"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices

Iulia Ion
Google
iuliaion@google.com

Rob Reeder
Google
rreeder@google.com

Sunny Consolvo
Google
sconsolvo@google.com

ABSTRACT

The state of advice given to people today on how to stay safe online has plenty of room for improvement. Too many things are asked of them, which may be unrealistic, time consuming, or not really worth the effort. To improve the security advice, our community must find out what practices people use and what recommendations, if messaged well, are likely to bring the highest benefit while being realistic to ask of people. In this paper, we present the results of a study which aims to identify which practices people do that they consider most important at protecting their security online. We compare self-reported security practices of non-experts to those of security experts (i.e., participants who reported having five or more years of experience working in computer security). We report on the results of two online surveys—one with 231 security experts and one with 294 MTurk participants—on what the practices and attitudes of each group are. Our findings show a discrepancy between the security practices that experts and non-experts report taking. For instance, while experts most frequently report installing software updates, using two-factor authentication and using a password manager to stay safe online, non-experts report using antivirus software, visiting only known websites, and changing passwords frequently.

1. INTRODUCTION

Frightening stories about cybersecurity incidents abound. The theft of millions of credit card numbers from a retail chain [10], a billion passwords from various websites [25], and a large set of nude celebrity photos [24] are just a few examples of stories that have been in the news lately.

In response to such security incidents, thousands of online articles and blog entries advise users what to do to stay safe online. Advice ranges from choosing a strong password [27] and having good security questions [38] to making email addresses unguessable [7] and entirely disabling photo backups in the cloud [27]. Besides such incident-related articles, many service providers, enterprises, and universities offer tips and training on how to stay safe online [2, 3, 17, 35].

If one hour of time from all US users is worth $2.5 billion [19], carefully considering the most worth-while advice to recommend is imperative. Even if users accept some responsibility for protecting their data [23, 43] and want to put in some effort [41], we should be thoughtful about what we ask them to do [20] and only offer advice that is effective and realistic to be followed.

Existing literature on giving good advice suggests that for recipients to follow it, the advice should be (a) useful, comprehensible and relevant, (b) effective at addressing the problem, (c) likely to be accomplished by the recipient, and (d) not possess too many limitations and drawbacks [34]. Therefore, to improve the state of security advice, we must assess which actions are most likely to be effective at protecting users, understand what users are likely and willing to do, and identify the potential challenges or inconveniences caused by following the advice. Furthermore, lessons from health advice in outreach interventions suggest that people will not initiate certain actions if they do not believe them to be effective [53]. Therefore, to learn how to best deliver the advice to users, we must also understand how users perceive its effectiveness and limitations.

In preliminary work, we surveyed security experts to identify what advice they would give non-tech-savvy users. The most frequently given pieces of advice were, in order of frequency: (1) keep systems and software up-to-date, (2) use unique passwords, (3) use strong passwords, (4) use two-factor authentication, (5) use antivirus software, and (6) use a password manager. In this paper, we report on results of a study which tries to identify what security advice users currently follow and how their attitudes and practices differ from those of security experts. To this end, we conducted a survey with 294 participants recruited from Amazon's Mechanical Turk crowdsourcing platform and another with 231 security experts recruited through an online blog. Our results help inform what important security advice users aren't following.

Our results show that expert participants considered keeping the operating system and applications up-to-date, using strong and unique passwords, turning on two-factor authentication, and using a password manager the most important things they do to stay safe online. Non-expert participants, however, considered using antivirus software, using strong passwords, changing passwords frequently, and visiting only trusted websites to be very effective, but admitted to delaying installation of software updates and expressed some lack of trust in password managers. We found that generally experts' security practices matched the advice they would give non-tech-savvy users, with a few exceptions. Experts recommended not clicking on links or opening emails from unknown people, yet they reported to do so at a higher rate than non-experts reported. Other security practices that non-experts considered very important, such as visiting only known websites, were not being followed by experts nor were they considered good security advice by experts.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

Our findings can help inform better security advice that might actually be followed and design campaigns to improve security education. Security practices that experts follow and consider good security advice for non-tech-savvy users, but that non-experts do not yet follow, are good candidates to be recommended to non-tech-savvy users.

2. RELATED WORK

There has been a good deal of past work that investigated specific areas of security-related behavior and others that, like ours, have considered security-related practices and behavior generally.

We cover related work on general security-related attitudes and behavior, and work that focuses specifically on the four primary areas we cover later: updates, antivirus software (and more generally, malware protection), account security, and mindfulness.

2.1 Security-related behavior in general

Some past work has provided study and commentary of user attitudes or behaviors toward security in general. Wash interviewed non-expert users to elicit common mental models about security and showed how these various mental models lead to compliance or non-compliance with various forms of common security advice [52]. Herley has commented at length on the overall state of security advice, arguing that users may often fail to follow it for rational reasons [19], and that there are currently so many security-related demands on users that adding more would be counterproductive [20]. Adams and Sasse [4] were amongst the first to show that users often work around security requirements and some security practices that experts recommend. Similarly, Beautement et al. [6] note that users are often knowledgeable about good security practices and are willing to make some efforts toward complying with them, but that there are limits to how much effort they can or will exert. Howe et al. [21] provide an extensive review of work on home users' security-related behavior.

Some prior work has covered the communications angle of security advice, arguing that perhaps users would be more likely to comply with security advice if it were communicated differently, or at least more effectively. Stewart and Lacey [47] argue for more effective ways to communicate security advice. Camp [9] describes a number of common user mental models about security that might be leveraged to better explain security advice to users. Rader et al. [39] show that stories about others' security-related experiences are a common means by which users learn about security practices, so stories may be a good way to communicate advice to users.

2.2 Security-related behavior in specific areas

In this section, we focus on four top areas of security-related behavior: updates, antivirus software, account security, and mindfulness.

2.2.1 Updates

Vaniea et al. [50] identified some of the reasons users often don't install security updates. They found three main reasons why participants in their study did not install updates: participants found security updates often bundled with other undesirable features, they had difficulty assessing the value of an update, and they were confused about why updates were needed. Vaniea et al.'s work follows on that of Khan et al. [28], who showed that users do not consistently update all their systems and application software in a timely manner.

2.2.2 Antivirus software

Levesque et al. [32] gave instrumented laptops to 50 people to show how user behavior is correlated with malware infections. They note that antivirus effectiveness and vulnerability to malware infections are dependent on user behavior in various respects, from whether users install antivirus software, to how users configure their antivirus software, to what websites they visit. They found that 38% of the participants in their study were exposed to malware that antivirus software cleaned, so they demonstrate that the behavior to install and configure antivirus software can actually make users more secure.

2.2.3 Account security

There has been a great deal of work studying users' selection and use of passwords. Kelley et al. analyzed a set of 12,000 passwords collected from sites with different password strength and composition policies [26]. The authors evaluated the resistence of passwords created under different policies to guessing attacks. Shay et al. evaluated eight password composition policies with the help of 8,143 online participants and a password cracking algorithm. The authors found that longer passwords are more usable than those containing a mix of character classes and, in some cases, more secure as well [44]. Other work has investigated the effect of strength meters on password creation [15, 30, 49].

Hayashi and Hong collected 1,500 password typing events in a diary study with 20 participants. The authors collected data on where participants logged in and how frequently they did so from computers they did not own [18]. Similarly, Inglesant and Sasse had 32 people in 2 organizations, a university and a financial company, keep a diary of their password use. They found that these users were motivated to be secure, but struggled to change passwords, to create new passwords, and to comply with password policies [22]. Florencio and Herley conducted a large scale study in which they monitored participants' password habits through specially designed software running on participants' machines [16]. The authors found that users have a set of passwords which they used on multiple sites. Participants sometimes used trial and error to remember which password goes with which website. Das et al. estimated through a user study and by analyzing hundreds of thousands of leaked passwords from different websites that 43 to 51% of users reuse passwords [12]. Furthermore, users apply a few basic transformations to existing passwords before using them on different sites, which makes it possible for an attacker to guess such transformed passwords.

Chiasson et al. evaluated the usability of two proposed password managers [11]. The authors found that users had incomplete or incorrect mental models of the software. Furthermore, users were not convinced that using a password manager would bring them significant security benefits and were reluctant to give up control over their passwords to a piece of software.

2.2.4 Mindfulness

Actions that we categorize as mindfulness, including practices such as visiting only known websites, checking for HTTPS indicators, and email habits, are typically aimed at guarding against phishing, malware, and man-in-the-middle attacks. A number of past works have covered user behavior related to preventing these attacks.

Early work on phishing awareness and prevention includes Dhamija et al. [13], Wu et al. [54], and Egelman et al. [14]. These works showed that participants had difficulty telling phishing sites from their legitimate counterparts, largely because participants looked at the wrong indicators for legitimacy. At the time, browsers usu-

ally had hard-to-notice indicators of possible phishing attempts, and non-blocking phishing warnings that were easy to miss or ignore. Sheng et al. [45] studied susceptibility to phishing attacks through an online role-playing-scenario study of 1001 participants. They found that participants would click on around half of phishing links presented in the role-playing scenario.

HTTPS indicators range from lock icons in browsers and the URL shown in browser address bars to full-page, blocking interstitial warnings. Early studies of user behavior related to SSL indicators and warnings includes Sunshine et al. [48], Sotirakopoulos et al. [46], and Schechter et al. [42]. These papers presented results from lab user studies that showed some of the faults of early browser warnings. More recently, Akhawe and Felt [5] presented telemetry data from millions of real-world browsers showing that warnings work for many users in many situations, but that large percentages of Firefox and Chrome users still proceed through SSL warnings. Lin et al. [33] studied how highlighting the domain over other URL elements can help some users better identify what websites they visit.

