Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice

Karoline Busse and Julia Schäfer, *University of Bonn;*
Matthew Smith, *University of Bonn/Fraunhofer FKIE*

https://www.usenix.org/conference/soups2019/presentation/busse

This paper is included in the Proceedings of the
Fifteenth Symposium on Usable Privacy and Security.
August 12–13, 2019 • Santa Clara, CA, USA

ISBN 978-1-939133-05-2

Replication: No One Can Hack My Mind
Revisiting a Study on Expert and Non-Expert Security Practices and Advice

Karoline Busse
University of Bonn
busse@cs.uni-bonn.de

Julia Schäfer
Univeristy of Bonn
s6juscha@gmail.com

Matthew Smith
University of Bonn / Fraunhofer FKIE
smith@cs.uni-bonn.de

Abstract

A 2015 study by Iulia Ion, Rob Reeder, and Sunny Consolvo examined the self-reported security behavior of security experts and non-experts. They also analyzed what kind of security advice experts gave to non-experts and how realistic and effective they think typical advice is.

Now, roughly four years later, we aimed to replicate and extend this study with a similar set of non-experts and a different set of experts. For the non-experts, we recruited 288 MTurk participants, just as Ion et al. did. We also recruited 75 mostly European security experts, in contrast to the mostly US sample from Ion et al. Our findings show that despite the different samples and the four years that have passed, the most common pieces of expert advice are mostly unchanged, with one notable exception. In addition, we did see a fair amount of fluctuation in the long tail of advice. Non-expert self-reported behavior, however, is unchanged, meaning that the gap between experts and non-experts seen in Ion et al.'s work is still just as prominent in our study. To extend the work, we also conducted an A/B study to get a better understanding of one of the key questions concerning experts' recommendations, and we identified types of advice where research by the usable security community is most sorely needed.

1 Introduction

Whenever the media picks up on the latest data breach, various sources seize the opportunity to give advice such as "Do not use the same passwords for all systems" [9] or "Antivirus software is crucial to protecting your computer." [23] Under this barrage of different advice, selecting and following "good" advice is a difficult task for users [10]. Factors such as socioeconomic status, consumer habits, or conveniences also play a role in the decision-making process [24, 26]. Even when advice is regarded as "good" by a user, it is not necessarily a given that they know how to apply it in their own individual context. We must not overlook the limits of users' capability taking into account the complexity of any advice we give [5].

In 2015, Ion, Reeder, and Consolvo explored the opinions and beliefs of expert and non-expert users in a survey study and found that users neglect three vital security practices that experts strongly advise: installing software updates, using two-factor authentication, and using a password manager. On the other side, non-experts regarded antivirus software as a very important security practice, unlike the experts, who were not convinced by it. Almost four years have passed since that study, which is a long period of time in terms of technological innovation and security practices. Security and privacy continue to gain more widespread recognition, so we were interested to see what, if anything, had changed with respect to expert advice and non-expert self-reported behavior.

We thus conducted two online surveys, one for experts and one for non-experts, and compared the results to the previous study by Ion et al. Many of the past security topics and advice covered in the original work are still relevant today. We also discovered that some of the topics relevant to users in the past have been replaced by newer topics, for example, the spread of blocking extensions for web browsers, which are able to manage cookies. Where in the past, users were concerned with regularly deleting cookies, they now rely on blocking extensions.

Apart from seeing if and how our sample differed from the original, we wanted to explore a methodological issue in the original study. One of the central parts of the original study concerned how effective *and* realistic particular types of advice are. This information from experts was gathered using compound questions, and the advice was ranked and compared on that basis. Compound questions can be problematic because it is not clear how participants combine the separate

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

components [4]. For example, when asked to rank advice on a five-point scale, a 3 could mean an expert thought that a piece of advice was extremely effective (5) but completely unrealistic (1), or vice versa, and the expert combined the two values into a simple average. However, a 3 could also be given because the expert thought the piece of advice was a 3 regarding realism and a 3 in effectiveness. To make matters worse, the same separate assessment from above (extremely effective (5) but completely unrealistic (1)) could also be combined by the expert into a 1 if the expert takes the view that if a piece of advice is unrealistic, then the combined effectiveness is also a 1 . So the same separate assessments can lead to very different combined scores and separate results from the same assessments can lead to very different combined scores.

While the combined score is useful because it reflects the personal assessment of an expert participant using whatever weighted combination they deem most appropriate, it potentially hides interesting discrepancies that could highlight which pieces of advice could be particularly important for researchers to improve and, more specifically, which areas need improvement. For example, a piece of advice that gets a 5 for effectiveness but a 1 for realism is probably a good candidate for researchers to improve the usability. On the other hand, a 4 on realism and a 2 on effectiveness could indicate that systems research is needed to improve effectiveness or it might be best if the advice is discouraged, since it uses up valuable security budget without being particularly effective. To be able to compare our data directly with the original work by Ion et al., in addition to gaining the insights described above, we gave half our expert participants the original compound questions and half the experts got the questions broken down into their compound elements.

Based on our analysis, we suggest four fields where usable security research is needed to improve existing methods or invent new ways of handling the implied security issues. The areas are: password security, two-factor authentication, links and attachments, as well as application updates. Out of these four fields, three were already prominently discussed in the original work, suggesting that the research and engineering communities in usable security still have a lot of work to do.

The remainder of this paper is structured as follows: Section 2 gives an overview of relevant work regarding security and privacy advice, as well as an in-depth look at the original study by Ion et al. Section 3 documents our survey methodology for both the expert and non-expert surveys and discusses the design changes we made. In Section 4, we present our replication results and compare them to the original work. The discussion of results, replication efforts, design changes, and fields of action follows in Section 5. We conclude by outlining the limitations of our study (Section 6) and summarizing our work's contributions in Section 7.

2 Related Work

In 2008, MacGeorge et al. proposed that for recipients to follow good advice, it should: be useful, comprehensible, and relevant; be effective at addressing the problem; be likely to be accomplished by the recipient; and not possess too many limitations and drawbacks. When giving advice, experts should make sure that the advice is solicited by the recipient, they only give advice if they are a qualified source on the topic; they consider the recipient's point of view; and they exercise sensitivity in phrasing and formulation [20].

Redmiles et al. researched which kinds of advice users adopted and which they rejected. They found that IT professionals, the workplace environment, and negative events, whether personally experienced or told by news media, are users' main sources of digital security advice [26]. As a result of being unable to evaluate the content of a piece of advice, users tend to wager the acceptance of advice based on the trustworthiness of the source. Rejection of advice is influenced by many factors, such as believing that the responsibility for security lies with someone else, perceiving that the advice contains too much marketing material, or believing that the advice might threaten the user's privacy.

In a follow-up US-representative survey on security advice and trusted sources in 2016, Redmiles et al. identified a digital security divide along lines of the socioeconomic status of participants. Wealthier people tended to have better skills and acquired advice from the workplace, while disadvantaged users relied on family and friends for advice [24].

A Pew Research study by Lenhart et al. investigated where teens between the ages of 12 and 17 get their privacy advice from [17]. A focus group study revealed that teens mainly research and iterate through privacy settings on their own, while a follow-up survey suggests that they also relied on personal advice from friends, parents, or siblings. In general, younger teens relied more on interpersonal advice, while older teens tried to figure things out for themselves.

Harbach et al. explicated in a 2014 survey that risk awareness is often the primary stage for the adoption of security mechanisms and their interactions [13]. While being an essential part of the study of human aspects of security research, it needs to be explored in detail in the context of users' daily lives. A fundamental part of devising usable IT security mechanisms is evaluating which risks and consequences are known to users and, therefore, are already accounted for in their mental budget of coping with security behaviors.

