PHYS ORG

A fresh perspective on internet security

December 21 2011, By Douglas Gantenbein

People don't do enough to protect themselves on the Internet. They don't use good passwords. They're poor at recognizing the URL of "phishing" sites. They ignore certificate errors.

Yet, to Cormac Herley, that's perfectly rational behavior, because people sense that all the headaches of keeping up to date on security probably aren't worth the trouble. Time spent constantly changing passwords or taking other security steps is valuable time lost, he says. By comparison, Herley says, the reduction of risk of having an account hacked or another security problem is relatively minor.

Herley—a principal researcher in Microsoft Research's Redmond's Machine Learning Department—has gained attention for his argument that much of what security experts insist people do to protect themselves not only ignores the real threats out there, but it's also a waste of money.

"An ounce of prevention may be worth a pound of cure," he says, "but a pound of prevention is not better than an ounce of cure. If you can't quantify how much of each you need, you're simply hand-waving."

In the past five years, Herley—working solo or with colleagues—has written about 20 papers that address many aspects of computer security: the prevalence of cybercrime, security advice for computer users, phishing prevention, and much more. With a deep background in signal processing and data analysis, he has taken an empirical approach to the problem of security, casting a critical, cost-benefit eye on what "everyone knows" is the best way to stay safe on the web.

In particular, Herley says, we rely too much on password strength. We are encouraged to use “strong” passwords that go beyond the name of a pet or “12345”—and to change them regularly.

Such guidance isn’t necessarily a bad thing.

“A strong password does make it harder for someone to guess or brute-force your password—this is unarguably true,” Herley says. “Stronger passwords have benefit. But they also have a cost. What’s unclear is whether the benefit is greater or less than the cost. ”

Hidden Costs of Security

That’s because adhering to strict security standards takes time and effort. In a paper published in 2009, Herley argues that people who break the usual password “rules”—using weak passwords, not changing passwords regularly, using the same password for multiple accounts—are acting rationally, not simply being lazy or careless.

In his paper So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, Herley notes that Internet users, on average, have 25 password-protected accounts to manage. Most also have an average of 6.5 passwords, using each of them at an average of 3.9 sites—breaking the common guidance to avoid reusing passwords.

Adhering to guidance against reusing passwords, Herley argues, costs a user a 3.9 times the effort, yet the benefit is hard to quantify.

Or, as Herley writes, with 180 million online adults in the United States, an hour of user effort is worth $2.6 billion and a minute per user per day is worth $15.9 billion per year. Instead of viewing users as incomprehensibly lazy, he suggests that security experts should treat them “as a professional who bills at $2.6 billion per hour and whose time is far too valuable to be wasted on unnecessary detail.”

These are the “externalities”—such as assuming that computer users’ time is free, when, in fact, it adds up rapidly—to which Herley refers in the title of his paper.

Fishy Approach to Phishing

Herley says that other common efforts to enhance security suffer from similar faults. Because of phishing and other spoofing attacks, it’s clear that Internet users need protection.

But to “read” a URL for phishing, an Internet user must look for numeric IP addresses, subtle spelling changes in the address bar, incorrect top-level domains, misplaced punctuation, and more. All of that takes time—again, against a threat that might be remote or mitigated relatively easily.

In Herley’s analysis, efforts by web users to master the intricacies of phishing should average no more than 2.6 minutes per year. Anything more, and the individual costs begin to outweigh the annual cost of phishing in the United States, about $60 million.

The same caution pertains to recognizing certificate errors, which occur when a browser is not connected to a website via a Secure Sockets Layer (SSL), indicated by the “https” in the URL, rather than “http.”

But Herley says that to gain the benefit of SSL connections, the user must type the entire URL, including “https”, or have the secure URL bookmarked. They also need to pay more attention to browser warnings about certificate errors.

And for all of that, there is relatively little benefit. He asserts that virtually 100 percent of certificate errors are false positives caused by legitimate sites that have name mismatches or expired certificates.

“The effort we ask of people is real,” Herley writes, “while the harm we warn them of is almost always theoretical.”

Herley certainly believes in web security. Strong passwords can prevent some attacks, for instance. But he advocates an approach to passwords that recognizes that people tend to pick common words to use. Why not take an approach that lets people use whatever they want—as long as that password has not reached a certain threshold of popularity within a website? He and two co-authors suggest that in a 2010 paper, Popularity is Everything: A new approach to protecting passwords from statistical-guessing attacks.

For the most part, Herley argues that most of what security experts ask people to do ignores the biggest threats. Forcing a password change every 60 days makes no sense if a person’s computer is infected with a keystroke-logging program, which captures keystrokes people use—including passwords—and directs them to a malicious recipient. The new password will be compromised immediately. It would be better to invest in software that detects a logging virus than to constantly change passwords and then try to remember them.

Laughs During a Conference

Herley has delved into security issues relatively recently. He earned his bachelor’s degree in electrical engineering at University College Cork in his native Ireland, received a master’s degree in the same field from Georgia Tech, then earned a Ph.D. from Columbia University.

Early in Herley’s career, he specialized in image processing and signal analysis. But in the mid-2000s, he saw that password practices had been the subject of almost no rigorous research.

“It was very under-studied, which surprised me,” he says. “People were spending all sorts of energies on lots of different security problems, but there was this gigantic elephant in the room, which was passwords. As far as the 2 billion users of the Internet are concerned, that would seem to dwarf everything else, yet it was receiving almost no attention.”

Herley realized he was on to something in 2007, when he was giving a talk on a paper he had co-written with Microsoft Research colleague Dinei Florêncio, titled A Large-Scale Study of Web Password Habits. The paper examined the password behavior of a half million web users—their average number of passwords, how often they are changed, password strength, and more.

During the talk, given to a crowd of security experts, Herley noticed that whenever he showed a slide or graph depicting poor password habits, he got a laugh.

“I’m used to giving dry technical talks, and usually, you really have to work for the laugh,” Herley says. “So I thought this was odd. What’s funny about it?”

Herley began to think that security experts’ mockery of everyday web habits showed that the experts were the ones out of touch, not the Internet users.

“The job of the security experts is to produce technology that serves the need,” he says. “If it isn’t serving the need, don’t laugh at it. Maybe some people on the web are dumb and lazy, but they are what they are.”

Rather than acknowledging that, Herley says, the security world instead keeps blasting people with more advice: Change passwords! Read URLs!

Watch for phishing attacks!

“The stuff has been accreting for 40 years,” Herley says of security guidelines. “It never goes away.”

Provided by Microsoft Corporation

Citation: A fresh perspective on internet security (2011, December 21) retrieved 27 April 2024 from https://phys.org/news/2011-12-fresh-perspective-internet.html