demonstrated the trust they had in their online interactions. This statement, from a Midwest participant is indicative of non-expert responses. "*Yeah. I think for me there's a lot of trust that isn't always probably properly earned. You know, I don't read through the PayPal stuff because it's a big-- I trust that. And I trust that Amazon or any number of websites are not either going to sell my information, or they'll protect it"* (MWGP:05–2:51). As with the participant above, most non-experts trusted that "big", well-known sites were safer, and would protect them and their information (a Reputation mental model) or that security was the responsibility of the sites they visited (a Not My Job mental model). Non-experts generally drew on multiple mental models which were partially and ill-formed [28].

While non-experts often believed they would be safe online, experts believed the opposite, that security was a myth, and could never totally exist, which also led them to not trust. *"So I think my answer to that would be never [in response to the question do you feel safe online?]. I'm not saying there won't come a time when people could be made safer online, but sure I would be open to that. But right now it's almost like a dream. So if that could come true that would be great [laughter]. Hopefully in my lifetime"* (FedE:05–34:50). The expert above never felt safe online, he did not trust. This directly contrasts with non-experts who believed that they were and could be safe online. "*I guess I'm going with the whole, "Oh well everybody else was okay, so I'll be okay too," just hope for the best*" (MWGP:09–9:53).

Because experts did not trust in the online environment and saw security as a myth, they believed in being proactive about protecting themselves and their information. They could not leave cybersecurity to others or to chance, and therefore they put plans in place that could protect them from risk.

B. To plan or not to plan

Experts, in general, took a risk-based approach to cybersecurity where they saw risk everywhere and therefore needed to use cybersecurity tools to protect themselves. They were proactive in their approach. We operationalized Proactive as: "Protection and/or a plan against potential consequences before they happen." On the other hand, non-experts, in general, took an avoidance-based approach, either relying on the people and sites they interacted with to protect them or believing they had nothing of value and therefore did not really need to worry about security. Without a plan in place, they were reactive only when/if something happened. We operationalized Reactive as: "Response to something that has happened".

Because experts did not trust the people, places, and interactions they engaged with and in online, they believed it was necessary to have a plan in place in order to mitigate or recover from any risk they might encounter. One NIST expert put it this way: "*I think I'm pretty aware of my environment, so I have adopted a set of best practices, I would say, about interacting with the technology. So I think I tend to have the right kind of measure for whatever I do*" (FedE:04–10:32).

This expert, like many, was aware of potential threats and risks and had adopted particular practices for online protection. For experts, having a plan entailed being proactive in their thoughts and actions, something most experts thought the general public did not do. "*I work with security people, so we take all kinds of precautions, but the average person... I don't think they take enough precautions*" (FedE:18–13:20).

The non-experts recognized this lack of preparedness in their approach to being online. As one non-expert put it: "*I think people in general I think are more reactive versus proactive*" (DCGP:04–11:38). Similarly, a Midwest participant noted: "*No, I think I will be reactionary and not proactive. I think that if something happens, if something bad were to happen, then I would be the type of person to change all my passwords... but I'm not very proactive about my own security, I'm much more reactive*" (MWGP:02–19:32).

Unlike the experts, non-experts rarely described proactive behaviors they took and instead often spoke of reasons why they, or others, did not have plans in place. For example, one non-expert noted: "*I honestly don't know much about online security. I don't know how that works at all. I really don't so it's sometimes uncomfortable to me... You know how I feel about security is that avoidance means it's going to go away. That's pretty much how I deal with it*" (MWGP:01–2:13 & 2:53). Another spoke of why non-experts did not engage in proactive behaviors. "*I think there's the same sort of invincible aspect that exists in the sort of physical world exists online of like, "There's nothing I have that is worth stealing so I don't believe that somebody will come after me. No hacker will come after me." So, I think people just assume that they're not worth stealing from and therefore why would they spend their time coming up with a new password every three months"*. (MWGP:02–8:04). Here non-experts use mental models like Avoidance or Lack of Value [28] to highlight why they do not worry about being proactive in their online security behaviors. They did not understand it, they did not believe it would happen to them, or they had nothing of any value—so why worry about it. Again, non-experts did not have a solid mental model related to cybersecurity. Instead they drew on multiple mental models that were ill-formed and that only partially helped them understand and navigate cybersecurity.

Having a plan in place made experts feel safe and like they could deal with potential risks or issues. One result is that they had very different emotions about cybersecurity than non-experts. We explore the experience of fear and other emotions in the next section.