We add to the existing body of knowledge an analysis of user behavior and attitudes accross all of these areas of security advice. We compare experts and non-experts and identify how the security practices of each group differ.

3. METHODOLOGY

We gathered data through two online surveys: one of security experts and one of non-security-expert Internet users. To help develop our expert survey, we started with a set of interviews. We describe these next.

3.1 Expert Interviews (N=40)

To design the surveys, we first conducted in-person semi-structured interviews of 40 security experts at the 2013 BlackHat, DefCon, and USENIX Security conferences. We defined experts as conference attendees who reported having at least 5 years of experience working in or studying computer security. We started every interview with our *top-3-advice question*:

> *What are the top 3 pieces of advice you would give to a non-tech-savvy user to protect their security online?*

We asked follow-up questions to clarify responses. Interviews lasted 8 minutes on average. We transcribed all of the interviews and coded the advice we collected. Interview data informed many of the questions we asked in the surveys, as we note below. In this paper, we report on the data we received from the surveys, but we also include a small number of interesting quotes from the interviews to help ilustrate some points.

3.2 Expert Survey (N=231)

Following our preliminary interviews, we conducted a survey with security experts in February to April 2014. The "expert survey" allowed us to gather data from a larger number of experts than we could through interviews, to gather quantitative data about some of the advice we heard in the interviews, and to inquire about participants' security practices. The survey was written and administered using Google Forms.

3.2.1 Expert Survey Participants

Our expert survey data is based on 231 responses from non-compensated volunteer security experts. As with the interviews, we defined a "security expert" as a survey participant who reported having at least 5 years of experience working in or studying computer security. Participants who did not meet the criteria were eliminated from further analysis.

We recruited participants through a post on the Google Online Security Blog [40] and a request to colleagues to spread a link to the survey via their social media accounts. About 80% of participants were recruited via the blog entry and about 20% via social media (the vast majority of survey responses were received in the days following the blog post, which occurred weeks after the social media effort).

Of the 231 participants who met our expert criteria, 4% were female. Ages ranged from 18 to over 65, with 30% in the 25-34 year-old range, 32% in the 35-44 range, and 18% in the 45-54 range. While 47% of participants were from the United States, others were from 25 countries around the world, including Australia, Germany, India, Israel, Japan, South Africa, and the UK. Participants held a vast range of job titles within computer security including CEO, Chief Information Security Officer (CISO), consultant, grad student, IT specialist, network administrator, security researcher, software engineer, and whitehat hacker. 73% of the sample held a Bachelor's degree or higher. In a check-all-that-apply question, 69% reported working in industry, 15% in academia, 13% in self-employment, 11% in government, and 7% in corporate research labs.

3.2.2 Expert Survey Content

The expert survey asked the same open-ended top-3-advice question with which we started the earlier interviews, then asked another open-ended question about what they actually did, the *things-you-do question*:

> *What are the 3 most important things you do to protect your security online?*

It went on to ask 34 fixed-response questions, 1 branching question, 4 quality-assurance questions, and 8 demographic questions. The 34 fixed-response questions were developed using advice from the interviews and were divided into two sections. The first section asked 14 questions about whether participants followed a set of 14 pieces of advice commonly mentioned in the interviews. An example question in this set was: *Do you use two-factor authentication (e.g., 2-step verification) for at least one of your online accounts?*

The second section asked experts to rate the "goodness" of 20 pieces of advice we heard frequently in the interviews (e.g., *Use two-factor authentication for online accounts*). In rating goodness, experts were asked to consider both how effective the advice was at keeping the user secure and how realistic it was that users could follow it.

The branching question asked whether the participant owned a personal computer and gated 2 of the 14 behavioral questions; in results, when we report a number of expert participants under 231, it's because some answered "No" to the branching question, so they did not encounter these 2 behavioral questions.

Quality-assurance questions had an answer we considered obviously correct, and we eliminated participants who answered more than one incorrectly from further analysis. An example is: *Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response.* (We allowed one incorrect response because all participants offering only one incorrect response to a quality-assurance question provided otherwise thoughtful answers to open-ended questions. We piloted the survey with security experts from our organization.

3.2.3 Limitations

Our recruiting methods may have produced a sample with some bias relative to the overall population of security experts, but our

sample was large and diverse, so it likely represents a substantial portion of the security expert community. Since most participants came from the Google blog, some readers of the blog may be favorably predisposed toward Google and its products.

3.3 Non-expert Survey (N=294)

To get the non-security-expert perspective on security behaviors, we conducted another survey with non-experts whom we recruited via Amazon Mechanical Turk (MTurk). Like the expert survey, the non-expert survey was written and administered using Google Forms. The "non-expert survey content" was nearly identical to the expert survey content, with a few exceptions noted below.

3.3.1 Non-expert Survey Participants

Non-expert survey participants responded to our task description on MTurk, calling for participation in a Google study about Internet use. Participants were compensated $1 each for completing the survey. We required that MTurk participants be located in the United States, have a task approval rate of 95% or better, and have completed at least 500 tasks.

According to responses to demographic questions in our survey, our non-expert sample was 40% female. Ages ranged from 18 to over 65, with 50% of the sample in the 25-34 age range, and 19% each in the 18-24 and 35-44 age ranges. Participants held a wide range of occupations including artist, cashier, farmer, homemaker, sales, and youth advisor. Educational range was wide, with 47% of participants holding a Bachelor's degree or higher.

3.3.2 Non-expert Survey Content

The non-expert survey started by asking the things-you-do question. The non-expert survey also asked 54 fixed-response questions, the same branching and quality-assurance questions from the expert survey, and 5 demographic questions. We piloted the survey with 20 participants (whose data is excluded from our analysis) from Mechanical Turk.

To assess if poor advice adoption among non-experts stems from a lack of understanding of the security benefits that the advice brings or from other factors altogether, we asked non-experts questions on the perceived effectiveness of different pieces of advice and their likelihood to follow the advice.

We eliminated 6 non-expert participants who answered one quality-assurance question incorrectly from further analysis.

3.3.3 Mechanical Turk as a Recruiting Platform

Our non-expert survey used MTurk, which is sometimes called into question as a recruiting platform for studies. Concerns include whether demographics of its participants are biased relative to the Internet-using population at large, and whether remote participants will provide quality data. MTurk has already been used in prior usable security research including [15, 43], and in other usability work has been found to yield quality results and populations more diverse than typical university samples [8, 29, 37]. Although MTurk is becoming a generally accepted platform for recruiting user study participants, we included quality-assurance questions to filter out any MTurk participants who may be have been answering all required questions as quickly as possible and providing junk data in the process. Only 6 participants were filtered out for providing incorrect quality-control responses.

3.4 Coding open-ended responses

Two raters coded the open-ended responses. The raters read the responses and consulted to develop a codebook of distinct pieces of advice, then assigned codes to each open-ended response to the things-you-do question. The raters achieved a Cohen's κ, a measure of inter-rater reliability, of 0.77—a value generally considered substantial agreement [31, 51].

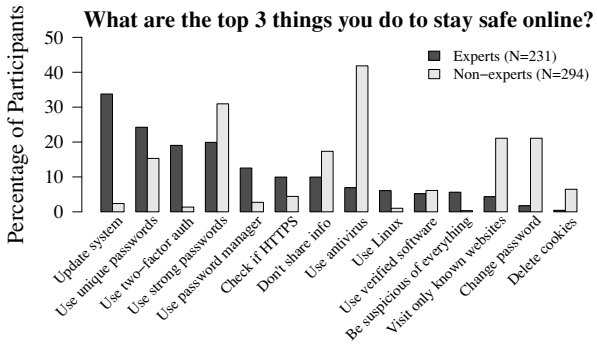

Figure 1: Security measures mentioned by at least 5% of each group. While most experts said they keep their system updated and use two-factor authentication to stay safe online, non-experts emphasized using antivirus software and using strong passwords.

4. RESULTS

Figure 1 shows all security measures that were mentioned by at least 5% of experts or by 5% of non-experts in response to the open-ended things-you-do question. The most common things-you-do responses from each group varied, with only one practice, using strong passwords, in common within each group's top 5 responses. While most experts said they install software updates (35%), use unique passwords (25%), use two-factor authentication (20%), use strong passwords (19%), and use a password manager (12%), non-experts mentioned using antivirus software (42%), using strong passwords (31%), changing passwords frequently (21%), visiting only known websites (21%), and not sharing personal information (17%).

Note that we've chosen to visualize and discuss only security measures mentioned by at least 5% of experts or non-experts as a matter of convenience for presenting our results and due to space constraints; in fact, we collected a long list of security measures that were each mentioned by only a few respondents.

Figure 2 depicts the percentage difference between the groups. The practices mentioned least by non-experts relative to experts were: (1) keep your system up-to-date (31%), (2) use two-factor authentication (18%), and (3) use a password manager (10%).

The security practices mentioned by experts are consistent with experts' rating of different pieces of advice, when we asked them to rank how *good* these are on a 5-point Likert scale. As shown in Figure 3, most experts considered installing OS (65%) and application (55%) updates, using unique (49%) and strong (48%) passwords, using a password manager (48%), and using two-factor authentication (47%) *very good* advice (the highest Likert-scale rating). Other advice that was not frequently mentioned by experts in the top three things they do, but ranked high in this multiple choice question of the advice they'd consider good, included turning on automatic updates (72%), being suspicious of links (60%), not entering passwords on links in emails (60%), and not opening email attachments from unknown people (55%).

