152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users

Robert W. Reeder, Iulia Ion, Sunny Consolvo
rreeder@google.com, iuliaion@google.com, sconsolvo@google.com
Google

ABSTRACT

Users often don't follow expert advice for staying secure online, but the reasons for users' non-compliance are only partly understood. While some experts express frustration with users for ignoring existing advice, others argue that the advice itself is part of the problem. To inform this debate, we surveyed 231 security experts and asked, *"What are the top 3 pieces of advice you would give to a non-tech-savvy user to protect their security online?"* We received 152 unique pieces of advice -- all in at least one expert's top 3 -- that span 15 categories. These results suggest that, although individual experts give thoughtful, reasonable answers, the expert community as a whole lacks consensus on the most important advice to give. We conclude with a call to action for usability and security experts to work toward a prioritized, concise set of security advice that users can more easily consume and follow.

KEYWORDS

D.2.14.a User interfaces < D.2.14 Human Factors in Software Design < D.2 Software Engineering < D Software/Software Engineering, K.6.m.b Security < K.6.m Miscellaneous < K.6 Management of Computing and Information Systems < K Computing Milieux

INTRODUCTION

With almost daily news of high-profile cybersecurity incidents, users naturally wonder what they can do to protect themselves against attacks. Indeed, as cybersecurity professionals, we've often been asked by concerned friends and family for advice on what they can do to stay safe online. But, somewhat to our own surprise, we've been dumbfounded about what to say in these situations. On the one hand, there are perhaps hundreds of things we could say about online security; after all, the security field is so complex, it takes years to learn. On the other hand, those asking us for advice just want a few easy-to-remember things they could start applying right away. Getting from the hundreds of things down to a handful of the most important seems surprisingly challenging.

We set out to find the most important security advice on offer from experts today. Our goal in this work was to find advice for a general audience that could be used, for example, in a public awareness campaign or on an informational website. To inform such general cybersecurity communications, the security field should have a consistent, prioritized set of advice that could be shared with those users looking for the most important things to start doing right away. The entire set may be long, but as long as the most important things are consistently communicated to users at large, users have a better chance of understanding and remembering them.

Our approach has its limitations. There are many different computing contexts, and good advice can be highly context-dependent. Advice that works for one user may be irrelevant or impossible to follow for another. In some cases, users need assistance to respond to some specific situation, and providing such assistance is important, but not our goal. While there is a need for contextualized advice and assistance, this work targets a different need: the most important advice to share with a general audience.

Our work is guided by two primary research questions: (1) what advice is considered most important by security experts?; and (2) is there expert consensus and consistency on what advice is considered most important? To identify the prevailing advice of the security community, we surveyed 231 security experts and asked them this question:

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

Our results give us a broad sample of expert opinion about the highest-priority advice to share with users, and reveal a lack of expert consensus. Moreover, upon examining the advice we collected more closely, we found several areas with confusing advice variants (e.g., to not click on links in email from unknown sources versus not clicking links in email at all). While almost all of the thoughtful advice we received makes sense in isolation, the security expert community is not in agreement on how to prioritize the set of advice as a whole or on how to resolve confusing variants within the set. It's understandable if users are confused about what to do; even experts, as a field, don't seem to agree.

While the question of what advice to give seems fundamental to online security, we identify some clear problems with the existing set of expert advice. We acknowledge that arriving at consensus about the right set of advice is quite difficult, and we don't solve that problem in this work. Instead, we contribute:

- Data on existing expert opinion on what security advice to give to non-expert users;
- An analysis of the consensus and consistency of the overall set of advice we found;
- Identification of the problem that the set of the most important security advice is not widely agreed upon.

We identify the problem of a lack of expert consensus on what advice to give. We conclude with a call to action to usability and security experts to work toward a concise, effective, actionable, consistent, and prioritized set of security advice to communicate to users. Our findings will help focus research on the right set of advice to communicate to users and on what advice is most important and what can be deprioritized.

BACKGROUND AND RELATED WORK

Although we are not aware of past research that has evaluated the state of security advice as a whole, there has been extensive research on advice in specific areas and users' struggles to

follow it. We give a brief overview of sources of security advice and research on users' compliance with it.