C. To fear or not to fear

While we did not specifically operationalize Fear, we coded Fear as an Emotion (an emotional reaction based on the belief that someone or something was a threat or was potentially dangerous). Because experts had a plan in place and were proactive in their approach, they did not express fear or worry in relationship to online activity. It is not that they did not feel risk, but that they believed they could avoid or recover from any risk they might face. The two following quotes, from the same NIST expert, demonstrate how being proactive has led this participant to be comfortable with the measures he has in place to protect himself. *"I basically assume that my technical skills will help me to recover from anything that might happen, and I take reasonable steps to protect my computer and myself. But I don't want to worry about it too much, suck the joy out of life. Right? [laughter]"* (FedE:11–10:46). "*I'm confident that no matter what happens, I'll be able to recover*" (FedE:11–14:47). Most of the experts could not give an example of when they felt at risk—they were confident that they had plans in place to protect themselves adequately and were not afraid of what would happen in the case of a security incident. "*I think that comes out in technical knowledge. I mean, I'll see a report online about some vulnerability and I know that it won't affect me and I can easily patch it and fix it"* (FedE:17–11:53).

In contrast, the non-experts often expressed very different emotions when talking about the risks they faced. They used words such as: uncomfortable, fear, helplessness, anxiety, worry, afraid, and confusion. Most said they often felt at risk (even though they had expressed earlier that they had high levels of trust in their online interactions), and many gave stories of how they or someone they knew had faced problems with online security. Some recounted instances where their credit cards had been compromised while others gave examples of information getting out on social media without their knowledge or consent. These examples made them fearful of what could happen. However, non-experts continued to assert that there was little they could do to protect themselves in advance, thus their fear was warranted.

Instead of fear or other negative emotions, many experts felt a sense of excitement when thinking about cybersecurity. *"There is excitement on my end, because there's so much to learn. It's crazy. Cybersecurity is such an umbrella term for so many different domains under security. I mean there's encryption, access control, physical control. ... But there's also learning for the sake of learning – you can work with some cutting edge technologies on some very sophisticated stuff.* (FedE:18–22:43). In addition to excitement, many experts felt that cybersecurity represented a challenge, a challenge they were eager to address. *"I think the only other emotion that I personally would have would be continued optimism, not necessarily optimism. Maybe just eagerness of the continued challenge. It's a worthwhile, I don't want to say fight, but it's a worthwhile effort*" (FedE:10–19:31). This participant, like many of our experts, felt excitement at the possibilities that the world of cybersecurity held—mostly related to work and to the potential in helping create solutions.

However, some experts did express frustration and anger—mostly directed at people who did not take cybersecurity seriously or who did not work to protect themselves—like our non-experts. "*I guess it's just sometimes you get frustrated with people that aren't taking it seriously... If they haven't followed the procedures that they need to*. (FedE:19–8:19). And another expert noted: "*I get frustrated about the lack of critical thinking about the issues"* (FedE:02–14:33). Exciting and frustrating—both contributed to a sense on the part of our experts that there needs to be a different way to reach non-experts and help them understand how to protect themselves online.

V. Discussion

The codes of Don't Trust/Trust Too Much, Proactive/Reactive, and Fear/No Fear provide insight into the different ways in which experts and non-experts perceive and

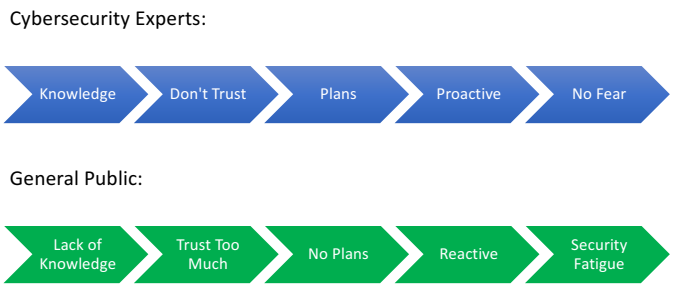

Fig. 1. Figure Security Expert and General Public Security Behavior Models

experience the online environment. Analysis of the relationship amongst these codes shows the ways in which they work together to either provide protection while online or not. Perhaps most important is the way in which the beliefs (Trust Too Much) and behaviors (No Plans) of non-experts result in the need for reaction which contributes to security fatigue [34]. The relationships amongst these codes are depicted by the behavioral model in Figure 1.

