Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes

Alain Forget*, Sarah Pearman*, Jeremy Thomas*
Alessandro Acquisti*, Nicolas Christin*, Lorrie Faith Cranor*
Serge Egelman†, Marian Harbach†, Rahul Telang*
*Carnegie Mellon University, †International Computer Science Institute
{aforget, spearman, thomasjm, acquisti, nicolasc, lorrie, rtelang}@cmu.edu
{egelman, mharbach}@icsi.berkeley.edu

ABSTRACT

Computer security problems often occur when there are disconnects between users' understanding of their role in computer security and what is expected of them. To help users make good security decisions more easily, we need insights into the challenges they face in their daily computer usage. We built and deployed the Security Behavior Observatory (SBO) to collect data on user behavior and machine configurations from participants' home computers. Combining SBO data with user interviews, this paper presents a qualitative study comparing users' attitudes, behaviors, and understanding of computer security to the actual states of their computers. Qualitative inductive thematic analysis of the interviews produced "engagement" as the overarching theme, whereby participants with greater engagement in computer security and maintenance did not necessarily have more secure computer states. Thus, user engagement alone may not be predictive of computer security. We identify several other themes that inform future directions for better design and research into security interventions. Our findings emphasize the need for better understanding of how users' computers get infected, so that we can more effectively design user-centered mitigations.

1. INTRODUCTION

Humans are critical to the security of computing systems [8]. Unfortunately, computer security problems frequently arise because of the disconnect between what users do and what is expected of them, sometimes with disastrous consequences. For example, the Conficker botnet was successfully taken down in 2009 and abandoned by its operators. Yet, six years later we can still find evidence of over one million infected machines that are attempting to re-infect other vulnerable machines [2]. This may be due to users not following elementary security precautions, such as ignoring warnings or using out-of-date software.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

Some suggest that greater computer security can be achieved with greater user involvement [1, 4, 5]. To help users make better security decisions, we need to identify specific insecure behaviors and understand how often and why users behave insecurely. Unfortunately, we still lack a holistic understanding of how users process and address security threats. Past work [7, 12, 15, 19] has explored how users model computer security threats and use them to make decisions. While informative, this work has largely relied on surveys or lab studies rather than users' actual computing behaviors or focused on narrow behaviors and scenarios rather than comprehensively capturing end-users' *in situ* usage. We know of no work that longitudinally examines user behavior and directly maps users' decisions and self-reported understandings to the observed security states of their machines.

As part of an ambitious research project attempting to answer these questions, we developed the Security Behavior Observatory (SBO) [14], which is a panel of participants consenting to our monitoring of their general computing behaviors, with an eye toward understanding what constitutes insecure behavior. Technically, the SBO consists of a set of "sensors" monitoring various aspects of participants' computers to provide a comprehensive overview of user activity that regularly reports (encrypted) measurements to our secure server. Our monitoring provides us with the opportunity to characterize *which* user actions led to insecure computing states. We can also directly interact with our participants to solicit insights into their behaviors that may have led to their machines' states.

We present an initial study conducted with the SBO. After observing 73 users over the course of 9 months, we conducted interviews with 15 users whose computers were in a variety of security states to better understand users' attitudes and motivations toward computer security and to understand why their computers were in a state of (in)security. Qualitative inductive thematic analysis of the interviews produced "engagement" as the overarching theme.

We found that some *engaged* users actively maintain their computers' security, while other *disengaged* users prefer to ignore or delegate security tasks. Surprisingly, we found that engaged users' computers were not necessarily more secure than those of disengaged users. Thus, for user engagement with computer security to be effective, it has to be done correctly. Otherwise, it may be better that users not even try, lest they inadvertently subvert their machines' security.

Due to the SBO population at the time, our 15 interviewees had a median age of 63 and were mostly female. This gave us a unique opportunity to examine an often understudied population. Future work will test the extent to which the theme of engagement is applicable across demographics.

Our study's primary insight is that user engagement alone may not be predictive of computer security, which challenges past assumptions [1, 4, 5]. We also found that misunderstanding computer security leads users to adopt ineffective (though perhaps rational [18]) security postures. This *in situ* finding validates similar observations that have been made previously in other security contexts [7, 18]. Finally, we also found that disengaged and engaged users seem to have distinct sets of behaviors, needs, and problems. As such, our findings suggest that both types of users may not find the same type of computer security interventions effective (i.e., one size may not fit all).

2. RELATED WORK

While the SBO is distinct in its breadth and longevity, our study's qualitative approach is similar to past work [35, 37, 38]. Our findings both confirm and build upon results from many past publications regarding users' difficulties in understanding computer security, observing their challenges, and applying software updates to eliminate vulnerabilities.

Problematic understanding of security. Wash [37] conducted interviews to investigate how people conceptualize home computer security threats. The "folk" models Wash identifies do not match actual threats, which may explain why users inadvertently put themselves at risk when ignoring or misunderstanding expert advice. Wash recommended that security advice include recommendations of appropriate actions as well as explanations of why the actions are effective. Howe et al.'s [19] literature review highlighted that users get advice from relatives, friends, or co-workers much more frequently than from experts. Ion et al. [20] found that non-experts' security advice is less likely to overlap with that of experts. Dourish et al.'s [10] interviews found that users frequently delegate security to others (e.g., friends or family) who are perceived as more knowledgeable.

Observing end users' security challenges. Multiple surveys [4, 5, 26] show that home users have difficulty securing their computers, either because of lack of knowledge or ignoring (or misunderstanding) security advice. Furnell et al.'s [15] survey respondents had difficulty understanding the security feature interfaces of various Microsoft software, despite their respondents having above average technical expertise. This parallels our observation that users more engaged with their computers' security (and perhaps more knowledgeable) may still have poor security outcomes.

A few user studies have focused on specific aspects of personal computing behavior "in the wild." Christin et al. [7] found a large number of people were willing to download, execute, and give administrative access to untrusted software, since they felt protected by their antivirus software. We also observed an over-reliance on security software and lack of attention to other advisable security practices.

Perhaps most closely related to our work is Lalonde Lévesque et al.'s [22] 50-subject, 4-month study focusing on the effectiveness of antivirus software. Participants were given an instrumented Windows 7 laptop with antivirus software. Every month, researchers collected data from the machines and met with participants to complete a survey about their computer usage. The authors found that participants with greater computer expertise were *more* at risk of being exposed to threats than less knowledgeable users, which resonates with our findings about the disconnect between user engagement in computer security and observed security issues. The SBO differs from this study in that we are observing user behavior across a broader spectrum of security- and privacy-related issues over a longer period of time.

To our knowledge, the only existing work on older users and computer security examined their knowledge of Internet hazards [16]. They found that older, particularly female, participants had less knowledge of security hazards. This motivates our work to better understand the challenges faced by the understudied population of older (female) computer users, who may be particularly vulnerable to security risks.

Trouble with updates. Timely installation of software updates and use of security software are generally considered by experts to be essential security practices. Non-experts are often aware that using security software is advisable, but are less likely to perceive updates as important for security [20].

Wash et al. [38] surveyed 37 users about their understandings of Windows updates, comparing those self-reports to participants' Windows update logs. The majority of their participants were unaware of their update settings or of when updates were being installed, and the states of their machines often did not reflect the users' intentions, for better or worse. In 12 cases, users' machines were actually *more* secure than intended, in part because some users had intended to turn off automatic updates but had not done so successfully. Other users successfully turned off automatic updates due to the inconvenience of automatic reboots, causing them to install updates less promptly. Wash et al. focused solely on update logs at the time of the interview, whereas we collected data over a longer period and cover a broader range of computer security attitudes, behaviors, and outcomes.

Comprehension is not the only updating barrier. Vaniea et al. [35] found non-experts often fail to install updates due to prior bad experiences, such as unexpected user interface changes, uncertainty about their value, and confusion about why updates to seemingly-functioning programs are needed. Fagan et al. [13] report on negative emotional responses to update messages, including annoyance and confusion.

