152 Simple Steps to Stay Safe Online:

Security Advice for Non-Tech-Savvy Users

Robert W. Reeder, Iulia Ion, and Sunny Consolvo | Google

Users often don't follow expert advice for staying secure online, but the reasons for users' noncompliance are only partly understood. More than 200 security experts were asked for the top three pieces of advice they would give non-tech-savvy users. The results suggest that, although individual experts give thoughtful, reasonable answers, the expert community as a whole lacks consensus.

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're often asked by concerned friends and family for advice on what to do to stay safe online. But, somewhat to our own surprise, we're dumbfounded about what to say in these situations. On one hand, we could say hundreds of things 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 can start applying right away. Getting from the hundreds of things down to a handful of the most important is surprisingly challenging.

We set out to find the most important security advice on offer from experts today. Our goal 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 can be shared with those users looking for the most important things to start doing right away. The entire set might be long, but as long as the most important things are consistently communicated to users at large, users will 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 might 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 it's not our goal. Although there's a need for contextualized advice and assistance, this work targets a different need: the most important advice to share with a general audience.

We Asked the Experts

Our work is guided by two primary research questions: What advice do security experts consider most important? And 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 to name the top three pieces of advice they'd give to a non-tech-savvy user to protect their security online.

Our results provide a broad sample of expert opinion about the highest-priority advice to share with users and reveal a lack of expert consensus. Moreover, on examining

1540-7993/17/$33.00 © 2017 IEEE

the advice we collected more closely, we found several areas with confusing advice variants (for instance, not clicking on links in email from unknown sources versus not clicking links in email at all). Although almost all of the thoughtful advice we received makes sense in isolation, the security expert community isn't in agreement on how to prioritize the set of advice as a whole or on how to resolve confusing variants in the set. It's understandable if users are confused about what to do; even experts, as a field, don't seem to agree.

Although 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 article. Instead, we contribute

- data on existing expert opinion on what security advice to give to nonexpert users,
- an analysis of the consensus and consistency of the overall set of advice we found, and
- identification of the problem that the set of the most important security advice isn't widely agreed on.

Background and Related Work

Although we're 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.

A great deal of security advice is 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 nontechnical users is provided by US-CERT (www.us-cert.gov/ncas/tips), which by our count spans 57 pages and offers 534 individual pieces of advice. Recommendations range from common advice like "keep your antivirus 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 might 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's 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 weren't 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 nonexperts about their security practices and found that nonexperts clearly do follow security practices, but often not the same ones experts do.[1] These findings suggests a need to better communicate expert practices and advice to nonexperts. Rick Wash 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.[2] Richard Shay and his colleagues found that users—at least those who've 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.[3]

Need to Limit, Prioritize, and Communicate

Cormac Herley 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.[4] He argues in another work that, for security advice, "more is not the answer" but acknowledges that some advice is probably needed.[5]

How advice is communicated is a critical part of getting users to follow it. Emilee Rader and her colleagues show that people learn lessons about security via stories they hear, that these lessons can change behavior, and that stories might thus be an effective way to communicate advice to users.[6]

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 (www.google.com/forms/about) to write and host the survey, which 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 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 didn't provide compensation. We considered a "security expert" to be anyone who reported having at least five years of experience working in or studying computer security. Our results are based on responses from 231 such expert respondents.

Survey Content

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

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

The survey also asked demographic questions, quality-assurance questions, and a series of other questions, which are reported in our work comparing expert and nonexpert security practices.[1]

We chose to elicit qualitative, freeform responses to our top-three-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 it maximized our chances of getting experts' unvarnished opinions.

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

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 percent of respondents were from the US, others were from 25 countries around the world, including, in order of frequency, the UK, Germany, Australia, Japan, India, Israel, and South Africa. In a check-all-that-apply question, 69 percent reported working in industry, 15 percent in academia, 13 percent self-employed, 11 percent in government, and 7 percent in corporate research labs. Respondents reported a vast range of job titles in information security including chief executive officer, chief information security officer, consultant, graduate student, IT specialist, network administrator, security researcher, software engineer, and whitehat hacker.

Of the 231 respondents in our sample of experts, 4 percent were female. Ages ranged from 18 to over 65, with 2 percent in the 18–24 range, 30 percent in the 25–34 year-old range, 32 percent in the 35–44 range, 18 percent in the 45–54 range, 9 percent in the 55–64 range, 3 percent over 65, and 5 percent not providing their age.

Coding Procedure

We analyzed freeform responses to the top-three-advice question using a general inductive approach.[8] 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 interrater reliability, both raters independently coded the same subset of our data (10 percent of our sample) using the final codebook and achieved a Cohen's κ of 0.77, which is generally considered substantial agreement.[8]

Ethics

Only voluntarily provided survey data was collected and analyzed for this work. Our organization doesn't have an institutional review board (IRB), so the study wasn't subject to IRB review; however, multiple researchers who have received human subjects training reviewed the survey instrument prior to the experiment. Respondents weren't required or asked to identify themselves. Raw survey data access was restricted to investigators on the research team.