In their self-assessments of knowledge related to online privacy and security and in their interviews, experts reported high levels of knowledge about cybersecurity and different types of threats. This is one reason they didn't trust the online environment. As a result, they felt it necessary to make plans and be prepared for when a security incident happened. These plans often entailed proactive behaviors to prevent or mitigate a potential security event thus enabling a confident and a non-fear inducing experience as illustrated in Figure 1.

Figure 1 also shows the General Public's security behavior model. In this model, the general public has little knowledge of the security threats that exist. This lack of knowledge leads the general public to trust the online environment too much. As a result, they do not believe security incidents will happen to them, and therefore there is no need to be prepared and to put a plan in place. All their security actions are reactive. For every security incident, the general public must make decisions. The more security incidents there are, the more decisions they need to make, thus leading to security fatigue.

As security fatigue rises due to the increasing number and severity of security incidents and decisions about them, so do the indicators of security fatigue like complacency and resistance. Lack of planning only increases as these symptoms of security fatigue increases. Lack of planning, as we have noted, leads to more reactive decisions, leading to more security fatigue and so on [34].

A. Advice from the experts

Experts and non-experts drew on different mental models as they talked about cybersecurity. "The difference in mental models between technical experts and their audiences are not only caused by differences in beliefs and their connections, but also by problems with terminology" [35, p.33]. Several experts discussed the ways in which they felt the language of cybersecurity contributed to different thinking and behavior on the part of non-experts. *"In putting it into context, if you just give this high-level, hand waving recommendation, I don't think people can absorb that. It'll be too vague. It's not actionable, so you can't really blame them for not adopting good practices, because you're not being a good communicator with them*" (FedE:04–15:53). Another NIST expert noted: "*I think one of the things we struggle with, generally, in the cybersecurity space is actually talking to the audience. We're good at [talking] to other cybersecurity experts, for example, but when we try to change our audience... to the average consumer, I think we get lost in our cyberspeak. Actually, we continue our cyberspeak and they get lost in it and it glazes over, and maybe they become desensitized to the whole issue*" (FedE:09–9:23). "*Cyberspeak*" and overly technical language may contribute to a lack of understanding on the part of non-expert users and result in an avoidance of behaviors that would keep them safe, including not having a plan in place.

In our coding of the expert transcripts, we looked for rules, processes, or procedures the experts used in their cyber activities or the advice they would give to others. They often articulated these in non-technical language, especially when asked how they might describe online security to a child, or what advice they would give to non-experts. So while they recognize that their language is often "cyberspeak" they are in fact able to put their ideas into non-technical terms. A one NIST expert explained (FedE:13–04:46): "*I would try to explain things on the internet aren't really secrets..say like you are in the bathroom telling your friend something, but you don't know there's someone in that stall with their feet up so you don't know that they're there, and they're listening to everything you are saying, and after you leave they are going to tell everyone your secret.*" Clearly, many of their ideas would need greater clarification and/or specificity, it is not enough to say Practice good password habits and Watch out for certificates. However, these ideas may be instructive when considering how best to develop more contextualized and individualized ways of approaching cybersecurity. This goes back to Stewart and Lacey's [35] contention that a technocratic approach that merely gives non-experts facts and information is not enough. Instead we need a more multifaceted approach that recognizes the continuum of user knowledge and experience.

Experts' ideas about cybersecurity fell into two major categories: general advice and specific behavioral rules. Some of the general advice experts would give included the importance of limiting the information shared online. From "*limit the amount of information they post about themselves*" (FedE:14–23:04) to "*Why should you give your personal information just to read an article from Washington Post?*" (FedE:04–15:53), experts believed in limiting the information shared online. In addition, they believed people need to be more aware when they are online. Statements like the following represent this very general, but meaningful, piece of advice: "*stop and think a little bit*" (FedE:01–09:09); "*Just be cognizant, be aware"* (FedE:08–05:16); and "*It takes vigilance to be safe"* (FedE:19–33:56).

Another piece of general advice related specifically to social media. Many of the experts did not use social media, "*I don't use Facebook or anything like that*" (FedE:05–16:58). Others recommended that if using social media, users should be selective about what is posted. "*So you really want to think about what you're putting out there*" (FedE:21–06:18). As many of the experts talked about being selective about what is shared on social media, they talked about the permanence

and traceability of this information, noting that many people, especially young people, did not understand these longer term consequences. For example, "*Once it's out there, it's out there"* (FedE:08–20:16).