In the following, we present and compare expert and non-expert practices and attitudes. We focus on the security practices most mentioned by experts and non-experts. We group these into soft-

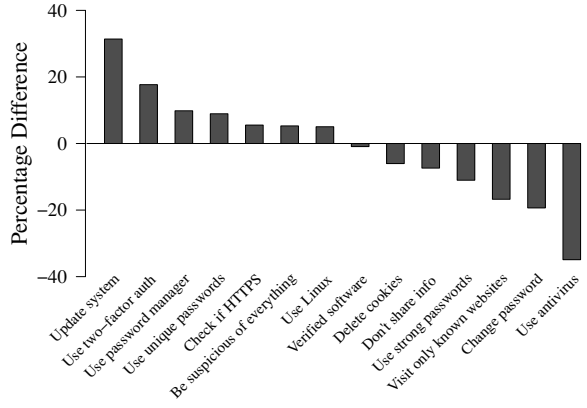

Figure 2: Percentage difference of experts and non-experts mentioning these security practices when asked what are the top three things they do to stay safe online. Security measures with a positive percentage difference were mentioned more by experts than non-experts; those with a negative percentage difference were mentioned more by non-experts.

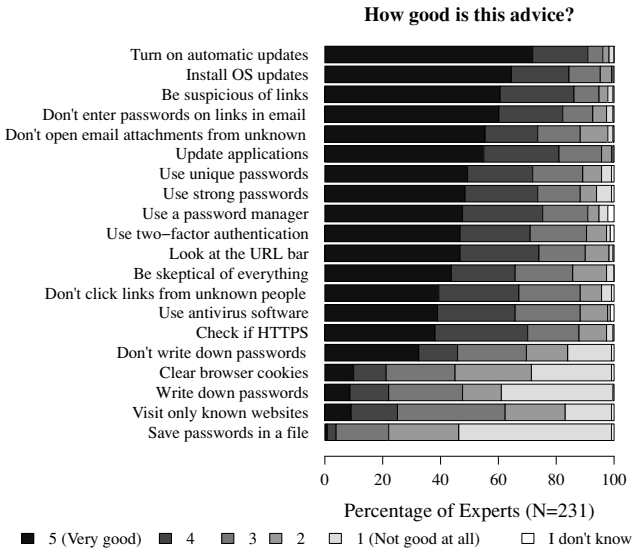

Figure 3: Advice considered "good" (i.e., both in terms of effective and realistic) by experts.

ware updates, antivirus software, password management, and mindfulness. In presenting our results, we draw upon participants' responses to both open-ended and fixed-response questions in the survey.

We refer to expert participants as E1, E2,... E231, and non-experts as N1, N2,... N294. We focus on data collected in the online surveys, but also include some quotes from the expert interviews. We explicitly state when a quote was collected during the interviews. The p values we report refer to Chi-Squared tests and are corrected for multiple tests using the Holm-Bonferroni method. We applied the Holm-Bonferroni correction in R for all the tests we conducted. R adjusts each p-value, rather than reducing alpha (though both techniques are equivalent), so we stuck with alpha=0.05 for determining statistical significance.

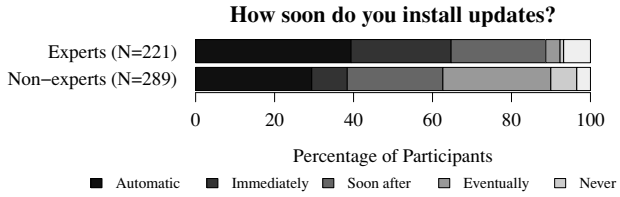

Figure 4: More experts than non-experts reported installing software updates in a timely manner.

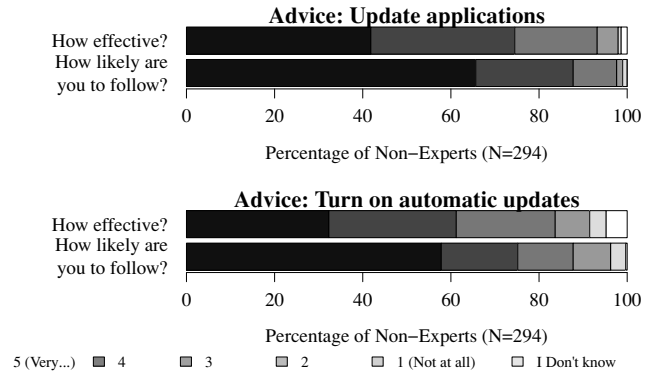

Figure 5: Most non-experts considered the advice to install software updates not effective as a security measure, but said they would be likely to follow it if they heard it was effective.

4.1 Install Software Updates

When asked for the top three things they do to stay safe online, the most common reponse from experts was installing software updates. For instance, E128 said: *"Update all the software and firmware to fix any possible vulnerability."* Furthermore, E78 also said: *"Patch, patch, patch."* Installing updates was also the security measure with the highest percentage difference between experts and non-experts; it was mentioned by 35% of experts, but only by 2% of non-experts. In addition, 2% of experts said they turn on automatic updates—an action that no non-expert mentioned.

To investigate whether the difference in the number of experts and non-experts mentioning updates is also reflected in reported behavior, not just attitudes, we asked both groups in a multiple-choice question how soon after they discover a new version of their operating system is available they install it. Consistent with the previous finding, experts reported installing updates in a more timely manner than non-experts. As shown in Figure 4, 39% of experts—but only 29% of non-experts—answered "Updates are automatically installed." In addition, 25% of experts versus 9% of non-experts said that updates are installed "Immediately." The differences are statistically significant, as summarized in Table 2. Note, however, that these questions did not differentiate between major OS releases and patches. The exact question is included with the survey instrument in the appendix.

We found a similar result for the advice to "Update applications", which only 42% of non-experts considered very effective, yet 66% said they were very likely to follow it (see Figure 5). Table 2 summarizes non-experts rating of effectiveness and likelihood to follow for this and other pieces of advice.

Reported Behavior (Experts & Non-Experts)	Chi-Square Result
How soon do you install updates?	$\chi^2(4, N_e = 221, N_n = 289) = 75.78, p < 0.001$
Do you use antivirus software?	$\chi^2(1, N_e = 221, N_n = 289) = 31.44, p < 0.001$
Do you use two-factor authentication?	$\chi^2(1, N_e = 231, N_n = 294) = 23.37, p < 0.001$
Do you remember you passwords?	$\chi^2(3, N_e = 231, N_n = 294) = 94.68, p < 0.001$
Do you write down your passwords?	$\chi^2(3, N_e = 231, N_n = 294) = 24.78, p < 0.001$
Do you save your passwords in a file?	$\chi^2(3, N_e = 231, N_n = 294) = 1.68, p = 1$
Do you use a password manager?	$\chi^2(3, N_e = 231, N_n = 294) = 131.31, p < 0.001$
Do you reuse passwords?	$\chi^2(3, N_e = 231, N_n = 294) = 37.25, p < 0.001$
Do you look at the URL bar?	$\chi^2(3, N_e = 231, N_n = 294) = 56.29, p < 0.001$
Do you check if HTTPS?	$\chi^2(3, N_e = 231, N_n = 294) = 132.62, p < 0.001$
Do you visit websites you have not heard of?	$\chi^2(3, N_e = 231, N_n = 294) = 62.84, p < 0.001$
Do you enter your password on links in emails?	$\chi^2(3, N_e = 231, N_n = 294) = 2.06, p = 1$
Do you open emails from unknown senders?	$\chi^2(3, N_e = 231, N_n = 294) = 99.60, p < 0.001$
Do you click on links from unknown people?	$\chi^2(3, N_e = 231, N_n = 294) = 51.37, p < 0.001$

Table 1: Results of χ^2 tests comparing expert and non-expert reports on their security behavior. p-values are corrected for multiple testing using the Holm-Bonferroni method.

Security Advice	How Effective is this Advice?	How Likely are You to Follow?	Chi-Square Result
Use antivirus	$\mu = 4.57, \sigma = 0.76$	$\mu = 4.67, \sigma = 0.80$	$\chi^2(5, N = 294) = 15.40, p = 0.12$
Install latest OS updates	$\mu = 4.14, \sigma = 0.94$	$\mu = 4.35, \sigma = 1.03$	$\chi^2(5, N = 294) = 32.38, p < 0.001$
Turn on automatic updates	$\mu = 3.82, \sigma = 1.11$	$\mu = 4.18, \sigma = 1.15$	$\chi^2(5, N = 294) = 49.29, p < 0.001$
Update applications	$\mu = 4.12, \sigma = 0.93$	$\mu = 4.5, \sigma = 0.80$	$\chi^2(5, N = 294) = 39.28, p < 0.001$
Clear cookies	$\mu = 3.6, \sigma = 1.22$	$\mu = 4.21, \sigma = 1.15$	$\chi^2(5, N = 294) = 62.48, p < 0.001$
Use unique passwords	$\mu = 4.58, \sigma = 0.78$	$\mu = 4.30, \sigma = 1.02$	$\chi^2(5, N = 294) = 20.39, p = 0.01$
Use strong passwords	$\mu = 4.61, \sigma = 0.80$	$\mu = 4.63, \sigma = 0.77$	$\chi^2(5, N = 294) = 7.10, p = 1$
Don't write down passwords	$\mu = 3.58, \sigma = 1.54$	$\mu = 3.78, \sigma = 1.55$	$\chi^2(5, N = 294) = 14.16, p = 0.17$
Save passwords in a file	$\mu = 1.75, \sigma = 1.08$	$\mu = 2.15, \sigma = 1.45$	$\chi^2(5, N = 294) = 21.01, p = 0.01$
Use a password manager	$\mu = 2.89, \sigma = 1.46$	$\mu = 2.98, \sigma = 1.60$	$\chi^2(5, N = 294) = 20.03, p = 0.02$
Write down passwords	$\mu = 2.31, \sigma = 1.51$	$\mu = 2.61, \sigma = 1.61$	$\chi^2(5, N = 294) = 14.36, p = 0.17$
Check if HTTPS	$\mu = 4.29, \sigma = 0.89$	$\mu = 4.38, \sigma = 0.93$	$\chi^2(5, N = 294) = 12.57, p = 0.30$
Be skeptical of everything	$\mu = 4.43, \sigma = 0.92$	$\mu = 4.38, \sigma = 1.01$	$\chi^2(5, N = 294) = 6.38, p = 1$
Be suspicious of links	$\mu = 4.78, \sigma = 0.51$	$\mu = 4.76, \sigma = 0.64$	$\chi^2(5, N = 294) = 6.55, p = 1$
Visit only known websites	$\mu = 3.93, \sigma = 1.04$	$\mu = 3.61, \sigma = 1.33$	$\chi^2(5, N = 294) = 24.99, p = 0.002$
Use two-factor authentication	$\mu = 4.46, \sigma = 0.74$	$\mu = 4.25, \sigma = 1.02$	$\chi^2(5, N = 294) = 16.89$, p =0.07
Don't click links from unknown people	$\mu = 4.74, \sigma = 0.57$	$\mu = 4.73, \sigma = 0.67$	$\chi^2(4, N = 294) = 3.85, p = 1$
Don't enter passwords on links in email	$\mu = 4.82, \sigma = 0.46$	$\mu = 4.82, \sigma = 0.48$	$\chi^2(3, N = 294) = 3.89, p = 1$
Look at the URL bar	$\mu = 4.68, \sigma = 0.62$	$\mu = 4.66, \sigma = 0.65$	$\chi^2(5, N = 294) = 1.3986, p = 1$
Don't open email attachments	$\mu = 4.82, \sigma = 0.47$	$\mu = 4.80, \sigma = 0.60$	$\chi^2(4, N = 294) = 3.70, p = 1$