Wash et al.'s study [38] indicates that automatic operating system updates (such as those now required by default in Windows 10) do increase the security of machines in many cases. However, they and others [6, 11, 29, 36] also highlight problems that prevent automatic and opaque update systems from being panaceas, including possible negative effects on users' understanding, trust, convenience, and/or control. Some users may object to and override such systems, preferring manual updates. Tian et al. [33] present survey results indicating that Android smartphone users preferred manual app updates for reasons including desiring control, wanting to know more about updates before installing them, preferring to apply updates only to certain apps, and wishing to work around system performance limitations (e.g., primary tasks being slowed by updates in the background).

3. SECURITY BEHAVIOR OBSERVATORY

Time- and scope-focused lab and online computer security studies have yielded valuable insights over the past 20 years. However, such experiments often do not reflect users' actual behavior in their natural environments [31], while large-scale field studies can capture users' security and privacy behaviors and challenges with greater ecological validity. This is the objective of our IRB-approved Security Behavior Observatory (SBO) [14], which longitudinally monitors user and computer behavior *in situ*. We can also interview participants to better understand their computer security attitudes and behaviors, to compare with the security state of their machines over time.

Participant recruitment. We recruit SBO participants from a university service that telephones individuals to notify them about ongoing experiments in Pittsburgh, Pennsylvania. Potential participants are contacted to complete a brief pre-enrollment survey to ensure they are over 18 and own a Windows Vista, 7, 8, or 10 personal computer. A member of our research team then calls participants to walk them through the following tasks while they are in front of their computers:

1. Read and complete a consent form, which clearly informs participants that the researchers may collect data on all activity on their computer, except personal file contents, e-mails sent or received, contents of documents on Google Docs, and bank card numbers.
2. Provide the names and e-mail addresses of others users of the computer to be instrumented, so we may obtain their consent.
3. Download and install the SBO data collection software.
4. Complete an initial demographics questionnaire.

Once all the computers' users have consented and we begin receiving data, we send participants a $30 Amazon.com gift card. Participants are then paid $10 per month their computers continue transmitting data to our server. Data transmission occurs in the background, requiring no user action. We encourage and promptly respond to questions about the study via phone or e-mail. We assert that maintaining the confidentiality of their data is our primary concern. Participants may withdraw from the SBO at any time. If we unexpectedly stop receiving data from a machine, we contact the participant to attempt to resolve the issue.

SBO data is complemented by optional questionnaires and interviews that elicit participants' perspectives on issues, events, and behaviors we observe throughout the study, for which participants receive additional compensation.

Data collection architecture. The SBO relies on a client-server architecture with several client-side sensors collecting different types of data from participants' machines [14]. Examples of collected data include processes, installed software, web browsing behavior, network packet headers, wireless network connections, Windows event logs, Windows registry data, and Windows update data. The SBO data collection architecture is implemented with multiple technologies: Java, C#, C++, Javascript, SQL, Python, PHP, WiX, and command-line batch scripts.

The SBO architecture provides security and confidentiality of participants' data as follows. All communication between users' machines and our collection server is authenticated and encrypted using unique client-server key pairs. The server only accepts connections from authenticated machines on one specific port. Finally, the data collection server is not used for analysis. Instead, a data analysis server retrieves participants' data from the collection server for long-term storage. The data analysis server is only accessible from within our institution's network. All data analysis must be performed on the server. No collected data is authorized for transfer from the data analysis server.

4. METHODOLOGY

To explore the challenges users face in protecting themselves from and addressing security problems, we conducted semi-structured interviews with a subset of SBO participants in which we asked about security-related beliefs, practices, understandings, and challenges. We chose interviews because they provide more detailed information than other methodologies (e.g., surveys). We also examined the SBO data collected from interviewees' machines to compare users' understandings of their machines' states to reality. This qualitative analysis leverages the SBO's unique nature to acquire insights that are not normally available in interview studies.

We have been enrolling SBO participants since November 2014. As of March 2016, we had collected data from 131 participant machines. As the SBO is a long-term endeavor, participants are continuously recruited and may leave any time, so the amount of data collected from each participant varies. For this paper, we analyzed data from the 73 participant computers that had sent us data for at least 3 months within a 9-month window. We sent interview invitations to 28 active participants whose machines had been regularly sending us data and who had previously responded to our e-mail and phone communications. We interviewed the 15 participants who responded to our invitations.

4.1 Interviews

We conducted 15 pre-scheduled voluntary semi-structured one hour phone interviews. We asked participants about their and others' use of their computers, computer maintenance, precautions taken to reduce computer security risks, and whether they performed a variety of insecure computing behaviors (Appendix A). We used follow-up questions to elicit information about the beliefs that informed users' security-related decisions, as in similar qualitative usable security interview studies [37]. Our questions were phrased to not imply positive or negative behaviors, not be leading, and generally avoid biases [35]. We did not ask interviewees about specific events observed on their computers, since we were concerned about participants' possible difficulty in recalling particular event details. Our questions did not allude to our knowledge of their machines' states through the SBO-collected data, to avoid influencing participants' responses.

The interviewer also established a remote session to the interviewee's computer as a common frame of reference for portions of the interview. Throughout the interview, the interviewer (with the participant's permission) verified whether or not the computer reflected the state reported by the participant. The remote session also allowed the researcher to show participants examples of Internet browser warning

messages to ask participants about their past experiences with such messages (if any), understanding of the source of such messages, and actions taken after seeing such messages. After each interview, we sent the interviewee a $50 Amazon.com gift card and a debriefing e-mail explaining the purpose of our interview and provided information on reputable free security software and tips for avoiding malware.

4.2 Qualitative Coding Methodology

Each interviewee was assigned a pseudonym. Similar to past exploratory qualitative studies in this area [32, 35, 37], we performed an inductive thematic analysis. One researcher first open-coded the transcripts, building a low-level detailed codebook. After identifying main themes, that researcher drafted a higher-level codebook of 25 codes related to a single main emergent theme. That researcher then worked iteratively with a second coder to code the interviews with that high-level codebook. The second coder was instructed to note problems with, unclear distinctions between, or possible missing codes. Both coders initially met after each coded interview to reconcile discrepancies and refine the codebook. After iteratively coding the first 8 interviews in this way, both coders agreed on a final version of the codebook. During this process, the coders agreed to adding three new codes and remove two codes by collapsing them into other existing code categories. Using the final codebook of 27 codes (Table 4 in Appendix C), both coders coded the remaining 7 transcripts independently and then met to resolve any remaining discrepancies in their codes.

Cohen's kappa, a measure of inter-coder agreement over categorical items, was calculated to be 0.64, which is considered "substantial" agreement [23]. The coders reached consensus on all codes. The reconciled codes were used for all analyses.

4.3 Examination of SBO Data

In addition to interviews, we also inspected the SBO data collected from interviewees' machines to compare participants' understanding of their computers' states (from the interviews) to the actual states of their machines. We investigated configurations and behaviors parallel to the types of interview questions asked, including:

1. Presence or absence of security software[1]
2. Presence or absence of outdated vulnerable software, particularly Adobe Flash Player and Adobe Reader
3. Presence of known malicious software or other software displaying suspicious behaviors
4. Windows update settings
5. Regularity and promptness of installation of Windows updates

Installed Software All software-related data was regularly collected from participants' machines' Windows registry, including the software name, publisher, version, and date of installation. To determine if historically-vulnerable software (e.g., Adobe Flash Player, Adobe Reader)[2] was outdated, we manually collected update and version release data from the software publishers' official websites. To determine if any of the installed software was malicious or suspicious, we manually researched the online reputation of each of around 2,900 distinct software packages found on clients' machines. In doing so, we found that the website `ShouldIRemoveIt.com` was an excellent resource for this software categorization task, since it provides scan results from multiple security software suites, as well as information about the software's known behaviors, purpose, publisher, and more. Thus, we categorized any software as *malicious* if `ShouldIRemoveIt.com` reported, "multiple virus scanners have detected possible malware." We otherwise categorized software as *suspicious* if our online research revealed any of the following:

- The software's primary purpose was to show advertising to the user (via popups, injected advertising, etc.).
- The majority of search results were complaints about the software and requests for assistance in its removal.
- The software's rating on `ShouldIRemoveIt.com` was extremely negative (based on subjective user ratings and their data on how many users remove the software).
- The software was reported as changing settings unbeknownst to the user in undesirable ways (e.g., changing default browsers, homepages, or search engines).
- The software disguised itself, such as using false names in program or plug-in lists.
- The software was known to re-install itself or to be difficult to remove.

