This is a pre-publication version of the column that appeared in IEEE Security & Privacy May/June 2015

Security & Privacy Economics

Editors: Michael Lesk, lesk@acm.org | Jeffrey MacKie-Mason, jmm@umich.edu

Scaring and Bullying People into Security Won't Work

Angela Sasse | University College London

Usable security and privacy research began more than 15 years ago. In 1999, Alma Whitten and J.D. Tygar explained "Why Johnny Can't Encrypt,"[1] and Anne Adams and I pleaded that, even though they don't always comply with security policies, "Users Are Not the Enemy.[2] Today, there are several specialist conferences and workshops: publications on usability security and privacy are featured in top usability conferences, such as ACM SIGCHI Conference on Human Factors in Computing Systems (CHI), and top security conferences, such as the IEEE Symposium on Security and Privacy.

An ongoing topic in usable security research is security warnings. Security experts despair that the vast majority of users ignore warnings—they just "swat" them, just as they do with most dialog boxes. Over the past six years, continuous efforts have focused on changing this behavior and getting users to pay more attention. SSL certificate warnings are a key example: all browser providers have evolved their warnings in an attempt to get users to take them more seriously. For instance, Mozilla Firefox increased the number of dialog boxes and clicks users must wade through to proceed with the connection, even though it might not be secure. However, this has made little difference to the many users who decide to ignore the warnings and proceed. But creating more elaborate warnings to guide users towards secure behavior is not necessarily the best course of action, as it doesn't align with the principles of user-centered design.

Refining Warnings

At ACM CHI 2015, two studies reported on efforts to make more users heed warnings. Adrienne Porter Felt and her colleagues at Google designed a new SSL warning for Google Chrome, applying recommendations from current usable security research: keep warnings brief, use simple language to describe the specific risk, and illustrate the potential consequences of proceeding.[3] The authors hypothesized that if users understand the risks associated with a warning, they will heed rather than ignore it.

They tested these improved warnings in a series of mini surveys and found a modest but significant (12 percent) improvement in the number of participants who correctly identified the potential risks of proceeding, but no significant improvement in the number of participants who correctly identified the data at risk. In addition, compared to existing browser SSL warnings, there was no improvement in the number of participants who thought the warning was likely to be a false positive.

Felt and her colleagues reasoned that if they couldn't improve users' understanding, they might still be able to guide users toward secure choices. They applied what they called *opinionated design* to make it harder for participants to circumvent warnings, and visual design techniques to make the secure course of action look more attractive. In a field study, this technique led to a 30 percent increase in the number of participants who didn't proceed upon seeing the warning. The authors concluded that it's difficult to improve user comprehension of online risks with simple, brief, nontechnical, and specific warnings, yet they urge fellow researchers to keep trying to develop such warnings. In the meantime, they advise designers to use opinionated design to deter users from proceeding in the face of warnings by making them harder to circumvent and emphasizing the risks associated with doing so.

In the second paper, Bonnie Anderson and her colleagues examined 25 participants' brain responses to warnings using a functional magnetic resonance imaging (fMRI) scanner.[4] Previous studies using eye tracking showed that users habituate: the first time around, a warning catches their attention, but after repeated showings, it does not. Anderson and her colleagues found that the brain mirrors this habituation: when encountering a warning for the first time, participants' visual processing center in the superior parietal lobes showed elevated activation levels, but these disappeared with repeated showings of the warning.

The authors hypothesized that varying a warning's appearance, such as its size, color, and text ordering, should prevent habituation and keep participants paying attention. They found that participants indeed showed sustained activation levels when encountering these polymorphic warnings; participants' attention only decreased on average after the 13th variation of the same warning. They concluded that users can't help but habituate, and designers should combat this by creating warnings that force users to pay attention.

Usability: when does 'guiding' become 'bullying'?

Both teams' work was motivated by an honorable intention—to help users choose the secure option. But as a security researcher with a usability background and many years of studying user behavior in the lab as well as in real-world settings, I am concerned by the suggestion that we should use design techniques to force users to keep paying attention and push them toward what we deem the secure—and hence better—option. It is a paternalistic, technology-centered perspective that assumes the security experts' solution is the correct way to manage a specific threat.

In the case of SSL, the authors recommended counteracting people's habituation response and keeping their attention focused on security. However, habituation is an evolved response that increases human efficiency in day-to-day interactions with the environment: we stop paying attention to signals we've deemed irrelevant. Crying wolf too often leads to alarm or alert fatigue; this has been demonstrated over many decades in industries such as construction and mining and, most recently, with the rapid increase of monitoring equipment in hospitals.