Many experts also said they would tell people to be pay attention to abnormal requests or behavior and to avoid suspicious sites. "*The same as I would tell someone to be aware of their surroundings in a physical environment, it would be the same thing in a virtual environment as well"* (FedE:20–24:19). "*Okay, so just as with physical security, you need to be aware of where you are and what's going on around you. The same is true in cyberspace. You should learn how to know what your digital tracks are"* (FedE:19–31:22). Both of these experts also used analogies to the physical world when presenting advice, something experts did often with many of the rules and the advice they gave.

A specific rule that experts discussed was to practice good password habits, which included including having strong passwords and changing them often. "*Make sure they're strong passwords. Definitely, don't use the same passwords on sites that are important to you like banking and social media*" (FedE:17–22:58). In addition, experts believed in practicing email safety, which included being attentive to phishing emails and other links that could signal a danger. "*Make sure that you don't open attachments in email that you're not supposed to... that person might not know that his or her computer is infected and that his address book has been hacked into and then its sending out all of these things*" (FedE:05–15:47).

Another rule related to running anti-virus or other security software to protect themselves. "*But you still need to run antivirus at home*" (FedE:01–10:54). In addition to security software, experts encourage keeping devices updated and performing regular backups. "*To make sure they keep their system up-to-date as far as the updates are concerned - operating system updates - and don't forget the application updates as well"* (FedE:20–24:19). "*From a security point of view I think that biggest problem that my wife and my daughter have is that they don't have their files adequately backed up*." (FedE:10–30:34).

Other specific rules included using two-factor authentication and using encryption and HTTPS. "*I feel safer at places that require two-factor authentication*" (FedE:13–21:34). "*If I'm going to do banking, oftentimes there's an argument to be made that it's important to actually type in 'https' instead of going to a bookmark or just Googling it and clicking*" (FedE:02–16:51). Experts also thought it useful to check for certificate errors. "*Certificate error messages are, I think, probably the number one thing that a lot of people should respond to*" (FedE:02–16:51).

Some experts also talked about risks in using public Wi-Fi and advocated avoiding it. "*When I'm at a hotel, I'm not going to try to do something with my taxes or my banking stuff. [My employer] obviously offers a VPN, so I'm going to get that fired up as soon as possible*" (FedE:06–40:28).

Ultimately, all of this advice and these rules point toward an important conclusion: *Be prepared*. This idea of being prepared permeated the expert interviews, whether we were asking specifically about the advice they would give, what they would say to children, or whether or not they thought the general public protected themselves adequately. As one NIST expert noted: "*Don't just wing it*" (FedE:12–29:08). Experts believe we need to help the general public understand the need to be prepared, as well as the actions they can take to be prepared. However, this will rely on changing their mental models related to cybersecurity, which is no easy task.

VI. Conclusions

Our results demonstrate that U.S. Government experts think and behave differently about cybersecurity than the non-experts we interviewed. In particular, the government experts are less trusting, always prepared with a backup plan, and are proactive. As a result, the government experts that we interviewed have little or no personal fear with respect to the cybersecurity of their personal computer systems, even when things go wrong. In contrast, our non-experts are trusting, unprepared, reactive and fearful (see Figure 1).

In his book *The Power of Habit*, Charles Duhigg argues that in order for people to overcome "inflection points," or times of duress, they need to have a plan. However, it is important for this plan to be their own. It needs to be individualized and contextualized if it is to be effective. The experts in this study each had their own plan. They had constructed the plans, put them in place, reviewed them, and as a result being prepared had become habit for them—so that they always had security "running in the back of [their] minds." [15]

More work is required to investigate how to change the practice of the general public so that people are more proactive about cybersecurity measures. If we want users to be more proactive in their approaches to cybersecurity, we need to help experts listen to them, understand what they believe and experience, and speak in a language non-experts can understand. Our experts have formed good cybersecurity habits and know how to be prepared. It is still an open question how best to instill security habits to the general public. Gaining a better understanding of expert and non-expert beliefs and experiences may provide greater direction for helping both groups help each other, insuring that everyone knows how to be prepared.

VII. Acknowledgments

Thanks to Julie Haney for her interviews of federal experts.

References

[1] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security Privacy*, vol. 3, no. 1, pp. 26–33, Jan 2005.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999. [Online]. Available: http://doi.acm.org/10.1145/322796.322806

[3] D. Armstrong, A. Gosling, J. Weinman, and T. Marteau, "The place of inter-rater reliability in qualitative research: an empirical study," *Sociology*, vol. 31, pp. 597–606, 1997.