We acknowledge that our identification of malware and suspicious software is limited by including only software listed in the registry. A deeper examination of SBO machines for more insidious and covert malware is left to future work.

Windows Updates We examined the SBO computers' operating system updating behavior in two ways. First, we determined whether Windows settings were set to automatically install updates. Second, we examined the download and installation timestamps for Windows updates and noted cases where SBO computers failed to install security updates for long periods of time or installed updates sporadically despite the computer being in regular use.

4.4 Demographics

Table 1 lists the self-reported demographics of each of the 15 interviewees. Our interviewees were a median age of 63 (SD=11), 73.3% female, and earned a median household annual income of $50,000 (SD=$83,333). This group of mostly older women provided a unique perspective of an understudied population (who may be at particular risk against security threats [16]), versus the typical demographics of other studies in our field of young and/or technically-savvy users (often university students).

All users reported performing sensitive tasks on their computers. All but one interviewee, Monica, explicitly reported performing financial tasks (e.g., online banking, e-commerce). However, Monica reported performing other sensitive activities, such as searching for medical information online. Table 3 in Appendix B summarizes interviewees' reported computer usage. This self-reported data establishes how participants *perceive* themselves using the computer.

[1] Security software is strongly recommended [34, 37].

[2] While Java could also be considered historically-vulnerable software, we excluded it since our data collection software (which is partially-written in Java) automatically updates Java upon installation on participants' machines out of necessity. Thus, Java being up-to-date is not necessarily indicative of user behavior in this case.

Pseudonym	Age	Sex	Occupation	Annual income
Agnes	63	F	Travel	$50K-$75K
Betty	68	F	Homemaker	$200K-$500K
Carl	55	M	Tradesman	$25K-$50K
Denise	50	F	Psych. Tech.	$50K-$75K
Ed	66	M	Retired	$25K-$50K
Fiona	46	F	Education	$75K-$100K
Gina	80	F	Retired	$75K-$100K
Hailey	67	F	Retired	$25K-$50K
Ingrid	65	F	Retired	$25K-$50K
John	62	M	Clergy	$100K-$200K
Katrina	72	F	Retired	$25K-$50K
Laina	45	F	Admin.	$25K-$50K
Monica	42	F	Medical	$25K-$50K
Nancy	61	F	Medical	$50K-$75K
Oscar	70	M	Retired	Declined to respond

Table 1: Self-reported demographics of interviewees.

5. FINDINGS

The primary emergent theme from the interviews was that users had differing degrees of computer security *engagement*: a desire to control and manage their computer's functionality and security.[3] Interviewees' security engagement was distinct from their level of technical expertise. Some users with relatively little technical or security-related knowledge still expressed a desire to actively engage in computer security behaviors, while some relatively technically-knowledgeable users seemed to be largely disengaged. Furthermore, when participants' *perceived* levels of computer expertise were misaligned with their actual levels of expertise, their computers were likely to exhibit poorer security states. We also highlight additional themes expressed by our interviewees, including issues related to name recognition, trust, and legitimacy; update behavior; problematic gaps in users' knowledge; and an over-reliance on security software.

Table 4 in Appendix C lists the high-level codes in the final codebook. Our codes ultimately focused on traits, expressed beliefs, and self-reported decision-making related to user engagement. During the iterative coding process, the two coders grouped the high-level codes in the final codebook into *engaged* and *disengaged* categories. Interviewees were split into *engaged* and *disengaged* categories based on which code group was more common during their interviews. All interviewees clearly belonged in one of the two categories. When relevant, we use qualifiers such as "highly engaged" or "moderately disengaged" to highlight an interviewee's degree of (dis)engagement. Table 2 lists which interviewees were engaged versus disengaged, as well as other findings discussed in Section 5.2.

5.1 Security Engagement

We found that some users reported *disengaged* attitudes and behaviors regarding computer security. These users were likely to respond passively to events on their computers, either by ignoring them entirely or by requesting outside assistance for all but their most habitual tasks. They generally avoided making choices or independently seeking out information about their computers' functionality. They tended to make (often incorrect and dangerous) assumptions about their computers' default states. Their assumption that their computers would "just work" led to dangerous behaviors (e.g., accepting most or all prompts indiscriminately, assuming all security updates installed automatically).

In contrast, other users were relatively *engaged*. They seem to desire control and choice in computer security and maintenance tasks. They independently sought information on which to base their computer- and security-related decisions. However, more engaged users were not necessarily more knowledgeable. Some users who seemed fairly knowledgeable displayed disengaged behaviors, while some engaged users showed severe gaps in expertise.

Disengaged and engaged users alike desired to prevent security and functionality problems, but they differed in how they addressed these problems. Disengaged users did nothing or relied on automated features or outside help, while engaged users sought information and attempted to control both functionality and security.

5.1.1 Disengaged: "I just don't do anything."

Disengaged participants exhibited several similar behaviors and attitudes. Seven interviewees were classified as primarily disengaged: Betty, Fiona, Gina, Hailey, Laina, Nancy, and Katrina. Hailey and Nancy seemed to be especially disengaged, with no segments from their interviews corresponding to the "engaged" code group at all.

Outsourcing maintenance and security tasks. First, many of these users outsourced computer maintenance to a *resident expert*: a person (typically a family member) to whom the user entrusted the responsibility of performing computer security and maintenance tasks. When asked about how her computer was maintained, Hailey said, "It's my daughter who always fixes all my mistakes, I don't know." Hailey indicated that her daughter performs a variety of maintenance tasks for her, including organizing files, deleting unwanted e-mails, and offering remote troubleshooting: "she's installed [a firewall]. And I don't know if there's anything else other than the firewall. She checks it to make sure that I'm not being hacked or something?" However, we did not find any third-party security software running on Hailey's computer during her participation in the SBO.

Unfortunately, in some cases, we found evidence that these resident experts' technical expertise was lacking, which put participants and their computers at risk. Betty's spouse maintains her computer (and its security). Betty and her spouse (who was offering additions to Betty's responses in the background during the phone interview) thought it had security software named "Fix-it," but no such software could be found on the machine during the interview's remote session. According to the SBO data, this machine did have Avanquest's Fix-It Utilities Professional[4] installed at one time, but it does not provide anti-virus protection and was uninstalled months before the interviews.

Several users in this group outsourced computer maintenance to paid services, whether via remote sessions or physically taking their machines to a computer store for either regular maintenance or to fix problems (e.g., too slow, annoying behavior, malfunctioning). Users who outsourced computer maintenance were often oblivious to what types of changes their "resident experts" or paid technicians made.

[3]We define engagement more broadly than some sources in the HCI literature [27]. A more deconstructed analysis of security engagement is left for future work.

[4]`http://www.avanquest.com/USA/software/www.avanquest.com/USA/software/fix-it-utilities15-professional-501513`

For example, when asked questions about how she maintained her computer, Katrina simply replied, "I'm not sure what that is, unless you're talking about [paid technicians] taking over my computer [with a remote session]."

When asked similar questions, Hailey said, "all [the technician] does is take over the computer like you do [with a remote session]."

Passive responses to problems. Left alone to use and manage their computers, disengaged users were more likely to avoid taking action than to try to investigate or resolve problems independently. Betty, Gina, and Hailey tended to avoid unfamiliar tasks and those that their resident experts or paid services had advised against, such as installing software.

