Tech companies eye security that goes beyond passwords

June 19 2013, by Paresh Dave

In late February, a thief or thieves cracked into Evernote's digital vault filled with log-ins, passwords and email addresses belonging to 50 million users. It was a shocking cyberattack considering the Redwood City, Calif., company offers online lockers for people to safely store their files.

With its reputation on the line, the company quickly developed a security feature that may become the standard procedure for accessing online accounts: demanding two digital keys to gain entrance.

After inputting their passwords, Evernote customers who have opted to use the two-step feature must wait until the company sends a security code to their cellphones. Users must type in this additional code to gain access to their accounts.

Banks and other financial institutions have long had double-layered protection (i.e. asking a preset personal question such as "What was the name of your first pet?"). But a recent spate of major cyberattacks that have exposed hundreds of millions of personal accounts to hackers is increasing pressure on nonfinancial Web services to fortify their digital doors beyond a single password.

That's fueling a booming industry. Researchers are experimenting with futuristic electronics that are wearable or even digestible. And companies are working on making existing products harder to crack. Efforts include equipping smartphones and USB sticks with fingerprint scanners to identify users and developing keyboards that recognize an individual's touch.

Some of these technologies could take years to hit the market, if ever. Still, many in the industry say two-step authentication eventually will become as routine as brushing teeth.

Apple, Twitter, LinkedIn, Facebook, Dropbox, Microsoft, Yahoo and Google all offer some form of two-step verification. Typically, users can opt to receive the security code either through a text message or a smartphone application.

Getting consumers to take advantage of this extra security is another matter. At present, customers of these firms must voluntarily sign up to use the two-step verification. None of the companies would say how many of their users have opted in, but security experts said the numbers are probably small.

Although many people are willing to endure extra security to access computer systems for their jobs or to protect their banking or health insurance information, going through an extra layer to use social media or email is a hassle, said John Chuang, an information professor at the University of California-Berkeley.

"If I'm an employee and I need it to get my work done, I'm going to do it," Chuang said. "Logging into LinkedIn, that's a different calculus."

Still, Google security engineer Mayank Upadhyay predicts users will become more accustomed to text-messaged codes as more companies offer the feature.

"The more people who have it, the faster the next set of people are enrolling in it, because they've been told about it by friends," he said.

Google is speeding ahead developing what it considers more secure and usable methods of two-step verification that could catch on with users.

By the end of this year, Google expects to have a limited number of users testing a USB thumb drive that could be used like a key. Users would first have to enter their personal identification number on the device before using it. When plugged into the computer, the USB stick would automatically log users into Google and other websites.

Google is part of an industry alliance trying to get more websites and technology companies to use the same security standards. The alliance's goal is to let users use any device of their choice, whether it's the USB stick, a phone with a special chip or a laptop with a fingerprint scanner.

Companies that manufacture the USB keys could choose to offer a fingerprint scanner or some other technology as a bonus. Users may scan their fingerprint once every morning to unlock their online life. A new scan and a PIN entry could be required before any financial transaction.

Mike DiPasquale, chief executive of fingerprint technology provider Bio-Key, said he expects fingerprint scanners to become a standard feature on phones because the technology costs just $2 a device. Mobile devices could also validate based on location, voice, touch or other biometrics.

DiPasquale said handset makers are realizing that smartphones and tablets are becoming a platform for every type of transaction.

"If security starts to fail, the whole premise behind e-banking, e-payments and e-commerce will come to a screeching halt," he said.

At Berkeley, Chuang's idea for the future is called Passthoughts. Users log into their accounts by connecting to a brain wave reader and thinking about a secret phrase that they have saved. Every thought generates a unique set of brain waves. The computer will recognize the thought each time. The price of these special readers has come down from thousands of dollars to $99, making the idea more plausible.

Last month, Motorola Senior Vice President Regina Dugan showed off two other futuristic ways that someone can authenticate themselves.

One technology involves an electronic tattoo that would transmit information to unlock a battery-operated device and access websites. Chuang said that although the idea holds a great deal of promise, it's unlikely the technology will reach consumers in the next couple of years. The problem is electricity.

"When they showed the demo, it's not very appealing to show that you attach a battery to that circuit to drive it," Chuang said. "The limit is in the battery technology and miniaturizing it to be able to include it within the flexible electronics."

Dugan also showed off a small pill that creates an energy signal within the body once it's swallowed. The FDA-approved pill technology was originally designed for medical use, but researchers discovered it could turn the entire body into an authenticating device.

Dugan said it has already been adapted to successfully unlock a phone. Dennis Woodside, chief executive of Google-owned Motorola Mobility, cautioned that neither technology was close to being finalized.

Other researchers have looked into validating a person's identity by tracking the pace at which they type.

The Obama administration has waded into the password problem too. The National Institute of Standards and Technology funded five test projects as part of an initiative to develop a voluntary online network that would enable credentials for one website to be used to access all other websites.

In the meantime, companies such as Duo Security in Ann Arbor, Mich., are trying to ease the pain for users who might have switched to two-step log-ins but are tired of managing multiple accounts. Duo's product taps into services that already have open standards. Log-in requests get filtered through the application, and the user need only tap "accept" or "deny."

Among Duo's clients, according to its website, are the University of Michigan's Departmental Computing Organization and the CedarCrestone technology consulting company in Atlanta. Google's venture-capital arm is among Duo's investors.

Richard Li, Duo's vice president of product and strategy, said he's afraid two-step verification won't catch on quickly because it's being written off as agonizing.

"We want people to understand that it's not all the same," he said. "We don't want people's first experience to be horrible and say it's not easy to use."

Evernote and many others who recently launched two-step verification have closed systems that are incompatible with Duo's service. Experts said each company has unique security requirements, and that could thwart the vision of Google and others.

Evernote product manager Jaime Hull said the company would certainly make sure to keep up with developments as the industry settles on a standard.

"We also don't want to burden users with trying out every new technology that comes along," she said.

Citation: Tech companies eye security that goes beyond passwords (2013, June 19) retrieved 27 April 2024 from https://phys.org/news/2013-06-tech-companies-eye-passwords.html