Wash researched so-called *folk models* of home computer users, conducting a series of interviews to identify common models about security threats, namely hackers and viruses. After identifying four virus and four hacker models, Wash set them in relation to popular security advice and suggested which type of user would react in what fashion to each individual piece of advice. This gives a possible explanation for why users do not follow security advice given by experts [34].

Fagan and Khan further investigated why some users follow advice and others do not. They conducted a survey study where they asked participants about their motivations regarding (not) updating, using a password manager, using two-factor authentication, and changing passwords frequently. The authors determined that following security advice was mainly a trade-off decision between convenience and security, where users actively considered features such as set-up time and weighed that against the potential security benefits [10].

2.1 The Original Study

In 2015, Iulia Ion, Rob Reeder, and Sunny Consolvo presented their survey-based study on the differences and similarities in online security-related behavior of expert and non-expert users [15]. They developed a four-part survey asking about top security advice and the respondent's own security and privacy habits, as well as asking respondents to rate pre-formulated advice statements for their effectiveness and practicability.

The two surveys that make up the core of their study are based on data gathered by conducting semi-structured interviews with 40 security experts at the 2013 BlackHat, DefCon, and USENIX security conferences.

The expert survey, crafted from the information gathered in the preliminary interviews at security conferences, was conducted from February to April 2014. A minimum of 5 years of work experience in a security-related field was required to be counted as an "expert." Participants were recruited through a post on the Google Online Security Blog [28] and social media. The survey first asked participants to enter three pieces of advice for non tech-savvy users and the three things the participants do themselves to protect their security online. The second part consisted of multiple-choice questions inquiring on certain security-related behaviors and practices. The main part asked the participants to rate pieces of advice directed at non-tech-savvy users. Experts were then asked to rate each piece of advice with regard to both the advice's effect on security and the probability that the user would follow the advice. The survey closed with demographic questions. 231 participants met the criteria for being an expert of working or studying in a security-related field for at least five years.

The non-expert survey was conducted with 294 US-based participants recruited via Amazon Mechanical Turk (MTurk).

The results showed that experts and non-experts followed different approaches to protecting their security online, with the practice of using strong passwords being the only commonality for both groups, ranking in the top 5 responses to the question about the respondents' personal top three security practices (cf. Figure 1). The security practices mentioned by experts were consistent with the experts' ratings of different pieces of advice. These pieces of advice were grouped into four categories: *software updates*, *antivirus software*, *password management*, and *mindfulness*. The security practices utilized by the non-experts received mixed ratings from the experts. Some non-expert practices were considered by the experts to be a good practice, like installing antivirus software and using strong passwords. However, the non-experts' failure to comply with some practices were considered bad habits by the experts, including failure to delete cookies and failure to visit only known websites, among others.

The authors found three security practices that experts followed and recommended that were not employed by the non-experts (see Figure 3), namely installing system updates, using a password manager, and using two-factor authentication, which were considered most important by a majority of the experts. Their results suggest that a combination of better communication and improvements in the systems and their usability were necessary to get non-experts to adhere to these three security practices.

3 Methodology

The authors of the original study shared their study materials with us so that we could recreate the surveys as precisely as possible. They also shared the data shown in Figure 1 from their original paper; however, the raw data could not be shared.

The questionnaire featured mostly closed questions that allowed participants to enter free-text data in an "other" answer option. The questions on the practicability of advice with featured the compound design in the original study were 5 point Likert-scale item batteries with optional free text comment fields in between. Our split-question design thus increased the number of questions for participants who answered our modified survey.

The full questionnaires can be found in the appendix A. In total we had three different questionnaires: the expert and end-user questionnaires from the original study and our modified expert questionnaire which separated the compound questions. All questionnaires as well as the pre-study interviews started by getting informed consent. Audio recordings were made in the pre-study with participant consent and then stored on encrypted storage and deleted after evaluation. In compliance with the EU-GDPR, we did not store any personal identifying data such as IP addresses for any online survey.

The responses to the open-ended questions regarding the top three pieces of security advice and the top three personal security practices of experts were coded by two of the authors. First, both researchers coded the results independently and then codes were compared and differences were discussed. Since the coding was straight-forward, full agreement on the codes was reached.

3.1 End User Survey

We replicated the end user survey with the same MTurk recruitment criteria as the original authors used: Participants were required to be from the United States, have a task approval rate of 95% or better and have completed at least 500 tasks. For the sake of replication, we advertised the study with the original payment of 1$, but for fairness reasons we awarded an additional 2$ through MTurk's worker bonus system after the study was concluded. The study was conducted in May 2018.

3.2 Expert Interviews and Survey

Based on the expert survey from Ion et al., we conducted 40 interviews with IT security experts at the CeBIT international trade fair on information technology in 2018. Our goal was to evaluate the survey design and gather first impressions for the experts group.

During the course of the interviews, it became clear that the compound question regarding the evaluation of advice[1] led to confusion and insecurities in participants. They often misinterpreted or morphed the question's phrasing after rating a couple of items, leading to decreased comparability of results.

We discussed this finding and the problem of compound questions with the authors of the original study. They chose the compound question due to time constraints. Their pretesting suggested that the length of the survey had to be limited and thus this compromise was made. Also, they were mainly interested in what the experts' overall assessment of advice was and thus the separate components were not as relevant for their work.

Nonetheless, compound questions can be tricky to interpret and important nuances can be lost. In particular, we thought it would be valuable to see if there are any pieces of advice where effectiveness and realism diverge, since these could highlight areas of improvement.

To this end, we separated the compound rating tasks for advice effectiveness and realism. Since this is a divergence from the replication, we assigned half the participants to this survey and the other half completed the original survey with the compound questions. We chose a between-groups design over a within-groups one because we wanted to limit fatigue effects, as the survey was already rather long and repetitive. In addition, we randomized the order of appearance of individual advice items within the 5-piece rating blocks for both groups (see Appendix A) to minimize cross-influencing effects between advice items.

The original survey was advertised with a blog posting on the Google Online Security Blog [28]. Despite the support of the original authors, it was not possible to recruit developers the same way.

So instead we recruited experts through social media and mailing lists. We announced the survey link with a short advertising statement on Twitter[2] , asked selected professional contacts (e.g., the original authors) to repost or share the advertising; and also announced the study, together with a link to the tweet, on a hacking and security community mailing list. All in all, the tweet was retweeted 28 times and received 5,540 impressions, according to Twitter's analytics tool. In addition, the survey link was shared in the following reddit communities: r/Defcon, r/cybersecurity, r/netsecstudents, r/netsec, r/sysadmin, r/SampleSize, r/computerscience, r/information_Security, r/privacy.

4 Results

Of the 300 end user surveys that were completed, 12 participants got more than one of three quality assurance questions wrong and were, therefore, excluded from further analysis. This is the same procedure used in the original work. Our final sample thus consisted of 288 participants.

The collected demographic data is displayed in Table 1. The sample contained 48% female participants and was relatively young, with almost 80% of participants being younger than 45 years old. A little more than half have at least a bachelor's degree, and the majority, at 66%, reported an employment status of full-time employee. In comparison, the original study's sample had 40% female respondents, and 88% of the participants were younger than 45 years old. In the original study, 47% of the participants held a bachelor's degree or higher. In the original study, 47% of participants were from the US, data for EU-located participants was not given. In our sample, 70.4% of participants were from the EU and 26.8% were from the US.

The expert survey was conducted between June and November 2018. We recruited 75 expert participants online using our A/B testing design, 44 expert participants for survey form A (with compound questions), and 31 participants for survey form B (without compound questions). Participants were allowed one mistake regarding the three attention checks in the survey, as was done in the original study. We also excluded one participant who clearly gave nonsensical answers.