In the case of problems or warnings, disengaged users stated that they would often cease their tasks entirely. When asked what she would do if she saw a web browser warning, Betty replied, "I should not click on it; I just don't do anything."

Some disengaged participants indicated that they would also contact their resident experts without attempting to independently resolve problems. When asked about her response to browser warnings, Hailey said, "I'd call my daughter... I'd close Google Chrome, I'd just close the computer."

When asked a question about her response to scareware-style pop-up messages, Laina indicated her response would be, "call my dad, tell him what I saw, and then he would tell me what to do," rather than independently performing any action, such as closing the web browser or navigating away from the web page.

Lack of technical awareness and interest. In some cases, disengaged users' awareness of their own knowledge limitations seemed to protect them from exploratory but risky behaviors. They reported a reluctance to download or install new software, visit unknown websites, or change default settings that may put their machines at risk. When asked about whether Hailey had ever disabled her anti-virus or firewall, she replied, "I would not know how to do that."

Some disengaged users also reported that they found computer maintenance unenjoyable. For example, Gina recalled when Binkiland adware needed to be removed, and stated, "[My husband] enjoys that garbage. I don't... My husband and the folks at McAfee sort of sorted through that."

It is important to note that disengaged users did not necessarily lack *motivation* to keep their computers secure. All of our users reported performing sensitive tasks (Section 4.4) and disengaged users reported being affected by and concerned about computer security problems. For example, Laina was a highly disengaged user, but ransomware seizing her personal files was catastrophic for her work-related tasks. While she desired to avoid such an outcome in the future, she still did not express any desire for additional personal control over her computer's security and instead continued to outsource all maintenance to a family member. This illustrates that users could be highly motivated to keep their computers secure while still having little interest in performing such management themselves.

5.1.2 Engaged: "I'm trying to be self-taught"

Eight interviewees (Agnes, Carl, Denise, Ed, Ingrid, John, Monica, and Oscar) seemed to be more engaged. These users were more wary of specific security risks and more likely to respond proactively to problems indicative of potential security breaches. Engaged users desired more granular control of their computers, displayed more complex approaches to maintaining the security and functionality of their computers, and exhibited more tendencies to troubleshoot problems and research topics independently.

However, these more engaged users did not seem to be substantially more knowledgeable or to make better decisions in all cases. In fact, their engagement sometimes caused them to make risky decisions in situations where the less-engaged groups might have been protected by inaction. For example, Agnes reported that she uninstalled her Norton security software about a year before the interview because she did not feel it was necessary, and she had not installed any other security software since. SBO data showed Norton was still present on Agnes's computer, but was not running. We suspect she simply chose not to renew a subscription without actually removing the software.

Proactive maintenance and responses to problems. Proactive maintenance to prevent problems and active responses to perceived problems were both hallmarks of engaged users. We specifically asked all interviewees whether they performed any regular maintenance tasks, and while disengaged users generally only performed maintenance in reaction to a problem that halted other tasks, engaged users sometimes had specific routines that they reported performing regularly to maintain their computers.

The routines described by engaged users seemed to reflect their intentions to proactively maintain their computers. However, some aspects of engaged users' routines indicated incomplete understandings of the computer's functionality. For example, every time Denise logs into her Windows machine, which she reportedly uses for approximately three hours every day, she will "perform virus checks" and "clean the internet files." Both of these are probably good habits, but she also mentioned that she defragments her hard drive with the same frequency, which is likely unnecessary and possibly even detrimental to the drive's functionality.

Engaged users also reported more active responses to past scenarios such as scareware messages or when asked what they would do in response to browser warnings (examples of which were displayed to users by the interviewer via remote session). Rather than "just doing nothing," engaged users often offered examples of ways in which they sought the source of the problem and/or tried to prevent it from recurring. However, being engaged did not imply that participants had an accurate technical understanding of the problem or how to resolve it. For example, Denise's default response to perceived security threats while browsing was to try deleting her browser history and cache because she believed that would keep malicious sites or pop-ups from "popping up again."

A common (and possibly somewhat more effective) default response to any perceived threat or problem was to "run a security scan" manually with whatever security software was present on the machine. However, this behavior was also taken too far as a default response in some cases. For

example, Oscar described having network connectivity problems (which, given his description, we believed were likely to be hardware or ISP problems), to which he reportedly conducted "a thorough manual scan." Two other users had also installed multiple conflicting security applications during past attempts to troubleshoot problems, likely making any existing performance problems worse and possibly hindering the programs' effectiveness as they compete with each other for access to the client machine's resources.

Information-seeking behaviors. Engaged users also tended to mention seeking out and reading product reviews and other kinds of publicly-available information about software and operating systems. In Oscar's words, "I'm trying to be self-taught." They seemed motivated to proactively seek information for a variety of reasons, including a desire for granular control, to preemptively avoid potentially problematic software, or simple curiosity. When making computer-related decisions (e.g., choosing software to purchase, whether to upgrade to Windows 10), engaged users commonly stated, "I Google it," and regularly read reviews from `CNET.com` or similar sources. The SBO data confirmed that at least four engaged participants (Carl, Denise, Ed, and Monica) and one less-engaged participant (Fiona) had searched online for information about their computers and their performance.

The tendency to perform independent research resulted in largely positive outcomes for engaged users. For example, it seemed to help users choose reputable software to install. Ed described how he chose Kaspersky as his security suite: "I checked out reviews, I read articles and PC magazines and CNET-type reviews to get an idea of what was the best security suite for the money, what offered the best protection for the lowest cost. What was the most reliable, what had the best customer service, things of that nature. And that's how I decided to go with the Kaspersky Security Suite." Carl also mentioned various kinds of research that he might perform to find information about software, including reading Internet forums.

In some cases, these investigations may have had negative impacts on users' attitudes and behaviors towards legitimate security products or upgrades. For example, Agnes said she avoids updates with negative reviews: "you'll hear people say 'don't install version 8.1.2 because... my computer slowed down immensely or my printer isn't functioning right,' so I usually [read reviews] before I install it." When participants discussed research performed before installing updates, they mentioned factors such as compatibility and performance, but not security.

Aware of and involved in updates. Engaged users were more actively involved with the update process overall, for better or worse. In some cases, this had positive effects: some engaged users mentioned actively and habitually checking for updates. On the other hand, some engaged users were more likely to "pick and choose" updates in strategic ways, and their strategies for doing so did not always seem to be well-informed. Many engaged users were at least aware that updates could be helpful in resolving problems with software in general, but not all were fully aware of the security purposes of some updates.

Unlike disengaged users, engaged users sometimes searched for updates without being prompted by their software. Some reported doing so as part of habitual, proactive maintenance. Monica, for example, said that she normally spent about half an hour performing a list of habitual maintenance tasks each time she logged onto the computer to "run my internet security, [do] my updates." Monica reported using the computer for five to six hours per day, three to four days per week.

Some would also look for updates manually to troubleshoot problems with specific programs. For example, Oscar described a situation in which a piece of software was not functioning as desired, and part of his response was to "check just to make sure that they didn't sneak a new version in that I didn't know about." Ed also mentioned troubleshooting his Kaspersky security software by searching Kaspersky's site and finding a download that resolved a conflict between Kaspersky and Windows 10.

However, engaged users' more active relationships with updates also resulted in sometimes explicitly choosing to avoid operating system and software updates that may fix critical security vulnerabilities. The reasons users cited for this behavior included prior negative experiences with updates or aversion to feature changes, confirming findings of past studies [33, 35, 36, 38].

Ed said that his behavior differs depending on whether the update seems to be critical or optional: "Sometimes I'll have something that, I don't know if they call it critical or what, and then there's recommended...or maybe it'll say 'recommended,' and it'll say 'in addition to,' and sometimes I'll ignore those, where it's an option of yes or no."

