T
Secur

DON'T BLAME THE USERS

Instead let's make computer security more usable, says the head of a new Ph.D. program.

BY MIKE VARGO

There is a growing consensus that the weakest link in computer and Internet security is not vulnerable software, but user behavior. Every year, according to various surveys, surprising numbers of users still fall for phishing scams. Others download things they shouldn't or disregard the most basic good practices, often wreaking havoc across their employers' networks.

Where Lorrie Cranor differs from many experts is in refusing to believe that user lapses are inevitable by-products of the ignorance of the masses. "Most security breaches can be attributed to human error," she says, then quickly adds the punch line: "which means they come from the failure of systems designers to meet human needs and accommodate human capacities and limitations."

Cranor is one of the founders of an emerging research field called "usable privacy and security." At Carnegie Mellon — where she holds cross-appointments in Computer science and Engineering and Public Policy — she directs one of the few comprehensive research centers in the field, CUPS: the CyLab Usable Privacy and Security Laboratory. Now she and her colleagues are building the world's first usable privacy and security Ph.D. program.

The CUPS Doctoral Training Program is being launched with a five-year, $3 million grant from the National Science Foundation. A charter class of six students enrolled in the fall of '09 and the program will take about 10 more each year. To grasp what students learn and do in this little-known field, let's join Lorrie Cranor for a whirlwind intro.

Usable Privacy and Security 101

Privacy and security are related but distinct issues. Clearly a website or computer must be secure (safe from malicious hackers) in order to give you privacy (control over what others can learn about you). On the other hand, Cranor points out, "a site that you visit may have good security yet offer little privacy." The site's owners might be selling customer data to telemarketers, for instance.

Research has shown that most users want privacy and security but aren't sure how to get either. The goal of usability work, in a nutshell, is to maximize their chances.

Cranor says there are three main strategies for doing so, one being to take obvious

A Ph.D. STUDENT STAKES OUT THE HOME FRONT

In the newly launched Ph.D. program for usable privacy and security, Michelle Mazurek is the "Home Storage Student." She is working with partners including her faculty advisors, ECE professors Lujo Bauer and Greg Ganger, on new systems for managing digital storage in households.

That is a growing problem. As Mazurek notes, many of us have text and multimedia files scattered across a multitude of devices at home: desktop PCs and laptops, video and music players and more. The project assumes that all devices can be wirelessly linked, and one nifty feature, Mazurek says, is a file-tagging system for "seeing that all files go where they're supposed to be, regardless of where they're created. For instance, you can specify that 'all my work files go on the laptop' in addition to the desktop."

In a distributed environment of this type, privacy and security concerns loom large. Mazurek's role is to address these, helping to develop methods to let each user in the home specify who can have access to what, under which conditions. As a first step, she and team members interviewed sample households to learn about needs and desires. Among the findings, Mazurek says, are that "presence" matters: "people feel more comfortable with others seeing their files if they can be present to monitor it. And people want the ability to make ad-hoc access decisions instead of just setting policies a priori."

Mazurek also learned that some people have strange habits. "For instance, they try to hide sensitive files by giving them funny filenames; burying them in sub-folders. It's like burying valuables in the bottom of a drawer." The downside, of course, is that you can forget where you hid the gold watch and a persistent thief can still find it. But to Mazurek such things are more than amusing tidbits. "What we're seeing are unmet needs, or imperfectly met needs, for privacy and security," she says. "Our job is to find better ways."

decisions out of people's hands by automating them. As she noted in a research paper, early antivirus programs "prompted users to make a decision about every detected virus," whereas today the common default mode is to just delete or quarantine infected files. But many choices aren't so conducive to automation. That leaves the other two approaches: designing features so they're intuitive and easy to use and educating the users.

Research by Cranor et al has shown that a great deal of confusion reigns. Many people conflate privacy and security. Some claim to be militant about privacy rights (they're known as "privacy fundamentalists"), yet in experiments they will enter more personal data than needed for an online transaction. We all judge by appearances, and many judge a website to be trustworthy if it looks "professionally done." The list goes on; solutions are needed.

Fish Stories and Nutrition Labels

Solution-wise, the CUPS research group has made perhaps its biggest splash thus far in user education. Have you seen Anti-Phishing Phil? He's a cartoon character, a young fish, who was created by recent EPP Ph.D. graduate Steve Sheng and former Communication Design student Bryant Magnien.

Phil and an older and wiser fish named PhishGuru star in an interactive, online game that teaches players how to recognize phishy emails and avoid getting hooked. Better still, Phil and PhishGuru are now being bundled into training programs for firms and organizations. Some organizations like to warn their members about phishing by the use of "simulated" phishing scams. (In one case, the U.S. Military Academy sent cadets an email signed by a fictitious colonel, asking for sensitive information. About 80 percent dutifully took the bait.) So Cranor and other CUPS faculty — through a spinout company called Wombat Security Technologies — are offering an added wrinkle: they'll write the simulated email, and rig it so that if you click on the baited link, you get an instant lesson from PhishGuru.

"It's taking advantage of a teachable moment," Cranor says. "People are more likely to be receptive to teaching when they realize they just fell for an attack."

Other projects now in the works at CUPS have to do with usable design. A survey of location-sharing services, with which you can use your GPS cell phone or Wi-Fi laptop to let people know where you are, found that systems on the market tend to lack good privacy-preference settings. Some leave you "open" to anyone who comes looking while others are confusing or don't give meaningful control. CUPS is piloting a system called Locaccino which, Cranor says, "makes it easy to set up privacy rules. For instance, 'my students can access my location only while I'm on campus on weekdays, but close friends and family any time, anywhere.'" (This too looks to be the basis of a spinout company.)

And speaking of confusion: most public websites have privacy policies but it's often hard to find them or figure out what they really mean. Thus Cranor and the CUPS team hope to create the equivalent of a "nutrition label" for privacy. Just as the labels on food products list the key ingredients in a standard format to help you comparison shop, the envisioned system would link with search engines to display various websites' privacy policies in a uniform fashion. The CUPS team operates a search engine called Privacy Finder, which demonstrates the privacy nutrition label concept.

The unifying theme in all CUPS projects is enabling people to make more informed choices more easily. This has been done in other areas; Cranor sees no reason it can't be done in online privacy and security. "We've already had faculty and students from many disciplines doing research," she says, "and the students in the new Ph.D. program are going to help us develop new methodologies." Visit the CUPS website for more information about the CUPS Ph.D. program and CUPS research projects and to try out Anti-Phishing Phil, Locaccino and Privacy Finder, http://cups.cs.cmu.edu.