One prominent difference between our expert sample and the original expert sample is that our experts had less experience. The original study required experts to have at least five years of work or study experience in IT security or a related field. Only 59 participants fulfilled this requirement in our set, so we lowered this requirement to one year. We will discuss this in more detail in the limitations section.

---

[1] "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."

[2] "Dear #security experts, I'm conducting a study about security advice targeted at non-technical users and need your help. Please participate in this 10-Minute survey: https://studyportal-bonn.de I appreciate RTs and (cross-platform) shares. Questions? DM or busse@cs.uni-bonn.de" (`https://twitter.com/kb_usec/status/1047080662312898560`)

Item	NE		E	
Female	137	47.6%	7	9.3%
Male	150	52.1%	59	78.7%
Transgender	1	0.4%	2	2.7%
No Answer	0	0%	7	9.3%
18 - 24	25	8.7%	3	4%
25 - 34	130	45.1%	30	40%
35 - 44	72	25%	26	34.7%
45 - 54	39	13.5%	9	12%
55 - 64	16	5.6%	2	2.7%
65 or older	6	2.1%	0	0%
No answer	0	0%	5	6.7%
Professional Doctorate	5	1.7%	3	4%
Doctoral Degree	3	1%	6	8%
Master	28	9.7%	29	38.7%
Bachelor	114	39.6%	18	24%
Associates Degree	38	13.2%	3	4%
Some college, no degree	45	15.6%	4	5.3%
Technical/Trade School	13	4.51%	2	2.7%
Regular HS Diploma	32	11.11%	0	0%
GED or alternative	5	1.74%	0	0%
Some high school	2	0.69%	0	0%
Other	0	0%	4	5.3%
No answer	3	1.04%	6	8%
Employed full-time	190	65.97%		
Employed part-time	26	28.26%		
Self-employed	36	12.50%		
Homemaker	16	5.56%		
Retired	6	2.08%		
Student - Undergrad	6	2.08%		
Student - Doctoral	2	0.69%		
Looking for work	9	3.13%		
Other	2	0.69%		
Industry			38	50.7%
University			16	21.3%
Corporate research lab			7	9.3%
Government			1	1.3%
Self-employed			2	2.7%
Other			9	2.7%
No answer			2	2.7%
1-5 years of security exp.			16	21.3%
5-10 years of sec. exp.			18	24.0%
10-15 years of sec. exp.			20	26.7%
15+ years of sec. exp.			21	28.0%

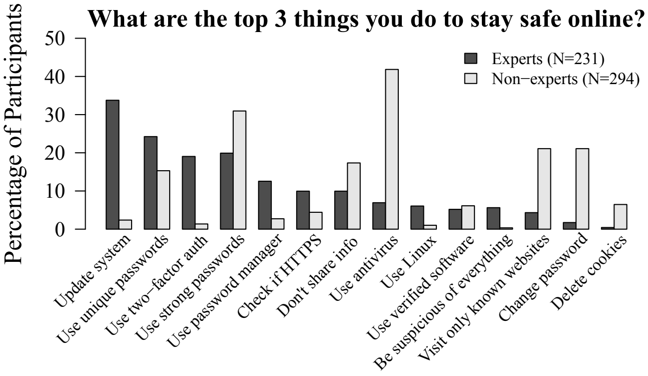
Table 1: Demographic information for expert (E, $n = 75$) and non-expert (NE, $n = 288$) survey participants.

The p values we report refer to chi-squared tests or, where not enough data in all categories was available, Fisher's exact test. Dependent on the original authors' approach, we applied the Holm–Bonferroni correction in R for all the tests conducted. To further illustrate our results, we utilized participants' comments provided by the optional clarification questions and "other, please specify" options of the survey.

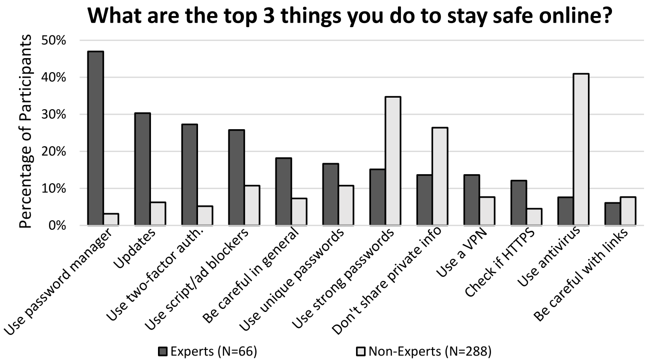
4.1 Differences between Experts and Non-Experts

For this section, we focus on experts and non-experts to follow the approach of the original work. Experts A and B were combined in behavior-related questions since these questions were identical, but split when advice rating was considered.

The first question asked about the top three things participants do to protect their security online. The comparison of the answers is displayed in Figure 1. In accordance with the original work, we only considered items mentioned by at least 5% of the participants in each group.



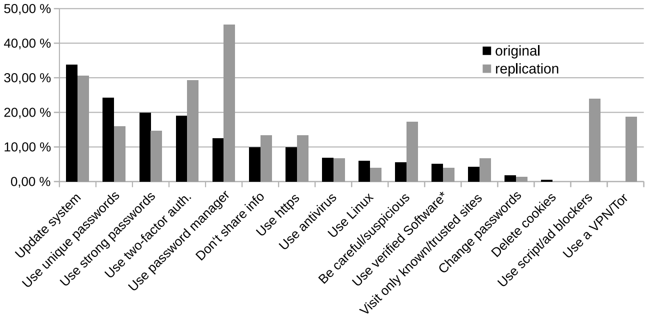
(a) original study



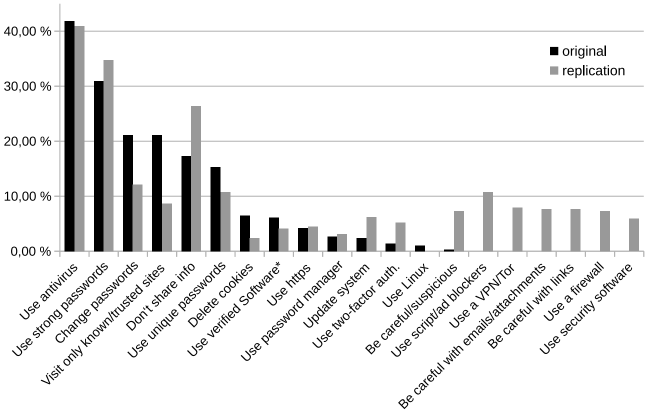
(b) replication study

Figure 1: Security measures mentioned by at least 5% of each group

While most experts rely on a password manager (45%) and updates (31%) as well as two-factor authentication (29%) to stay safe, non-experts count on the usage of antivirus software



(a) Expert Comparison



(b) Non-Expert Comparison

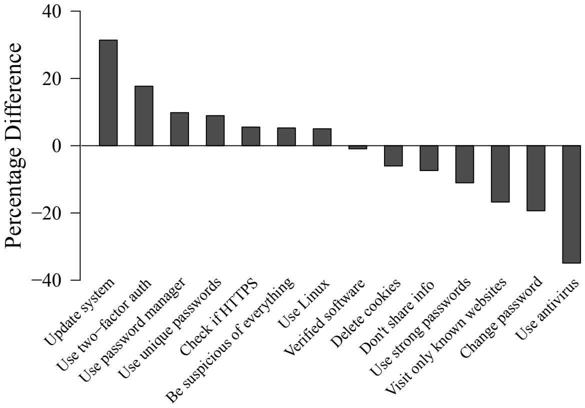
Figure 2: Answer comparison for the question "What are the top 3 things you do to stay safe online?" between the original study and our replication. Missing values for original data were mentioned by less than five percent of expert participants. (*) We aligned the original authors' code with our code "be careful with downloads".