Table 2: Results of χ^2 tests comparing non-expert ratings of security advice in terms of effectiveness versus how likely they are to follow it. p-values are corrected for multiple testing using the Holm-Bonferroni method.

Our results suggest that one reason some non-experts don't install updates might be the lack of awareness on how effective updates are. This hypothesis is also supported by additional feedback that participants provided when given the chance to explain their ratings with a question titled "(optional) Please use this space to clarify any of the above." For example, N56 said: *"I don't know if updating software is always safe. What it you download malicious software?"* Even some experts expressed similar concerns. For example, E163 agreed: *"Automatic software updates are not safe in my opinion, since it can be abused to update malicious content."* In contrast, E143 favored automatic to manual updates *"because update dialogs can be spoofed."*

Seven non-experts reported delaying updates out of concern that new versions of software might contain bugs. For example, N80 explained: *"there are often bugs in these updates initially, that must be worked out by the software vendor."* He, therefore, preferred to wait for the next update *"to make sure it is actually a stable release."* For the same reason, N142 did not like automatic updates: *"sometimes the patches [...] are glitchy [...]. I prefer to have control and know what's being installed by applications."* Even some experts expressed similar concerns. When asked how soon he installs updates, E168 said he only installs updates *"after i do the tests on spare machine."* Eight non-experts said they prefer having control over when updates happen, and seven said they do not like auto updates. N278 went as far as to say: *"I hate automatic updates."* Our findings are consistent with those of Vaniea et al. [50], who found in a study with 37 non-expert Windows 7 users that they frequently decided not to install updates after past negative experiences.

We found some controversy among experts on the difficulty of keeping software updated. While E178 considered it *"easy,"* E161 believed software updates are often *"cumbersome."* E28 pointed out that *"every Windows application uses a different update mechanism,"* and E97 confirmed that users find it difficult to deal with updates: *"I help a lot of non tech savvy users. Panic ensues when an update button shows up."*

4.2 Use Antivirus Software

At the other end of the spectrum depicted in Figure 2 is using antivirus software—the security action mentioned by most non-experts relative to experts. Thirty-five percent more non-experts than experts said that running antivirus software on their personal computers is one of the top three things they do to stay safe online. Figure 1 shows that 42% of non-experts and 7% of experts mentioned using antivirus software among the top three things they do to stay safe online. Five percent of non-experts and 1% of experts also reported keeping the antivirus software up-to-date.

This finding is in line with the high rates of adoption of antivirus software reported in a multiple choice question. When asked if they use antivirus software on their personal computers, 85% of non-experts reported doing so—compared to the 63% of experts who said they do. The difference between the two groups is statistically significant ($\chi(1, N_e = 221, N_n = 289) = 31.44$, $p < 0.001$). One factor explaining this finding might be the fact that experts and non-experts may use different operating systems. We did not ask what operating systems participants used, but a higher percentage of experts than non-experts (6% vs. 1%) named using Linux as one of the top three things they do to stay safe online. Several experts did mention that the need to run antivirus software is operating system dependent.

Further data we collected also confirms that non-experts consider using antivirus software very effective at protecting their security. We asked non-experts to rate on a 5-point Likert scale *how effective* they consider the security advice *Use antivirus software*. As shown in Figure 7, 69% rated it "5 (Very effective)" and 21% rated it "4 (Effective)". When asked *how likely* they would be to follow this advice if they heard that using antivirus software was effective, 80% of non-experts considered themselves "5 (Very likely)" to do so and another 12% said they were "4 (Likely)." Non-experts' high appraisal for antivirus software is also reflected in optional feedback comments that some non-experts provided. For example, N159 said that *"keeping a good antivirus along with a good malware program [...] is the best way to stay safe."*

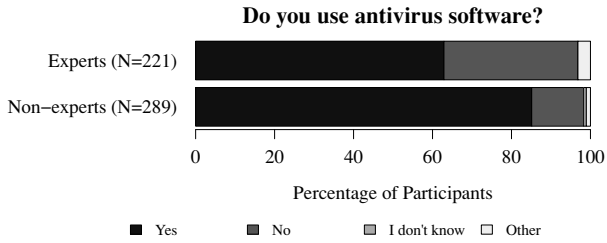

Figure 6: More non-experts reported to use antivirus software on their personal computer than experts.

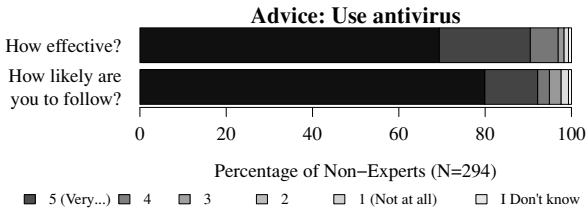

Figure 7: Most non-experts rated the advice 'Use antivirus software' effective or very effective. Similarly, they considered themselves very likely to follow this advice.

The high adoption of antivirus software among non-experts and their high willingness to follow this advice might be due to the good usability of the install-once type of solution that antivirus software offers. Similar to running antivirus, firewalls were also popular among non-experts. Although only 3% of the experts we surveyed mentioned using a firewall as one of the top three things they do, 17% of non-experts mentioned firewalls—often in conjunction with antivirus software. While experts acknowledged the usability of antivirus software, some also cautioned that antivirus is not a bulletproof security solution. For example, E47 believed that *"AV is simple to use, but less effective than installing updates."* Similarly, E116 believed that an antivirus *"is good at detecting everyday/common malware. But nothing that's slightly sophisticated."* E27 also cautioned that an antivirus *"also needs to be kept up-to-date, which is often not the case."*

4.3 Account Security

In the top three things they do, both experts and non-experts spoke frequently of passwords. Using strong and unique passwords were some of the most mentioned strategies by both groups. However, while more experts than non-experts emphasized having *unique* passwords (25% vs. 15%), fewer talked about having *strong* passwords (18% vs. 30%). Similarly, experts mentioned more frequently using a password manager (12% experts vs. 3% non-experts), but spoke less of changing passwords frequently (2% experts vs. 21% non-experts).

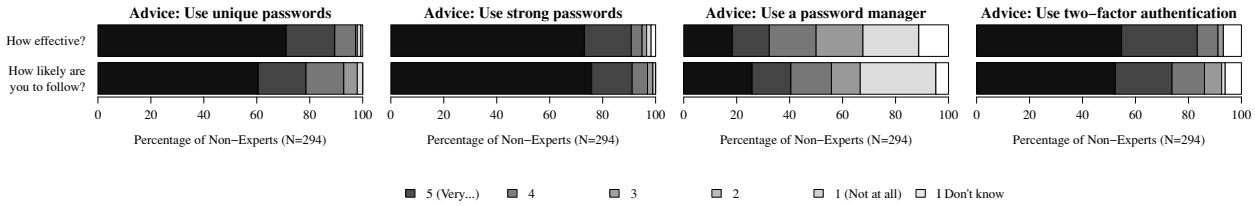

Figure 8: Non-experts considered the advice to use unique and strong passwords very effective, but were less aware of the security benefits of using a password manager or two-factor authentication.

4.3.1 Use a Password Manager

To better understand how the two groups differ in their password management habits, we asked a series of multiple-choice questions about password behavior. While more experts said they *use a password manager* to keep track of their passwords, more non-experts said they *write down* passwords, *remember*, or *reuse* them. As Figure 9 shows, three times more experts than non-experts reported using password managers for at least *some* of their accounts (73% vs. 24%, $\chi(3, N_e = 231, N_n = 294) = 131.31$, $p < 0.001$). This difference is in line with the fact that four times more experts than non-experts said that using a password manager is one of the most important things they do to stay safe online (13% vs. 3%, see Figure 1). To experts such as E123, *"Password managers change the whole calculus,"* because they make it possible to have both strong and unique passwords.