There is a great deal of security advice available to those looking for it. Many service providers, enterprises, universities, and other organizations offer advice in the form of tips and training on how to stay safe online. One of the most comprehensive and authoritative sources of advice intended for non-technical users is provided by US-CERT [11], which by our count spans 57 pages and offers 534 individual pieces of advice. Recommendations range from common advice like "keep your anti-virus software current" to less common advice like "consider challenging service providers that only use passwords to adopt more secure methods"). With such a large set of advice, it may be unclear to many users where to get started, to whom the advice applies, and why following the advice will help.

Past research on security advice and users' security behaviors suggests that there is an opportunity for advice to change behavior for the better, but also a need to limit, prioritize, and better communicate the advice.

Opportunity to change behavior

If users were not willing or able to take any security measures, formulating good advice would be a moot issue. However, past work has found that users do have some, albeit limited, willingness and ability to follow good security practices. We surveyed security experts and non-experts about their security practices and found that non-experts clearly do follow security practices, but often not the same ones experts do [4]. These findings suggests a need to better communicate expert practices and advice to non-experts. Wash [13] examined users' reactions to 12 common pieces of security advice and found that users would follow some diligently while ignoring others, depending on their mental models of security. Shay et al. found that users -- at least those who have experienced an account hijacking -- generally accept some responsibility for protecting their online accounts and acknowledge their role in security behaviors like selecting and protecting passwords [9].

Need to limit, prioritize, and communicate

Herley [2] argues that users often reject security advice because the cost of following all commonly given security advice is much greater than the cost of the relatively few low-frequency attacks that succeed. He argues in another work [3] that for security advice, "more is not the answer," but acknowledges that some advice is probably needed.
How advice is communicated is a critical part of getting users to follow it. Rader et al. [6] show that people learn lessons about security via stories they hear, that these lessons can change behavior, and that stories may thus be an effective way to communicate advice to users.

METHODOLOGY

We conducted an online survey of security experts about the security advice they would share with non-tech-savvy users. We used *Google Forms*[1] to write and host the survey. The survey ran from February through June 2014. We recruited security experts via the *Google Online Security Blog* [7], a public blog that is published by Google and is widely read by security experts and enthusiasts, and by promoting the survey through our social media accounts. Participation in the survey was voluntary, and we did not provide compensation. We considered a "security expert" to be anyone who reported having at least 5 years of experience working in or studying computer security. Our results are based on responses from 231 such expert respondents, to whom we refer as R1, R2,... R231.

Survey content

The survey started with the single, open-ended question:

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

The survey also asked additional questions, including demographic questions, quality-assurance questions, and a series of other questions which are reported in our work comparing expert and non-expert security practices [4].

We chose to elicit qualitative, free-form responses to our top-3-advice question, rather than the quantitative responses that multiple choice or Likert-scale questions would provide. Qualitative data can be difficult to analyze and introduces risks of subjective interpretation by experimenters, but maximizes our chances of getting experts' unvarnished opinions.

We received 245 responses to our survey from experts meeting our criteria of 5 years or more of experience in security. Of these, we eliminated 14 from analysis for answering 2 or more of our 4 quality-assurance questions incorrectly.

Security expert demographics

Security professionals often have demanding jobs and are highly paid, so we expected a small sample, perhaps a few dozen, to be willing to complete our survey for free. Contrary to expectations, many security experts responded, giving us a sample size and diversity that exceeded our expectations.

Respondents reported diverse geographies, workplaces, and job titles. While 47% of respondents were from the United States, others were from 25 countries around the world, including, in order of frequency, the UK, Germany, Australia, Japan, India, Israel, South Africa, and more. 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. Respondents reported a vast range of job titles within information security including CEO, CISO,

[1] https://www.google.com/forms/about/ (link verified Dec 22, 2016)

consultant, grad student, IT specialist, network administrator, security researcher, software engineer, and whitehat hacker.

Of the 231 respondents in our sample of experts, 4% were female. Ages were from the 18-24 range 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.

Coding procedure

We analyzed free-form responses to the top-3-advice question using a general inductive approach [5]. Two of the authors served as raters. The two raters, working independently, read a subset of the responses and proposed codes for common responses. They then met to discuss the codes and agreed on an initial codebook. Having formed an initial set of codes, the raters split up the data and began coding responses independently. They coordinated to add new codes to the codebook as needed. To assess inter-rater reliability, both raters independently coded the same subset of our data (10% of our sample) using the final codebook and achieved a Cohen's κ of 0.77, which is generally considered *substantial agreement* [5].

