Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture

Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala,
and Kent Seamons, *Brigham Young University*

https://www.usenix.org/conference/soups2017/technical-sessions/presentation/ruoti

This paper is included in the Proceedings of the
Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).
July 12–14, 2017 • Santa Clara, CA, USA
ISBN 978-1-931971-39-3

Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture

Scott Ruoti[‡][†][*], Tyler Monson[‡], Justin Wu[‡], Daniel Zappala[‡], Kent Seamons[‡]
Brigham Young University[‡]
Sandia National Laboratories[†]
scott@ruoti.org, *monson@isrl.byu.edu*, *justinwu@byu.edu*, *zappala@cs.byu.edu*, *seamons@cs.byu.edu*

ABSTRACT

Understanding how people behave when faced with complex security situations is essential to designing usable security tools. To better understand users' perceptions of their digital lives and how they managed their online security posture, we conducted a series of 23 semi-structured interviews with mostly middle-aged parents from suburban Washington state. Using a grounded theory methodology, we analyzed the interview data and found that participants chose their security posture based on the immense value the Internet provides and their belief that no combination of technology could make them perfectly safe. Within this context, users have a four-stage process for determining which security measures to adopt: learning, evaluation of risks, estimation of impact, and weighing trade-offs to various coping strategies. Our results also revealed that a majority of participants understand the basic principles of symmetric encryption. We found that participants' misconceptions related to browser-based TLS indicators lead to insecure behavior, and it is the permanence of encrypted email that causes participants to doubt that it is secure. We conclude with a discussion of possible responses to this research and avenues for future research.

1. INTRODUCTION

Security has been a persistent problem for the Internet; attacks against corporations [7, 16, 24, 29, 32, 40] and individuals [36, 19, 26] are now commonplace. The literature is rife with recommendations and tools (e.g., password managers, secure email) from security experts for improving users' security postures [6, 8, 39, 34]. Unfortunately, users are slow to adopt these practices, leading them to fall victim to the same categories of attack that have been pervasive for over a decade (e.g., weak passwords, phishing).

To address this problem, it is important to ask why users reject this advice, as the answer to this question should guide the direction of future research. If users are unaware of available protections, then the community needs to research how to best disseminate this knowledge. If users do not want to be bothered with security, then research should focus on technologies that act without user input or awareness. If instead, users reject security advice because it is too costly to implement (e.g., time, effort, money), then we need to better understand users' internal models of security and design protections that fit within that context.

We conducted a grounded theory study [9] on how users perceive their digital lives and how they manage their online security posture. As part of this effort, we conducted a series of 23 semi-structured interviews with mostly middle-aged parents in a suburban location in Washington state. While participants were free to self-guide the interview, the following topics were discussed: (a) their awareness of the potential risks associated with their online activity, (b) which risks they actively mitigated, (c) the steps they took to mitigate those risks, and (d) why they chose not to mitigate others. To explore how they viewed specific security contexts, we asked participants about their understanding and opinions regarding various security technologies associated with the web (e.g., encryption, TLS, secure messaging).

Our analysis revealed that the context within which participants select their security posture is dominated by two key factors. First, the perception that the Internet has brought incredible value into their lives, and most limitations on its usage would be extremely damaging. Second, the perception that regardless of what steps are taken, they can never be perfectly safe, which curbs any desire to implement security mechanisms that carry a high cost of adoption. Because perfect security is perceived as unattainable, users instead engage in a four-step process wherein they weigh the costs and benefits of various coping strategies designed to minimize the likelihood or impact of online risks against the benefits they derive from online activity.

1. **A user learns about a new security threat.** This happens by word of mouth, news reports, television shows, and movies.

2. **The user evaluates the risk presented by the threat.** If the attack seems sufficiently unlikely, they will generally ignore it.

3. **The user estimates the impact of a successful attack.** The amount of damage is commensurate to the effort they are willing to expend to address the threat.

[*] Scott Ruoti now works at MIT Lincoln Laboratory

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

4. **The user selects an appropriate coping strategy.** This selection is based on trade-offs between the cost of implementing the coping strategy (e.g., diminished ability to use the Internet) and its ability to mitigate risk by reducing attack surface and/or impact.

Importantly, users are fluid in their application of this process and do not necessarily proceed linearly through a series of steps. Rather, they may skip some steps or re-evaluate past steps as they learn new information.

As part of our grounded theory methodology, we avoided investigating related work before completing our analysis of participants' responses. This was done to avoid biasing ourselves as we designed, administered, and analyzed our study, allowing us to focus on what the data was saying, and not what prior research had found. After reviewing the related work, we found that the above process has a strong relationship to the inputs and outputs of protection motivation theory [33]. Our work is useful in demonstrating how users adapt this model to online activity and also extends upon this model by describing how users weigh trade-offs when selecting coping strategies.

Our analysis of the data also revealed several other topics that were particularly interesting:

- *Most participants understand the basic principles of symmetric key cryptography.* They correctly identified that encryption relies on a shared key, and only owners of this key could read an encrypted message.
- *Participants' belief that TLS indicators represented site safety, not connection security, led them to click through TLS connection warning pages.* More troubling, they were most likely to ignore the warning pages for well-known sites (e.g., Amazon, Microsoft, Google) when, in reality, warnings on these sites are relatively more likely to indicate malicious behavior.
- *Participants felt that secure email was less secure than texting because of its permanence.* In line with their views that nothing is 100% safe, permanence meant that at any time in the future an attacker (e.g., government, hacker) could choose to break their old email, whereas text messages were viewed as ephemeral and only vulnerable to an active wire-tapper.

2. RELATED WORK

There is a large body of literature that relates to understanding user motivation, perception, and behavior in the context of security. We first discuss general theories of user behavior and then examine relevant work in the usable security field that relates to the perception of risk, cost-benefit tradeoffs, user motivation, and experience with security warnings.

2.1 Theories of User Behavior

Numerous theories have been developed by psychologists regarding how users can be persuaded to take some action, such as adopting health advice or purchasing a product [18]. Several of these have been used to study persuasion in the context of security and privacy behaviors. For example, the elaboration likelihood model states that there is a central route to persuasion, in which a person carefully considers the merits of information presented, and a peripheral route that involves positive and negative cues [30]. For example, this model has been applied to understand adoption of electronic health records [4] and trust in online retailers [45].

Protection motivation theory states that people react to fears by assessing the severity and probability of the threat and then appraising the efficacy of a recommended behavior and their ability to carry out that recommendation effectively [33]. This theory has been used to explain home computer user's security behavior [3], the use of anti-virus software [28], and the effectiveness of security policies in the workplace [21]. LaRose et al. [27] use both of these theories, along with social cognitive theory, to develop a framework for motivating safe behavior online.

Witte developed the extended parallel process model (EPPM) to explain how people react when confronted with communications that appeal to fear [44]. In EPPM, user reactions to threats are driven by the assessment of a threat and efficacy, and their reaction is either determined by fear control or danger control. If there is a perception of high threat and high efficacy, then people will take the appropriate protective action (danger control). However, if there is high threat and low efficacy, people will lose hope and reject the proposed remedy (fear control). Based on this theory, appeals to take protective security measures need to ensure that people respond more strongly to the effectiveness of the proposed remedy and their capability to implement it than to the fear of the threat. Too strong of an appeal to fear leads to inaction.

Our theory is most similar to EPPM, with overlap in the concepts that people appraise the risk and severity of a threat, as well as the use of cognitive defense mechanisms to manage anxiety. Many users have internalized a fear that nothing is safe on the Internet, but this fear has generally not been strong enough to override the belief that the Internet nonetheless offers significant value. However, users may choose to avoid certain activities if their fear is too strong. Extending this model, we find that users weigh cost-benefit trade-offs in their evaluation of response- and self-efficacy. This is similar to work by Herley [22], which argues that users' rejection of some security advice is rational from an economic perspective. He discusses how in the context of password composition, phishing, and TLS warnings users have an economic incentive to ignore security advice; the cost of addressing these issues is greater than the reduction in harm. While Herley's work was theoretical, our study grounds his ideas in data, demonstrating that users do think through these economic arguments—though, in a simpler form—when deciding what security decisions to make.

2.2 Risk Perception and Behavior

Other work in usable security has examined users' perception of risk and how this motivates behavior. Wash interviewed participants regarding their perceptions of digital security [41] and identified eight "folk models" describing participants' understanding of viruses, malware, and hackers. Wash also discussed how these models could explain why participants ignored security warnings. This paper has many similarities to our work, using a similar methodology and population. While both works discuss online threats, our work provides more details regarding the harm that users associate with risk and the context under which users make security decisions.

Wash and Rader have also studied security beliefs and how this affects how people choose to protect their home computer [42]. They find that direct and visible threats lead to positive security decisions, while beliefs that require more technical knowledge lead to fewer precautions. The educated and older are more likely to hold these more sophisticated beliefs. We confirm these finding in our research, finding that users feel overly-technical solutions often offer marginal benefits in comparison to their adoption cost.

Harbach et al. surveyed users and asked them what risks they were most concerned about for five different online scenarios [20]. In addition to stating potential risks, participants were also asked to rank them. Finally, participants were presented with a list of 22 common risks and asked to rate how relevant they found those risks. They found that users were aware of far fewer risks than had previously been believed and recommended that more work be done in risk communication and education. Contrary to Harbach's supposition, users' failure to report on certain risks (e.g., phishing) showed their unawareness of those risks. We find that users are aware of those threats but have already implemented coping strategies that eliminate the need to worry about those risks. Additionally, we provide greater detail regarding the harm that users associate with various risks.