In 2013, the US Joint Commission issued an alert about the widespread phenomenon of alarm fatigue.[5] The main problem was desensitization to alarms, which led to staff missing critical events. An increase in workload and decrease in patient satisfaction were also noted.

Eminent software engineer and usability expert Alan Cooper identified the use of warnings in software as a problem more than a decade ago.[6] He pointed out that warnings should be reserved for genuine exceptions—events software developers couldn't reasonably anticipate and make provisions for. Perhaps on their legal advisors' suggestion, most developers have ignored Cooper's recommendation, and the increasing need for security has led to a marked further increase in the number of dialogue boxes or warnings that user have to 'swat' today.

Strategies such as opinionated design and forcibly attracting users' attention disrupt user activities is not usability. As Cooper pointed out, usability's overall guiding principle is to support users in reaching their primary goals as efficiently as possible. Security that routinely diverts the attention and disrupts the activities of users in pursuit of these goals is the thus the antithesis of a user-centered approach.

And where, in practical terms, would this approach lead us? A colleague with whom I discussed the studies commented: "Even with this polymorphic approach, users stop paying attention after 13 warning messages. I suppose the next step is to administer significant electrical shocks to users as they receive the warning messages, so that they are literally jolted into paying attention." (The colleague kindly allowed me to use the quote, but wishes to remain anonymous.) Scaring, tricking, and bullying users into secure behaviors is not usable security.

Cost versus Benefit

In 2009, Turing award and von Neumann medal winner Butler Lampson pointed out that[7]

> *[t]hings are so bad for usable security that we need to give up on perfection and focus on essentials. The root cause of the problem is economics: we don't know the costs either of getting security or of not having it, so users quite rationally don't care much about it. ... To fix this we need to measure the cost of security, and especially the time users spend on it.*

Lampson's observations haven't been heeded. User time and effort are rarely at the forefront of usable security studies; the focus is on whether users choose the behavior that researchers claim to be desirable because it's more secure. Even if users' interaction time with specific security mechanisms, such as a longer password, is measured, the cumulative longer-term effect of draining time from individual and organizational productivity isn't considered.

Over the past few years, researchers have declared the task of recalling and entering 15- or 20-character complex passwords 'usable' because participants in Mechanical Turk studies were able to do so. But being able to do something a couple of times in the artificial constraints of such studies doesn't mean the vast majority users could—or would want to—do so regularly in pursuit of their everyday goals.

Factors such as fatigue as well as habituation affect performance. In real-world environments, authentication fatigue isn't hard to detect: users reorganize their primary tasks to minimize exposure to secondary security tasks, stop using devices and services with onerous security, and don't pursue innovative ideas because they can't face any more "battles with security" that they anticipate on the path to realizing those ideas.[8] It's been disheartening to see that, in many organizations, users who circumvent security measures to remain productive are still seen as the root of the problem—"the enemy"[2]—and that the answer is to educate or threaten them into behavior security experts demand – rather than considering the possibility that security needs to be re-designed.

A good example is the currently popular notion that sending phishing messages to a company's employees, and directing them to pages about the dangers of clicking links, is a good way to get their attention and make them less likely to click in the future. Telling employees not to click on links can work in businesses in which there's no need to click embedded links. But if legitimate business tasks contain embedded links, employees can't examine and ponder every time they encounter a link without compromising productivity.

In addition, being tricked by a company's own security staff is a negative, adversarial experience that undermines the trust relationship between the organization and employees. Security experts who aim to make security work by "fixing" human shortcomings are ignoring key lessons from human factors and economics.

In modern, busy work environments, users will continue to circumvent security tasks that have a high workload and disrupt primary activities because they substantially decrease productivity. No amount of security education—a further distraction from primary tasks—will change that. Rather, any security measure should pass a cost–benefit test: Is it easy and quick to do, and does it offer a good level protection?

Cormac Herley calculated that the economic cost of the time users spend on standard security measures such as passwords, antiphishing tools, and certificate warnings is billions of dollars in the US alone—and this when the security benefits of complying with the security advice are dubious.[9] SSL warnings have overwhelming false-positive rate—close to 100 percent for many years[9]—so users developed alarm fatigue and learned to ignore them. In addition, longer (12- to 15-character) passwords, which are associated with a very real cost in recall and entry time and increased failure rates—especially on the now widely used touchscreens—offer no improvement in security.[10]

Fitting the Task to the Human

The security-centered view assumes that users want to avoid risk and harm altogether. However, many users choose to accept some risks in pursuit of goals that are important to them. Security experts assume that users who don't choose the secure option are making a mistake, and thus preventing mistakes and educating users are the way forward.