John said that he "has the update button set to contact me to let me know. I'm real careful about updating," citing past negative experiences with updates. This matched SBO data from his machine: Windows was set to notify him before downloading updates and multiple important updates had not been installed throughout his participation. John also noted, "What I tend to do is read the descriptions of the updates and pick and choose what seems to me to be of value." This is a distinct contrast from disengaged users' tendencies towards blanket approaches to updates and prompts: disengaged users tend to either ignore or avoid updates entirely or to accept prompts rather indiscriminately.

5.2 Computer Security State

We used the information available to us from the SBO data collection software to assess the states of interviewees' machines both in terms of their compliance with some of the most common points of standard end-user security advice (e.g., install updates regularly, run security software) and in terms of the presence or absence of undesirable software. These findings are summarized in Table 2.

5.2.1 Prevention: security software and updates

Three interviewees (Gina, Katrina, and Nancy) had machines that were relatively secure in their configurations, with security software running and updated versions of the vulnerable programs we examined. The remaining interviewees all had evidence of at least one of the following: a lack of third-party security software, outdated versions of vulnerable programs, or problematic Windows update behavior. Betty, Carl, and John possessed the machines with the most problems. Betty's machine lacked security software, was not installing Windows security updates regularly, and

		Security deficiencies						
		No	Updates OS		Out of date		Presence of	
	User	security software	Manually	Irregularly	Reader	Flash	Suspicious	Malicious
Disengaged	Betty	●		●	●		●	●
	Fiona				●			
	Gina						●	●
	Hailey	●				●	●	●
	Katrina						●	●
	Laina				●	●	●	●
	Nancy						●	●
Engaged	Agnes	●				●		
	Carl	●	●			●		
	Denise					●	●	●
	Ed					●	●	
	Ingrid					●	●	●
	John		●	●		●	●	
	Monica					●	●	
	Oscar	●						

Table 2: List of interviewees' machines' security deficiencies. ● denotes interviewee machines with *no security software*, *manual* or *irregular operating system (OS) updates*, *out of date* versions of Adobe *Reader* or *Flash*, or the presence of *suspicious* or *malicious* software.

was running an outdated and vulnerable version of Adobe Reader. Carl and John were not automatically installing Windows updates, which past work has shown can result in users installing updates more slowly and leaving vulnerabilities unpatched longer [38]. Carl was still manually installing operating system updates fairly regularly, but John had failed to install multiple important updates. Carl's machine also had no third-party security software.

In our sample, we observed a variety of combinations of levels of engagement and computer security states. Both engaged and disengaged users had machines that were generally configured according to common security advice such as installing updates and running antivirus software [20, 34].

Conversely, other engaged and disengaged users alike had very poorly-configured machines, including Carl, who was one of the most engaged, and Betty, who was especially disengaged and reliant on a "resident expert."

As one might expect, some disengaged users' computers were less secure. It seemed these users' lack of engagement resulted in a lack of awareness of (and/or interest in) their machine's security state. Betty and Hailey, for example, believed that their resident experts were maintaining security software on their computers, but we found that both of their machines lacked third-party security software and had malicious programs installed.

However, disengagement sometimes led to more secure states. For example, disengaged users seldom changed their Windows update settings from the default automatic installation (typically resulting in security updates being installed as soon as they are available). When asked whether she usually installed Windows updates, Fiona replied, "I don't know if it's a choice. I mean, I could make it a choice, I guess. But it doesn't. It just, automatically, it updates stuff."

On the other hand, since less-engaged users felt ill-equipped to make security decisions when their resident experts were unavailable to assist them, their inaction sometimes put their machines at risk. For example, they seemed less likely to install software updates, including those with security patches. Hailey mentioned several times that she sometimes delayed or refused updates for fear of making a mistake: "Sometimes Java sends me updates, and I don't really know what it is, so I don't download it 'cause I'm always afraid I'm gonna do something wrong." This type of response from disengaged participants also seemed to indicate that they sometimes went too far in taking advice to avoid installing unknown software: they sometimes seemed to conflate this with the installation of updates and as a result might not patch vulnerable software if they did not recognize it. In these cases, their intentions are to avoid security problems, but the effect is exactly the opposite.

Carl and John are examples of different security states between two engaged users. They were the only two interviewees who set their Windows update settings to notify them before installing updates so they could choose which to install. They cited previous bad experiences where updates were perceived to "change things" (undesirably) or "break things" (requiring troubleshooting). Despite their similar attitudes, the resulting states of their computers were quite different. The SBO data showed that Carl installs Windows updates very regularly, but John does not. John's interview responses confirmed that he is averse to updates that do not seem useful to him, even though he also understands that updates to software can sometimes be important for security. While he reported periodically installing software updates, it was unclear if he was aware that Windows operating system updates could also contain security updates.

5.2.2 *Evidence of outcomes: presence of suspicious and malicious software*

Both disengaged and engaged users exhibited good outcomes as measured by the lack of undesirable software found by the SBO's sensors (to the extent that we could detect it). Fiona and Oscar, for example, display very different approaches to security: Fiona is quite disengaged, while Oscar aims to be "self-taught" and is actively involved in configuration and

troubleshooting of his computer. Regardless, both seem to be successful, with no suspicious software detected on their machines.

Denise had relatively negative outcomes in terms of the unwanted software detected on her computer, despite being relatively engaged and having a computer with security software running regularly and software kept up-to-date (other than Flash Player). We detected three malicious and six suspicious programs on Denise's computer. Denise did not report awareness of the unwanted programs detected in the SBO data. However, she did have vague memories of having some sort of "Trojan" or "worm" in the past. She noted, "[her] icons were doing weird things, so I ran Norton," but she did not seem to remember how malicious programs had gotten installed, nor did she remember whether past problems were resolved fully or exactly why she chose particular courses of action, implying a lack of awareness of the actual state of her machine as a contributor to her problems.

Misdirected application of security advice may have also been a factor in Denise's case. When asked about hypothetical or actual past responses to situations such as scareware messages or browser warnings, Denise's preferred default response was to delete her temporary internet files and/or browser history. Denise may have learned that deleting cached files can solve certain kinds of problems or that removing the browser history might be beneficial for privacy, and she seemed believe this same solution might prevent more potential security problems than it actually does. Denise simply seemed to be trying to take any kind of action she could think of to address problems at the time. Accordingly, Denise may have installed undesirable programs like "BrowserSafeguard with RocketTab, Ad-Aware Security Toolbar," "RegCure Pro," and "Hardware Helper" while trying to troubleshoot security or performance problems. Her poor outcomes might have been mitigated if the operating system and software required fewer decisions from the user, or if she had been provided with more comprehensive advice about what actions to take in which situations.

In some cases, less-knowledgeable engaged users were sometimes more likely to take the wrong actions and put themselves at risk of security problems (for example, by picking and choosing types of updates that they deem unnecessary without understanding that those updates might contain security content). In contrast, sometimes the computers of certain disengaged users appeared to be more secure due to their users' inaction and deferral to defaults. Fiona, for example, describes an approach in which she generally clicks update prompts whether or not she fully understands their purpose. She also reports that she simply avoids installing new software altogether because she recognizes that she lacks the knowledge to know "what's safe and what's not safe." These factors may be contributors to the relatively clean state of her machine (mostly up-to-date software other than Adobe Reader and no detectable unwanted software). In this type of scenario, users may be protected by their recognition that the system might be more equipped to make security-related decisions and their reluctance to override system defaults.

On the other hand, sometimes disengaged users had poor outcomes, which frequently seemed to be due to over-reliance on their "resident experts" or professional help. This left disengaged users disempowered to resolve problems or make decisions independently. For example, Betty seemed to think that her husband was maintaining her computer, including keeping security software running, but this was not the case. Betty and her husband chose to seek additional paid assistance to resolve problems related to unwanted software on at least one occasion during the course of the study.