2.3 Cost and Benefit Tradeoffs

Other work in usable security provides evidence that users weigh costs and benefits when deciding what security advice to adopt. For example, Fagan et al. examined the basic question of why some people follow security advice but others do not [11]. They find that the benefits of following security advice are rated higher by those who follow the advice than by those who do not. Likewise, the risks and costs of not following it are rated higher by those who follow advice. They find that individual concerns are rated higher than social concerns, confirming work by Anderson et al. [3].

Beautement et al. conducted interviews of 17 employees from two companies to determine why they do or do not comply with security policies [5]. Their findings suggest that business users weigh the cost and benefit of compliance to design which policies to adopt. Further, they theorize that users have a limited compliance budget that must be managed, restricting users' focus to the security practices that would be most effective. Our work shows that home users have an analogous 'compliance budget' that dictates which security behaviors they are willing to adopt.

Stobert and Biddle [37] conducted a grounded theory study regarding users' behaviors in managing passwords. They found that while users took steps commonly considered insecure (e.g., writing down passwords), these choices were often rational and represented a self-management of personal resources. Our results complement their results and demonstrate that this type of rationale extends beyond password behavior into all parts of a user's digital life.

Ion et al. [23] conducted two online surveys to identify discrepancies between expert and non-expert security practices in order to improve security education for non-experts. They report that non-experts focus on using anti-virus software, making strong passwords, changing passwords frequently, watching for phishing, and visiting trusted websites. Our results reveal similar practices among non-expert users and further discuss how they select these behaviors and reject others that were adopted by experts in Ion et al.'s study.

Redmiles et al. [31] investigate the acquisition of security behaviors by focusing on how users decide which items of security advice to follow and which to ignore. They find that users commonly learn about security behaviors from the media, peers, family, and IT professionals. They found that the trustworthiness of computer security advice was largely correlated with the perceived trustworthiness of the source, in contrast with physical security advice which individuals felt capable of assessing on their own. Participants described many more reasons to reject security advice than to put it into practice, including concerns about its role as a marketing tactic and the perception that the security of their data was the duty of service providers. This work contextualizes ours by characterizing the external sources from which users learn their coping strategies. Our work extends this idea by describing additional elements that factor into the equation of how users determine which security behaviors and mechanisms to adopt.

2.4 User Motivation and Understanding

Some work has also explored user motivation. Adams and Sasse [1] challenged the view that users are not motivated to behave securely by exploring why they ignore corporate password policies. They argue that a lack of user-centered design is a result of insufficient communication between designers and users.

Furnell et al. conducted a qualitative study of novice Internet users and their awareness of, attitudes toward, and experience with online security [17]. Their work concludes that "users do not seem sufficiently interested or motivated to protect themselves" and posits that developers should discontinue reliance on users or remove users' choices in matters of security. In contrast, our work finds that users do take responsibility for their online security postures and that their decisions to reject additional security behavior are rational considering the cost of adopting those behaviors and the limited harm that would be prevented.

Kang et al. applied grounded theory to explore the connection between users' understanding of the Internet and their privacy practices [25]. Their results indicate that people with a better understanding of the Internet perceive more threats, but their analysis found no connection between the level of understanding and security practices. Relatedly, Forget et al. [15] compared users' self-reported engagement with computer security against their actual security practices and found that there is not a strong link between the two. Our results suggest that this disconnect between knowledge of threats and security practices can be explained by users' unwillingness to compromise the usefulness of the Internet. Additionally, we find that even if users are aware of certain risks, they will ignore them if they have a low probability of occurring or have minimal potential harm.

3. METHODOLOGY

We conducted an IRB-approved user study to interview individuals about their perceptions and behaviors related to online risk, risk mitigation strategies, encryption, and browser security indicators. This section gives an overview of the interview process, discusses participant recruitment and demographics, and describes our methodology for analyzing the interviews. The full details are in Appendix A.

3.1 Interview Process

Interviews were performed over a five-day period beginning November 2, 2015. In total, 23 participants were interviewed. Interviews lasted between 15 and 45 minutes, with most taking roughly 25–30 minutes. Each participant was compensated $25 USD irrespective of interview duration.

Interviews were mostly conducted in either the home or place of employment of each interviewee. This was done to avoid requiring participants to meet at a specific location, as well as to make participants feel more at ease during the interview. In two cases where this was not an option, participants were instead interviewed in public locations.

At the start of the interview, the participants were presented with a consent form notifying them that the interview would be recorded. After completing the consent form, participants completed a short demographic survey.

Interviews were semi-structured. Participants were informed that the survey was not an assessment of their understanding of the Internet or its security, but rather was designed to help our research group understand what people thought of these issues so that we might build systems that addressed their concerns. Participants were encouraged to share all of their thoughts and opinions, no matter how off-topic those might seem. The interviewer took great effort to allow participants to guide the discussion, such as changing the sequence of topics or discussing topics that were not a part of the interview guide.

3.2 Interview Guide

The interviewer was provided with an interview guide containing an ordered list of questions intended to spark discussion as necessary.

First, participants were asked how they used computers and mobile devices in their day-to-day lives. This included how many devices they owned, what they used them for, and how often they were used. Participants were also specifically asked to detail the types of online activities they engaged in.

Second, participants were asked to describe the risks and threats they were concerned about when using the Internet and whether they had personally suffered harm online. They were then asked what steps they took to protect themselves while using the Internet. This portion of the interview lasted the longest.

Third, participants were queried about encryption.[1] Participants were shown a browser address bar with an HTTPS lock icon, asked whether they had previously seen the icon, and what they thought it meant (see Figure 1). They were also asked whether they had heard the term encryption before. Those indicating they recognized the term were asked what they thought it entailed. Participants were then asked what sensitive information they had previously communicated over the Internet (either through Facebook or email), whether they would like the ability to encrypt those messages in the future (e.g., encrypted email), and how they would like that process to work.

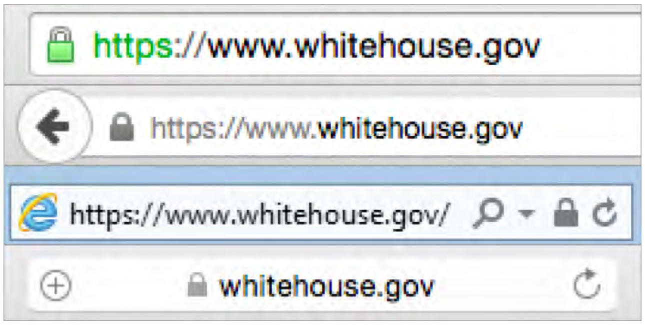

https://www.whitehouse.gov
https://www.whitehouse.gov
https://www.whitehouse.gov/
whitehouse.gov

Figure 1: Examples of the lock icon from Chrome, Firefox, Internet Explorer, and Safari.

Fourth, participants were asked about their experience with security notifications. They were asked to describe what they liked and disliked about the notifications they had seen and to describe their ideal notification.

Fifth, participants were shown invalid TLS certificate warnings from the major browsers. (see Figure 8 in Appendix A.4). They were asked whether they had seen these warnings before, and if so, what they thought the warning was describing. They were then asked if they ever ignored this warning by clicking through, and if so, under what circumstances they would make this decision. They were also asked how often these warnings interfered with their day-to-day tasks, and whether they wished they would go away.

Sixth, participants were asked whether they had any other thoughts or opinions they would like to share. In this portion of the interview, participants were free to talk about whatever subjects they wished, and the interviewer avoided guiding this discussion by only asking clarifying questions as needed.

3.3 Participants

We recruited adult participants (aged 18 or older) living in Gig Harbor, Washington, U.S.A. This location was not proximal to our institution. Our aim in choosing a remote location was to seek opinions from individuals dissimilar to our research group members. Similarly, the location allowed us to survey a non-university population, which is distinct from most studies in the literature.

Initially, we tried to recruit participants from the wider Seattle/Tacoma region using craigslist, but ultimately this method yielded no participants.[2] We then posted flyers at several public locations (e.g., library, church), which resulted in recruiting eleven participants. Of these participants, one introduced us to five coworkers (teachers), six introduced us to their spouse, and one introduced us to their sister.

Demographic data for participants is shown in Table 1. In general, our participants skewed female. Participants were nearly all middle-aged and older. Most participants were currently married, with all participants having some children, the ages of whom ranged from infants to adults. Participants

[1] We asked participants about secure messaging (and by extension encryption) and TLS warnings because these are all topics that our group is actively exploring.

[2] In hindsight, it would have been possible to conduct video interviews online with several individuals that were interested, but were unable to meet in person.

		Total	%
Gender	Male	7	30%
	Female	16	70%
Age	25–34 years old	1	4%
	35–44 years old	7	30%
	45–54 years old	5	22%
	55 years or older	10	43%
Education	Some higher education, no degree	4	17%
	College or university degree	13	57%
	Graduate Education	6	25%
Career	Homemaker	7	30%
	Special Education Specialist	5	22%
	K-12 Teacher	3	13%
	IT Support	2	9%
	Medical Professional	2	9%
	Computer Scientist	1	5%
	Entrepreneur	1	4%
	University Professor	1	4%
	Unknown	1	4%
Marital Status	Married	21	91%
	Single	1	4%
	Other	1	4%
Have Children	Yes	23	100%
	No	0	0%

Table 1: Participant Demographics

had all received at least some higher education, with the majority having finished a university or graduate degree.