The low adoption rate of password managers among non-experts might stem from a lack of understanding of it's security benefits. To explore non-experts' attitudes, we asked them to rate in terms of effectiveness on a 5-point Likert scale the advice "Use a password manager." Only 18% considered this advice *very effective*, and another 14% thought it was *effective*. Thirty-nine percent believed that the advice was not effective and 11% said that they did not know. In the optional feedback, seven non-experts explicitly expressed distrust in password managers. For example, N278 said: *"I wouldn't use a password manager even if it helps because I don't trust it."* A reason for this lack of trust was the fear that, if stored or written down, passwords could be leaked. For example, N53 explained, *"I try to remember my passwords because no one can hack my mind."* The fear that software can be hacked is reflected also in N251's comment that password managers should be *"completely trustworthy and impregnable. No other applications seem to be that safe so how can I believe password managers are."* In fact, 2% of non-experts thought that not letting browsers remember their passwords was one of the top things they do.

In addition to perceived lack of effectiveness, other factors such as poor usability might stall adoption of password managers among non-experts. In another Likert scale question, only 40% of non-experts said they would be likely or very likely to follow this advice if they heard it was effective. This percentage is much lower than the 91% who said they would use strong passwords if they heard this security measure was effective, and the nearly 80% who said they would use unique passwords. Some additional comments made by experts might help explain these answers. For example, E71 pointed out that password managers *"tend to be complicated for non-technical users still."* E9 named a specific problem, that when starting to use a password manager *"it is difficult to update existing passwords."* Our results are in line with those of Chiasson et al. [11] who found that the usability of password managers could be improved.

4.3.2 Write Passwords Down

Writing down passwords was seen by some experts as a substitute to using a password manager. E121 believed that *"People understand a paper system very well, and know how to secure it."* Similarly, E79 noted another benefit: *"Malware can't read a piece of paper."* As Figure 9 shows, more non-experts than experts reported to *write down* passwords for at least *some* of their accounts (38% vs. 20%, $\chi(3, N_e = 231, N_n = 294) = 24.78$, $p < 0.001$). Only one expert said that writing down passwords is fundamentally bad, but several expressed concern for how securely the paper would be stored.

As shown in Figure 9, three times more non-experts than experts said that they *remember all* of their passwords (17% experts vs 52% of non-experts, $p < 0.001$). Furthermore, six times more non-experts say that they *use the same* password for *all or most* of their accounts (19% of non-experts vs. 3% of experts, $\chi(3, N_e = 231, N_n = 294) = 37.25$, $p < 0.001$). Only 4% of experts and 15% of non-experts said they do not remember any of their passwords. From the additional feedback we received, a couple of techniques for making passwords easier to remember stood out: (a) using an algorithm for creating passwords—mentioned by 19 non-experts and 21 experts—and (b) having different password "levels"—mentioned by 8 experts and 7 non-experts. For example, N277 described the algorithmic approach: *"I use a base password and just have a suffix that is usually unique."* N241 reported using the password levels approach: *"I have three levels of passwords, actually four. I have a password for my bank, Amazon, Paypal accounts."*

Our results are consistent with Florencio et al. [16], who, back in 2007, found that users have a set of passwords which they cycle through, and use trial and error to remember which password they used.

Some participants occasionally forgot passwords, or did not remember which password they used. For example, E163 has a *"few [passwords], so if one doesn't work, I'll try another."* Similarly, N43 tried to *"remember them by trial and error."* Three non-experts mentioned that sometimes they resort to password reset to get back into their accounts. For example, N200 said: *"I don't do anything other than try to remember them and I often have to reset because I've forgotten."*

4.3.3 Change Passwords Frequently

The security action with the highest percentage difference for non-experts compared to experts was changing passwords frequently. 21% of non-experts, but only 2% of experts mentioned changing passwords when asked what are the top three things they do to stay safe online. We did not ask experts to rate how good the advice to change passwords frequently is, but some researchers have questioned the effectiveness of this action. Zhang et al. raised concerns over how effective this action is at protecting against an attacker who has captured an old password [56]. The authors showed that, by knowing the old password and applying simple transformations

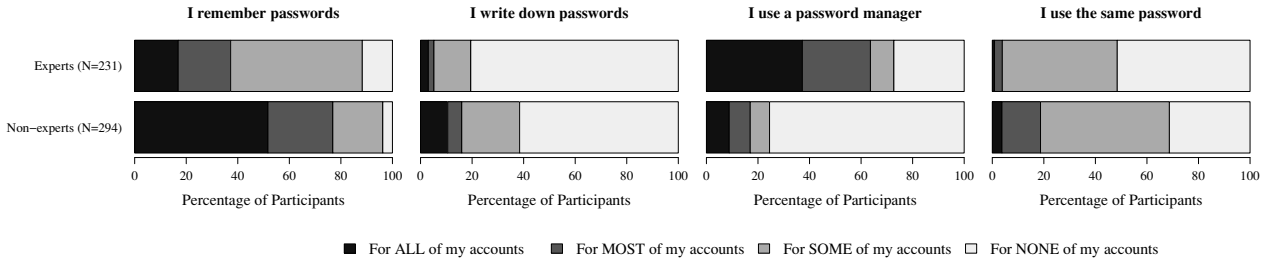

Figure 9: More non-experts than experts reported remembering passwords and using the same password on several accounts, while more experts say they use a password manager.

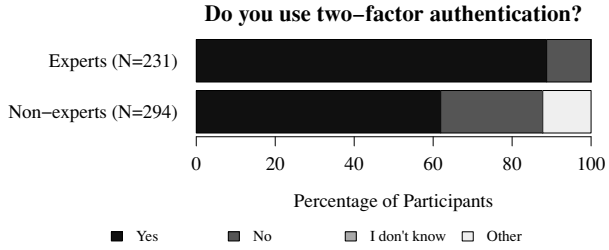

Figure 10: More experts than non-experts reported to use two-factor authentication for at least one of their online accounts.

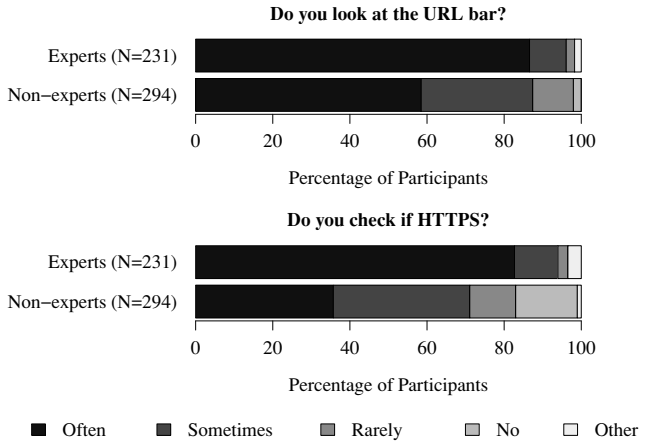

Figure 11: More experts than non-experts reported to look at the URL bar to verify if they are visiting the website they intended to, and to check whether the website uses HTTPS.

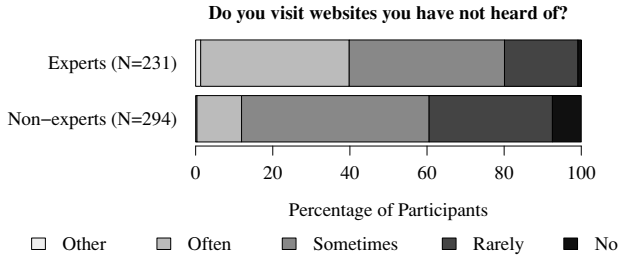

Figure 12: More non-experts than experts reported to only visit websites they have heard of.

to it, an attacker is able to guess the new one 41% of the time for an offline attack, and 17% within five online attempts.

4.3.4 Use Two-Factor Authentication

Another popular security action among experts was to use two-factor authentication. For example, E50 considered two-factor authentication *"hugely important for high-value services (such as Gmail)."* Non-experts rated this advice significantly higher than using a password manager, both in terms of effectiveness (83% vs. 32%, $\chi(4, N = 294) = 177.53$, $p < 0.001$) and likelihood of following the advice (74% vs. 40%, $\chi(4, N = 294) = 107.24$). However, the adoption rates of two-factor authentication among non-experts still lag behind those of experts. When asked if they use two-factor authentication for at least one of their online accounts, more experts than non-experts answered that they do (89% vs. 62%, $p < 0.001$). 12% of non-experts said they don't know if they do, which suggests they may not know what two-factor authentication is.

Ten experts expressed concerns that two-factor authentication is still too difficult for many users or not widely available. For example, E161 said that *"On average most don't yet understand two factor very well,"* and E207 said that two-factor authentication *"will need good instructions on how it works"*. Furthermore, E132 noted that *"using two-factor authentication will likely not be possible or feasible for a lot of sites."*

4.4 Mindfulness

The remaining security actions mentioned by experts and non-experts did not have as stark of a percentage difference as using antivirus, installing software updates, and managing passwords (see Figure 2). In this section, we discuss these remaining items. We focus on visiting only known websites and checking if the websites use HTTPS. We also discuss security advice related to emailing habits, which was not mentioned frequently by either group as a top 3 practice, but was ranked highly when we explicitly asked about it.

4.4.1 Visit Only Known Websites

After using antivirus and changing passwords frequently, the practice most mentioned by non-experts relative to experts (see percentage difference in Figure 2) was visiting only known websites. 21% of non-experts—but only 4% of experts—said they only go to known or reputable websites to stay safe online. In addition, 4% of non-experts said they provide personal information only to trusted websites and 3% said they make purchases only from trusted websites; no expert mentioned these practices.

One might wonder how realistic it is to only visit known websites. The answers to a multiple-choice question we asked seem to suggest that both experts and non-experts sometimes make exceptions to this rule. We asked both groups in a multiple choice question if they visit websites they have not heard of. Figure 12 shows the results. Seven percent of non-experts said they *do not* visit unknown websites—compared to the 21% who mentioned this practice as one of the three most important things they do to stay safe online. Only 1% of experts said they do not visit unknown websites—also lower than the percentage who mentioned this in their top three. Thirty-two percent of experts and 19% of non-experts said they *rarely* visit unknown websites. The difference is statistically significant ($\chi^2(3,\ N_e = 231,\ N_n = 294) = 62.84$, $p < 0.001$). It is unclear how the browsing needs of experts and non-experts differ and how they influence behavior. Perhaps non-experts visit a more limited number of websites because they do not have as high of a need as experts to explore new things and conduct research on the Internet.