Limitations

Although the sample's size and diversity give us some confidence that it's representative of a large portion of the security expert community, our recruiting methods could introduce sample bias, as virtually all recruiting methods can. Because we recruited via the Google Online Security Blog, it's likely respondents are regular readers of the blog, so they might feel some loyalty to Google. For most security advice, this loyalty probably makes no difference, but some bias might 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 experts' responses (some responses were coded as providing more than three 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—that is, 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 four or more experts, grouped by category. Table 2 provides examples of verbatim quotes that were coded as some

Table 1. The 45 pieces of advice that at least four respondents mentioned.

Advice	Count	Representative quotes
Account security	**128**	
Use unique passwords	68	Different passwords everywhere. Do not reuse passwords on multiple sites.
Use strong passwords	58	Choose a strong password. Complex password for every site.
Use multifactor authentication	36	Enable multifactor 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 passphrase. Use long-form plain language passwords.
Write passwords down	5	Write them down in a notebook and keep it safe.
Other account security	24	Routinely change 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 autoupdate.
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 to confirm that 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 the 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 didn't ask for the attachment, don't 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 sender	9	Don't click on links or images in an email from an unknown source.
Be suspicious of email in general	7	Don't trust email. Be skeptical about email.
Be alert for phishing emails	5	Beware spam and phishing emails. Don't fall for phishing attempts.
Beware emails requesting private data	5	No legitimate financial institution will ask for our personal or financial information through email.
Be suspicious even of email from known sender	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; don't trust everybody.
Too good to be true probably is	15	If it seems too good to be true, it likely is. Be aware of "too-good-to-be-true" offers.

Continued

Table 1. The 45 pieces of advice that at least four respondents mentioned. (Cont.)

Advice	Count	Representative quotes
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 antimalware current. Keep antivirus updated.
Other antivirus	3	Leverage two antivirus engines.
Privacy	**30**	
Limit personal information sharing	14	Never give out personal information. Share less. Don’t give out your email.
Be careful what you share	13	Be 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 plug-ins 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 backing/purchases only on a trusted computer.
Lock devices	4	Put passwords/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	Don’t use free/open Wi-Fi. Don’t trust open networks or three-party networks; this 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 back up 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 OS	4	Using a less-common OS makes you less likely to be attacked.
Other OS and platform	5	If you know how to deal with virtual machines, use them. If possible, use Linux.
Other	34	

Table 2. Examples of less common advice provided by respondents.

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.
Don't write down passwords.
Don't add absolute strangers to your social media accounts.
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 hard drive.
Install Microsoft EMET (Enhanced Mitigation Experience Toolkit) and turn the systemwide settings up to maximum.
Let Gmail render your mail attachments instead of opening them locally.
Make sure to 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.

of the 107 pieces of advice mentioned by three or fewer experts.

Our 837 codes assigned to 231 responses gives an average of 3.26 (with a standard deviation of 1.24) codes assigned per response. Even though the top-three-advice question asked for three pieces of advice, some responses received either more than or fewer than three codes, either because respondents deliberately provided a number other than three pieces of advice, or because the advice a respondent provided as one piece received more than one code (for example, we assigned "make sure your computer and its antivirus software are kept up to date" codes for "keep systems and software up to date" and "keep antivirus software up to date").

In cases in which related advice was given at different granularity levels, for example, "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 versus 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, these 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, and other.

Pieces of advice mentioned by three or fewer experts fall into either category-specific "other" advice, or 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.

Most-Mentioned Advice

As Table 1 shows, the top three 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 didn't ask experts to compare one piece of advice against another; we simply asked each individual for his or her own version of the top three. In any case, Table 3 shows the 10 (11 actually, because there is a three-way tie for ninth) most-mentioned pieces of advice, with number of respondents mentioning them.

Table 3. Ten most mentioned pieces of advice, coded.

Advice	No. of respondents who mentioned
Keep systems and software up-to-date	90
Use unique passwords	68
Use strong passwords	58
Use multifactor authentication	36
Use antivirus software	35
Use a password manager	33
Use HTTPS	24
Use only software from trusted sources	20
Use automatic updates	19
Be careful/think before you click	19
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 appears that 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's perhaps unsurprising 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, 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).[9]

Effective. Good advice, if followed by a user, should actually improve the user's security situation and lead to better security outcomes. Almost all 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 (for instance, using 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 shouldn't overly interfere with a user's primary goals. Advice that requires excessive skill (for instance, running a virtual machine), requires expert knowledge (for instance, requiring a user to judge something as "suspicious"), or excessively restricts user activity (for instance, "simply stay offline") might not be reasonably actionable for a user seeking general advice. Although most of the advice we collected is actionable (for instance, "use multifactor authentication"), some advice is less actionable (for instance, "be suspicious in general").