(41%), strong passwords (35%), and not sharing personal information (26%).

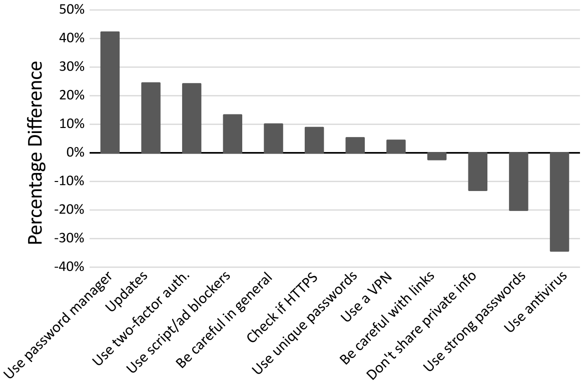
In comparison with the original study, the most common security practice mentioned by experts has shifted. Instead of updating regularly, the use of a password manager was now the most frequently mentioned habit among our experts. The use of unique passwords, which was the original study's second most common practice, ranked sixth in our sample. Since the use of password managers usually includes the use of unique passwords, these two are linked. The adoption of two-factor authentication was unchanged, in position three.

Overall, there were four new practices frequently mentioned: using ad and/or script blockers, being careful in general as well as when following links, and using VPNs. In contrast, the once common practices of using Linux, using verified software, changing passwords regularly, and manually deleting cookies were not present in our sample. The replacement of "carefulness" with "practicing suspicion," however, might have been a product of different coding approaches.

The percentage differences between the groups of experts



(a) original study



(b) replication study

Figure 3: Percentage difference of security practices mentioned by experts and non-experts as answer to the "things-you-do" question. Security measures with a positive percentage difference were mentioned more by experts than non-experts; a negative percentage difference indicates topics mentioned more by non-experts.

and non-experts are displayed in Figure 3. The practices mentioned least by non-experts relative to experts were: (1) use a password manager (42%), (2) keep your system up-to-date (24%), and (3) use two-factor authentication (24%). While the rankings of these three pieces of advice have shifted a bit (password managers climbed from difference position three to one), we still see the same overall trend as in 2014.

4.1.1 Software and OS Updates

As in the original study, we differentiated between operating system and application updates. In the question block about behavior with personal devices, we asked "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?" We saw that exactly half of all experts as well as non-experts reported installing their updates either *automatically* or *immediately* after they become available (cf.

Reported Behavior	χ^2	p
How soon do you install updates?	7.95	< 0.001
Do you use antivirus software?	77.43	< 0.001
Do you use two-factor authentication?	23.41	< 0.001
Do you remember your passwords?	35.43	< 0.001
Do you write down your passwords?	20.03	< 0.001
Do you save your passwords in a file?	1.79	0.651
Do you use a password manager?	55.59	< 0.001
Do you reuse passwords?	21.43	< 0.001
Do you look at the URL bar?	22.28	0.001
Do you check if HTTPS?	5.48	< 0.001
Do you visit websites you haven't heard of?	48.16	< 0.001
Do you enter your PW on links in emails?	63.95	< 0.001
Do you open emails from unknown?	91.67	< 0.001
Do you click on links from unknown?	16.52	0.013

Table 2: Comparing expert and non-expert reports on their security behavior. $N_e = 74, N_n = 282$ for the first two questions, otherwise $N_e = 75, N_n = 288$. Degrees of Freedom: 4 for the first, 1 for the second and third question, 3 otherwise. Fisher's Exact test instead of Pearson's Chi-Squared was used to calculate p whenever not enough data was available in any category.

Figure 4). However, we can see that if compared to the findings of the original study, where 64% of experts and only 38% of non-experts installed their updates either automatically or immediately, fewer experts but more non-experts are reporting this behavior in our replication. While the numbers are closer together, the differences between the groups are still statistically significant ($\chi^2(4, N_e = 74, N_n = 282) = 7.95, p < 0.001$, cf. Table 2). This could be an artifact of widespread operating systems that employ automatic updates per default, as for example Windows 10 does.

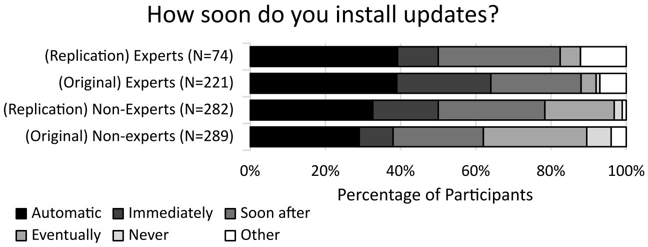


Figure 4: Answer distributions for the question "How soon after you discover that a new version of your operating system (OS) software is available do you (or somebody else managing your computer) install it? Examples of operating systems include Windows, Mac OS, and Linux.".

Among the pieces of advice, we had the statements "turn on automatic updates," "install OS updates," and "update applications." In all three cases of update-related advice, less than 50% of non-experts rated the advice very effective, yet around 60% said they were very likely to follow it. Especially for the advice regarding application updates, we found a strong discrepancy within our A/B testing setup. More about this is reported in Section 4.2

4.1.2 Antivirus and Protection Software

Using antivirus software is still the security practice with the biggest difference in number of mentions between end users and experts (cf. Figure 3). As Figure 1 illustrates, 41% of non-experts and only 7% of experts stated that using antivirus software is one of the top three things they do to protect their security online. This coincides with the findings of the multiple-choice questions on security-related behavior in the second part of the survey, where twice as many non-experts as experts ($E = 82\%$ vs. $NE = 41\%$) reported using antivirus software on their personal computers. As shown in Table 2, this difference is statistically significant ($\chi^2(1, N_e = 74, N_n = 282) = 77.43, p < 0.001$).

Several experts stated that the perceived usefulness of antivirus software might be higher than the actual usefulness. One expert stated, "*I think antivirus software creates more problems than it solves (including the feeling of being safe).*" Some experts strongly suggested caution when dealing with antivirus software. One expert participant commented, "*Antivirus software often is snake-oil and detects only old viruses, but prevents users from these viruses. Also, they often implement suspicious features like breaking https without being clear to the end user about it.*"

Non-experts were asked to use a five-point Likert scale to rate how effective they see the security advice of using antivirus software: 63% rated it *very effective* and 19% rated it *effective*.

When asked how likely they would be to follow this advice if they heard that using antivirus software was effective, 73% of non-experts said they would be *very likely* to follow this advice, and 9% said they *likely* would. This strong acceptance of antivirus software is mirrored by the comments and feedback provided by non-experts.

A new type of security advice that emerged in the things-you-do question was the use of ad and/or script blockers. A proportion of 24% of experts and 11% of non-experts mentioned this security practice as one of their personal top three (cf. Figure 1).

4.1.3 Password Management

In many cases, both experts and non-experts cited password-related practices as an answer to the question "What are the top three things you do to protect your security online?" Using strong and unique passwords were frequently mentioned strategies by both groups. Where experts spoke more of having unique passwords than non-experts ($E = 16\%$ vs. $NE = 11\%$), using strong passwords was reported twice as often by non-experts than experts ($NE = 35\%$ vs. $E = 15\%$). While the practice of having unique passwords was mentioned less frequently than in the original data set (cf. Figure 2), having strong passwords was slightly less frequently mentioned by experts (then 20%, now 15%), but slightly more frequently mentioned by non-experts (then 31%, now 35%).

Similarly, experts named using a password manager substantially more often than non-experts ($E = 45\%$ vs. $NE = 3\%$), but almost did not mention changing passwords frequently (1% experts vs. 12% non-experts). Changing passwords is still not very prominent for experts (then 2%, now 1%), and has decreased in mentions by non-experts, as well (then 21%, now 15%; cf. Figure 2).