[4] F. Asgharpour, D. Liu, and L. J. Camp", ""mental models of computer security risks"," in *WEIS 2007—Sixth Workshop on Economics of Information Security*, Pittsburgh PA, 7-8 Jun. 2007.

[5] F. Asgharpour, D. Liu, and L. J. Camp, "Mental models of security risks," in *Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security*, ser. FC'07/USEC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 367–377. [Online]. Available: http://dl.acm.org/citation.cfm?id=1785594.1785641

[6] S. E. Baker and R. Edwards, "How many qualitative interviews is enough," 2012, discussion Paper. [Online]. Available: http://eprints.ncrm.ac.uk/2273/

[7] R. S. Barbour, "Checklists for improving rigour in qualitative research: a case of the tail wagging the dog?" *BMJ (Clinical research ed.)*, vol. 322, pp. 115–117, May 2001. [Online]. Available: http://www.bmj.com/content/322/7294/1115

[8] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: Managing security behaviour in organisations," in *Proceedings of the 2008 Workshop on New Security Paradigms*, ser. NSPW '08. New York, NY, USA: ACM, 2008, pp. 47–58. [Online]. Available: http://doi.acm.org/10.1145/1595676.1595684

[9] M. Bishop, "Psychological acceptability revisited," in *Security and Usability: Designing Secure Systems that People Can Use*, L. Cranor and S. Garfinkel, Eds. O'Reilly and Associates, 2005, pp. 1–11.

[10] C. Bravo-Lillo, L. F. Cranor, J. Downs, S. S. Komanduri, and M. Sleeper, "Improving computer security dialogs," *Human-Computer Interaction–INTERACT*, pp. 18–35, 2011.

[11] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, Fall 2009.

[12] S. D. Carberry, "Workforce tops cyber commission to-do list," *FCW*, Sep. 19 2016. [Online]. Available: https://fcw.com/articles/2016/09/19/todt-cyber-commission.aspx

[13] K. Charmaz, *Constructing grounded theory: A practical guide through quantitative analysis*. Sage Publications, Inc, 2012.

[14] H. M. Collins and R. Evans, *Rethinking expertise*. Chicago IL: University of Chicago Press, 2007.

[15] C. Duhigg, *The Power of habit: Why we do what we do in life and business*. Random House, 2012.

[16] S. Furman, M. F. Theofanos, Y. Y. Choong, and B. Stanton, "Basing cybersecurity training on user perceptions," *IEEE Security & Privacy*, vol. 10, pp. 40–49, 2012.

[17] P. Fusch and L. Ness, "Are we there yet? data saturation in qualitative research," *The Qualitative Report*, vol. 20, pp. 1408–1416, 2015.

[18] N. Golafshani, "Understanding reliability and validity in qualitative research," *The qualitative report*, vol. 8, pp. 597–606, 2003.

[19] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, ser. NSPW '09. New York, NY, USA: ACM, 2009, pp. 133–144.

[20] ——, "More is not the answer," *IEEE Security Privacy*, vol. 12, no. 1, pp. 14–19, Jan 2014.

[21] I. Ion, R. Reeder, and S. Consolvo, "... no one can hack my mind: Comparing expert and non-expert security practices." in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 327–346.

[22] J. Kinchelo, *Teachers as researchers: Qualitative inquiry as a path to empowerment*. New York: Falmer Press, 1991.

[23] Y. S. Lincoln and E. G. Guba, *Naturalistic inquiry*. Beverly Hills, CA: Sage, 1985.

[24] J. A. Maxwell, "Understanding and validity in qualitative research," *Harvard Educational Review*, vol. 62, pp. 279–300, 1992.

[25] J. M. Morse, "Qualitative generalizability," *Qualitative Health Research*, vol. 91, pp. 5–6, 1999.

[26] I. Newman and D. Covrig, "Building consistency between title, problem statement, purpose, and research questions to improve the quality of research plans and reports," *New Horizons in Adult Education and Human Resource Development*, vol. 25, pp. 70–79, 2013.

[27] J. Popay, A. Rogers, and G. Williams, "Rationale and standards for the systematic review of qualitative literature in health services research," *Qualitative Health Research*, vol. 8, pp. 341–351, 1998.

[28] S. S. Prettyman, S. Furman, M. Theofanos, and B. Stanton, "Privacy and security in the brave new world: The use of multiple mental models," *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 260–270, 2015.

[29] H. J. Rubin and I. Rubin, *Qualitative interviewing: The art of hearing data*. SAGE Publications, 1995.

[30] J. Saldana, *The Coding Manual for Qualitative Researchers*, J. Seaman, Ed. Los Angeles: Sage, 2013, second Edition.