Ethics

Only voluntarily provided survey data was collected and analyzed for this work. Our organization does not have an Institutional Review Board (IRB), so the study was not subject to IRB review; however, multiple researchers who have received human subjects training reviewed the survey instrument prior to the experiment. Respondents were not required or asked to identify themselves. Raw survey data access was restricted to researchers on the research team.

Limitations

While the size and diversity of our sample give us some confidence that our sample is representative of a large portion of the security expert community, our recruiting methods could introduce sample bias, as virtually all recruiting methods can. Since we recruited via the *Google Online Security Blog* post, it's likely respondents are regular readers of the blog, so may feel some loyalty to Google. For most security advice, this loyalty probably makes no difference, but some bias may be present in advice such as the recommendation to *Use Chrome*. We note, however, that some respondents recommended products made by other organizations as well.

RESULTS

Having coded all survey responses, we deemed each code to represent a piece of advice. We assigned 837 codes to our 231 responses (some responses were coded as providing more than 3 pieces of advice). Of these 837 pieces of advice, 152 were unique. Having found 152 unique pieces of advice, we then counted the frequency of each piece of advice received, i.e., how many unique experts mentioned each piece of advice. Our frequency count of 68 for *Use unique passwords*, for example, means 68 unique experts mentioned that piece of advice. These frequency counts form the basis of our results. Because we collected such a wide variety of advice, we assigned pieces of advice to categories to make the advice easier to understand and

present. We then counted the number of unique experts giving at least one piece of advice in each category.

Table 1 shows the 45 pieces of advice (of the 152 total pieces of advice) that were mentioned by 4 or more experts, grouped by category. Table 2 shows examples of verbatim quotes that were coded as some of the 107 pieces of advice mentioned by 3 or fewer experts.

Our 837 codes assigned to 231 responses gives an average of 3.26 (*sd=1.24*) codes assigned per response. Even though the top-3-advice question asked for 3 pieces of advice, some responses received more or fewer than 3 codes, either because respondents deliberately provided a number other than 3 pieces of advice, or because the advice a respondent provided as one piece received more than one code (e.g., we assigned "Make sure your computer and its antivirus software are kept up to date" (R123) codes for *Keep systems and software up-to-date* and *Keep antivirus software up-to-date*).

In cases where related advice was given at different levels of granularity, e.g., *Be suspicious in general* versus *Be suspicious of links in email*, we strove to create codes that stayed true to the literal responses from respondents. In these cases, we assigned different codes to both the more generic and the more specific pieces of advice. We elaborate on this issue further in the discussion on generic vs. specific advice.

Advice collected, by category

We grouped the pieces of advice into 15 categories. In order of the number of unique experts mentioning at least one piece of advice in the category, the categories were:

- *ACCOUNT SECURITY*
- *UPDATES*
- *BROWSING HABITS*
- *EMAIL HABITS*
- *MINDFULNESS*
- *ANTIVIRUS*
- *PRIVACY*
- *BROWSER SECURITY*
- *DEVICE SECURITY*
- *SOFTWARE SECURITY*
- *NETWORK SECURITY*
- *BACKUPS*
- *EDUCATION*
- *OS AND PLATFORM*
- *OTHER*

Pieces of advice mentioned by 3 or fewer experts fall into either category-specific *Other* advice or into the general *OTHER* category, for advice that matched none of the 14 established categories. Category counts shown in Table 1 are unique experts mentioning at least one piece of advice in the category.