Likewise, experts mentioned the use of two-factor authentication more than five times as much as non-experts ($E = 29\%$ vs. $NE = 5\%$). This practice has gained in prominence for both experts (then 19%, now 29%) and non-experts (then 1%, now 5%). This could be partially attributed to the fact that more services now offer two-factor authentication than in 2014.

The most common answer of experts to the things-you-do question was "using a password manager" ($E = 45\%$), in contrast to a very small group of non-experts ($NE = 3\%$). In comparison with the original study, the mention of password managers by experts had more than tripled, from 13% to 45%. This difference is in line with the fact that twice as many experts as non-experts reported using a password manager for at least some of their accounts ($E = 83\%$ vs. $NE = 40\%$, $\chi^2(3, N_e = 75, N_n = 288) = 55.60$, $p < 0.001$). One expert commented, *"Using a proper password manager is the best solution. In the end, it is about using different passwords for different accounts."*

Writing down passwords was seen by some experts as a user-friendly compromise to a password manager. One expert said, *"[The advice to use] different passwords is effective, but can be difficult for users if they don't use a password manager. Writing passwords down isn't really bad, as long as the paper is kept secure. This is basically just an offline password manager."*

While the advice to "write down passwords on paper" and "save passwords in a file" were rated poorly by non-experts for both effectiveness and the likelihood that they would follow the advice if they heard it was secure, especially the practice of writing down passwords on paper, was rather common among our participants. As can be seen in Figure 5, 45% of non-experts reported writing down passwords for at least some of their accounts (vs. 33% of experts, $\chi^2(3, N_e = 75, N_n = 288) = 20.02$, $p < 0.001$). Almost all experts commented on the importance of storing the paper securely.

Also shown in Figure 5, six times more non-experts than experts remember all of their passwords (36% non-experts vs. 5% experts, $\chi^2(3, N_e = 75, N_n = 288) = 35.42$, $p < 0.001$). These numbers have decreased in comparison to the original study, where 17% of experts and 52% of non-experts cited being able to remember all of their passwords.

In addition, seven times more non-experts than experts stated that they reuse passwords for most or all of their accounts (23% of non-experts vs. 3% of experts, $\chi^2(3, N_e = 75, N_n = 288) = 21.43$, $p < 0.001$). While the proportion of end users who employ this practice rose slightly in comparison with the original study (19%), the rate among experts stayed about the same (3%).

4.1.4 Mindfulness

Among the remaining pieces of advice, the ones about checking the URL bar when browsing and looking for HTTPS connections are most interesting in comparison to the original study, since there have been major changes in the SSL/TLS certificate ecosystem within the last few years.

The rise of Let's Encrypt and automated certificate issuance and renewal have greatly increased the level of TLS-encrypted web traffic [2]. In consequence, HTTPS has become more widespread, but the indication about whether a site should be trusted because it features HTTPS has been weakened, since even phishing websites often come with security certificates [33].

When asked about the advice to check if the website they're visiting uses HTTPS, 54% of non-experts rated it very effective, and 61% considered themselves very likely to follow that advice. In comparison, the original data featured a proportion of 60% of non-experts rating this advice as *very effective*, and 50% saying they would likely follow it.

To put this in context, we asked all participants whether they practice checking for HTTPS while surfing. The portion of experts who *often* do so decreased from 82% in the original study to 73% in our replication. The portion of non-experts increased from 36% in the original study to 47% in our replication.

Regarding the more general question about checking the URL bar when visiting a website, 76% of experts and 60% of non-experts said they often look at the URL bar (original study: 86% and 59%). Some experts emphasized that it is not only important to look at the URL bar, but also to be aware of the specific information it displays. For example, one expert said, *"Watch out for correct URLs, valid SSL certificates, and enabled encryption (HTTPS) if sensitive information is requested."*

The question whether a participant enters their passwords on websites after they click on a link in an email is the only behavior question for which the chi-squared test for expert and non-expert answers yielded a different result than in the original study. While Ion et al. found no significant difference between the groups, our samples showed a large effect size ($\chi^2(3, N_e = 75, N_n = 288) = 63.95$, $p < 0.001$). This results from a large proportion of expert users choosing the *Other* option to further explain their behavior in that case. While some experts stated in the comments that they generally do

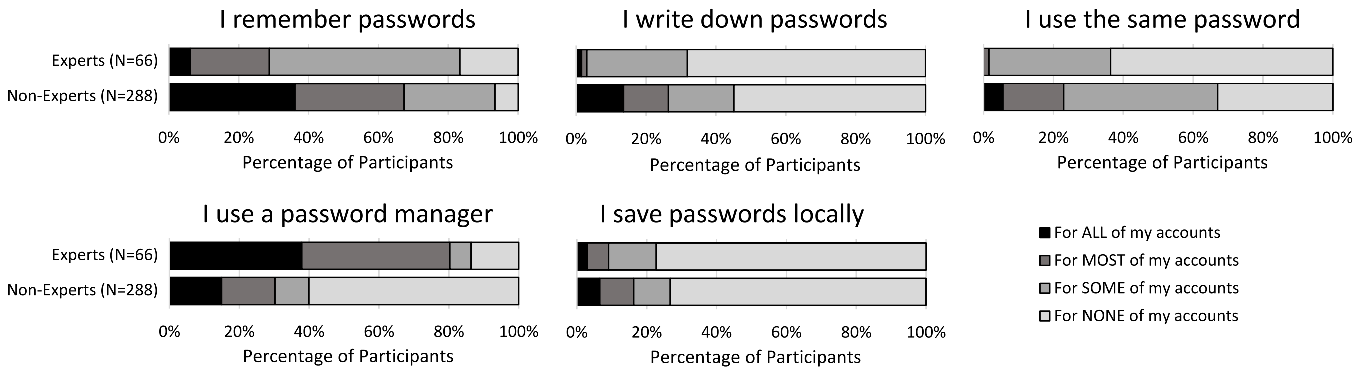


Figure 5: Non-expert habits regarding password management from our replication study.

not click on links in emails, another proportion of experts further differentiated, making comments such as, "*It depends. Am I expecting that email, is it from a reputable source, and does the URL match what I expect? Then yes; otherwise no.*" When excluding the *Other* option, the test results align again with the original study ($p = 0.63$ after correction).

4.2 Compound Question Results

As described in section 3.2, half the experts received the original survey with the compound questions (Group A) and for the other half we split up the goodness rating into effectiveness and realism (Group B). In the following, we compared the ratings of the split questions to those of the original compound questions.

In Figure 6, we look at the distribution of ratings given by experts A and B. Some pieces of advice, like installing OS updates, were rated very "effective" as well as very "realistic" by both expert groups. In the following, we will focus on the cases in which a piece of advice did not receive high scores in all cases, especially in terms of realism.

For example, not opening email attachments from unknown senders was rated positive in terms of goodness and effectiveness by experts A and experts B (64% *very good* and 16% *good* and 58% *very effective* and 35% *effective, respectively*). However, the *realistic* rating given by experts B peaks at a Likert score of 3, with 35%. Only 19% of experts B said this advice was very *realistic*, and 6% said it is *not realistic at all* (cf. Figure 7).

A piece of advice was classified as *good* and *effective* if a rating of 4 or better was present. We are most interested in those cases where this condition was met as well as having a realism rating of less than 4. As depicted in Table 3, this applies for eight pieces of advice.

We can group these pieces of advice in four categories.

