Protecting You

M. Angela Sasse | University College London
Charles C. Palmer | IBM

Approximately 2 billion people around the world use the Internet today. In the developed world, most commercial and public services are now available online, and most of us wouldn't want to go back to the pre-Internet age. But as the value of transactions we can do online has increased and the amount of data we generate has grown, so too has the number of those looking to redirect these transactions for their own benefit. Some criminals want access to our computers to make them part of their botnets; others want our authentication credentials and financial information so they can steal our money or sell us nonexistent goods. Commercial organizations collect our personal data, including potentially sensitive information, from our online behavior, preferences, locations, and contacts. And if we suffer a security breach, it can affect our family, friends, and neighbors—even our service providers. As users learn about these risks, they're coming to the realization that controlling what personal data is online and who can access it can mitigate those risks.

This special issue of *IEEE Security & Privacy* focuses on what we—individually and collectively—can do to protect ourselves and our information as it's gathered, shared, used, and managed. What do we have to know, and be able to do, to protect ourselves? Do computer security and privacy experts currently provide us with realistic, actionable advice? Do companies and governments that encourage us to use online communications and transactions do what's necessary to protect us?

Today's computer security professionals can draw from a set of well-established concepts and mechanisms, such as authentication and access control, to keep attackers out of systems. But as Cormac Herley argues in his article, "More Is Not the Answer," many of these measures are ineffective because they require too much attention and effort from inexperienced users. Even

experienced users often ignore security advice because the workload and complexity required to follow that advice exceed the risks those individuals expect to face.

Traditionally, security researchers and practitioners didn't consider user effort as a limited resource—and this has to change. Security mechanisms that might have required reasonable effort when first deployed in the pre-Internet age aren't fit for protecting today's much larger and more diverse user community; people juggle many devices with different interaction modes and use dozens of online services in a variety of environments. Herley demonstrates that, in the Internet age, security designers and practitioners should consider user attention and effort first and foremost when putting protection mechanisms in place.

This echoes Mary Theofanos and Shari Lawrence Pfleeger's Guest Editors' Introduction to *S&P*'s special issue on usable security in March/April 2011[1]: to be effective, security must be usable—it is not a luxury or optional extra:

> Usability and security complement one another. We need to make it easy for the user to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens anyway.

But despite a flurry of activity in research on usable security over the past 10 years, we've seen little change in practice. While practitioners accept that security ought to be usable, they can't deliver it in the manner of Captain Jean-Luc Picard: with a nod of the head and saying "Make it so." As Theofanos and Pfleeger pointed out, it requires changing the thinking and processes of everyone involved in system and service design and delivery:

> [B]oth usability and security have been poor stepchildren during system development, often added to an application only at the end of the development process. Understanding that these attributes must be built as an integral part of a system's design, experts in both security and usability have developed methodologies to do just that.

Unfortunately, many software applications weren't delivered in this way. As Simson Garfinkel shows in his contribution to this issue, "Leaking Sensitive Information in Complex Document Files—and How to Prevent It," the software tools we use every day can trip up even security-aware and highly motivated users who are trying to redact sensitive information from documents. His analysis reveals that this happens largely because one of the oldest usability principles—what you see is what you get—isn't supported. Existing software gives users the impression that information they've tried to redact is no longer accessible to a reader when in fact it's only superficially obscured. Garfinkel's conclusion confirms Theofanos and Pfleeger's point: the features that support redaction seem to have been "tacked on," requiring a rare in-depth understanding of the way the software renders documents to get it right. To ensure their redaction is working, users must carry out tests that take more time and effort than most are willing to spare (see Herley's article).

Herley's insight that "more is not the answer" conflicts with the traditional security view that users should be prepared to make more effort because security is important. Many advocate security awareness and education to increase users' ability to recognize threats and change their behavior to minimize risk. In "Going Spear Phishing: Exploring Embedded Training and Awareness," Deanna D. Caputo and her colleagues studied the effects of training against spear phishing attacks under realistic conditions in the workplace. They found that the embedded training they tried to provide—using an approach that previous usable security research reported to be effective—did not lead to fewer employees clicking a link in a spear phishing message. When none of the four training variants they created—based on state-of-the-art psychology research—made a difference, they concluded that "effective embedded training must take into account not only framing and security experience but also perceived security support, information load, preferred notification method, and more."

This again confirms Herley's assertion that security measures that require more user attention and effort are likely to fail. It also indicates that we must be extremely careful not to adopt new usable security solutions based on results from one-off laboratory or short-term crowdsourcing studies. The competing demands for user attention and effort are rarely replicated adequately in these studies, and short-term changes in behavior in response to interventions can fade over time.

"Helping You Protect You," our roundtable discussion with two experts representing major online service providers (Markus Jakobsson from PayPal and Sunny Consolvo from Google) and two leading academic researchers (Rick Wash from Minnesota State University and L. Jean Camp from Indiana University), shows that service providers understand that effective security can't require too much knowledge and effort. Authentication is a key example; we learn that many service providers are now moving to two-factor authentication (2FA) solutions, which can deliver improved security at lower user effort. But we must be mindful that those solutions must be accessible to all online users not just in terms of knowledge and effort but also in terms of cost.

Camp, who has carried out many studies with older users, points out that these are keen users who have much to gain from online participation but are risk averse. Warnings saying "you are at risk" are off-putting and unhelpful here. Furthermore, older users might be unable or unwilling to own a smartphone, which is the second factor of choice in many 2FA solutions currently deployed or planned.

Our experts agree that we need a fair division of responsibility between users and service providers. Many commercial service providers understand that it makes sense for them to take care of those aspects of security requiring expert knowledge and resources. They also understand that it doesn't make sense for them to scare their customers. As Jakobsson says, "It creates a sense of paranoia and fear, which makes some people throw up their hands and say, 'there's nothing to be done about security,' and then totally ignore it."

This isn't what we want; individuals have to take some responsibility to get effective and affordable protection online. But these responsibilities must be stated clearly and be understandable and manageable. As Camp points out, we can't protect online users from all risks all the time: "if people are aware they're taking a risk, I don't think that you should stop them. People have the right to be wrong and silly and everything else we are, but they should only take these risks knowingly."

Currently, most users are given no choice, because what they would need to do to protect themselves requires more experience than they have and more attention and effort than they can spare.

Usable security is often seen as simply an enabler of good security behavior: if the actions required aren't too difficult or effortful, users will comply. But human-centered design of security means enabling users to make informed security choices. First, their preferred choice needs to be available. Authors of privacy policies should take note here, and service providers need to manage their security issues without burdening legitimate customers (solving CAPTCHAs to prove you are human isn't something a customer would choose to do, ever). Second, we need to accept that users sometimes choose to take risks. Protecting users means giving them an accurate understanding of possible consequences—along with the likelihood of them occurring. ■

Reference

1. M.F. Theofanos and S.L. Pfleeger, "Shouldn't All Security Be Usable?," *IEEE Security & Privacy*, vol. 9, no. 2, 2011, pp. 12–17.

M. Angela Sasse is the professor of human-centered technology in the Department of Computer Science at University College London. Contact her at a.sasse@cs.ucl.ac.uk.

Charles C. Palmer is CTO for security and privacy at IBM. Contact him at ccpalmer@us.ibm.com.