Advice	Count	Representative quotes
ACCOUNT SECURITY	128	
Use unique passwords	68	"different passwords everywhere"; "Do not re-use passwords on multiple sites"
Use strong passwords	58	"Choose a strong password"; "complex password for every site"
Use multi-factor authentication	36	"enable multi factor authentication features, if available"
Use a password manager	33	"Forget your password - Use a password manager to remember it for you."
Use a passphrase	7	"use a pass-phrase"; "Use long form plain language passwords a la xkcd.com/936"
Write passwords down	5	"Write them down in a notebook and keep it safe"
Other Account Security	24	"Routine changing of passwords."; "Don't leave a shared computer logged in as you"
UPDATES	97	
Keep systems and software up-to-date	90	"Always be updating (OS and applications)"; "Patch, patch, patch"
Use automatic updates	19	"Activate auto-update"
Other Updates	0	
BROWSING HABITS	76	
Use HTTPS	24	"use https if available"; "Watch for and understand why HTTPS is important."
Be careful / think before you click	19	"Think before you click"; "Be careful what you click on"
Check URL for expected site	11	"always look at the url bar if it's the right site"
Check the hyperlink before you click	8	"examine a link before you click it"; "Compare links via mouse hover with printed link"
Sensitive info only over HTTPS	6	"Check for https every time you provide personal/sensitive data."
Check for lock icon	5	"Look for the lock"
Pay attention to security warnings	5	"don't click through security warnings"; "Don't ignore security warnings - they are there for a reason."
Check for "https" in URL	4	"Check for a green HTTPS to the left of the domain name"
Visit only reputable websites	4	"don't enter sites whose 'reputation' isn't clearly (and positively) assessed in a public database"
Other Browsing Habits	19	"Take the time to read before clicking"; "check ssl certificates"
EMAIL HABITS	59	
Don't open unexpected attachments	19	"If you did not ask for the attachment DO NOT OPEN IT"
Don't click links in emails at all	11	"Never click on a link in an email"
Don't click links in email from unknown	9	"Do not click on links or images in an email from unknown source"
Be suspicious of email in general	7	"Don't trust email"; "Be sceptical about email"
Be alert for phishing emails	5	"Beware Spam & Phishing Emails"; "don't fall for phising attempts"
Beware emails requesting private data	5	"No legitimate financial institution will ask for your personal or financial information through email"
Be suspicious even of email from known	4	"Don't blindly trust every message even if it came from someone you know and trust"
Be suspicious of links in email	4	"Be careful following links, especially in email"
Other Email Habits	19	"if a message you receive seems strange, pick up the phone and verify it"
MINDFULNESS	42	
Be suspicious in general	16	"Be skeptical"; "Always be suspicious, do not trust everybody."
Too good to be true probably is	15	"If it seems to good to be true, it likely is"; "be aware of 'to good to be true' offers"
Apply real-world judgment online	4	"Common sense"; "Think 'would I do this out in the real world?"'
Other Mindfulness	19	"Stay alert, because you are in charge"; "Assume you don't understand the risks."
ANTIVIRUS	41	
Use antivirus software	35	"Use antivirus/antimalware software"
Keep antivirus software up-to-date	16	"Keep Anti-Malware current"; "keep antivirus updated"
Other Antivirus	3	"Leverage Two AV Engines"
PRIVACY	30	
Limit personal information sharing	14	"Never give out personal information."; "Share less."; "Don't give them your email"
Be careful what you share	13	"Be very wary of information you post on social media"
Other Privacy	5	"Remain anonymous as much as feasible and practicable."; "Always browse in private mode"
BROWSER SOFTWARE	29	
Use Chrome	13	"Use Chrome to browse the web"
Use an ad blocker	5	"Use a modern browser with an Adblock and Web Reputation add on."
Don't use Java	4	"Disable Java browser plugins or uninstall Java"
Other Browser Software	17	"Run NoScript browser add-on"; "Disable third party cookies"
DEVICE SECURITY	24	
Don't run as admin	12	"Limit privileges. Don't log in as an admin unless necessary."
Do sensitive tasks on dedicated devices	4	"Use separate devices for casual browsing ... and sensitive ones"
Do sensitive tasks on trusted devices	4	"Do online banking/purchases only on a trusted computer"
Lock devices	4	"Put password/pins on all your devices"; "Lock your phone."
Other Device Security	0	
SOFTWARE SECURITY	22	
Use only software from trusted sources	20	"Execute only software coming from reputable websites."
Other Software Security	2	"Only install software you absolutely need"
NETWORK SECURITY	15	
Don't trust open networks	4	"Dont use free / open wifi"; "Dont trust open networks or three party networks, can be unsafe."
Other Network Security	11	"Use a VPN service"; "Keep your firewall turned on"; "Use a Hardware Firewall at Home"
BACKUPS	10	
Back up your data	10	"Back up your data, nothing beats a good backup."; "always backup your data"
Other Backups	0	
EDUCATION	11	
Learn about security	4	"Educate yourself on common security problems."
Seek expert help when needed	4	"Get help if you are uncertain - quickly."; "If in doubt, ask"
Other Education	3	"Be aware of why your computer asks you for permission or passwords"
OS AND PLATFORM	9	
Use an uncommon operating system	4	"using a less-common operating system makes you less likely to be attacked"
Other OS and Platform	5	"If you know how to deal with VMs, use them."; "If possible use Linux"
OTHER	34	