Using unique and strong passwords as well as using a password manager all relate to *Password Security*. The advice to adopt *Two-Factor Authentication* stands on its own. Being suspicious of links, not entering passwords after having clicked on a link in an email, and not opening attachments can be grouped as *Links and Attachments*. The last piece of (controversial) advice, *Updating Applications* regularly, again stands on its own.

5 Discussion

In the following, we will discuss the popularity of selected findings and advice.

5.1 Advice Rating

While in the original study, the advice to regularly update showed the greatest difference between expert recommendations and non-expert usage, we found that using a password manager is now the piece of advice with the biggest gap between experts and end-users. Microsoft's shift toward mandatory automatic updates in Windows 10 might be the cause of this change. Because the operating system now takes care of keeping the system up to date, and thus secure, experts might not regard this advice to be as urgent as they did four years ago [22].

Password managers have the potential to solve the usability issue of passwords. Additionally, password managers might be a currently trending topic, which is reflected in the popularity of this practice as the single most frequently suggested piece of security behavior reported by experts (cf. Figure 1).

Installing and using antivirus software was the most frequently cited security measure by non-expert users in both the original study and our study. While antivirus software doesn't offer reliable protection against new and modified types of malware, the presence in advertising, as well as easy setup procedures, might have led to its unbroken popularity.

The advice to not share private information has become more important to both expert and non-expert users. However, one could argue that unconsciously shared information might, indeed, be more dangerous for users, whether it is conversation metadata [18, 31], tracking networks [1], or behavioral data like smartphone usage habits [19].

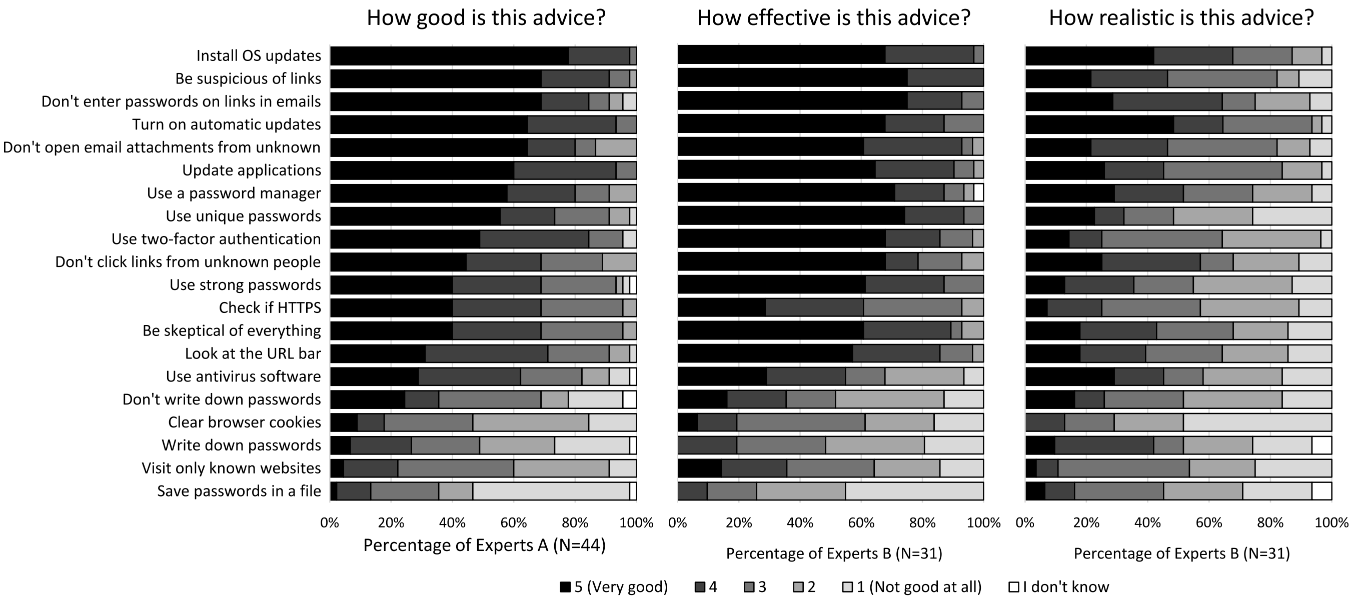


Figure 6: Side-by-side comparison of rating distributions in our replication study, showing from left to right: goodness ratings by experts A, efficiency ratings by experts B and realism ratings by experts B. The twenty pieces of advice are sorted by goodness ratings.

Advice	δ_μ	μ_e	μ_r	σ_e	σ_r	δ_m	m_e	m_r
Use unique passwords	1.90	4.68	2.77	0.60	1.52	3	5	2
Use strong passwords	1.58	4.48	2.90	0.72	1.27	2	5	3
Use two-factor authentication	1.55	4.52	2.97	0.81	1.19	2	5	3
Be suspicious of links	1.35	4.71	3.35	0.46	1.28	2	5	3
Use a password manager	1.16	4.6	3.48	0.77	1.29	1	5	4
Don’t open email attachments	1.16	4.48	3.32	0.72	1.17	2	5	3
Don’t enter PW on links in emails	1.13	4.68	3.55	0.60	1.34	1	5	4
Update applications	1	4.51	3.52	0.77	1.12	2	5	3

Table 3: Pieces of advice that were received a mean effectiveness rating (μ_e) of at least 4, and a mean realism rating (μ_r) of less than 4, ordered by decreasing difference δ_μ. Also shown are standard deviations for effectiveness and realism ratings as well as medians and their difference.

5.2 New Advice

When looking at the free text answers for personal top three security practices, we found four new items within the top 18 most frequently mentioned statements: using script and/or ad blockers, being careful when online, using a VPN, and being careful when interacting with links (cf. Figure 1). In addition, five additional practices made it just beyond the 5% threshold: only visiting known or trusted websites, using incognito browsing, employing virtual machines, compartmentalizing systems for different tasks or levels of security, using a firewall, and employing security software in general. For the sake of brevity, we excluded these five practices from our further discussion.

While the more general advice of being careful might have arisen from different coding approaches between the original study and our replication, the other two pieces of advice suggest new developments.

Internet advertising has become more aggressive, invasive, and risky over the last few years [6], and blocking extensions are a powerful tool to combat this. In addition to the rise of this security practice, which 24% of the expert participants and 11% of the non-experts employ, the practice of manually deleting cookies was not included in the list anymore. This might be a replacement process, since many blocking tools also go after tracking cookies.

Using a VPN was a common response to the things-you-do question, but unfortunately, none of our participants elaborated on the meaning of this short statement. It is unclear exactly what kind of VPN participants were referring to. Just as Ferguson and Huston discovered two decades ago, “*VPN*