3.4 Limitations

Due to the nature of our methodology, our findings are subject to some limitations. First, the semi-structured interview process has some standard limitations. For example, interviewees have a desire to appear knowledgeable and competent to the interviewer, leading them to report security behaviors that exceed their actual behaviors.[3]

Second, the homogeneous nature of our interview sample's demographic—and the city from which it was drawn—limits the generality of our results. Future work could replicate this study with different populations, as well as examine specific results in a more quantitative and large-scale fashion (e.g., Mechanical Turk survey).

4. DATA ANALYSIS

After all the interviews had been completed, the audio from each interview was transcribed. These transcripts served as the primary resource used during our analysis of the data, though the audio data was referenced whenever there was ambiguity regarding the text or tone of a particular line. Throughout this paper, when quoting participants, they are labeled as P[1–23], respective to the order in which they were interviewed. This transcribed data, along with materials produced during our analysis are available at `https://soups2017.isrl.byu.edu`. Transcripts have been modified to remove personally-identifying information.

Our analysis of the data followed a four-stage grounded theory approach (open coding, axial coding, selective coding, and theory generation). Throughout the discussion process, we kept detailed research notes that outlined the thought process underlying our codes, concepts, categories, and theories. These notes were consulted frequently to guide our process. As is often the case in grounded theory, these notes were just as important—if not more—than the concepts and categories derived from the various phases of coding.

In the first stage, our research group reviewed each transcript phrase-by-phrase and word-by-word to assign codes that classified users' responses. These codes were generated using a mixture of open coding (assigning a code that summarizes the participant's statement) and in situ coding (using the participants own words as the code). To ensure that we were assigning the correct meaning to various codes, we paid attention to the context of each statement and reviewed the interview audio as needed to hear the tone the participant was using.

In the second stage, we used the constant comparative method to group codes into concepts. Specifically, we collapsed distinct codes referring to the same topic (e.g., one was an open code, the other in situ) into a single code, reducing the original set of 2,442 codes to a more manageable 503 codes.

In the third stage, we printed each code onto an index card, then organized those index cards into related categories. In total, there were nine categories describing participants' responses: The Internet, Nothing Is 100% Safe, Online Threats, Harm, Coping Strategies, Encryption, Browser-Based TLS Indicators, Secure Messaging, and Notifications. Within these groups, we drew and labeled connections between related concepts. We also drew and labeled connections between the categories.[4] Figures for each category are found throughout the paper and in the Appendix.

In the fourth and final stage, we used the categories, their connections, and our results to derive a theory describing the process users employed in selecting which security behaviors to adopt and which to reject. This theory is based both on the raw data we collected and our analysis of that data. As it is drawn from only 23 participants, it is not conclusive but does provide a theory grounded in the data we gathered.

4.1 Limitations

Due to the nature of grounded theory, our analysis of the data represents one view on that data. Different researchers coding the same data are likely to focus on different aspects leading to distinct categories, connections, and theories. We generated several theories during our research. This paper focuses only on what we determined to be the strongest and most compelling theory. To address this limitation, we will make the transcripts of our interview public.

5. THEORY

The result of our analysis was the generation of a theory that describes the process by which users select their online security posture. Before discussing the process, it is important

[3] Interestingly, participants in our studies often freely admitted that they were doing less than they should. While it is likely that illusory superiority had an effect, it is also possible that the snowball sampling led users to feel the interviews were more personable (i.e., recommended by their friends). This most likely led to more honest answers.

[4] Due to the visual complexity of the complete theory graph, we have not included it in this paper.

to understand the context (i.e., environment) under which this process operates. This context is dominated by two components, the utility of the Internet in users' lives and that users believe perfect security is not achievable.

The participants in our study unanimously indicated that the Internet has been transformational in their lives (see Figure 2). All participants derive value from their use of the Internet, with many noting that it was now a central part of their lives. For example, P13 emphatically expressed, *"I love the Internet. It's become my world."* For others, the Internet has allowed them the freedom to live their lives as they want. P3 described this saying,

> *[The Internet] made our whole home schooling process possible. So our kids grew up to be different than they would have been if they had just gone to the local public school, which was real poor quality. [...] If we had been teaching our kids ten years sooner, it would have just been a huge impact. I mean our lifestyle would not have been possible before the Internet.*

Participants also indicated near unanimously that no matter how much effort was put into strengthening their online security posture, it was impossible to be 100% safe (see Figure 3)—as described by P19, *"I don't think there's ever a place that is perfectly safe."* This viewpoint was derived from three sources:

1. Dramatized depictions of hackers on television and in movies, where security is broken in dramatic fashion, e.g., in 30 seconds or less.
2. Frequent news reports that even companies with large security budgets were routinely compromised—P4 explained, *"there are some big companies that get hacked, that I would expect would have good security in place, but they still get hacked."*
3. An interpretation of the cyber-world as seen through the lens of the physical-world. Specifically that, like the physical world, nothing was ever completely safe—

   > *They got into [the] Pyramids; they got into King Tut's tomb. They can walk in here [at] any time, even with the doors locked. So, I guess I've come to believe there's a segment of society that's gonna make trouble for the rest of us, no matter what generation or what age or what media or [by] what means.* (P14)

Because they did not believe it was possible to completely stop an attacker, participants' security behaviors derived from a focus on addressing the most common threats and making themselves a less appealing target. As expressed by P14, *"you throw enough stumbling blocks in [an attacker's] way, they're gonna look for somebody else that's easier to take care of, to get into. I would imagine it's very much the same way with Internet and security or through encryption."* All the while, participants were careful that their security posture did not unduly affect their ability to derive value from their Internet use.

Within this context, we identified a four-step process which guides a user's selection of which security behaviors to implement. More specifically, users weigh the advantages of online activity against the cost of implementing security practices or mechanisms intended to minimize the likelihood or negative consequences of online risks. While this process is described linearly, users are fluid in their application of it. As they learn and evaluate new information, they may skip some steps or re-evaluate others.

1. **A user learns about a new security threat.** This happens by word of mouth, news reports, television shows, and movies.
2. **The user evaluates the risk presented by the threat.** If the attack seems sufficiently unlikely, they will generally ignore it.
3. **The user estimates the impact of a successful attack.** The amount of damage is congruent to the effort they are willing to expend to address the threat.
4. **The user selects an appropriate coping strategy.** This selection is based on trade-offs between the cost of implementing the coping strategy (e.g., diminished ability to use the Internet) and its ability to mitigate risk by reducing attack surface and/or impact.

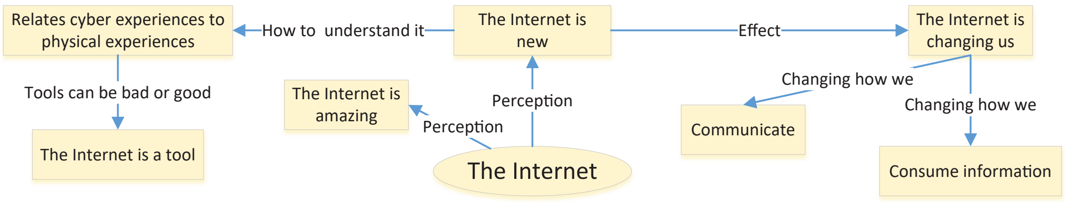
5.1 Learning about Threats

Participants reported learning about threats through four primary sources, all media-based: advertisements, news reports, television dramas, and movies. For example, roughly a quarter of participants asked the study coordinator about LifeLock, an identity protection product, noting that they had heard about it on a radio advertisement. Similarly, P11 described how she learned about cybersecurity from the nightly news:

> **P11:** *Yeah. It wasn't until a couple of weeks ago that they talked about the dark side of the Internet. I didn't know there was one until they started it. You know, it is pretty interesting.*
> **Interviewer** *Where did you hear about that?*
> **P11:** *On the news!*
> **Interviewer** *Local news?*
> **P11:** *Yes. Local news was talking about the darker side of the Internet.*

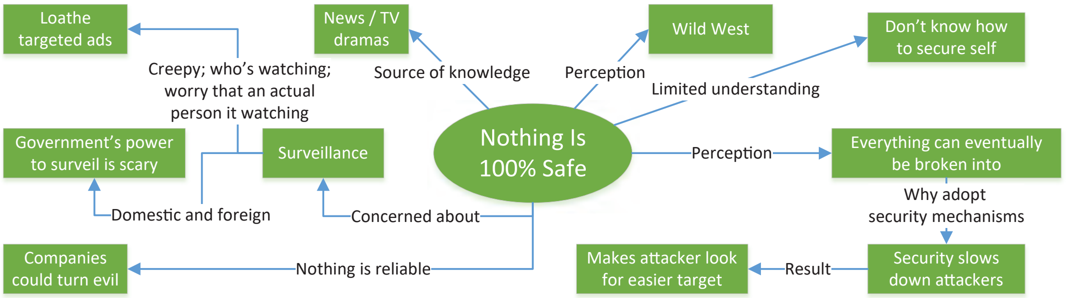
Participants' understanding of encryption and hackers was tied to television dramas or movies. When asked how strong they thought encryption was, P12 replied, *"I would think it might be fairly easy. At least from the movies, they make it sound like they try all these combinations on a computer, and then in thirty seconds, the code's cracked."*

While participants did not report learning about *new* online threats from friends, they did describe using them as a clarifying source that provided greater details regarding the threat and helped identify potential coping strategies. In several cases, participants noted that they relied entirely on their spouse as the de facto security expert. For example, P10 described her key method for evaluating the risk of unknown content: *"If I get something that I don't know, I'm not calling someone until—I actually just call my husband first."*



Participants overwhelmingly expressed wonder at all the Internet has allowed them to do. Many noted that it is a tool that can be used positively or negatively. Others pointed out that it is changing human behavior, including how we communicate and consume information.