When asked to rank the advice "Visit only known websites" on a Likert scale, 76% of non-experts rated it *very effective* or *effective* (see Figure 15). After marking this advice *effective*, N191 commented *"Visiting websites you've heard of doesn't mean they are completely safe, but there is a higher chance of this."* When asked how likely they would be to follow this advice if they heard it was effective, 57% of non-experts said they were *likely* or *very likely* to follow it—lower than the 76% who rated the advice effective. This finding might suggest that 'Visit only known websites' is not always practical. In fact, four non-experts explicitly commented on this. N236 said: *"It would be impossible to only visit websites you know. Why not hide under the bed too?"* For N98, not visiting new websites is *"missing the point of the internet."* Some experts pointed out problems with this advice as well. For example, E134 said: *"Visiting only known websites is great, but paralyzing."* E7 reported another shortcoming: *"Visiting websites you've heard of makes no difference in a modern web full of ads, cross-site requests."*

4.4.2 Check if HTTPS

After software updates and account security (use strong and unique passwords, use a password manager and two-factor authentication), the most mentioned practice by experts when asked about their top three was using HTTPS. As Figure 1 shows, 10% of experts and 4% of non-experts said they check if the website they are visiting uses HTTPS as a top 3 action. In addition, 2% of non-experts said that they do not provide credit card information, and 3% said they don't give credentials or private information, unless the connection is over HTTPS. Looking at the URL bar to check what website they are visiting was mentioned by 3% of experts, but only by one non-expert.

In a multiple-choice question, we asked both groups if they look at the URL bar to verify that they are visiting the intended website. Figure 11 shows the results. 86% of experts and 59% of non-experts said they do so *often*. When asked in a similar question if they check whether the website they are visiting uses HTTPS, 82% of experts and 36% of non-experts said they *often* do. Both differences are statistically significant ($p < 0.001$). Note that for experts, the likelihood of checking for HTTPS and looking at the URL bar to verify the name of the site are equal, whereas non-experts are far more likely to report looking at the URL bar but not checking for HTTPS.

When asked to rate the advice, 75% of non-experts said that checking the URL is *very effective*; 74% said that they would be *very likely* to follow it (see Figure 15). When asked about the advice "Check if the website they're visiting uses HTTPS", 60% rated it *very effective*, but only 50% considered themselves *very likely* to follow it. It is unclear why some participants claim they would look at the URL bar but not check for HTTPS or why some consider checking for HTTPS effective, but would not follow this advice.

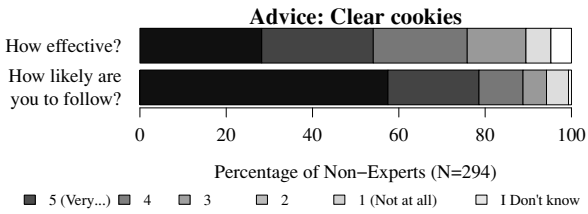

Figure 14: Most non-experts considered themselves very likely to delete cookies if they heard it was an effective security measure.

4.4.3 Clear Browser Cookies

Six percent of non-experts and only one expert said that deleting or restricting cookies is one of the top three things they do to stay safe online. When asked how good the advice "Clear browser cookies" is, 54% of experts rated it not good or not good at all. Only 21% rated it good or very good. E127 said that *"Clearing cookies might be OK to prevent some session hijacking, but the annoyance of logging in again might throw some users off."* E8 specified that *"Clearing cookies is more of a privacy measure."* It is likely that, while experts distinguished between privacy and security measures, non-experts conflated the two areas. In fact, N103 explicitly stated: *"Clearing cookies might not protect you from viruses but 'online security' is a very broad term and I believe privacy is part of online security."*

Figure 14 shows that 78% of non-experts considered themselves likely or very likely to clear browser cookies if they heard this measure helped protect their security online. Fifty-four percent considered deleting cookies an effective security measure. N284 commented *"I forget to clear cookies."* N281 believed that *"If it was an easy solution–like clearing cookies–I'd do it all the time."*

4.4.4 Email Habits

Some email-related security advice that we collected during our interviews was not frequently mentioned by survey participants but was rated highly on Likert scales when explicitly asked about. In the following, we discuss two such pieces of advice: 'Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password' and 'Don't click on links that people or companies you don't know send you.' However, when explicitly asked about them, these pieces of advice were rated as good advice by experts (see Figure 3)

Similarly, when asked how effective this advice is, 85% of non-experts rated *very effective* the advice 'Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password.' Eighty-six percent considered themselves themselves very likely to follow this advice. A similarly high number—80%—said that not clicking on links that people they don't know send them is *very effective* advice (see Figure 15). Eighty-two percent said they would be likely to follow this advice if they heard it was effective. In a multiple choice question, both groups reported to generally follow these two pieces of advice (see Figure 13).

It is noteworthy that a significantly higher percentage of experts than non-experts reported to *often* click on links that people they

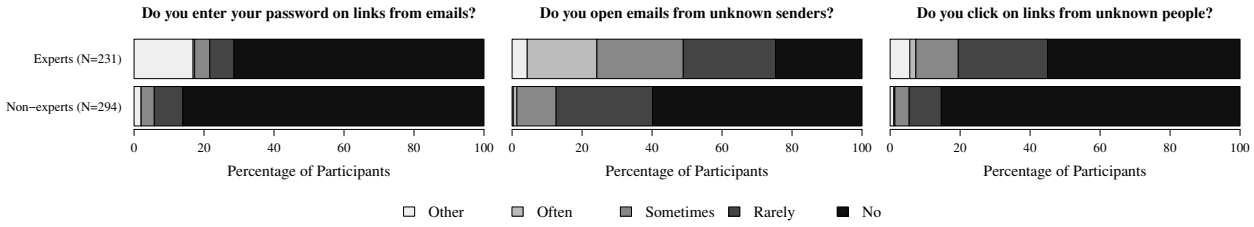

Figure 13: Both experts and non-experts said they follow good email practices. More experts said they sometimes click on links and open attachments received from unknown senders.

don't know send them (38% vs. 12%, $\chi(3, N_e = 231, N_n = 294) = 51.37$, $p < 0.001$). This result suggest that, although some security advice is being followed more by experts than by non-experts (e.g., installing updates, using a password manager), other advice is perhaps paradoxically being followed more by non-experts. During our interviews, some experts admitted that they do not follow some of the advice they give. For example, after recommending that non-tech-savvy users never open emails from unknown people, an expert admitted: *"I do all the time, [laughter] but I tell my mother not to."* Another expert explained during our interviews: *"I never really found a way of giving more precise advice for people who are not technical on what is really safe and what is not."* A couple other interview participants said that they don't follow their own advice because, unlike non-tech-savvy users, they can distinguish between when it's safe and when not to take certain actions.

Other habits mentioned by experts and non-experts include restricting the amount of personal information they share (10% of experts vs. 17% of non-experts), installing only trusted or verified software (5% of experts vs. 6% of non-experts), using Linux (6% vs. 1%), and deleting cookies (0% vs. 6%).

5. DISCUSSION AND FUTURE WORK

Our results show that experts and non-experts follow different practices to protect their security online. The experts' practices are rated as good advice by experts, while those employed by non-experts received mix ratings from experts. Some non-expert practices were considered "good" by experts (e.g., install antivirus software, use strong passwords); others were not (e.g., delete cookies, visit only known websites).

In the pursuit of better security advice, we should ensure that valuable user time is being spent on the things that would bring them the most benefit. Our results suggest that at least some things that experts do and recommend are not being done by non-experts. In this work, we identified three security practices that experts report to do but non-experts do not: installing updates, using a password manager, and using two-factor authentication.

These three pieces of security advice that we highlight are the security actions that most experts relative to non-experts said they do and consider important. These three security actions were ranked highest by percentage difference in Figure 2. This recommendation is also supported by differences among experts and non-experts in self-reported behavior around these three security actions (Figures 4, 9, and 10). Our results suggest that not just better messaging, but also systems and usability work is necessary to get non-experts to follow these three security practices.

In line with the findings and the recommendations provided by Vaniea et al. [50], our results suggest the need to invest in developing an updates manager that downloads and installs available software updates for all applications—much like mobile application updates on smartphones. Such a centralized updates manager could also access a central repository to check if any problems with available updates have been reported, and, if so, delay the installation. In addition, software developers should separate security updates from those introducing general software features. The update manager could give users the option to install only security updates automatically, while feature updates could be manually reviewed and installed. To that end, a notable area for further research is developing a standard way for applications to communicate what UI changes and security fixes are included in the update.

Another practice employed by experts but not by non-experts was using a password manager to keep track of passwords. Some participants reported cycling through multiple passwords to remember which they used for a given site. Trying various passwords on a website until one works leaves the user vulnerable to a rogue or compromised website. Furthermore, as rainbow tables used to crack password hashes evolve to incorporate password rules used by users, password-creation algorithms that some participants used will most likely not offer real protection against offline attacks, as demonstrated by Das et al. [12]. Password managers can make it feasible to use truly random and unique passwords and help move users away from memorable passwords, which are vulnerable to smart-dictionary attacks [36]. However, non-experts might place a higher emphasis than experts on usability. Previous work has evaluated two different password managers and identified significant usability shortcomings [11]. Perhaps such usability drawbacks are harder to deal with for non-experts than for experts. To that end, more work needs to be done to improve the usability of password managers before recommending them strongly to users. Our results also suggest that users' reluctance to adopt password managers may also be due to an ingrained mental model that passwords should not be stored or written down—advice users have been given for decades. But as threat models are shifting from offline to online attacks and password reuse is becoming an increasing problem, using password managers or writing passwords down in a secure location seems to be a promising solution.