The worst observed outcome was on Laina's computer, which became infected with ransomware. Through an in-depth analysis of her SBO data, we identified this ransomware as "Ransom:Win32/Tescrypt.A," reported by Microsoft.[5] This type of ransomware has been frequently observed throughout 2015 and is most commonly spread through known vulnerabilities in out-of-date versions of Adobe Flash Player, Adobe Reader, and Java. In the few days before the ransomware seized her machine, Laina was both browsing the web and opening e-mail attachments with out-of-date versions of Adobe Flash Player and Adobe Reader. This disastrous outcome occurred in spite of her father, described as an IT expert, maintaining her computer. This illustrates that delegating computer security to a trusted third-party is not without considerable risk, suggesting that effective solutions tailored for disengaged users are essential.

In summary, disengaged users had machines in a variety of security states, since their lack of involvement or action had both positive and negative consequences. More engaged users also had machines in a variety of states, but for different reasons. Highly-engaged users might have been expected to have more secure machines because they were making more proactive efforts to manage their computer security (and were sometimes noticeably more knowledgeable). However, since these users were not experts, their efforts may have backfired at times when they made dangerous choices in configuring their machines. They took more action, but not always the correct action. They sought out and acquired more information, but sometimes that information was flawed or not reputable.

5.2.3 Discussion

A major insight revealed from our findings above is that users' levels of engagement in computer security tasks do ***not*** necessarily imply:

- how knowledgeable they are about correctly securing and maintaining their computers;
- how interested or motivated they are to keep their computers and data secure;
- the importance of the tasks performed on their computers (e.g., all users performed financial tasks, regardless of engagement); or
- how secured and/or compromised their computers will be.

One possible explanation for our observations here is that the state of a machine, both its configuration and theoretical risk and its actual health, is likely determined in some part by a *combination* of a user's level of technical expertise, her own ability to evaluate her expertise, and her subsequent engagement. On the one hand, we have noted users

[5] `http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Ransom:Win32/Tescrypt.A`

like Oscar, who demonstrated greater computer expertise and confidence in his technical ability than other interviewees. He was more engaged as a result of feeling that he was sufficiently knowledgeable to find information and make decisions himself. He also had fairly good outcomes: despite choosing not to install security software, the relatively malware-free state of his machine may be evidence that he was making correct security decisions.

There are also users like Fiona, who states that she does not have much technical expertise. She is an archetype of a disengaged user, whereby her approach is largely to "set it and then let it go." She mostly avoids installing software altogether: "I don't get a lot of new software, partly 'cause I don't know that I really need anything, but partly I don't know enough about computers to be a good judge of what's safe and what's not safe so I tend to just kinda shy away from doing much of anything." Since she is running an operating system that automatically updates by default (Windows 10), this approach seems to work well. Besides a lone outdated version of Adobe Reader, her self-assessment of her limited technical ability appears to have led her to a successful and relatively secure course of action.

In contrast, we have both engaged and disengaged users who have have unsuccessful outcomes. For example, John is highly engaged, but may place too much faith in his own ability to micromanage decisions about updates, since he does not install some important security updates. Thus, users at both ends of engagement spectrum can have positive security states and outcomes, if their levels of expertise and awareness of their (lack of) expertise are in alignment. We will suggest possible security solutions that respectively cater to engaged and disengaged users' needs and expectations in Section 6, inspired by some of the additional themes we identified in our data (Section 5.3).

5.3 Other Themes, Codes, and Findings

In addition to the concept of engagement with computer security and its varying relationships with users' computer security states and outcomes, we also identified some other themes below that warrant further mention since they impact users' participation in computer security.

5.3.1 Name recognition, trust, and legitimacy

Multiple participants reported that *legitimacy* was a major factor in their decisions to trust or not trust specific websites, software, or prompts. Participants generally defined legitimacy as a function either of the familiarity of a program or website's name or of subjective visual cues (e.g., the appearance of logos, the grammatical accuracy of a message).

A good example is Hailey, who will download and install updates from sources she recognizes and trusts, "...the Epson, I know that's my printer, so I, um, I download whatever they send me, and HP used to be my printer, but they still have some kind of thing on my computer, so I download that."

However, in some cases, interviewees did not recognize or trust legitimate software or brands, which can lead to poorer computer security. Hailey is again a good example: "Sometimes Java sends me updates, and I don't really know what it is, so I don't download it 'cause I'm always afraid I'm gonna do something wrong." As a result of not updating Java, her computer has unpatched Java vulnerabilities.

Oscar trusts his online news sources to not send him anything malicious, "If I'm on a site, like let's say [main local newspaper] or [another well-known local news source], and they're blocking something, I kinda trust that they wouldn't have something that's super bad." Unfortunately, Oscar seemed unaware that legitimate websites can still be a vector for malicious behavior, such as through malicious ads served by less reputable third parties (unbeknownst to the website owner) [24].

Participants had some difficulty clarifying specifically how they decide whether or not a digital event is from a trustworthy or legitimate source. For example, Agnes suggested she would only click on requests that either are related to her primary tasks or are from sources she recognizes (e.g., Adobe): "I'm just not gonna click on an e-mail and install somethin' that's gonna trash my computer, so I would say it has to be something legitimate. I can't say every time something comes up, 'if you wanna please click here to install,' I do it. It has to be related to what function I'm doing on the computer, and it has to just be legitimate. Usually it's Adobe, Adobe something..."

Similarly, Monica trusts messages that she recognizes from personal experience, and will override her computer's security settings if she feels that the request comes from a trusted source: "It all depends what it is. I've been using Adobe and Java for a long time, so I kinda know what's a good message and what's a bad message, so as long as it's something that's common to me, then I just ignore it, change my firewall settings, and let it run. A lot of times, the way my firewall's set up, it says maybe it didn't recognize the company, [but] I know the company. So I just let it slide through. Now if it was to say something like 'malicious' or 'malware,' I actually don't install it." It remained unclear how Monica would decide what to do if she was presented with conflicting information, whereby the request appeared to be from a legitimate source she trusted, but was flagged as malicious.

In addition to familiar names, users also mentioned relying on subjective cues to determine legitimacy. John, for example, noted that he paid careful attention to logos, "if the colors are right, to see if it's crisp and clear, because a lot of bogus stuff is copied, and every time you copy something you lose some fidelity." Unfortunately, these are typically very superficial cues that malicious sources can fake. Indeed, semantic attacks, such as phishing, rely on spoofing these types of untrustworthy trust indicators. Platforms and web browsers have attempted to combat this by creating trust indicators that cannot be modified by third parties, such as OS-level permission dialogs and web browser SSL indicators. However, previous research has found that many operating system and web security indicators fail because users do not notice them [40], cannot tell the difference between application-controlled content and immutable chrome [21], or view any professionally-designed logo as being trustworthy [25]. Our study is consistent with those findings in that none of our participants mentioned noticing the Windows User Account Control (UAC) prompts,[6] which they would have seen anytime that third-party software requested administrator privileges. Instead, they relied on ineffective cues that could have been spoofed.

[6] `http://windows.microsoft.com/en-us/windows/what-is-user-account-control`

5.3.2 Update behavior

Both *engaged* and *disengaged* interviewees mentioned avoiding and delaying updates. Some *engaged* users also discussed turning off automatic updates and manually picking and choosing updates to install.

These interviews contained a variety of examples that confirmed findings from past work on update behavior. Reasons for not installing updates may include, according to our interviewers' codes as well as previous work:

- Aversion to change (e.g., to UI changes) [35, 36]
- Inconvenience; interruption of tasks [38]
- Belief that that updates are not important, especially for software that is not used regularly [35, 36, 38]
- The "if it ain't broke, don't fix it" mentality [35]
- Past problems with updates (bugs, crashes, etc.) [33]
- Updates and upgrades with negative online reputations (e.g., from consumer reviews and forums) [33]
- Technical issues encountered during installation [36]

Some of our *disengaged* users also reported not installing updates for fear of making mistakes, and some, including Hailey and Laina, also mentioned relying on their resident experts to tell them when updates should be installed.