Figure 2: The Internet Category Graph


Loathe targeted ads
News / TV dramas
Wild West
Don't know how to secure self
Creepy; who's watching; worry that an actual person it watching
Source of knowledge
Perception
Limited understanding
Government's power to surveil is scary
Surveillance
Nothing Is 100% Safe
Perception
Everything can eventually be broken into
Why adopt security mechanisms
Domestic and foreign
Concerned about
Companies could turn evil
Nothing is reliable
Makes attacker look for easier target
Result
Security slows down attackers

Participants indicated that nothing could be perfectly safe. Critically, participants believed that given sufficient time, hackers could break any system; at best, security slows attackers down, causing them to choose different targets. Also, participants noted that currently trustworthy organizations—corporate and government—could become malicious in the future.

Figure 3: Nothing Is 100% Safe Category Graph

5.2 Evaluating Risk

When learning about a new threat, participants attempted to evaluate its risk (see Figure 4). Several participants noted that most threats did not imply personal risk because the chance they would be targeted was small. P22 explained that *“there’s so many of us. I think that kinda helps us, too. There’s so much information out there that it’s highly unlikely that you’d be targeted, but you can be.”* Still, P23 noted that this protection was not airtight: *“my only protection is that I am only one of 300 million. But you know, I got […]** *a year ago—that’s a 1 in 10,000 chance […]. Somebody gets picked.”*[5]

The threats that participants deemed most risky (i.e., likely to affect them) were largely threats that they had previously encountered—malware, phishing attacks, inappropriate content—or which they had heard discussed frequently on the news—data permanence and surveillance. While the former category of attacks has been discussed at length in the literature (e.g., [5, 41, 20, 36]), the latter is largely unexplored.

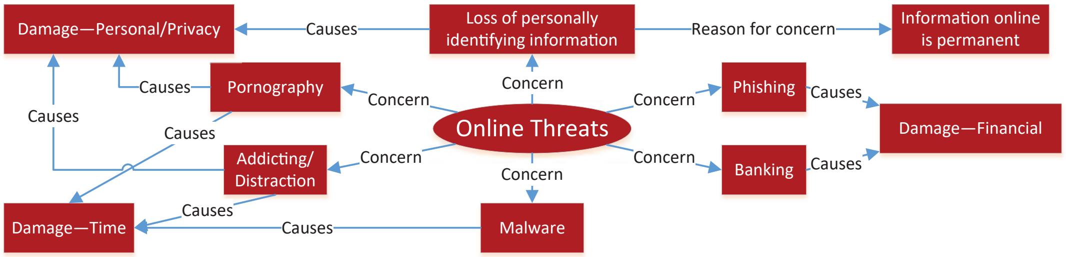
The permanence of online data without consent was a strong concern for many participants. Participants noted that once something was said or done on the Internet, it would remain forever (especially on social media). Several parents and teachers in our study indicated that they make an effort to educate children about the risks of posting information online. This threat troubled participants because once they uploaded any data they were unable to ensure it would be maintained according to their wishes. This led to a tension between using the Internet freely and ensuring that their personal data would not be used inappropriately.

Within this vein, P3 made a compelling argument that children’s inability to erase past online interactions could have a chilling effect on their ability to mature:

> **P3:** *[…] there is some concern with kids using Facebook and having a personality develop online. It would be nice to somehow have an opportunity to erase that as they get older. I don’t know what it will be like for this generation. We didn’t—we were able to grow and mature and change, and leave behind our old selves at some point. It would be nice if there was some way that kids could—*
> **Interviewer:** *That they don’t have to be haunted by the silly things they said as an adolescent.*
> **P3:** *Yeah, that things are permanent once they are leaked into the online world. That (encryption) would be very useful. I think I would feel more able to develop in classes, like writing classes, where you’re submitting things and opinions. You’d feel more free to develop in that way if you knew that they weren’t going to be a permanent part of your record to everybody for now and ever.*

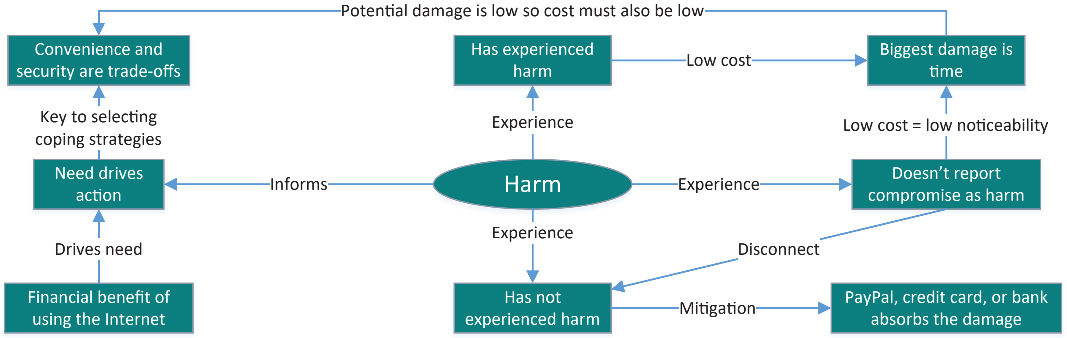
Participants also noted that surveillance of their online activities was a foregone conclusion, especially in relationship to government surveillance. P16 expressed,

[5] P23 described contracting a rare illness here, which has been redacted to preserve anonymity. The point being made is that even low-likelihood events affect *someone*.



Participants were concerned with a wide range of online threats. These threats were associated with three types of damage—financial, personal information and privacy, and time. Interestingly, malware was considered to cause no harm other than the time it took to remove it.

Figure 4: Online Threats Category Graph


Potential damage is low so cost must also be low
Convenience and security are trade-offs
Has experienced harm
Low cost
Biggest damage is time
Key to selecting coping strategies
Experience
Low cost = low noticeability
Need drives action
Informs
Harm
Experience
Doesn't report compromise as harm
Experience
Drives need
Disconnect
Financial benefit of using the Internet
Has not experienced harm
Mitigation
PayPal, credit card, or bank absorbs the damage

Many participants had personally experienced harm or knew someone that had. Still, these experiences were not impactful because they produced no lasting consequences. This lack of impact led users to avoid strengthening their security posture.

Figure 5: Harm Category Graph

> *Well, there's rumors that [the] government watches over everything that we do and that certain words, even in your conversation on the phone, could be flag words. Then you could suddenly have a person at your door. And I don't know [...] [i]f that's a lot of conspiracy theory, or how much reality that is. But it's a possibility, because everything that's good can be used for evil, you know?*

Concerns regarding surveillance were not limited to the government, but also included companies tracking online activities: *"there's just the generalized concern about what can people see me do? How many people are watching me? Who's watching me?"* (P19). This unease was reinforced when their actions on one site would result in related advertisements being shown on an entirely unrelated site. P7 shared,

> *I hate the ads. I hate the ads! [...] [S]ay I go online and I'm looking at a certain style of shoe. And then I come back a week later, and I just open my web browser to my home page, little ads are streaming about what I was looking at.*

5.3 Estimating Impact

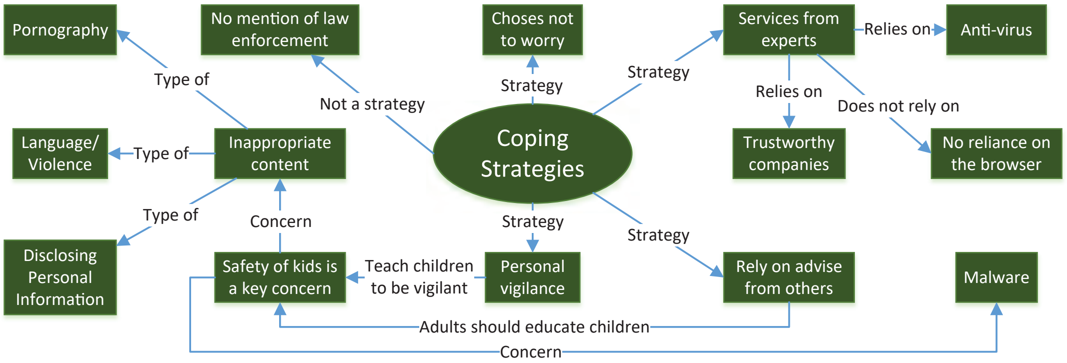
To further characterize threats, users estimated the impact threats could have on their lives (see Figure 5). Unsurprisingly, attacks which led to financial damage were viewed as the most impactful. P4 expressed that such harm was quite scary—*"something that you worked so hard for—your money, and your well-being—and then to have it disappear in a second, is a bit scary."*

While financial damage was a concern, some participants explained that it was unlikely that it would be permanent. They noted that for online shopping they used PayPal or a credit card, both of which would absorb the cost of any successful attack. As described by P3, *"We did have a credit card [company] call us, and let us know that there was a charge on there, and wondering if it was ours, and it wasn't, so they declined the charge before it even went through."* These protections reduce the damage of such attacks to only the time and effort it takes to get charges reversed.

Other than financial harm, participants expressed concern regarding their children's online safety. They worried that children had insufficient experience to avoid malware and that they were likely to disclose personal information without fully considering the ramifications of that disclosure. Additionally, they worried that it was easy for children to be exposed to inappropriate content online (e.g., violence, language)—P12 said *"my boy loves to get on YouTube and listen to Vines and stuff, and the language can be atrocious."*

For most other threats, potential harm was usually seen as negligible—usually only representing a small cost in time or effort to resolve. P14 described this issue,

> *Well, first of all, all [of a] sudden your computer is doing something that you can't get rid of, just, you know, no matter what you do, it's still there. So, the only*



Participants' key coping strategy was personal vigilance, as they believed that their security was ultimately their responsibility. Participants' primary concern regarding their children was teaching them to be vigilant online—to avoid downloading software from suspicious websites (i.e., malware), viewing inappropriate content on YouTube, and disclosing personal information on social media.