Consistent. Good advice should be both internally consistent—in that it shouldn't cause confusion with or subsume other advice in the whole set of advice—and 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 wasn't consistent. The same advice was phrased differently by different participants, and a few pieces of advice were contradictory (for instance, "write passwords down" and "don't 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's 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 three 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 this 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 nonexpert to choose among these techniques? The nonexpert 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 might 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" and "use automatic updates." Good antivirus software or automatic updates should require little user interaction after they're 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 might require cognitive attention, so it 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 versus specific. Variants of advice in the same area often differed in their level of specificity. Some advice was quite generic, like "use HTTPS," whereas 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*

represents a generic form of advice, whereas

> *Always look out for the HTTPS and padlock logo when entering credit card details*

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, whereas specific advice is usually more clearly actionable. Non-tech-savvy users 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, users 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 might 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 might be possible to combine them by offering the generic advice followed by specific instructions on how to implement it, for instance, "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 can't follow it, either because it's 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 too good to be true, looks like a scam, smells like a scam, or wants your personal details, IT IS A SCAM.*
>
> and
>
> *A Nigerian Prince would never ask you to launder money for them, nor would the FBI director, etc.*

The former quote is more direct and explicit in advising users 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's worth bearing these challenges in mind.

The right advice might change over time with the attack landscape, new technology, and experience. As new attacks arise, new pieces of advice might need to be communicated to users to address them. To make the challenge even harder, attackers might 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 might go out of style with experience or other changes. For example, Anne Adams and M. Angela Sasse's 1999 work talks about the difficulty users had with the advice to change passwords frequently,[11] which was common advice at the time, but seems to have fallen out of favor (only three 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's likely to change.

Even advice that's otherwise good—effective and consistently delivered—can face poor adoption if users don't believe the advice is effective or if they encounter significant drawbacks as a result of following the advice. For example, Kami Vaniea and her colleagues discuss some of the reasons users often reject the advice to install updates, such as the bundling of undesired new features with security updates and the potential for an update to break a working system.[12]

It simply might 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 are unknown. In other cases, there's 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.

We hope 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. In addition, we seek to alert the usability and security communities to some of the difficulties users might 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, the communities can pare the set down, prioritize it, standardize the way it is phrased, and package it for more effective dissemination to non-tech-savvy users. ■

References

1. I. Ion et al., "'… No One Can Hack My Mind': Comparing Expert and Non-expert Security Practices," *Proc. Symp. Usable Privacy and Security* (SOUPS 15), 2015, pp. 327–346.
2. R. Wash, "Folk Models of Home Computer Security," *Proc. Symp. Usable Privacy and Security* (SOUPS 10), 2010, pp. 1–16.
3. R. Shay et al., "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra: Experiences with Account Hijacking," *Proc. SIGCHI Conf. Human Factors in Computing Systems* (CHI 14), 2014, pp. 2657–2666.
4. C. Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *Proc. New Security Paradigms Workshop* (NSPW 09), 2009, pp. 133–144.
5. C. Herley, "More Is Not the Answer," *IEEE Security & Privacy*, vol. 12, no. 1, 2014, pp. 14–19.
6. E. Rader, R. Wash, and B. Brooks, "Stories as Informal Lessons about Security," *Proc. Symp. Usable Privacy and Security* (SOUPS 12), 2012, article 6.
7. R.W. Reeder, "If You Could Tell a User Three Things to Do to Stay Safe Online, What Would They Be?," Google Online Security Blog, 26 Mar. 2014; googleonlinesecurity.blogspot.com/2014/03/if-you-could-tell-user-three-things-to.html.
8. J.R. Landis and G.G. Koch, "The Measurement of Observer Agreement for Categorical Data," *Biometrics*, vol. 33, no. 1, 1977, pp. 159–174.
9. R.E. Rice and C.K. Atkin, *Public Communication Campaigns*, Sage, 2012.
10. B. Stone-Gross et al., "The Underground Economy of Fake Antivirus Software," *Economics of Information Security and Privacy III*, 2013, Springer, pp. 55–78.
11. A. Adams and M.A. Sasse, "Users Are Not the Enemy," *Comm. ACM*, vol. 42, no. 12, 1999, pp. 40–46.
12. K.E. Vaniea, E. Rader, and R. Wash, "Betrayed by Updates: How Negative Experiences Affect Future Security," *Proc. SIGCHI Conf. Human Factors in Computing Systems* (CHI 14), 2014, pp. 2671–2674.

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. Reeder received a PhD in computer science from Carnegie Mellon University. Contact him at rreeder@google.com.

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. Contact her at iuliaion@google.com.

Sunny Consolvo leads Google's Security & Privacy User Experience team, which focuses on usable privacy and security. Consolvo received a PhD in information science from the University of Washington. She's a member of the *IEEE Pervasive Computing* and *Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies* (IMWUT) editorial boards. Contact her at sconsolvo@google.com.