UC SANTA BARBARA

THE Current

October 27, 2015
Jim Logan

Web of Deceit

In an era when it seems every week brings a new story of large-scale hacking and identity theft, you might wonder if we're all just sitting ducks for bad guys with computers. The answer, say UC Santa Barbara researchers, is a firm *maybe*.

"There is no such thing as complete security," explained Giovanni Vigna, a professor of computer science who co-leads the university's Computer Security Group (SecLab) with Professors Christopher Kruegel and Richard Kemmerer. "I tell you, some things are more secure than others."

And Vigna would know. The SecLab does cutting-edge research on malware (malicious software), web security and cyber situation awareness. Its real-world research into cybercrime and hacking has drawn the support of such heavyweights as the National Science Foundation, Army Research Laboratory and Defense Advanced Research Projects Agency, better known as DARPA.

With October's designation as National Cyber Security Awareness Month, it's a good time to take a look at the evolution of online crime and security, and how we might mind our 1s and 0s to avoid becoming victims. To begin, it helps to understand how vast and quotidian the threat of cyber crime has become. Computers and cell phones — and for security purposes they should be treated the same — are ubiquitous, and the amount of personal data stored on them is staggering and growing. "We use them for banking, our health records, all sorts of different things," noted Vigna. "Someday we are going to store our genetic materials on a computer. Obviously, as we started using computers for more critical operations, the bad guys

realized, ‘Hey, there is money to be made.’ ”

Those bad guys are smart and connected with other malefactors happy to provide services designed to separate the unwary from their money and more. The threats are many, from identity theft, to cloned credit cards, to clever ways to trick the trusting into installing criminal software (“malware”) on their computers and smartphones.

“Nothing should surprise us at this point,” said Jennifer Holt, an associate professor in UCSB’s Department of Film and Media Studies who researches digital media infrastructure policy. “If it does, we are not paying attention.”

‘Hacking the User’

Sophisticated computer users aren’t going to fall for an email from a Nigerian prince looking to give away $50 million. But even they might click on a seemingly innocent link in an email that appears to come from a friend — a sneaky cyber attack known as “spear phishing.”

There’s a good chance they won’t even know the link took them to a website set up by criminals — until it’s too late, of course.

“One thing that has changed as technology has gotten better is that the focus has been more on hacking the user than hacking into computers,” Vigna explained. “So there is a trend in which attacks become more social engineering attacks, spear-phishing attacks, attacks that try to confuse users into doing something that will hurt their own environment and make it more insecure.”

Security experts say these types of attacks are on the rise and point up the need to educate the public. That’s not easy, Vigna said. “Educating large masses about the risk of using computers everyday is hard. It’s much easier to build good technology against these attacks than educating the users. We think that it’s difficult to detect malware. It *is* difficult, but it’s not as difficult as convincing everybody that they should not just click on every link they see in a piece of email.”

What You Can Do

Despite the panoply of threats today, experts say just a few steps will help keep you protected against cyber crime. And while nothing is foolproof in online security, nothing is more foolish than doing nothing. Here’s a look what every computer user

should do every day.

Monitor your assets: “Your financial assets, including your credit card, are your most valuable possessions,” Vigna noted. “Your personal information is also very valuable, and the only way to protect yourself for real is, first of all, to monitor your bank account, your credit card account, your credit report, your IRS returns because that is the only way in which you will find out. It’s very difficult to say, ‘Nobody will ever steal my credit cards.’ My credit card got stolen, and I work in security. So there is nothing that prevents that from happening.”

Use two-factor authentication: This makes logging on to a service like Facebook a two-step process that requires a smartphone app you can download from Apple’s iTunes Store or Google Play. It works like this: When you log on from a device Facebook doesn’t recognize, it will send a special code to your phone; enter that code and you’re in.

“If somebody steals your password to log into your Gmail account and tries to log in, they also need that number because they will be logging in from a location that has not been observed before, and if they don't steal your phone as well, they are out of luck. They cannot get in,” Vigna said.

‘Don’t do something stupid:’ Ill-considered behavior is the bane of computer security experts. No matter how brilliant the software — and Vigna and his SecLab crew are among the best in the world — it’s useless if you don’t use discretion while online. Don’t click on too-good-to-be-true links, and listen to your computer when it says you’re about to do something dumb. “If your operating system is telling you, ‘This site you’re connected to might compromise your computer,’ and you say, ‘I want to go anyway, because there's some good content there,’ well, then it’s on you,” he said.

‘Back up your stuff:’ One of the fairly new threats online is “ransomware,” and it’s odious. It’s a type of malware that typically encrypts the data on your computer and forces you to pay a hacker to get it back. Backing up your data — storing copies somewhere else — can protect you from that and other threats.

Exactly how you might do this is something on which Vigna and Holt have different perspectives. Holt is leery of data storage in the cloud — the digital realm of distant data centers — and points to the infamous hacks of Sony, Apple, Ashley Madison and others. “The only way to protect against data security breaches is to keep your

data *out* of the cloud, but that is not realistic in all cases," she said.

Vigna, however, believes the cloud is safe — especially for users looking to back up their data on one of the many inexpensive services. "Don't be scared of the cloud, and back up your stuff," he said. "Now, for like $12 a month you can have a bunch of services on the cloud continuously backing up all your stuff." As for security, he said, "Their whole business is being secure. Not the same thing with Ashley Madison; they were in a different line of business."

But wait, there's more: The potential threats to your online security are nearly endless, making it impossible to compile a complete list of tips to help keep you safe. The Internet, however, is here to help. With input from Vigna, here are just a few websites with gigabytes of good information:

• www.us-cert.gov — Official site of the U.S. Computer Readiness Team

• https://heimdalsecurity.com/blog/security-experts-roundup/ — Solid tips from a number of security experts.

• www.schneier.com/ — Bruce Schneier's security blog is invaluable.

• http://krebsonsecurity.com/ — Brian Krebs' blog is another must-read for the security conscious.

• www.fcc.gov/smartphone-security — The Federal Communications Commission's useful tips on smartphone security.

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.