Figure 6: Coping Strategies Category Graph

> *way to get rid of it is to completely go back, either in time, or go through and find out which program it is and determine a way to dump it. But, that's not always easy to do.*
> ...
> *It's just time-consuming! And you're looking to computers to do the opposite: allowing you more time. Instead, what you find is sometimes it takes a lot more time to either solve a problem or... If something goes down, then it becomes an issue.*

Surprisingly, due to the perception that costs in time and effort are negligible, participants who had been successfully attacked did not always relate those attacks with harm. When initially asked if they had experienced harm online, they would report that they had not. Later in the interview when discussing other topics, it would become clear that they had previously been compromised (e.g., installed malware, stolen credit card). When asked about this discrepancy, participants indicated that because it had been so easy to resolve, they did not consider it harm. This attitude towards harm helps explain why users are quick to ignore threats that only result in minor loss of time or effort.

5.4 Selecting Coping Strategies

Users select coping strategies based on their evaluation of trade-offs—harm addressed vs. cost to implement (see Figure 6). As the Internet is a critical piece of users' lives, even minor reductions in its utility can be viewed as costly. Also, as participants did not believe they could be perfectly safe, their effort was focused on the most effective coping strategies for reducing their likelihood of being attacked and/or minimized the negative consequences of victimization. Non-selected strategies were largely rejected because they were viewed as having marginal value that did not outweigh their cost of adoption. Depending on how users weigh these various factors, the selected coping strategies can be wildly different.

On one extreme, P13 stated that she did nothing to protect her online security:

> **Interviewer:** *When you are using the Internet, are there any risks or threats that you worry about?*
> **P13:** *No. I bank online and I don't care. I know people who worry about that, I don't.*
> **Interviewer:** *So you never have any concern, regardless of what you are doing on the Internet.*
> **P13:** *That's true. I should have concerns. I know I should.*
> **Interviewer:** *Tell me why you don't have any concerns.*
> **P13:** *Because I don't want to.*
> **Interviewer:** *Can you elaborate on that?*
> **P13:** *OK. I don't want to get trapped. I want to use the convenience of the Internet, and not feel scared of the Internet. People think that their identity is going to get stolen, and it can be, or their bank account is going to be gotten into. Which I understand it can be. Don't care. Because I don't want it trap me emotionally.*

While this attitude, at first, seems quite flippant, upon further examination, it becomes understandable. This participant was an entrepreneur whose business relied on access to plans stored in county buildings. Originally, access was physical, requiring transit to the buildings in question, a slow and time-consuming process. More recently, these documents had been uploaded to the Internet, saving her time and increasing the profitability of her business several times. To her, the Internet represents her livelihood, and any reduction in its utility represents a loss of money to her. In comparison, the coping strategies do little to protect her—the time she saves by using the Internet far outweighs the time she would lose by fixing her computer or working with a credit card company to roll back a transaction. As such, she is making a cost-efficient and rational choice.

On the other extreme, several participants were unwilling to perform any financial transactions (e.g., banking, shopping) online. In their eyes, third-parties (e.g., PayPal, credit cards) could not do enough to protect their financial safety, and the potential harm of financial compromise far outweighed any convenience brought by the Internet. As described by P11,

> **P11:** *I feel very uncomfortable doing banking online. I always have.*
> **Interviewer:** *I would love to hear why.*
> **P11:** *You know, I was doing pretty good with the con-*

> *cept, and then [...] one of the banks... Bank of America got tapped... somebody got tapped into, and I thought 'Oh, if it's that easy, I just, no, there is somebody else who is spending more time out there then what is needed.' I can go. I'm social; I can go and say hello and get my banking done.*

In general, participants fell between these two extremes, selecting to implement coping strategies which had acceptable trade-offs. The coping strategy described as most important was that of personal vigilance—namely, being careful about what sites they visited, what links they clicked, and what files they downloaded. This strategy was selected because it had low cost—it is easy-to-implement and easy-to-bypass as needed—and also because participants felt that they needed to take *personal* responsibility for their online safety. For example, P1 expressed,

> *That, of course, reminds you, that I myself am responsible for monitoring my personal information. Especially as it regards credit and banking, those kind of things. It is up to me to monitor those things on a consistent and regular basis.*

In addition to personal vigilance, other commonly reported coping strategies included installing an anti-virus, setting up a web filter (e.g., OpenDNS, NetNanny) to block inappropriate content, using PayPal and a credit card for online shopping, and relying on services provided by large, credible companies. As these are well studied coping strategies, we do not discuss them in further detail. Conspicuously, two coping strategies were absent from participants' responses—law enforcement and the browser. While participants did mention browser-based TLS securing indicators when asked about them, they did not proactively report these types of features when asked about their online security behaviors. Law enforcement, by comparison, was not mentioned even in passing, even when it came to descriptions of financial risks or sources for advice regarding online safety.

Interestingly, after describing what security strategies they had adopted, several participants indicated that they chose not to worry about remaining threats. The reasoning behind this was the remaining threats were less likely to impact their lives, that they were unaware how these threats could be addressed, and that they didn't want to worry while using the Internet (similar to the sentiment expressed by P13). For example, P4 stated, *"Well, there is a reason to worry, but I don't know what to do about it, so I can't obsess about it, get all panicky. Cause I don't know what to do.*

Ultimately, regardless of their selected security, participants were acting rationally based on the context of their Internet usage and their understanding of threats, potential harm, and trade-offs for various coping strategies. In each case, users were able to give a cogent explanation for why they adopted some coping strategies while rejecting others. Our results suggest that it is counterproductive to either browbeat users into compliance or to bypass them entirely. Instead, if security tools can be better aligned with users' environments and needs, then adoption is much more likely.

6. ADDITIONAL TOPICS

In addition to the topics covered in our theory, participants reported interesting thoughts regarding several additional security topics—encryption, browser-based TLS security indicators, and secure messaging. The category graphs for these remaining topics are in Appendix B.

6.1 Encryption

Two-thirds of participants had an understanding of the basic principles of symmetric encryption, that it *"keep[s] others from being able to see things they shouldn't."*[6] Participants referred to the process of encryption as "scrambling" data, and half were aware that it involved a shared secret.[7]

In accordance with participants' belief that nothing is 100% safe, participants did not believe that encryption is impenetrable, noting that a determined attacker could either find a way around the encryption or a way to break the encryption. Participants indicated that it would take *"huge, huge computers with lots of processing power"* to break an encrypted message. They also described breaking encryption as necessitating *"savvy"* reasoning and that while it might not keep everyone out, it would take skill that *"probably 95% of the population doesn't have."*

While several participants used encryption tools as part of their job, none used them in their personal lives. When asked if they could identify any personal uses (i.e., non-business, non-HTTPS) for encryption, almost half of participants indicated that they did not see a use for it, either because they did not upload sensitive information online or because they doubted that encryption of online information could ever be sufficiently secure (see Section 6.3).

Of the participants that identified uses for encryption in their personal lives, they mentioned protecting financial data, cloud data, work documents, and day-to-day communications. For several participants, encryption intrigued them because it offered a potential solution to two threats that they lacked adequate coping measures for: government surveillance and data permanence (see Section 5.2). For example, P3 indicated that encryption could be a solution to children's online interactions being too permanent (see Section 5.2).

6.2 Browser-based TLS Security Indicators

There are a wide range of papers that examine the effectiveness of TLS warnings in browsers [10, 38, 2, 13]. Collectively they find that many users ignore TLS warnings, but that over time users have become more likely to heed these warnings. We questioned participants regarding the browser's TLS indicators—HTTPS lock icon and TLS warning page—to better understand what they thought these indicators meant and why they sometimes choose to ignore them.

When presented with images of these indicators, it quickly became apparent that participant's mental models largely failed to account for the existence of connection-level attacks. Instead, participants associated the TLS indicators with site-level safety.[8] Importantly, we found that these misconceptions were directly correlated with insecure behavior.

[6] Other than one participant who was a software developer, participants never mentioned public key cryptography.

[7] The terms used to described the shared secret included calling it a key (most participants), a password, a credential, or a code.

[8] Similar misconceptions about connection-level security have also been observed in more technical users [12].

6.2.1 HTTPS Lock Icon

Participants largely felt that the lock icon indicated that the site was "safe" place to do business. For example, P9 said,

> *Well, to me it means that it is a secure site. That other people are not just going to be able to get into what I have put in. I'm sure that there are ways to do that, but they've made it harder—hopefully. So, that's what it has meant to me.*

Others thought that the lock icon indicated that the website was "locked", and that it would require credentials to access. For example, P8 said the following about the lock icon:

> *That would make me think that I need a password to get it. A password or login to get in. That it's secure. That it's only for those people, where you have to create an account, or for those that have already created an account.*

Regardless, participants indicated that they did use the lock icon to determine which sites they should use. P9 explained, *"if I'm about to use my credit card, I do look for it to make sure it is there. Sometimes if it is not there, I won't purchase. I'll just say, 'Well, I can go find it at the store.'"* Other noted that they used the lock icon to ensure they were on the "real" website. P15 stated, *"like Bank of America, if it's locked, they are telling me it is their website, and that it is the right website."*

While at first glance, users' attention to the lock icon might seem like a positive sign, it has troubling implications. Phishers could take advantage of users trust in the lock icon by transmitting their phishing websites over TLS, leading users to be more likely believe that the website is legitimate and safe. This idea is lent credence in the next subsection where we discuss how a similar misconception causes participants to click through TLS warnings. As such, efforts to increase user attention towards the lock icon [12] may end up being counterproductive.