Furthermore, additional work needs to be done to understand why non-experts are not using two-factor authentication. Some of the expert participants in our study offered several reasons, including the fact that this security feature is still too difficult to explain to non-tech-savvy users, that it is not available on all websites, and that it causes significant inconveniences. Our results suggest that more work needs to be done to explain two-factor authentication to users and to make it adequate to use by non-expert users.

A few additional areas for future research stand out based on our findings. Many more non-experts than experts said that, to stay safe online, they only go to trusted websites. This security advice was

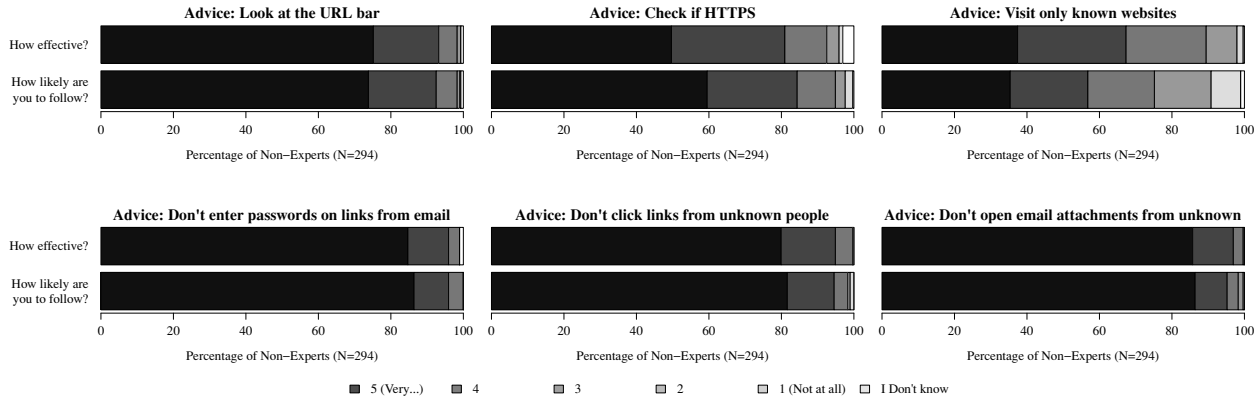

Figure 15: Most non-experts rated email advice very effective and said they are very likely to follow it. They considered looking at the URL bar more effective than checking for HTTPS and visiting only known websites.

not considered "good" by experts. Furthermore, Google's transparency report on safe browsing [1] shows that most malware websites are not malicious attack sites, but compromised sites that are used to spread malware. Therefore, not visiting new websites is not necessarily effective at keeping users safe. A good investment in this area is developing browsers and systems that more effectively warn users when they are about to go to a compromised or known phishing website, something that the Chrome and Firefox browsers already do [5].

Finally, further investigation is needed to understand why, unlike experts, some non-experts claimed they would look at the URL bar but not check for HTTPS. Another study could investigate why some non-experts consider checking for HTTPS effective, but they admit that they would not follow the advice. Our findings seem to indicate that more visible and intuitive HTTPS indicators could help some users better assess if a website uses HTTPS. Better URL indicators have been shown to help some users. Lin et al. found that domain highlighting in the URL helps some (though not all) users judge the legitimacy of a website and avoid phishing attacks [33].

5.1 Limitations

The study presented in this paper is not without its limitations. First, we recruited non-expert participants on the Mechanical Turk platform, which is known to provide a younger and more tech-savvy sample than the general population. All our non-expert participants were from the US; running the study in other countries might lead to different results. Furthermore, all behavioral data that we collected was self-reported and, therefore, unconfirmed. Such data can suffer from several biases, including social desirability, inaccurate recall, and lack of understanding. For example, participants may not be able to accurately remember how often they check if the website they are visiting uses HTTPS or how soon they install available software updates.

We compared expert and non-expert security behavior, but we note that experts by their nature may operate in different computing environments than non-experts, so their reported behavior may be different not because it is objectively better, but simply because it is more suited to the expert environment. For example, it may be the case that experts are more likely to use Unix-based systems while non-experts are more likely to use Windows-based systems, and appropriate security practices (at least some of them, like using antivirus software) may depend upon the operating system in use.

Defining a security "expert" is challenging, and we settled upon a definition that is simple (5+ self-reported years of experience in the area) but, intuitively, suggests strong expertise. However, even experts are not infallible. For example, Yen et al. [55], in a study of malware encounters in a large enterprise, found higher levels of encounters among users with technical job titles (e.g., "engineer") than among those with less technical titles (e.g., "assistant"). While this result could be due to the technical users simply spending more time using computers or perhaps taking greater risks, it shows that even the tech-savvy are prone to security threats. Thus, expert behavior should not necessarily be taken as the right standard for non-tech-savvy users.

6. CONCLUSIONS

Our results find discrepancies between what security practices experts and non-experts follow. While most expert participants install updates, use a password manager, and use two-factor authentication, most non-expert participants use antivirus software, change passwords frequently, and visit only known websites. Non-expert participants reported being reluctant to promptly install software updates, perhaps due to lack of understanding of their effectiveness or bad past experiences caused by software updates. Though using them was considered good advice by experts, password managers were regarded with skepticism by non-experts, who instead preferred to remember passwords, partly because, as one participant said, "no one can hack my mind." Other security advice, however, such as not clicking on links received from unknown people were known and followed by non-experts. More work has to be done on improving the limitations of security practices identified in this work which are used by experts but not by non-experts. Nevertheless, based on our findings, some promising security advice emerges: (1) install software updates, (2) use a password manager, and (3) use two-factor authentication for online accounts.

7. ACKNOWLEDGMENTS

The authors wish to thank the many security experts who volunteered their time to participate in our interviews and respond to our survey. We also wish to thank Eric Grosse, Tim Dierks, and Ulfar Erlingsson at Google for supporting this work and reviewing early paper drafts, and Cormac Herley and Adam Shostack for early discussions that guided our research direction. Finally, we wish to thank the many colleagues, friends, and paper reviewers who contributed valuable feedback. Thanks all!

8. REFERENCES

[1] Google transparency report: Safe browsing. Accessed Feb 2, 2014. **http://www.google.com/transparencyreport/safebrowsing/**.

[2] McAfee security advice center. Accessed Sep 8, 2014. **http://home.mcafee.com/advicecenter/**.

[3] US-CERT: Tips. Accessed Sep 8, 2014. **https://www.us-cert.gov/ncas/tips**.

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

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

[6] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: managing security behaviour in organisations. In *Proc. of NSPW*, pages 47–58. ACM, 2009.

[7] D. Bohn. How to make your email address as hard to guess as your password. *The Verge*, Sep 3, 2014. **http://www.theverge.com/2014/9/3/6100893/how-to-make-your-email-address-as-hard-to-guess-as-your-password**.

[8] M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, 6(1):3–5, 2011.

[9] L. J. Camp. Mental models of privacy and security. *IEEE Technology & Society*, 2006.

[10] B. X. Chen. Home Depot investigates a possible credit card breach. *The New York Times*, Sep 03, 2014. **http://www.nytimes.com/2014/09/03/technology/home-depot-data-breach.html**.

[11] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *Prox. of USENIX Security*, volume 6, 2006.

[12] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Proc. of NDSS*, 2014.

[13] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006.

[14] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proc. of CHI*, pages 1065–1074. ACM, 2008.

[15] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. Does my password go up to eleven?: the impact of password meters on password selection. In *Proc. of CHI*, pages 2379–2388. ACM, 2013.

[16] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proc. of WWW*, pages 657–666. ACM, 2007.

[17] Google safety center. Accessed Sep 8, 2014. **https://www.google.com/safetycenter/**.

[18] E. Hayashi and J. Hong. A diary study of password usage in daily life. In *Proc. of CHI*, pages 2627–2630. ACM, 2011.

[19] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proc. of NSPW*, pages 133–144. ACM, 2009.

[20] C. Herley. More is not the answer. *IEEE Security & Privacy*, 12(1):14–19, 2014.

[21] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 209–223. IEEE, 2012.

[22] P. G. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392. ACM, 2010.

[23] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In *Proc. of SOUPS*, page 13. ACM, 2011.

[24] M. Isaac. Nude photos of Jennifer Lawrence are latest front in online privacy debate. *The New York Times*, Sep 03, 2014. **http://www.nytimes.com/2014/09/03/technology/trove-of-nude-photos-sparks-debate-over-online-behavior.html**.

[25] M. Isaac. Russian hackers amass over a billion internet passwords. *The New York Times*, Aug 06, 2014. **http://www.nytimes.com/2014/09/03/technology/home-depot-data-breach.html**.

[26] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Proc. of Security and Privacy*, pages 523–537. IEEE, 2012.

[27] S. M. Kelly. How to protect your photos (nude or otherwise) from hackers on iCloud. *Mashable*, Sep 1, 2014. **http://mashable.com/2014/09/01/icloud-nude-photo-hack/**.

[28] M. Khan, Z. Bi, and J. Copeland. Software updates as a security metric: Passive identification of update trends and effect on machine infection. In *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*, pages 1–6. IEEE, 2012.

[29] A. Kittur, E. H. Chi, and B. Suh. Crowdsourcing user studies with Mechanical Turk. In *Proc. of CHI*, pages 453–456. ACM, 2008.

[30] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: measuring the effect of password-composition policies. In *Proc. of CHI*, pages 2595–2604. ACM, 2011.

[31] J. R. Landis and G. G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, pages 159–174, 1977.

[32] F. L. Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji. A clinical study of risk factors related to malware infections. In *Proc. of CCS*, pages 97–108. ACM, 2013.