[31] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sept 1975.

[32] D. Seltzer-Kelly, S. J.Westwood, and D. M. P. na Guzma, "A methodological self-study of quantitizing: Negotiating meaning and revealing multiplicity," *Journal of Mixed Methods Research*, vol. 3, pp. 258–274, 2012.

[33] A. Shenton, "Strategies for insuring trustworthiness in qualitative research projects," *Education for Information*, vol. 22, pp. 63—75, 2004.

[34] B. Stanton, M. Theofanos, S. S. Prettyman, and S. Furman, "Security fatigue," *IEEE IT Professional*, vol. 18, no. 5, pp. 26–32, 2016.

[35] G. Stewart and D. Lacey, "Death by a thousand facts: Criticising the technocratic approach to information security awareness." *Information Management & Computer Security*, vol. 20, pp. 29–38, 2012.

[36] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS '10. New York, NY, USA: ACM, 2010, pp. 11:1–11:16. [Online]. Available: http://doi.acm.org/10.1145/1837110.1837125

APPENDIX A: INTERVIEW PROTOCOL, EXPERTS

1. We know you work in the field of cybersecurity and privacywhat got you interested in this area?

2. What are you working on currently and how is it related to cybersecurity and privacy? Why do you believe this work is important?

3. What do you see as the difference between privacy and security?

4. How would you explain computer privacy to a young child? What about cybersecurity, how would you explain it to a child?

5. Why do you think we need to worry about cybersecurity and privacy, why do you think they matter? If they come back with "It's a federal mandate," follow up with a probe, either: 1) so why do you think we need a federal mandate? and/or 2) yes, there is a federal mandate, but we're interested in why you believe it's important?

6. Do you believe most people protect themselves and their privacy adequately? Why do you think this?

7. So, what kinds of issues or problems do you think individuals face when trying to stay safe online?

8. When you think about cybersecurity and privacy, what kind of problems do you think we as a country might face?

9. When you think about cybersecurity and privacy, what kind of emotions do you feel?

10. Tell me about a time when you felt at risk in an online situation, not while at work but in your personal life. 1) Why or when is it that you feel at risk online? 2) What triggers alarm bells for you when you're online?

11. Describe what makes you feel safe when you're online. 1) What do you do to feel safe? 2) Are there some places where you feel safer than others when you're online? Why is this?

12. As an expert, what kind of advice would you give to someone who is not an expert in this field? Do you follow your own advice?

13. Do you have kids or grandkids or nieces/nephews? If so, what do you tell them about being online? What do you

want them to think about when they're on the computer or online?

14. Is there a particular experience you've had online that you think demonstrates some of the topics we've been talking about?

15. Is there anything we haven't asked that you think would be important for us to know about cybersecurity and privacy?

APPENDIX B: INTERVIEW QUESTIONS, GENERAL PUBLIC

1. The internet is something we all seem to use on a daily basis. If you were describing your relationship to the internet to someone, how would you describe it? If there is a pause: For example, is it something you depend on like a good friend, to keep you updated, or is it just a tool, or . . . ?

2. We seem to be doing more and more things on the internet, like banking and shopping and gossiping. A lot of this involves giving information about ourselves to others, or to the internet. What do you think privacy means in that kind of an online setting?

3. What about security, what do you think computer or online security means?

4. What do you think is the difference between online privacy and security?

5. How would you explain online privacy to a young child? What about computer security, how would you explain it to a child?

6. Why do you think we need to worry about computer security and privacy, why do you think they matter?

7. Do you believe most people protect themselves and their online privacy adequately? Why do you think this?

8. So, what kinds of issues or problems do you think individuals face when trying to stay safe online?

9. When you think about computer security and privacy, what kind of problems do you think we as a country might face?

10. When you think about online privacy and computer security, what kind of emotions do you feel?

11. Tell me about a time when you felt at risk in an online situation, not while at work but in your personal life. a) Why or when is it that you feel at risk online? b) What triggers alarm bells for you when you're online?

12. Describe what makes you feel safe when you're online. a) What do you do to feel safe? b) Are there some places where you feel safer than others when you're online? Why is this?

13. Do you have kids or grandkids or nieces/nephews? If so, what do you tell them about being online? What do you want them to think about when they're on the computer or online?

14. Is there a particular experience you've had online that you think demonstrates some of the topics we've been talking about?

15. Is there anything we haven't asked that you think would be important for us to know about computer security and online privacy?