However, a combination of usability and economics insights leads to a different way of thinking about usable security:

- Usable security starts by recognizing users' security goals, rather than by imposing security experts' views on users.
- Usable security acknowledges that users are focused on their primary goals—for example, banking, shopping, or social networking. Rather than disrupting these primary tasks and creating a huge workload for users, security tasks should cause minimum friction.
- Security experts must acknowledge and support human capabilities and limitations. Rather than trying to "fix the human," experts should design technology and security mechanisms that don't burden and disrupt users.

Techniques from the human factors field can maximize performance while ensuring safety and security.

A key principle is designing technology that fits users' physical and mental abilities—fitting the task to the human. Rarely should we fit the human to the task, because this requires significant organizational investment in terms of behavior change through education and training. Security education and training are only worthwhile if the behavior fits with primary tasks. An organization could train its employees to become memory artists, enabling them to juggle a large number of changing PINs and passwords. But then employees would need time for routines and exercises that reinforce memory and recall.

Changing security policies and implementing mechanisms that enable employees to cope without training are more efficient. For instance, Michelle Steves and Mary Theofanos recommend a shift from explicit to implicit authentication[8]; in most environments, there are other ways to recognize legitimate users, including device and location information or behavioral biometrics, without disrupting users' workflow. They also point out that infrequent authentication requires different mechanisms that complement the workings of human memory—something Adams and I recommended after our first study 15 years ago[2]—but this rarely occurs in practice.

Users will pay attention to reliable and credible indicators of risks they want to avoid. Security mechanisms with a high false-positive rate undermine the credibility of security and train users to ignore them. We need more accurate detection and better security tools if we are to regain users' attention and respect, rather than scare, trick and bully them into complying with security measures that obstruct human endeavor.

References

1. A. Whitten and D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *Proc. 8th Conf. USENIX Security Symp.*, vol. 9, 1999, p. 14.
2. A. Adams and M.A. Sasse, "Users Are Not the Enemy," *Comm. ACM*, vol. 42, no. 12, 1999, pp. 40–46.
3. A. Porter Felt et al., "Improving SSL Warnings: Comprehension and Adherence," *Proc. Conf. Human Factors and Computing Systems*, 2015; https://adrifelt.github.io/sslinterstitial-chi.pdf. 4. B.B. Anderson et al., "How Polymorphic Warnings Reduce Habituation in the Brain—Insights from an fMRI Study," *Proc. Conf. Human Factors and Computing Systems*, 2015; http://neurosecurity.byu.edu/media/Anderson_et_al._CHI_2015.pdf.
5. "Medical Device Alarm Safety in Hospitals," *Sentinel Event Alert*, no. 50, 8 Apr. 2013; www.pwrnewmedia.com/2013/joint_commission/medical_alarm_safety/downloads/SEA_50_alarms.pdf.
6. A. Cooper, *The Inmates Are Running the Asylum: Why High-Tech Products Drive Us Crazy and How to Restore the Sanity*, Sams–Pearson, 2004.
7. B. Lampson, "Usable Security: How to Get It," *Comm. ACM*, vol. 52, no. 11, 2009, pp. 25–27.
8. M.P. Steves and M.F. Theofanos, *Report: Authentication Diary Study*, tech. report NISTIR 7983, Nat'l Inst. Standards and Technology, 2014.
9. C. Herley, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *Proc. 2009 Workshop New Security Paradigms*, 2009, pp. 133–144.
10. D. Florencio, C. Herley, and P.C. van Oorschot, "An Administrator's Guide to Internet Password Research," *Proc. USENIX Conf. Large Installation System Administration*, 2014, pp. 35–52.

Angela Sasse is a professor of human-centered technology at University College London. Contact her at a.sasse@cs.ucl.ac.uk.

//The following abstract and keywords will appear in our digital library. Please revise as desired.//

Abstract: Users will pay attention to reliable and credible indicators of a risk they want to avoid. More accurate detection and better security tools are necessary toregain users' attention and respect.

Keywords: security, usability, passwords, alarm fatigue