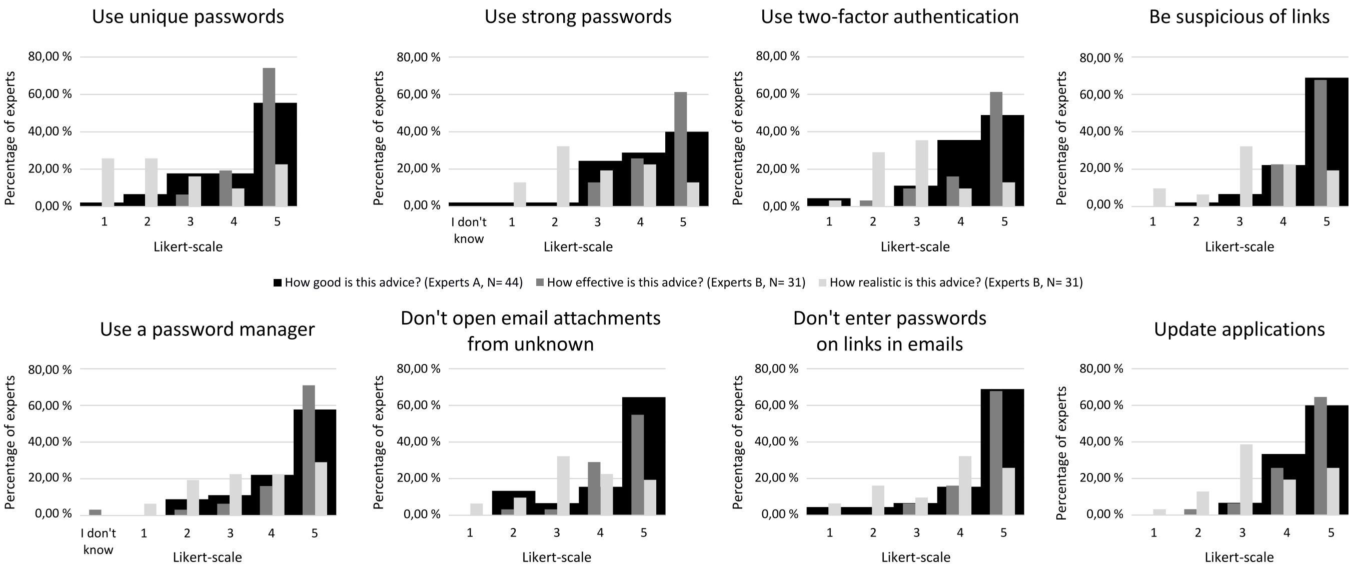


Figure 7: A/B comparison of advice rating from our replication study for pieces of advice identified as effective, but unrealistic. Descriptive statistics can be found in Table 3.

[has been and still is an almost] *recklessly used*" [12] collective term to describe various technologies and applications. VPNs and onion routing services such as Tor are effective tools for circumventing regional (e.g., governmental) censorship or content restrictions. However, using a VPN entails placing trust in its provider, which is a thing that users often overlook [14, 32].

5.3 Fields of Action

The pieces of advice that experts rated as very effective, but not very realistic for a user to follow, highlight areas where more research or better technical solutions are needed (cf. Table 3 and Figure 7). We identified four key fields of action; namely, password security, two-factor authentication, links and attachments, and application updates.

It is striking that these areas of advice are very similar to the advice not followed by users in the original study (cf. Section 2.1): recommending frequent system updates has been replaced with regular application updates, while using a password manager and enabling two-factor authentication have stayed the same.

5.3.1 Password Security

The advice ratings on unique and strong passwords indicate strongly that passwords are still an issue. The fact that the advice about adopting password managers also has a large delta between average effectiveness and realism ratings suggests that password managers are not yet fit for general adoption. Password managers should be approachable, easy to set up, and well-integrated into the operating system, without causing new security risks [8, 11].

However, even among experts, the use of password managers is not without drawbacks. One expert acknowledged a potentially "steep learning curve for non-tech-savvy users," while an end user stated that *"Storing passwords digitally and/or trusting a company to protect your data seems counterproductive."*

5.3.2 Two-Factor Authentication

Aside from the use of password managers, the adoption of two-factor authentication (2FA) is another relatively easy way to greatly increase account security. However, our expert group regarded this advice as not very realistic to be followed, while still acknowledging its effectiveness (cf. Table 3).

In general, more services need to support the setup of a second factor, since approximately 76% of websites do not offer users a full set of 2FA options [16]. Additionally, finding ways to increase user adoption of 2FA for accounts is a task for future research [3].

5.3.3 Links and Attachments

Three statements in our list of controversially rated advice related to links and attachments, specifically, being suspicious of links, not entering passwords on links received in emails, and not opening email attachments.

While the experts might have rated it as not very realistic, since opening attachments and following links is part of daily internet life, the risks arising from well-crafted phishing or malware emails should not to be neglected. A prominent example from recent years is the rise of ransomware, like wannacry [29].

Protecting against these types of threats purely from the technical side is rather difficult since they usually come with a measure of social engineering. Phishing URLs increasingly make use of invisible Unicode characters or identical-looking symbols from non-Latin alphabets [35].

One possible solution for preventing malware infection after opening an email or its attachments could be sandboxing technology. All attachments and links would be opened in an isolated, secure environment that doesn't harm the actual system.

5.3.4 Application Updates

Last but not least, our results suggest further research in the direction of update managers that not only reliably perform their task of keeping the system and its applications up to date, but also communicate clearly what updates include which features and fixes and that schedule their work intelligently without interrupting or hindering the user.

The need for a centralized, system-level update tool that takes care of application updates was already expressed by Ion, Reeder, and Consolvo in 2015 and recently confirmed by Mathur et al. [21]. Since then, some applications have started to implement their own more or less automatic update tools, while a centralized tool is not on the horizon. Microsoft tried establishing their own Windows Store as an app store-like entity with an integrated application updater, but adoption rates are still low.

6 Limitations

In the following, we will outline the limitations of our study to facilitate putting this work into context.

Because we could not recruit via the same channel as the original authors, our expert sample is drawn from a different population. Thus, there are two variables that are different, time and population from which our experts were recruited. For that reason, our results can be seen as extending the original results, but cannot be used to state that the effects are attributable to the intervening time or due to different populations.

In particular, we decided to include security experts with 1-5 years of experience in security or a related field, while the original study only considered participants with at least five years of experience as experts. Table 1 shows that participant distribution is almost equal between all age brackets. Since we saw no difference between experts with 1-5 years of experience and those with 5+ years of experience, we decided to include them to increase our overall sample size.

As for recruiting non-experts, we had to follow the same channel as the original work and thus suffer from the same limitations. While Amazon MTurk is heavily used for usable security and human–computer interaction studies, the population there tends to be younger, more female, and more tech-savvy than the general US population [7,25,30].

All data we collected were self-reported. It is known that people tend to put themselves in a better light in such situations; therefore, the adoption rates or likeliness of following a certain piece of advice are possibly skewed [27].

7 Conclusions

In this paper, we replicated a 2015 study by Ion, Reeder, and Consolvo examining expert and non-expert security habits and corresponding advice. While our general findings relate with the original work, we could identify some new trends, like the use of script and ad blocking software.

In addition, we identified an issue in the original study design and improved upon it. Our results identify critical areas of effective but unrealistic practices that could be improved upon by the research and practitioner communities. Most of these practices (password security, 2FA, securely handling links and attachments from emails, and centralizing application updates) were already present as emerging topics in the 2015 study. This shows that the usable security community has not succeeded in solving these grave issues and clearly outlines the need for future action in researching and developing new or better security tools that non-experts can adopt and use.

8 Acknowledgments

We thank Iulia Ion, Rob Reeder, and Sunny Consolvo for their cooperation and support of our replication efforts. Furthermore, we thank all the people who helped in distributing and sharing the expert survey. Many thanks go to Maximilian Häring, Emanuel von Zezschwitz, and Christian Tiefenau for feedback on the paper. We also thank all our study participants as well as the anonymous reviewers.

This work was partially funded by the ERC Grant 678341: Frontiers of Usable Security.

References

[1] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz. The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 674–689. ACM, 2014.

[2] M. Aertsen, M. Korczyński, G. Moura, S. Tajalizadehkhoob, and J. van den Berg. No domain left behind: is let's encrypt democratizing encryption? In *Proceedings of the Applied Networking Research Workshop*, pages 48–54. ACM, 2017.

[3] Y. Albayram, M. M. H. Khan, and M. Fagan. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction*, 33(11):927–942, 2017.

[4] E. R. Babbie and L. Benaquisto. *Fundamentals of social research*. Cengage Learning, 2009.