6.2.2 TLS Warning Page

In contrast with the shared, albeit vague, understanding of the browser lock icon, the browser's TLS warning pages were nearly unilaterally met with confusion, though several noted that it meant that *"I'm in trouble"* (P21). Many participants expressed confusion when seeing the warning—P7 said, (*"I don't know what a security certificate is. I've seen [the warning before], but I have no idea what that is."* Still, others thought it was an indication of the site's trustworthiness, similar to their HTTPS lock icon misconceptions.

Overall, participants reported seeing these warnings rarely—at most once a month. Most often these warnings were seen when accessing the participant's employer's intranet, which was described by some users as being rife with sites that required clicking through the TLS warning.

Most participants reacted to these warnings by opting to back off entirely, particularly if they felt at all uncertain. Others indicated that they would ignore the warnings only if they were consuming information and not inputting information. For example, P3 indicated that *"if I'm just looking for information, I have just ignored that. But if I am thinking of shopping, I think I have thought, 'I'm not going here.'"*

Disconcertingly, some participants believed that this warning was a judgment of the trustworthiness of the website being visited. For example, P12 (a Chrome user) said the warning meant that *"if there is an untrusted site that Google doesn't quite know, they are saying 'We don't really know about these guys, and if you want to continue, you can, but we don't really know about them.'"* This misconception led participants to believe that they could safely ignore the warning if it were for a website that they "knew" was safe. P7 stated, *"Well, if I see it, and I am going into some place I have never been before, then I will probably just not go. If it is a place that I know is OK, because I have been there before, then I usually go ahead."*

In these situations, participants attributed the error to a misconfiguration by the browser or website. P19 suggested, *"well, maybe they've just done an update or something like that and there's a glitch in the update."* Alarmingly, the choice to bypass the TLS warning was often associated with high-value sites (e.g., Amazon, email)—these sites were well known to the user—in direct contrast to the fact that the TLS warning is most likely to indicate an attack when it appears for these sites.

6.3 Secure Email and Messaging

Most participants indicated that they had no need for secure messaging and secure email in particular. Many noted that they rarely needed to send sensitive documents, and when they did (e.g., loan application) the company would request that those documents were uploaded directly to the company through a web portal. When asked how they transmitted sensitive data person-to-person, participants indicated that they would share it in person, over the phone, or through text. They viewed these activities as more secure because they felt that each of these transactions was ephemeral—requiring an adversary to actively be targeting them, while online communication (e.g., email) was permanent. For example, P12 described this at length:

> **Interviewer:** *And do you think phones are more secure than email?*
> **P12:** *I think they are, in the standpoint that there would have to be someone bugging your phone and catching it immediately. Whereas if you send it on the Internet, or email, it's logged, and anybody can... So, I guess just your window of opportunity is a lot larger in an email, or on a search engine. Whereas a phone, they would have to be listening that plus or minus maybe five seconds to get the information that they need. To my knowledge, I don't know that anyone is recording, for long periods of time, my phone conversations.*
> **Interviewer:** *So it is really... it seems to be that permanence.*
> **P12:** *Permanence.*
> **Interviewer:** *That with email if you send it once, they can come back later.*
> **P12:** *Exactly! Your window is much larger that you leave yourself exposed. Whereas a phone call you have only got five, six seconds. Blah blah blah blah blah, there is the credit card number. That's the biggest reason. [...] Everybody says that things are so permanent on the Internet. They dig up stuff that is twenty years old. Then they find dirt and information on politicians, and stuff like that. They're finding emails from Hillary Clinton, from years past, when she was at the State Department.*

> *They are digging up all sorts of stuff. And now they are saying SnapChat—where it is supposed to snap a picture and be gone instantly—ummm... is not.*

In most interviews, we asked participants to imagine a hypothetical secure email system that was both usable and fully secure. We then asked participants if they would find a use for such a system, and if so how would they use it. While most participants expressed an interest in such a secure email system, many of those who were interested struggled to identify when they could use it—they only rarely had the need to send sensitive information. Most were interested in its ability to make email messages containing sensitive information ephemeral, self-destroying after the information was no longer needed.[9] The two medical professionals were especially interested in the possibility that secure email could substantially expedite the process of sharing medical information between institutions.

Interestingly, when asked to imagine the hypothetical secure email system, several participants pushed back and stated that they *"would be very skeptical that something like that would ever exist"* (P12). This attitude was tied to their perception that nothing was 100% safe and therefore no secure email tool could protect their sensitive information from determined parties.

7. CONCLUSION AND FUTURE WORK

Our interviews demonstrate that users' online security posture is guided by an analysis of the cost-benefit trade-offs of various coping strategies, informed by their understanding of risks, potential harm, and the context of their online activities. While a user's set of coping strategies is insufficient to address all potential threats, those strategies are usually sufficient to protect them from the harm that they are most concerned about. While these results are drawn from a limited sample of participants and do not necessarily generalize to the entire population, they still provide a helpful guide for what future research can explore.

Because users make rational decisions and are actively engaged in considering their personal security posture, it means that they can be influenced to improve their security posture. While there are many areas where research could be done to better address user needs, we discuss below five areas that stood out as important and achievable as we interviewed participants and analyzed their responses.

Security Recommendations. Participants prefer coping mechanisms that have the greatest impact on reducing their attack surface—i.e., they are not interested in security behaviors that have marginal gains. For example, Florencio et al. [14] show that passwords that are 8–10 characters long are generally resistant to online attacks, whereas passwords of length 18–20 are needed to resist offline attack—passwords of length 11–17 offer marginal security gains at significant cost to users. By recommending that users select password 8–10 characters long, the users can focus on a coping strategy that has a significant impact, without trying to guilt them into adopting longer passwords that have either marginal benefit or become overly-difficult to remember. Future research should follow this cue for passwords, and distinguish which recommendations have low cost and high impact, and which only offer marginal returns.

User Education. Our study showed that most participants learned about online security through media—i.e., news reports, television shows, and movies. Ideally, the community could influence these mediums to correctly portray cybersecurity issues, but this is unlikely. Alternatively, participants noted that they and their children regularly watch content on YouTube and similar services. This presents a compelling avenue for disseminating accurate cybersecurity information to the masses. Future research could explore how to structure such online videos to both educate and to attain maximum dissemination. Based on several participants' responses, a good place to start would be Whiteboard-style videos.

Privacy-preserving Systems for Children. The literature on strong privacy-preserving systems is primarily focused on high-security situations—e.g., political dissidents. The resulting security model is often very strict and leads to relatively low usability. According to their parents (the participants), children are often unaware of the potential harm of disclosing personal information online and are thus unlikely to pay the high usability cost of adopting such solutions. Future research should examine how privacy-preserving technologies can be better adapted to the needs of children for use as they grow up.

Browser Indicators. Users are primarily concerned with the safety of the sites they are visiting, while browsers display information regarding the security of connections. While connection security is an important metric, it does not fully address users' primary concern. Future research should explore how the browser can be used to inform users regarding the safety of the sites they visit. This could have more impact than focusing on making users pay more attention to an indicator (i.e., HTTPS lock icon) that they misunderstand.

Secure Email. Participants indicated that their greatest worry regarding email was its permanence, yet current secure email research is focused on usability [43, 35, 34], not message permanence.[10] Future research should explore how to make email more ephemeral so that users can control the permanence of their messages.

8. ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1528022 and research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) via contract number HHSP233201600046C. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security. Also, this work was supported by Sandia National Laboratories, a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

[9] We note neither PGP, S/MIME, nor current research into secure end-to-end email encryption address this need.

[10] While short-lived keys address this problem, current systems do not actively support this use case.

9. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, Dec. 1999.

[2] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium*, pages 257–272, 2013.

[3] C. L. Anderson and R. Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, 34(3):613–643, 2010.

[4] C. M. Angst and R. Agarwal. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, 33(2):339–370, 2009.

[5] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*, pages 47–58. ACM, 2009.

[6] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy (SP)*, pages 553–567. IEEE, 2012.

[7] S. Buckley. Hackers stole 21.5 million Social Security numbers in government breach. `https://www.engadget.com/2015/07/09/hackers-stole-21-5-million-social-security-numbers/`, July 2015. Online; accessed 21-September-2016.

[8] J. Clark and P. C. van Oorschot. SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In *2013 IEEE Symposium on Security and Privacy (SP)*, pages 511–525. IEEE, 2013.

[9] J. Corbin and A. Strauss. Grounded theory research: Procedures, canons and evaluative criteria. *Zeitschrift fÃijr Soziologie*, 19(6):418–427, 1990.

[10] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074. ACM, 2008.

[11] M. Fagan and M. M. H. Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75. USENIX Association, 2016.

[12] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016.

[13] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo. Experimenting at scale with Google Chrome's SSL warning. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2667–2670, New York, NY, USA, 2014. ACM.

[14] D. Florêncio, C. Herley, and P. C. Van Oorschot. An administrator's guide to internet password research. In *LISA*, pages 35–52, 2014.

[15] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. Do or do not, there is no try: User engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, Denver, CO, June 2016. USENIX Association.

[16] L. Franceschi-Bicchierai. Hacker tries to sell 427 million stolen MySpace passwords for $2,800. `http://motherboard.vice.com/read/427-million-myspace-passwords-emails-data-breach/`, May 2016. Online; accessed 21-September-2016.

[17] S. Furnell, V. Tsaganidi, and A. Phippen. Security beliefs and barriers for novice internet users. *Computers & Security*, 27(7-8):235 – 240, 2008.