5.3.3 Problematic knowledge gaps

Basic concepts and terminology. Our interview questions avoided technical language whenever possible, but interviewees seemed unaware of some computing terminology. For example, when asked, "What web browser do you normally use?", three interviewees replied, "What's a web browser?" Furthermore, even those who were able to offer answers to the question sometimes answered by describing the appearance of the program's icon but were unable to give the name of the program.

One participant was also confused by our question regarding frequently-visited websites, asking, "What's a website?" Once offered examples, this participant did report using the Internet and visiting a few websites (e.g., Facebook, e-mail) primarily via AOL Desktop.

Terms such as "USB drive" or "flash drive" were confusing for some users. For example, one user was confused about whether her USB mouse would be considered a USB or flash drive. We advise that security interventions targeting end users be careful not to assume users are aware of what may be considered basic computing terminology.

Browser extensions. We asked participants about each of their installed browser extensions (including plug-ins and add-ons) to learn about users' decisions to install, uninstall, enable, or disable extensions. However, most participants were unaware and seemed unconcerned about their browser extensions. At best, a few users were vaguely aware of extensions' presence or purpose. We suspect this was partly a terminology issue as discussed previously. We also showed the participants their lists of extensions through the remote session, and multiple participants remarked that they did not know how to find such a list in their browser.

All participants had multiple browser extensions installed, but few could offer even vague information regarding experiences with extensions. Katrina installed an extension called Blur without fully understanding what it would do or the risks of providing her passwords to an extension: "[The Blur extension] just says it protects your passwords. It supposedly puts them in some type of an encryption, I think, [but] I didn't really see the value of it. I just kept getting prompts that I didn't want." She couldn't remember how she had gotten the extension, "I think it popped up. I was doing something with passwords. It said 'do you want to encrypt your passwords' or something like that...or maybe my email?" This illustrates that people in real-life situations will install software claiming to improve security (without verifying said claims) from unknown sources or e-mails, which is dangerous behavior that has been observed in previous experiments [7, 9]. We recommend that the capabilities of browser extensions, the risks of installing them, and methods of managing them be more clearly communicated to users.

5.3.4 Over-reliance on security software

When asked if she took any precautions when downloading files, Denise said "Norton checks all that out. It tells me if it's safe." This may have been an incorrect assumption, since we found that her Norton browser extension was disabled, preventing it from scanning downloaded files. She also recalled having a, "worm [or] I think it was a trojan. My icons were doing weird things, so I ran [Norton]." She did not know how her computer contracted the malware. Clearly Norton was insufficient to protect Denise from getting infected in the first place. This illustrates that, while using reputable security software is necessary, it alone is not sufficient. In fact, as Christin et al. previously observed [7], it is possible that the presence (or even the perception) of security software results in the Peltzman effect [28], whereby users engage in even riskier behaviors because they believe they are being protected.

6. DISCUSSION

Although our interviewees did not offer specific recommendations, our observations suggest that users with different degrees of engagement may benefit from distinct types and styles of interventions. Disengaged users, who want to minimize time spent on maintenance and security tasks, probably need concise, precise, simple, and easy-to-perform security instructions, as well as "fire-and-forget," "all-in-one" security solutions that, once applied, will remain effective without any user effort. Such solutions might also be effective for more engaged people, but they may want configurable settings to personally manage their systems and additional information supporting any suggested interventions. Still, engaged users are not computer security experts, so any information provided to them should use language that non-experts can understand, leveraging their existing understanding [3] and empowering them to make informed choices that avert dangerous errors [39].

The application of updates is a prime example of how this can be accomplished with varying degrees of success. Many of our users failed to install security updates for Adobe Reader and Flash Player, which are prone to security vulnerabilities. Modern software that updates automatically by default may overcome these problems in some cases in which users are not equipped to make good updating decisions. However, some of our users set Windows to prompt them before installing updates, because they did not want to risk updates changing how system features work (which

supports prior findings [35, 37]). Thus, we recommend that feature and interface modification updates be completely decoupled from security updates whenever possible. It may also be desirable for most security updates to be installed automatically, but we would not recommend automatic updating as a universal solution: our interviews and past studies [33,38] show that automatic updates can cause significant frustration and true functionality problems for users.

Disengaged interviewees reported that they would stop their primary tasks if their computers warned them of security problems. While doing so may sometimes be a safe course of action, it remains a severe usability problem, and it is not clear what users would do if time-critical tasks were halted while immediate assistance was unavailable. Thus, we recommend security warnings be designed to allow the user's task to proceed in a safe manner, rather than the typical all-or-nothing approach that forces users to proceed with risk, deal with the problem, or abort. Similarly, options presented to users should be framed with disengaged users in mind, offering concise recommendations that are more prominent than less-secure alternatives [12]. For example, when warning the user they may be accessing a dangerous website, secure alternative websites that may satisfy the user's primary goals should be suggested.

Past work [30] has shown that differences in technical training and knowledge may result in women being more at risk for falling for phishing attacks than men. While all four of our male interviewees fell into the engaged group, some women, such as Denise, were also highly engaged. Furthermore, Hailey said that her husband requests her help with the computer. Our sample is too small for us to draw conclusions regarding gender, so further research is warranted.

6.1 Limitations

Our analysis has some limitations. Given our small sample size, a distinction in engagement might not be as clear in a larger sample. However, given the marked distinction between groups within this exploratory study of a relatively small and homogeneous sample, we feel our main findings remain a valuable contribution worth further study.

Studies like ours may suffer from "observation effects," whereby subjects who know they are being observed alter their behavior. However, past work [17, 22] suggests that in-situ data collection does not affect users' natural behavior, and we believe SBO users are unlikely to significantly alter their computer usage since our software runs transparently in the background for months on their computers without affecting daily usage.

Our study is further limited by the fact that, when inviting participants for interviews, we ruled out some participants in the SBO panel who had previously been unresponsive to our communications. This may have biased our sample towards more extroverted participants or those with whom we had previous contact. While future work should attempt to reach out to all people in the target population, most user studies inherently have a similar selection bias whereby the data are collected from people who volunteered to participate.

7. CONCLUSION

In this paper, we explored the relationships between users' attitudes, behaviors, and understandings of computer security (collected from interviews) and the actual configurations and security outcomes observed on their computers (collected via the Security Behavior Observatory). Our interview analysis revealed that users vary in their degree of *engagement* in securing their machines. We then examined the relationship between each participant's level of security engagement and the actual state of their computer's security. Security experts might assume that greater user engagement in computer security would result in more secure machines and vice versa. However, our qualitative findings suggest that the relationship among users' security engagement and their computers' security states may be more complex. Engaged users desire more control and decision-making power, and thus have different needs from disengaged users who prefer delegating decisions to the machine or someone they trust. In addition to engagement, another important factor that may affect computer security is not only the user's own technical expertise, but also their *awareness* of their level of expertise. We found that, when an interviewee's estimation of their computer expertise was misaligned with their actual expertise, their computer's security was likely to suffer.

Our findings suggest a need for a more critical evaluation of the content, presentation, and functionality of security interventions we provide to users. Future research should also examine how to design security interventions tailored to users with differing levels of (perceived versus actual) technical expertise and computer security engagement, since they all have different information needs and expectations from computer security solutions.

This is the first of many studies leveraging the Security Behavior Observatory (SBO). The SBO provides a window into *in situ* computer usage, which can then be augmented with explanatory qualitative data from interviews and surveys. This provides multiple research communities (e.g., HCI, computer security and privacy, behavioral sciences) the opportunity to understand people's personal computing behaviors in the wild. As evidenced by the ransomware incident (Section 5.2.2), the SBO empowers researchers to observe critical events in real-time and reconstruct the sources and sequences of past events that led to incidents. The SBO's longitudinal data collection will provide more such critical insights in the years to come.

8. ACKNOWLEDGEMENTS

This work was partially funded by the NSA Science of Security Lablet at Carnegie Mellon University (contract #H9823014C0140); the National Science Foundation, Grant CNS-1012763 (Nudging Users Towards Privacy); and the Hewlett Foundation, through the Center for Long-Term Cybersecurity (CLTC) at the University of California, Berkeley. We also thank (Daisy) Xi Dai for her assistance with SBO data analysis, and the reviewers for their assistance in improving the paper.