[5] Z. Benenson, G. Lenzini, D. Oliveira, S. Parkin, and S. Uebelacker. Maybe poor johnny really cannot encrypt: The case for a complexity theory for usable security. In *Proceedings of the 2015 New Security Paradigms Workshop*, pages 85–99. ACM, 2015.

[6] R. Benes. Five Charts: Why Users Are Fed Up with Digital Ads. `https://www.emarketer.com/content/five-charts-users-are-fed-up-with-digital-ads`, 2018. last accessed on 2019-02-20.

[7] M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's mechanical turk. *Perspectives on Psychological Science*, 6(1):3–5, 2011. PMID: 26162106.

[8] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, pages 1–16, 2006.

[9] S. H. Drew. Drew: Tips on creating passwords to protect your privacy. `https://www.birminghamtimes.com/2018/11/drew-tips-on-creating-passwords-to-protect-your-privacy/`, November 2018. last accessed on 2018-12-09.

[10] M. Fagan and M. M. H. Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*, pages 59–75, 2016.

[11] S. Fahl, M. Harbach, M. Oltrogge, T. Muders, and M. Smith. Hey, you, get off of my clipboard. In *International Conference on Financial Cryptography and Data Security*, pages 144–161. Springer, 2013.

[12] P. Ferguson and G. Huston. What is a vpn? - part i. *The Internet Protocol Journal*, 1(1), 1998.

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

[14] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson. An analysis of the privacy and security risks of android vpn permission-enabled apps. In *Proceedings of the 2016 Internet Measurement Conference*, IMC '16, pages 349–364, New York, NY, USA, 2016. ACM.

[15] I. Ion, R. Reeder, and S. Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, Ottawa, 2015. USENIX Association.

[16] E. Katz. Dashlane research finds majority of two-factor authentication offerings fall short. `https://blog.dashlane.com/2fa-rankings/`, 2018. last accessed on 2018-12-19.

[17] A. Lenhart, M. Madden, S. Cortesi, U. Gasser, and A. Smith. Where teens seek online privacy advice. *Pew Research Center, Internet & Technology*, 2013.

[18] P. Leonard. Mandatory Internet Data Retention in Australia – Looking the horse in the mouth after it has bolted. Technical report, Gilbert & Tobin, 2015.

[19] Y. Li, W. Dai, Z. Ming, and M. Qiu. Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, 65(5):1339–1350, 2016.

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

[21] A. Mathur, N. Malkin, M. Harbach, E. Peer, and S. Egelman. Quantifying users' beliefs about software updates. *Proceedings 2018 Workshop on Usable Security*, 2018.

[22] J. Morris, I. Becker, and S. Parkin. In Control with no Control: Perceptions and Reality of Windows 10 Home Edition Update Features. In *Workshop on Usable Security and Privacy (USEC)*, 2019.

[23] NCSA. The stay safe online blog. `https://staysafeonline.org/blog_category/privacy/`, July 2018. last accessed on 2018-12-09.

[24] E. M. Redmiles, S. Kross, and M. L. Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[25] E. M. Redmiles, S. Kross, and M. L. Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples*, page 0. IEEE, 2019.

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

[27] E. M. Redmiles, Z. Zhu, S. Kross, D. Kuchhal, T. Dumitras, and M. L. Mazurek. Asking for a friend: Evaluating response biases in security user studies. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1238–1255. ACM, 2018.

[28] R. W. Reeder. If you cold tell a user three things to do to stay safe online, what would they be? `https://security.googleblog.com/2014/03/if-you-could-tell-user-three-things-to.html`, March 2014. last accessed on 2019-02-20.

[29] J.-L. Richet. Extortion on the internet: the rise of crypto-ransomware. *Harvard*, 2016.

[30] D. J. Simons and C. F. Chabris. Common (mis)beliefs about memory: A replication and comparison of telephone and Mechanical Turk survey methods". *PLOS ONE*, 7(12), 2012.

[31] C. Simpson. Data Mining of Telecom Metadata is “More Dangerous than Intercepting Conversations”. `https://newsmonitors.blog/2018/04/19/data-mining-of-telecom-metadata-is-more-dangerous-than-intercepting-conversations/`, 2018. last accessed on 2019-02-14.

[32] W. Strayer. Privacy issues in virtual private networks. *Computer Communications*, 27(6):517 – 521, 2004. Internet Performance and Control of Network Systems.

[33] E. Volkman. 49 percent of phishing sites now use https. `https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https`, 2018. last accessed on 2019-02-13.

[34] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[35] X. Zheng. Phishing with Unicode Domains. `https://www.xudongz.com/blog/2017/idn-phishing/`, 2017. last accessed on 2019-02-14.

A Surveys

All multiple-choice questions were single answer only. The questions were identical for the Expert A, Expert B, and Non-expert survey, unless otherwise stated. The questions marked "(Experts A only)", "(Experts B only)" or "(Non-experts only)" were asked in only one of the surveys.

- *(Experts A&B 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
- 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
  - I don’t know
- 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 *(open-ended)*
- Do you use anti-virus software on that computer? *(multiple-choice)*
  - Yes
  - No
  - I don’t know
  - Other *(open-ended)*
- 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 *(open-ended)*

- 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 *(open-ended)*

- Google began in January 1996 as a research project. Its initial public offering took place on August 19, 2004. Did the initial public offering of Google take place in 1996? *(multiple-choice)*
  - Yes
  - No
  - Other *(open-ended)*

- 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 *(open-ended)*

- Do you visit websites you have not heard of before? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other *(open-ended)*

- 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? *(multiple-choice)*
  - Yes, often
  - Yes, sometimes
  - Yes, rarely
  - No
  - I don't know
  - Other *(open-ended)*

  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 *(open-ended)*

- 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 *(open-ended)*

- *(Experts A 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 B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) 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
- *(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 & Experts A only)*(optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how 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
- *(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 & Experts B only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts A 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 B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) 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
- *(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 & Experts A only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how 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

- *(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 & Experts B only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts A 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 B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) 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

- *(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 & Experts A only)* (optional) Please use this space to clarify any of the above. *(open-ended)*

- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how 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

- *(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 & Experts B 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 B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how EFFECTIVE (at keeping the user secure) 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
- *(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 & Experts A only)* (optional) Please use this space to clarify any of the above. *(open-ended)*
- *(Experts B only)* For each of the following pieces of advice, please rate on a scale from 1 to 5 how 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

- *(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 & Experts B 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 *(open-ended)*
- 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)
  - Bachelor (for example, BS, BA; also German Berufsausbildung)
  - Associates Degree (or German Abitur)
  - Some college, no degree
  - Technical/Trade school
  - Regular High School Diploma (or German Realschulabschluss)
  - GED or alternative credential
  - Some High School (or German Hauptschulabschluss)
  - I prefer not to answer
  - Other *(open-ended)*
- *(Experts A&B only)* How many total years of experience do you have in computer security?
  'Experience' includes years at work or studying in a security-related field. *(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 A&B 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 *(open-ended)*
- *(Experts A&B only)* Which of the following best characterizes your workplace? *(multiple-choice)*
  - University
  - Corporate research lab
  - Industry
  - Government
  - Self-employed
  - Other *(open-ended)*
- *(Experts A&B only)* In what country do you work? *(multiple-choice)*

  - Australia
  - Canada
  - Germany
  - India
  - United Kingdom
  - United States
  - Other *(open-ended)*

- *(Experts A&B 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 *(open-ended)*

- *(Non-experts only)* What is your occupation? *(open-ended)*

- *(Non-experts only)* What is your Mechanical Turk Worker ID? *(open-ended)*

- *(Experts A&B only)* Do you remember taking a survey with similar questions in the past (ca. 2014)?
  - Yes
  - No

- (Optional) Is there anything else you'd like to add or clarify? *(open-ended)*