[18] R. H. Gass and J. S. Seiter. *Persuasion: Social influence and compliance gaining*. Routledge, 2015.

[19] GeekTime. Millions of victims lost $12.7b last year falling for Nigerian scams, 2014.

[20] M. Harbach, S. Fahl, and M. Smith. Who's afraid of which bad wolf? A survey of IT security risk awareness. In *2014 IEEE 27th Computer Security Foundations Symposium (CSF)*, pages 97–110. IEEE, 2014.

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

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

[23] 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)*, pages 327–346, Ottawa, July 2015. USENIX Association.

[24] M. L. Jordan Smith. Not so securus: Massive hack of 70 million prisoner phone calls indicates violations of attorney-client privilege. `https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/`, November 2015. Online; accessed 21-September-2016.

[25] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "my data just goes everywhere:" User mental models of the Internet and implications for privacy and security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, July 2015. USENIX Association.

[26] K. Kaspersky. Report: Ransomware in 2014–2016, 2016.

[27] R. LaRose, N. J. Rifon, and R. Enbody. Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3):71–76, 2008.

[28] D. Lee, R. Larose, and N. Rifon. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5):445–454, 2008.

[29] C. Osborne. 'discreet' cheating website Ashley Madison suffers data breach. `http://www.zdnet.com/article/discreet-cheating-website-ashley-madison-suffers-data-breach/`, July 2015. Online; accessed 21-September-2016.

[30] R. E. Petty and J. T. Cacioppo. The elaboration likelihood model of persuasion. In *Communication and persuasion*, pages 1–24. Springer, 1986.

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

[32] C. Riley. Insurance giant Anthem hit by massive data breach. `http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/`, February 2015. Online; accessed 21-September-2016.

[33] R. W. Rogers. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1):93–114, 1975.

[34] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons. "we're on the same page": A usability study of secure email using pairs of novice users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4298–4308, New York, NY, USA, 2016. ACM.

[35] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, and K. Seamons. Confused johnny: when automatic encryption leads to confusion and mistakes. In *Ninth Symposium on Usable Privacy and Security (SOUPS 2013)*, page 5. ACM, 2013.

[36] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo. My religious aunt asked why I was trying to sell her Viagra: Experiences with account hijacking. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, pages 2657–2666. ACM, 2014.

[37] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Tenth Symposium on Usable Privacy and Security (SOUPS 2014)*, pages 243–255, 2014.

[38] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *8th USENIX Security Symposium*, pages 399–416, 2009.

[39] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. SoK: Secure messaging. In *2015 IEEE Symposium on Security and Privacy (SP)*, pages 232–249. IEEE, 2015.

[40] L. Vaas. 154 million voter records exposed, including gun ownership, Facebook profiles and more. `https://nakedsecurity.sophos.com/2016/06/23/154-million-voter-records-exposed-including-gun-ownership-facebook-profiles-and-more/`, June 2016. Online; accessed 21-September-2016.

[41] R. Wash. Folk models of home computer security. In *Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*, page 11. ACM, 2010.

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

[43] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Eighth USENIX Security Symposium (USENIX Security 1999)*, pages 14–28, Washington, D.C., 1999. USENIX Association.

[44] K. Witte. Fear control and danger control: A test of the extended parallel process model (eppm). *Communications Monographs*, 61(2):113–134, 1994.

[45] S.-C. Yang, W.-C. Hung, K. Sung, and C.-K. Farn. Investigating initial trust toward e-tailers from the elaboration likelihood model perspective. *Psychology & Marketing*, 23(5):429–445, 2006.

APPENDIX

A. STUDY MATERIALS

This appendix lists all the materials used to conduct the study. Personally identifying information has been replaced by bracketed text describing the relevant information.

A.1 Consent to be a Research Subject

Introduction

This research study is being conducted by [study coordinators and affiliation]. You have been invited to share your opinions about Internet Security.

Procedures

If you agree to participate in this research study, the following will occur: You will be asked to provide some demographic data about yourself. No personally identifiable information will be gathered. You will be asked about your experience with computers. You will be asked to comment on your experience and feelings regarding Internet security. The interview will be audio recorded to ensure accuracy in reporting your statements. The entire study should take about one hour.

Risks/Discomforts and Benifits

If you experience any discomfort, you may stop the study at any time. There are no direct benefits to you for participating in this study.

Confidentiality

The audio recording of this study will be transcribed to computer and then destroyed. All research data will be kept on a password-protected computer in a keypad-locked room on the [storage location]. Only the researchers will have access to this data. A unique, random ID will be generated for each study participant, and this ID will be used in place of any personally identifying information. Data will largely be presented in aggregate, but when direct quotes are required, they will be provided alongside the associated ID and will not contain personally identifying information. We may share research data on the Internet, but will not include any personally identifying information with this data, only the unique, random ID.

Compensation and Participation

You will be compensated $25 for your participation. Participation in this study is entirely voluntary. You have the right to withdraw at any point during the study or to refuse participation entirely. If you withdraw before the end of the study, you will still receive the full $25 compensation.

Questions about the Research

If you have any questions about this study, feel free to contact any of the following: [contact info]

Questions about Your Rights as a Research Participants

If you have questions regarding your rights as a research participant contact IRB Administrator at [contact info].

Statement of Consent
I have read, understood, and received a copy of the above consent and desire of my own free will to participate in this study.

Name (Printed): ______________________________
Signature: ______________________________
Date: ______________________________

A.2 Demographic Handout

What is your gender?

○ *Male*
○ *Female*
○ *I prefer not to answer*

What is your age?

○ *18 – 24 years old*
○ *25 – 34 years old*
○ *35 – 44 years old*
○ *45 – 54 years old*
○ *55 years or older*
○ *I prefer not to answer*

What is the highest degree or level of school you have completed?

○ *Some school, no high school diploma*
○ *High school graduate, diploma or the equivalent (for example: GED)*
○ *Some college or university credit, no degree*
○ *College or university degree*
○ *Post-secondary education*
○ *I prefer not to answer*

What is your marital status?

○ *Married*
○ *Single*
○ *Other*
○ *I prefer not to answer*

Do you have children?

○ *Yes*
○ *No*
○ *I prefer not to answer*

A.3 Interview Guide

Introduction

- "Hello, my name is [name]. I am a researcher from [institution]. Before we begin, we have this consent form for you to read and sign."
- "Here is a short demographic survey."
- "Our research group is trying to understand how security affects you when you use the Internet. Our goal is to design software that makes it easier for you to be secure while you are online."

  "The opinions and ideas you share during this survey will be used to direct the future work of our research group. As such, feel free to be frank and honest. If at any time you have a thought or a comment, feel free to share it, regardless of whether you think it directly impacts the current topic."

Understand the Computing Environment

- How familiar would you say you are with computers?
  - How long have you been using them?
  - Do you use them at work/school?
- How many computers do you own?
  - Use on a daily basis?
  - Mobile devices?
- What sorts of things do you do on the Internet?

Threats

- When you are using the Internet, what dangers are you most concerned about?
  - Do your concerns change when you are at home/work/school?
  - Are there any dangers that affect your immediate family, but not you?
- Have you ever personally suffered harm from the Internet?
  - What was the nature of the harm?
  - What did you do to resolve the problem?
- What do you do to protect yourself while using the Internet?
  - Why do you do this?
  - How effective do you think these methods are?
  - Which one is most important?
  - Have you ever been unable to do something for fear of potential harm?

Encryption

- Have you seen this lock icon in your browser before? (Figure 7)
  - What does it mean to you?
  - If your website tells you that your connection is secure, what does this mean to you?
  - How do you feel when a website says it is secure?
- Do you ever send sensitive information over the Internet? For example, email or Facebook?
  - What types of sensitive information do you send.
  - What are you concerned about when sending sensitive information over the Internet?
- When I say "encryption", what do you think?
  - If they have heard of it.
    - ∗ What does it mean to you?
    - ∗ How do you encrypt data?
    - ∗ What assurances does encryption give you?
    - ∗ How easy is it for an attacker to steal encrypted data?
  - If they haven't heard of it.
    - ∗ Encryption is a process by which data is protected so that only you and intended recipients can read that data."
- Would you be interested in encrypting data you store or send over the Internet?
  - What data would you use encryption for?

- What services would you want it available with?
- How often would you encrypt data?
- Who would you send encrypted data?
- Would you want all of your messages encrypted? Why?

Notifications

- There are many ways that your computer can notify you of potential security problems.
  - What types of notifications that you currently see do you like best?
  - What annoys you the most about current notifications you receive?
- What would your ideal notification be like?
  - Could you please sketch a picture of your ideal notification.
  - How certain should the computer be before notifying you of a problem?
  - How often should you get a notification?

TLS Warning

- Here is a picture of a warning that browsers sometimes show (see Figure 8). Have you seen a similar warning before?
  - What do you do when you see this warning?
  - Under what circumstances do you ignore the warning and click through?
  - Under what circumstances do you stop trying to go to the website?
  - How often do you need to get to the underlying website, regardless of the warning.
  - Have you ever wished these warnings would just go away?

Closing

- "That is all we have time for. Thank you for your participation."