Table 1. The 45 pieces of advice that were each mentioned by at least 4 respondents, count of unique respondents mentioning them (out of 231 total), and representative quotes from respondents. Advice is grouped into categories. Counts at the category level

are unique respondents mentioning at least one code in the category, so component counts may sum to a greater number than the category count. Quotes are verbatim.

Other advice
"Always browse in private mode and delete cache after each browsing session"
"always double check the source of an email (the sender)"
"Disable root certificates for entities that you would be alarmed to see certifying your bank's login page"
"Do not write down passwords"
"Don't add absolute strangers to your social media account"
"don't click on ads"
"don't look for porn"
"If you notice anything suspicious, report it appropriately"
"if you travel, use the TOR browser from your encrypted harddrive"
"Install Microsoft EMET and turn the system-wide settings up to maximum"
"let gmail render your mail attachments instead of opening them locally"
"Make sure set up account recovery options for your Google account"
"Never install or upgrade software from a popup screen"
"Unless you really know what you're doing, you're better off with documents in the cloud"

Table 2. Examples of less common advice provided by respondents. These verbatim quotes from respondents were coded as *Other...* advice within categories or placed in the catch-all *OTHER* category

Most-mentioned advice

As Table 1 shows, the top 3 pieces of advice the security expert community would give to a non-tech-savvy user are: *Keep systems and software up-to-date*, *Use unique passwords*, and *Use strong passwords*. However, we caution against prioritizing the entire set of advice strictly by rank-ordering the advice by the count of experts who mentioned it. The problem with this approach is that we did not ask experts to compare one piece of advice against another; we simply asked each individual for their own version of the top 3. In any case, here are the 10 (11 actually, since there is a three-way tie for 9th) most-mentioned pieces of advice, with number of respondents mentioning them:

1. *Keep systems and software up-to-date* {mentioned by 90 respondents}
2. *Use unique passwords* {68}
3. *Use strong passwords* {58}
4. *Use multi-factor authentication* {36}
5. *Use antivirus software* {35}
6. *Use a password manager* {33}
7. *Use HTTPS* {24}
8. *Use only software from trusted sources* {20}
9. *Use automatic updates* {19}
9. *Be careful / think before you click* {19}
9. *Don't open unexpected attachments* {19}

DISCUSSION

Our results give a sense of the security expert community's overall thoughts on the most important advice today. Much of the advice we collected is familiar, and almost all of it seems reasonable in isolation. It seems expert respondents to our survey gave thoughtful and sensible responses. But our finding that there are 152 pieces of advice spread across 15 categories

suggests a wide breadth of security advice that experts consider important to follow. Just considering these numbers, it is perhaps not surprising that users don't follow all the advice on offer---there's a lot of it, it spans diverse areas, and it's not clear where to start. Users are probably not receiving a consistent message on what's most important and exactly what to do in each area.

We start our discussion by establishing criteria for what makes good general advice. We then report a series of observations about the advice we collected, discuss challenges with creating good advice, and suggest ways in which the set of advice as a whole might be improved.

Criteria for good general advice

We guide our discussion of the advice we found and the potential for improving it by first establishing four criteria that good general advice should meet. These criteria are drawn from work in public awareness communications [8], which highlights the need for advice that users believe will work (our *effective* criterion), that users can actually do (our *actionable* criterion), and that is understandable (our *consistent* and *concise* criteria).