[33] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2075–2084, New York, NY, USA, 2011. ACM.

[34] E. L. MacGeorge, B. Feng, and E. R. Thompson. "Good" and "bad" advice. *Studies in applied interpersonal communication*, page 145, 2008.

[35] Microsoft safety & security center. Accessed Sep 8, 2014. **http://www.microsoft.com/security/default.aspx**.

[36] A. Narayanan and V. Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In *Proc. of CCS*, pages 364–372. ACM, 2005.

[37] G. Paolacci, J. Chandler, and P. G. Ipeirotis. Running experiments on Amazon Mechanical Turk. *Judgment and Decision making*, 5(5):411–419, 2010.

[38] A. Peterson. How to game security questions to make yourself safer online. *The Washington Post*, Sep 4, 2014. **http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/04/how-to-game-security-questions-to-make-yourself-safer-online/**.

[39] E. Rader, R. Wash, and B. Brooks. Stories as informal lessons about security. In *Proc. of SOUPS*. ACM, 2012.

[40] R. Reeder. If you could tell a user three things to do to stay safe online, what would they be? *Google Online Security Blog*, March 26, 2014. **http://googleonlinesecurity.blogspot.com/2014/03/if-you-could-tell-user-three-things-to.html**.

[41] M. A. Sasse, C. C. Palmer, M. Jakobsson, S. Consolvo, R. Wash, and L. J. Camp. Helping you protect you. *IEEE Security & Privacy*, 12(1):39–42, 2014.

[42] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, page 51âĂŞ65, Washington, DC, USA, May 2007. IEEE Computer Society.

[43] 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 *Proc. of CHI*, pages 2657–2666. ACM, 2014.

[44] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor. Can long passwords be secure and usable? In *Proc. of CHI*, pages 2927–2936. ACM, 2014.

[45] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proc. of CHI*, pages 373–382. ACM, 2010.

[46] 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 *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 3:1–3:18, New York, NY, USA, 2011. ACM.

[47] G. Stewart and D. Lacey. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1):29–38, 2012.

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

[49] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, et al. How does your password measure up? the effect of strength meters on password creation. In *USENIX Security Symposium*, pages 65–80, 2012.

[50] K. E. Vaniea, E. Rader, and R. Wash. Betrayed by updates: how negative experiences affect future security. In *Proc. of CHI*, pages 2671–2674. ACM, 2014.

[51] A. J. Viera, J. M. Garrett, et al. Understanding interobserver agreement: the kappa statistic. *Family Medicine*, 37(5):360–363, 2005.

[52] R. Wash. Folk models of home computer security. In *Proc. of SOUPS*, pages 1–16. ACM, 2010.

[53] K. Witte. Theory-based interventions and evaluations of outreach efforts. *Research review. Seattle, WA: National Network of Libraries of Medicine Pacific Northwest Region, Outreach Evaluation Resource Centre.*, 9:2007, 1998.

[54] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.

[55] T.-F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels. An epidemiological study of malware encounters in a large enterprise. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1117–1130. ACM, 2014.

[56] Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: an algorithmic framework and empirical analysis. In *Proc. of CCS*, pages 176–186. ACM, 2010.

APPENDIX

We include here the questions asked the in Expert and Non-expert Surveys. All multiple-choice questions were single answer only. The questions were identical for the Expert and Non-expert survey, unless otherwise stated.

We mark with "(Experts only)" or "(Non-experts only)" questions that were asked in only one of the surveys.

Survey Instruments

- *(Experts only)* What are the top 3 pieces of advice you would give to a non-tech-savvy user to protect their security online? *(open-ended)*
- What are the 3 most important things you do to protect your security online? *(open-ended)*
- How did you learn about the things you listed above? *(open-ended)*
- Do you use a laptop or desktop computer that you or your family owns (i.e., not provided by school or work)? *(multiple-choice)*
  - Yes
  - No
  - Other
- When did you get that computer? *(multiple-choice)*
  - Less than 1 year ago
  - At least 1 but less than 2 years ago
  - At least 2 but less than 3 years ago
  - At least 3 but less than 5 years ago
  - 5 or more years ago
- How soon after you discover that a new version of your operating system (OS) software is available do you (or somebody else managing your computer) install it? *(multiple-choice)*
  - OS updates are installed automatically
  - Immediately
  - Soon after
  - Eventually
  - OS updates are never installed
  - Other
- Do you use anti-virus software on that computer? *(multiple-choice)*
  - Yes
  - No
  - I don't know
  - Other
- Which anti-virus software do you use? *(open-ended)*
- How do you keep track of your passwords for your online accounts? *(grid question)*
  Answer options: For ALL of my accounts, For MOST of my accounts, For SOME of my accounts, For NONE of my accounts
  - Remember them
  - Write them down on paper
  - Save them in a local file on my computer
  - Have my password manager (e.g., 1Password, LastPass) remember them
  - Use the same password on multiple accounts
- If you use a password manager, which one do you use? *(open-ended)*
- (optional) What other things, if any, do you do to keep track of your passwords? *(open-ended)*
- Do you use two-factor authentication (e.g., 2-Step Verification) for at least one of your online accounts? *(multiple-choice)*
  - Yes
  - No
  - I don't know
  - Other
- Do you look at the URL bar to verify that you are visiting the website you intended to? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know

  - Other
- Google began in January 1996 as a research project. Its initial public oïňĂering took place on August 19, 2004. Did the initial public offering of Google take place in 1996? *(multiple-choice)*
  - Yes
  - No
  - Other
- Do you check if the website you're visiting uses HTTPS? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other
- Do you visit websites you have not heard of before? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other
- When you click on a link in an email and that link takes you to a website that asks for your password, do you enter it? Do you open emails you receive from people or companies you don't know? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other
- Do you click on links that people or companies you don't know send you? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other
- *(Experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies
- *(Experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies

- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Use anti-virus software
  - Install the latest operating system updates
  - Turn on automatic software updates
  - Update applications to the latest version
  - Clear your Web browser cookies
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper
- *(Experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Use different passwords for each account
  - Use passwords that are not easy to guess
  - Don't write down passwords on paper
  - Save your passwords in a local file on their computer
  - Use a password manager (e.g., 1Password, LastPass)
  - Write down passwords on paper
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts
- *(Experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know

  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Check if the website you're visiting uses HTTPS
  - Be skeptical of everything when online
  - Be suspicious of links received in emails or messages
  - Visit only websites you've heard of
  - Use two-factor authentication for your online accounts
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how good (in terms of both EFFECTIVE at keeping the user secure, as well as REALISTIC that the user can follow it) you think they are at protecting a non-tech-savvy user's security online. *(grid question)*
  Scale: 5 (Very good), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know
- *(Experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE you think the advice would be at protecting your security online, IF YOU FOLLOWED IT. *(grid question)*
  Scale: 5 (Very effective), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Non-experts only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how LIKELY YOU WOULD BE TO FOLLOW the advice, if you heard it would help protect your security online. *(grid question)*
  Scale: 5 (Very likely), 4, 3, 2, 1 (Not at all), I don't know
  - Don't click on links that people or companies you don't know send you
  - Don't enter your password when you click on a link in an email and that link takes you to a website that asks for your password
  - Pay attention when taking online surveys. We appreciate your input. To let us know you're paying attention, select four for this response
  - Look at the URL bar to verify that you are visiting the website you intended to
  - Don't open email attachments from people or companies you don't know
- *(Non-experts only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- What is your gender? *(multiple-choice)*
  - Female
  - Male
  - Transgender
  - I prefer not to answer
  - Other
- What is your age? *(multiple-choice)*
  - 18-24 years old

  - 25-34
  - 35-44
  - 45-54
  - 55-64
  - 65 or older
  - I prefer not to answer
- What is the highest degree or level of school that you have completed? *(multiple-choice)*
  - Professional doctorate (for example, MD, JD, DDS, DVM, LLB)
  - Doctoral degree (for example, PhD, EdD)
  - Masters degree (for example, MS, MBA, MEng, MA, MEd, MSW)
  - Bachelors degree (for example, BS, BA)
  - Associates degree (for example, AS, AA)
  - Some college, no degree
  - Technical/Trade school
  - Regular high school diploma
  - GED or alternative credential
  - Some high school
  - I prefer not to answer
  - Other
- *(Experts only)* How many total years of experience do you have in computer security? *(multiple-choice)*
  - At least 1 but less than 5 years
  - At least 5 but less than 10 years
  - At least 10 but less than 15 years
  - 15 years or more
  - None
- *(Experts only)* What is your current job role? For example, Network Security Engineer, Penetration Tester *(open-ended)*
  - Researcher
  - Principal Architect
  - IT Strategist
  - CEO
  - Manager
  - Security Engineer
  - Engineer
  - Other
- *(Experts only)* Which of the following best characterizes your workplace? *(multiple-choice)*
  - University
  - Corporate research lab
  - Industry
  - Government
  - Self-employed
  - Other
- *(Experts only)* In what country do you work? *(multiple-choice)*
  - Australia
  - Canada
  - Germany
  - India
  - United Kingdom
  - United States
  - Other
- *(Experts only)* In what state do you work? *(open-choice)*
- *(Non-experts only)* Which describes your current employment status? *(multiple-choice)*
  - Employed full-time
  - Employed part-time

  - Self-employed
  - Care-provider
  - Homemaker
  - Retired
  - Student - Undergraduate
  - Student - Masters
  - Student - Doctoral
  - Looking for work / Unemployed
  - Other
- *(Non-experts only)* What is your occupation? *(open-ended)*
- *(Non-experts only)* What is your Mechanical Turk Worker ID? *(open-ended)*
- (Optional) Is there anything else you'd like to add or clarify? *(open-ended)*