A.4 Figures

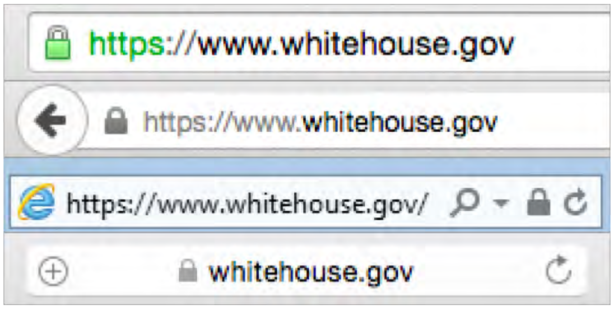
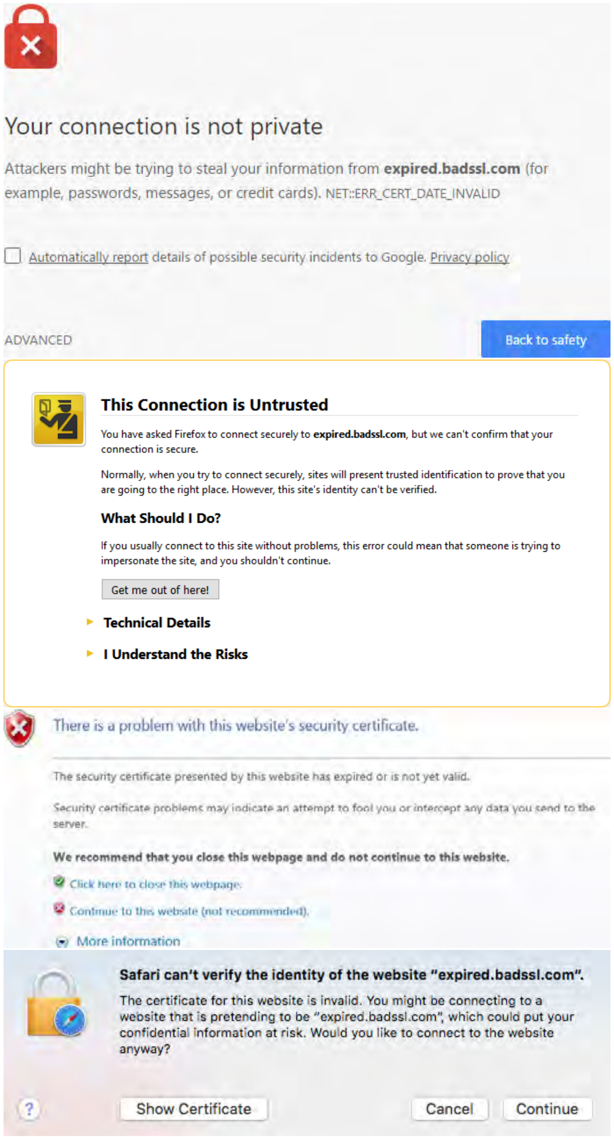

https://www.whitehouse.gov
https://www.whitehouse.gov
https://www.whitehouse.gov/
whitehouse.gov

Figure 7: Example of lock icon from Chrome, Firefox, Internet Explorer, and Safari that were shown to participants.



Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_DATE_INVALID

☐ Automatically report details of possible security incidents to Google. Privacy policy

ADVANCED

Back to safety

This Connection is Untrusted

You have asked Firefox to connect securely to **expired.badssl.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▸ **Technical Details**

▸ **I Understand the Risks**

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

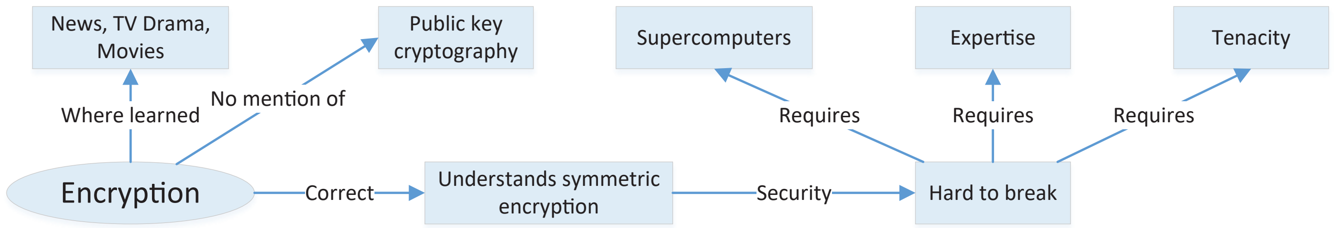
Safari can't verify the identity of the website "expired.badssl.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "expired.badssl.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

? Show Certificate Cancel Continue

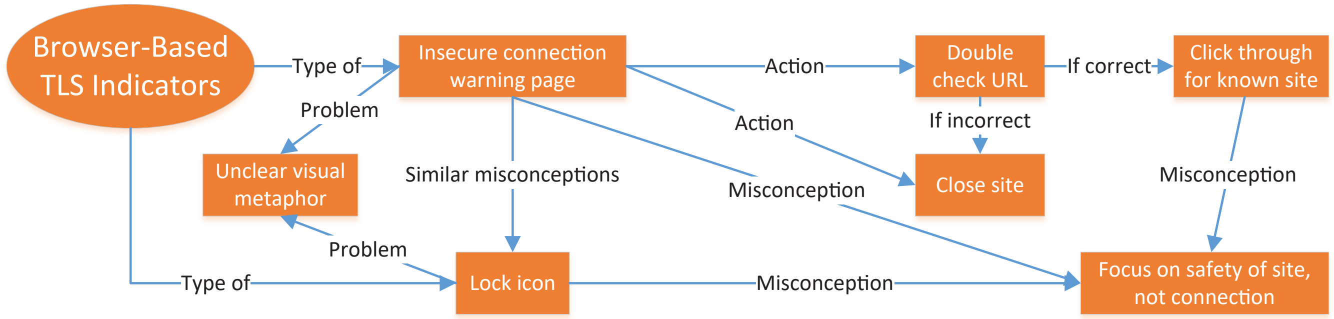
Figure 8: Example of TLS warnings from Chrome, Firefox, Internet Explorer, and Safari that were shown to participants.

B. ADDITIONAL CATEGORY GRAPHS



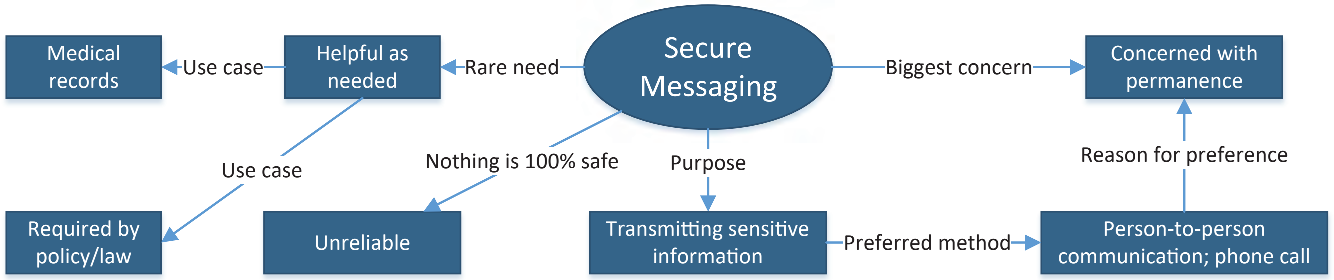
Participants learned about encryption from the news, TV dramas and movies. Most participants had a basic understanding of symmetric encryption, but almost no participants had knowledge of public key cryptography. In line with their belief that nothing is perfectly secure, participants noted that tenacious hackers could break encryption. This view accurately reflects the real world, as hackers consistently break systems that are "protected" by encryption.

Figure 9: Encryption Category Graph



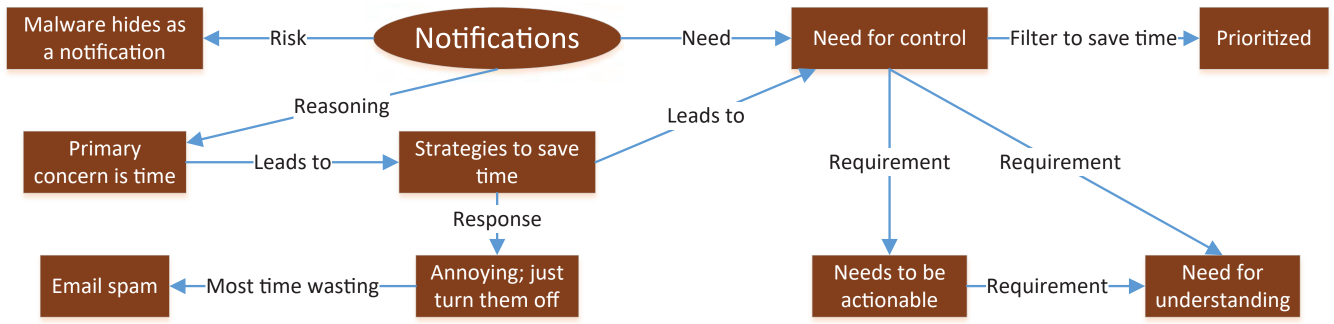
Many participants believed that the TLS lock icon and warning pages were related to site safety, and not the security of the connection. This misconception led them to ignore TLS warnings for well-known sites (e.g., Amazon) that they considered to be safe.

Figure 10: Browser-Based TLS Indicators Category Graph



Participants were interested in the potential of securing their online connections but were unsure whether this is even possible. They noted that the permanence of data from online communication (e.g., email) allows it to be attacked either during transmission or afterward. For this reason, they preferred to transmit information in person or over a phone call, which they viewed as non-permanent.

Figure 11: Secure Messaging Category Graph



Participants were largely apathetic towards notifications and warnings from security software (e.g., anti-virus). If viewed, participants wanted notifications to explain the problem to them, indicate the actions they could take, and explain the impact of those actions.

Figure 12: Notifications Category Graph