Good advice should be:

- **Effective**: Good advice, if followed by a user, should actually improve the user's security situation and lead to better security outcomes. Almost all of the advice we collected in this study (see Tables 1 and 2) seems effective against some security threat. Doing almost any of the actions advised by security experts (e.g., use strong passwords) should help improve users' online security.
- **Actionable**: Good advice should be easy for a user to remember and apply when needed, and it should not overly interfere with a user's primary goals. Advice that requires excessive skill (e.g., running a virtual machine), requires expert knowledge (e.g., requiring a user to judge something as "suspicious"), or excessively restricts user activity (e.g., "simply stay offline" (R224)) may not be reasonably actionable for a user seeking general advice. While most of the advice we collected is actionable (e.g., *Use multi-factor authentication*)*, some advice is less actionable (e.g., Be suspicious in general).*
- **Consistent**: Good advice should be both internally consistent, in that it should not cause confusion with or subsume other advice in the whole set of advice, and should be presented consistently, in that it should be phrased similarly each time a user hears it and should change as little as possible over time (as long as it remains effective). Consistency helps make advice easier for users to understand, remember, and follow. Looked at as a whole, the body of advice we collected was not consistent. The same advice was phrased differently by different participants and a few pieces of advice were contradictory (e.g., *Write passwords down and* "Do not write down passwords").
- **Concise**: The set of advice as a whole should be as small as possible. Less advice is easier for users to remember than more advice, and less advice to follow means it is easier to follow all of it. The ultimate goal of our work is to create more concise advice.

Given that we found 152 pieces of advice in this study, future work is needed to distill the 152 pieces of advice and communicate to users the most important ones.

Observations about advice we collected

We point out several observations about the advice we collected. These observations arose as we considered how the advice as a set could better meet our criteria.

Consensus within categories

Overall, we found a lack of consensus in what the top 3 pieces of advice are. But looking at our results by category, we find both pockets of consensus and pockets of divergence. Advice in the *UPDATES* category was consistent that all software and systems should be kept up-to-date. The other common piece of advice in that category, to enable automatic updates, is clearly in service of the first. *ANTIVIRUS*, *PRIVACY*, *SOFTWARE SECURITY*, and *BACKUPS* were categories with similar levels of general consensus. However, categories like *ACCOUNT SECURITY*, *BROWSING HABITS*, *EMAIL HABITS*, *MINDFULNESS*, and *BROWSER SOFTWARE* contain numerous pieces of advice, many of them potentially confusing variants or hard-to-discern options. For example, *ACCOUNT SECURITY* contains advice to *Use a password manager*, *Use a passphrase*, and *Write passwords down*. These pieces of advice are all options for solving the same problem: helping a user set strong and unique passwords but still manage to recall them when needed. Each method has its pros and cons, as security experts know, but how is a security non-expert to choose amongst these techniques? The non-expert confronted with all three pieces of advice is likely to be confused.

There's a lot of important advice

We set out with a goal to find just a handful of the most important advice that could be communicated to users whenever we have a few moments of their attention. Given our finding of a diverse range of advice, all of which is considered important by at least some experts, it may be the case that the security space is simply too complex for a small set of consistent advice to adequately protect the general user population. Perhaps advice communication efforts should focus not on communicating the same advice consistently to everyone, but on identifying particular audiences and customizing advice for each audience.

From set-and-forget to near-constant vigilance

Advice varies in the frequency with which it needs to be applied. Some is "set-and-forget"-- it needs to be done once (or rarely) and can then be ignored---some is needed on occasion, and some requires near-constant vigilance. In the set-and-forget category are pieces of advice like *Use antivirus software* or *Use automatic updates*. Good antivirus software or automatic updates should require little user interaction after they are initially set up. Advice needed on occasion includes advice related to choosing passwords and advice like *Do sensitive tasks on dedicated devices* and *Back up your data*. Much advice requires ongoing vigilance, like most of the *BROWSING HABITS*, *EMAIL HABITS*, *MINDFULNESS*, *PRIVACY*, and *EDUCATION* advice. Negative advice, like *Don't run as admin* or *Don't trust open networks*, falls somewhere in

between; it should be noted once, then applied whenever an applicable situation comes up (like considering whether to use the Wi-Fi at a coffee shop).

In general, vigilance may require cognitive attention, so can be difficult for users. Any advice that requires ongoing vigilance or frequent application should be given to users only if it has high efficacy.

Generic vs. specific

Variants of advice in the same area often differed in their level of specificity. Some advice was quite generic, like *Use HTTPS*, while other advice was more specific, such as to send *Sensitive info only over HTTPS*. Or, to compare exact quotes, “always browse with https if you can” (R224) represents a generic form of advice, while “always look out for the https and padlock logo when entering credit card details” (R114) represents a very specific version of similar advice.