9. REFERENCES

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

[2] H. Asghari, M. Ciere, and M.J.G. van Eeten. Post-mortem of a zombie: Conficker cleanup after six years. In *USENIX Security Symposium*, 2015.

[3] F. Asgharpour, D. Liu, and J. Camp. Mental models of computer security risks. In *Workshop on Usable Security (USEC)*. Springer, 2007.

[4] K. Aytes and T. Connolly. Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing*, 16(3), 2004.

[5] P. Bryant, S. Furnell, and A. Phippen. Improving protection and security awareness amongst home users. In *Advances in Networks, Computing and Communications 4*. University of Plymouth, April 2008.

[6] J. Camp. *Trust, Reputation and Security: Theories and Practice*, chapter Designing for Trust. Springer-Verlang, 2003.

[7] N. Christin, S. Egelman, T. Vidas, and J. Grossklags. It's all about the benjamins: An empirical study on incentivizing users to ignore security advice. In *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2011.

[8] L. Cranor. A framework for reasoning about the human in the loop. In *Usability, Psychology, and Security (UPSEC)*. USENIX, 2008.

[9] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2006.

[10] P. Dourish, R. Grinter, J. D. D. L. Flor, and M. Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 2004.

[11] T. Dumitras, P. Narasimhan, and E. Tilevich. To upgrade or not to upgrade: Impact of online upgrades across multiple administrative domains. In *International Conference on Object Oriented Programming Systems Languages and Applications (OOPSLA)*. ACM, 2010.

[12] S. Egelman, L. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Conference on Human Factors in Computing Systems*. ACM, 2008.

[13] M. Fagan, M. Khan, and R. Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51, 2015.

[14] A. Forget, S. Komanduri, A. Acquisti, N. Christin, L.F. Cranor, and R. Telang. Security Behavior Observatory: Infrastructure for long-term monitoring of client machines. Technical Report CMU-CyLab-14-009, CyLab, Carnegie Mellon University, July 2014.

[15] S. Furnell, A. Jusoh, and D. Katsabas. The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), February 2006.

[16] G. Grimes, M. Hough, E. Mazur, and M. Signorella. Older adults' knowledge of internet hazards. *Educational Gerontology*, (3), 2010.

[17] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2014.

[18] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *New Security Paradigms Workshop (NSPW)*. ACM, 2009.

[19] A. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *Symposium on Security and Privacy*. IEEE, 2012.

[20] I. Ion, R. Reeder, and S. Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2015.

[21] C. Jackson, D. Simon, D. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In *Financial Cryptography and Data Security*. Springer, 2007.

[22] F. Lalonde Lévesque, J. Nsiempba, J. Fernandez, S. Chiasson, and A. Somayaji. A clinical study of risk factors related to malware infections. In *Conference on Computer and Communications Security (CCS)*. ACM, 2013.

[23] J. Landis and G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, 33(1), March 1977.

[24] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang. Knowing your enemy: understanding and detecting malicious web advertising. In *Conference on Computer and Communications Security (CCS)*. ACM, 2012.

[25] T. Moores. Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM*, 48(3), 2005.

[26] National Cyber Security Alliance and Symantec. 2010 NCSA / Norton by Symantec Online Safety Study, October 2010. `http://und.edu/cio/it-security/awareness/_files/docs/2010-ncsa-home-user-study.pdf`.

[27] H. L. O'Brien and E. G. Toms. What is user engagement? a conceptual framework for defining user engagement with technology. *Journal of the American Society for Information Science and Technology*, 59(6), 2008.

[28] S. Peltzman. The effects of automobile safety regulation. *Journal of Political Economy*, (4), August 1975.

[29] E. Rescorla. Security holes...who cares? In *USENIX Security Symposium*, 2003.

[30] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs. Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2010.

[31] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on SSL Warnings. In *Symposium on Usable Privacy and*

Security (SOUPS). ACM, 2011.

[32] E. Stobert and R. Biddle. The password life cycle: user behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2014.

[33] Y. Tian, B. Liu, W. Dai, B. Ur, P. Tague, and L. Cranor. Supporting privacy-conscious app update decisions with user reviews. In *Conference on Computer and Communications Security (CCS) Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 2015.

[34] US-CERT. Security tip (ST15-003): Before you connect a new computer to the internet, 2015. `https://www.us-cert.gov/ncas/tips/ST15-003`.

[35] K. Vaniea, E. Rader, and R. Wash. Betrayed by updates: How negative experiences affect future security. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2014.

[36] K. Vaniea and Y. Rashidi. Tales of software updates: The process of updating software. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2016.

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

[38] R. Wash, E. Rader, K. Vaniea, and M. Rizor. Out of the loop: How automated software updates cause unintended security consequences. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2014.

[39] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX Security Symposium*, 1999.

[40] M. Wu, R. Miller, and S. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2006.

APPENDIX

A. INTERVIEW TOPICS

Although this paper only discusses participant responses that were of most interest, our questions and discussion with interviewees focused on several broad topics related to computer usage, behavior, and security, including:

- Who uses the computer and for what purpose
- Computer accounts and use of authentication
- Software installation and updating practices
- File sharing practices
- Use of security software
- Involvement in previous security incidents
  - Experiences with scareware messages
  - Experiences with browser warnings
  - Experiences with adware or malware
  - Experiences with being "hacked," identity theft, or other compromise of sensitive information
- Web browser usage and use of extensions
- Use of wired and wireless networks

B. SELF-REPORTED COMPUTER USAGE

Self-reported computer usage is presented in Table 3.

Pseudonym	*Communication*	*Education*	*Entertainment*	*Financial*	*Productivity*	*Programming*	*Research*	*Social*
Agnes				✓	✓			
Betty	✓	✓		✓			✓	
Carl	✓		✓	✓	✓		✓	✓
Denise	✓		✓	✓	✓		✓	✓
Ed	✓	✓	✓	✓	✓		✓	✓
Fiona	✓		✓	✓	✓		✓	✓
Gina	✓		✓	✓	✓		✓	✓
Hailey	✓			✓	✓		✓	
Ingrid	✓	✓		✓	✓		✓	✓
John	✓		✓	✓	✓		✓	✓
Katrina	✓		✓	✓	✓			✓
Laina	✓		✓	✓	✓		✓	✓
Monica		✓	✓		✓		✓	✓
Nancy	✓	✓	✓	✓	✓		✓	✓
Oscar	✓			✓	✓		✓	✓

Table 3: Summary of self-reported computer usage (based on initial SBO demographic survey and interview responses) for *communication* (e.g., e-mail, chatting), *education*, *entertainment* (e.g., gaming, watching videos), *financial* (e.g., online banking, e-commerce), *productivity* (e.g., Office-type applications and tasks), *programming* (i.e., building software), *research*, and online *social* networking.

C. CODEBOOK

Table 4 describes our codebook.

Primary	Secondary	Tertiary
Engaged	Active response to problem	-
	Actively seeking updates	-
	Actively selecting updates	-
	Independently installing software	-
	Independently removing software	-
	Learning from experience	-
	Other	-
	Proactive maintenance	-
	Self-education	-
	Takes specific software precautions	-
Neutral	Neutral response to problem	-
	Updates cause problems	-
	Other maintenance	-
Disengaged	Accepts prompts indiscriminately	-
	Avoids updates or installations	Change averse
		Fear of making mistake
		Inconvenient or unimportant
	No maintenance	-
	No specific software precautions	-
	Other	-
	Outsourcing maintenance	Friends or family
		Professional
	Overly reliant on security software	-
	Passive response to problem	-
	Rarely or never installs software	-
	Reactive maintenance	-
	Reliance on outside advice	-

Table 4: Final reconciled high-level codebook (organized by spectrum of engagement).