There are arguments in favor of both generic and specific advice. Generic advice applies in more situations and to more users, while specific advice is usually more clearly actionable. A non-tech-savvy user instructed to follow the generic advice, “always browse with HTTPS” would have to learn what HTTPS is, and how to determine whether they’re browsing with it. However, a user instructed to follow the more specific, “look for the padlock when entering credit card details” would already have a way to determine whether HTTPS is in use, but might fail to apply that knowledge when entering sensitive data other than credit card details.

Generic advice can help keep the overall set of advice concise, because it doesn’t require enumerating every situation in which the advice should apply and every detail of how to apply the advice. However, generic advice may require skills and judgment that non-tech-savvy users haven’t developed well, such as the advice to *Use only software from trusted sources*, which requires careful judgment about how to determine the source of the software and which should be trusted.

Given the merits of both generic and specific advice, balancing them is important. Sometimes, it may be possible to combine them by offering the generic advice followed by specific instructions on how to implement it, e.g., “Always browse with HTTPS if you can; to check for an HTTPS connection, look for the padlock logo in the browser’s address bar.”

Realistic for users to follow

Some advice we collected is likely not actionable because users cannot follow it, either because it is too restrictive or because it requires too much technical knowledge or skill. Advice like *Don’t click links in email at all* is probably too restrictive; for many users, advice like *Do sensitive tasks on dedicated devices* is probably too restrictive if they can’t afford multiple devices. Advice like *Don’t run as admin* and *Use an uncommon operating system* probably requires more technical knowledge than many users have.

Phrasing advice

Even advice to which we assigned the same codes could vary significantly in how experts phrased it. Examples of representative quotes from Table 1 show variants in respondents' phrasing of advice. Here are two quotes from respondents that were both assigned the code *Too good to be true probably is*:

> *If it is to good to be true, looks like a scam, smells like a scam, or wants your personal details, IT IS A SCAM. (R194)*

and

> *A Nigerian Prince would never ask you to launder money for them, nor would the FBI director, etc.' (R137)*

The former quote is more direct and explicit in advising the user to trust their instincts and judgment about online offers. The latter contains narrative examples, and suggests a lesson without explicitly stating it. It's hard to say which would more likely connect with users, but these examples illustrate the variety of potential ways to phrase the same advice.

Challenges in creating good advice

Our results suggest several challenges in creating good advice. As improvements to the overall state of advice are attempted, it is worth bearing these challenges in mind.

The right advice may change over time with the attack landscape, new technology, and experience. As new attacks arise, new pieces of advice may need to be communicated to users to address them. To make the challenge even harder, attackers may adapt as good advice is adopted. For example, the widespread adoption of antivirus software has presumably made rogue antivirus attacks viable for attackers [10].

Advice that was once thought good may go out of style with experience or other change. For example, Adams and Sasse's work from 1999 talks about the difficulty users had with the advice to change passwords frequently [1], which was common advice at the time, but seems to have fallen out of favor[2] (only 3 of our experts mentioned *Change passwords frequently*).

Changing advice is a risk to consistency of the advice set. Some change in the set of security advice over time is undoubtedly necessary---and even desirable when it leads to a smaller set of advice or adapts to new threats---but all things being equal, advice that stays constant over time is more likely to be followed than advice that is likely to change.

[2] For recent discussions about the wisdom of advising users to regularly change passwords, see https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf (links verified Dec 22, 2016).

Even advice that is otherwise good---effective and consistently delivered---can face poor adoption if users do not believe the advice is effective or if they encounter significant drawbacks as a result of following the advice. For example, Vaniea et al. discuss some of the reasons users often reject the advice to install updates [12].

It simply may not be realistic to have a small, consistent set of security advice for general use. However, prioritizing the set to make it easier for users to apply the most important pieces first seems especially important.

Improving the existing set of advice

Improving the state of security advice from today's rather scattered state to a more effective, actionable, consistent, and concise set of advice is no small task. Our exercise here, surveying the current state of top advice according to experts, is only a start; it merely reveals the extensive effort needed to produce a good set of advice.

Advice should also be informed by actual data about attacks, compromises, and breaches. For example, if data on account compromises suggests that password brute-forcing attacks are most prevalent, we should emphasize using password managers. However, this data is difficult to obtain; often, the causes of security issues like account compromise or database breaches is unknown. In other cases, there is reluctance to release such data publicly.

Once the existing set of advice has been pared down to a more concise and internally consistent set, it should be given to users and evaluated in longitudinal studies in which users are observed as they try to apply the advice over time and in multiple relevant situations. Such studies can inform questions about what advice is memorable, easy enough for users to follow, not overly restrictive, and actually likely to produce better security outcomes.

With this work, we hope to alert the usability and security communities to some of the difficulties users may have following the advice on offer today. We hope usability and security experts will focus on each piece of advice on our list and consider it carefully for inclusion in the set of advice as a whole, according to our four criteria. Through data-informed debate, we hope the communities will work to pare the set down, prioritize it, standardize the way it is phrased, and package it for more effective dissemination to non-tech-savvy users.

CONCLUSION

We asked 231 security experts to list the top 3 pieces of advice they would give to a non-tech-savvy user to protect their security online; we received a vast array of advice---152 unique pieces covering 15 categories. We found that, while individual experts provide plenty of thoughtful and considered advice, the security community as a whole has yet to form consensus on a prioritized set of advice. Unless the community changes its approach to providing security advice to users, we shouldn't expect to see a change in adherence to the advice -- which means that users will remain less secure than they otherwise could be.

Our results suggest a need for extensive research and discussion to define and prioritize general security advice for non-expert users. We call upon usability and security experts to start discussion and research on which of the prevalent pieces of advice we collected, each considered by at least one expert to be in the “top 3”, belong in the canonical set of advice to be shared broadly with the non-expert user community.

REFERENCES

1. Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM* 42, 12 (1999), 40–46.
2. Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. *In Proc. of NSPW*. ACM, (2009) 133–144.
3. Cormac Herley. More Is Not the Answer. *IEEE Security & Privacy* 12, 1 (2014), 14–19.
4. Iulia Ion, Robert W. Reeder, and Sunny Consolvo. “...no one can hack my mind”: Comparing Expert and Non-Expert Security Practices. *In Proc. of SOUPS*. 2015. The USENIX Association, 327–346.
5. J. R. Landis and G. G. Koch. The measurement of observer agreement for categorical data. Biometrics (1977), 159–174.
6. Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. *In Proc. of SOUPS*. 2012. ACM.
7. Robert W. 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.
8. Ronald E Rice and Charles K Atkin. Public communication campaigns. 2012. Sage.
9. Richard Shay, Iulia Ion, Robert W. Reeder, and Sunny Consolvo. My religious aunt asked why I was trying to sell her viagra: experiences with account hijacking. In *Proc. of CHI*. 2014. ACM, 2657–2666.
10. Brett Stone-Gross, Ryan Abman, Richard A Kemmerer, Christopher Kruegel, Douglas G Steigerwald, and Giovanni Vigna. The underground economy of fake antivirus software. In *Economics of Information Security and Privacy III*. 2013. Springer, 55–78.
11. US-CERT: Tips. Accessed Sep 8, 2014. https://www.us-cert.gov/ncas/tips.
12. Kami E Vaniea, Emilee Rader, and Rick Wash. Betrayed by updates: how negative experiences affect future security. In *Proc. of CHI*. 2014. ACM, 2671–2674.
13. Rick Wash. 2010. Folk models of home computer security. *In Proc. of SOUPS*. ACM, 1–16.

AUTHOR BIOS

Robert W. Reeder is a Senior User Experience Researcher at Google in New York. As a member of Google's Security & Privacy User Experience team, he conducts research at the intersection of human-computer interaction, security, and privacy. He has a PhD in Computer Science from Carnegie Mellon.

Iulia Ion is a software engineer at Google working on strong authentication and cloud security. She received a PhD in Computer Science with a thesis on usable security from ETH Zurich.

Sunny Consolvo leads Google's Security & Privacy User Experience team. Sunny and her team spend most of their time focusing on usable privacy and security. Sunny has a Ph.D. in Information Science from the University of Washington. She is a member of the Editorial Board for IEEE Pervasive Computing and the PACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies (IMWUT). She became a Certified Information Privacy Professional (US) in 2013.

AUTHOR EMAILS

Robert W. Reeder: rreeder@google.com
Sunny Consolvo: sconsolvo@google.com
Iulia Ion: iuliaion@google.com