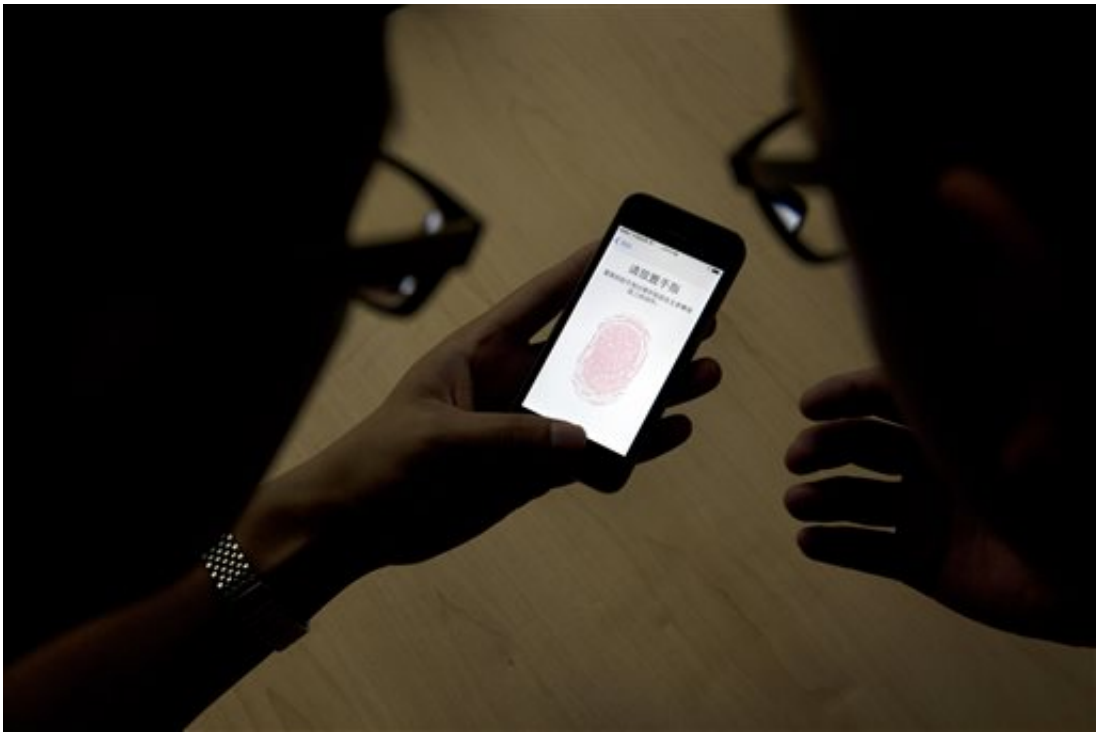
Tech Tips: Stay safe by reducing reliance on passwords

June 17 2015, byAnick Jesdanun



In this Sept. 11, 2013, file photo, an Apple employee, right, instructs a journalist on the use of the fingerprint scanner technology built into the company's iPhone 5S during a media event in Beijing. The latest iPhones and Samsung Galaxy phones have fingerprint IDs that make it easier to unlock phones. Instead of typing in the four-digit passcode each time, you can tap your finger on the home button. (AP Photo/Ng Han Guan, File)

Mix upper and lower case letters in your password? Substitute the

numeral 1 for the letter l? Throw in an exclamation point and other special characters? Who can remember all that for dozens of websites and services?

No wonder it's tempting to turn to apps and services that promise to keep track of your passwords, either on your device or online. All you need to remember is your master password.

But these password managers are like treasure chests for hackers. If your master password is compromised, all your accounts potentially go with it. Services that store password data online are particularly troublesome because they are easier for hackers to break.

Don't do it, I've been saying for years. Now, I hate to say, "I told you so."

LastPass, which offers a service that stores multiple passwords in encrypted form, says it has detected "suspicious activity." Although it says it found no evidence that individual passwords or user accounts were breached, it's advising users to change their LastPass master password.

I advise users to come up with a better system instead, one that relies less on just passwords.

Here are some tips:

___

ALL ACCOUNTS AREN'T EQUAL

Instead of having to remember dozens of complex passwords, maybe you need to remember only a half-dozen.

Focus on accounts that are really important: Bank accounts, of course. Shopping services with your credit card information stored. And don't forget email.

Who would want your mundane chatter? Well, email accounts are important because they are gateways for resetting passwords for other services, such as your Amazon account to go on a shopping spree.

___

WHAT ABOUT OTHER ACCOUNTS?

Maybe you don't need to worry about a password for a discussion forum or a news site. Yes, there's the embarrassment of someone posting on your behalf, but it's not the same as stealing thousands of dollars. Yet if it's a discussion forum you value, and you've established a reputation under that identity, you might want to prioritize that, too. That thinking applies to social-media accounts such as Facebook and Twitter.

For the rest of your accounts, it's not as bad to turn to a password manager, but it might not be necessary. Web browsers from Apple and Google have built-in mechanisms for storing frequently used passwords. You even have options to sync those online if you use multiple devices. Google's new Smart Lock feature extends that to Android apps, too, so you're not limited to Web browsing. Many services also let you sign in with your Facebook or other ID instead of generating new passwords each time. Make sure the ID service offers two-step verification, as I'll explain later. Turn that on.

Again, use these only for your less-important accounts. For the highly sensitive ones, choose a unique password and remember it. Write it down by hand and keep it in a safe place. If you must store it electronically, use password-protected files kept on your device—not

online.

—

PHONES AND FINGERPRINTS

If you haven't protected your phone with a passcode, tsk tsk! Someone can easily swipe your phone and get to your email account to unlock all sorts of other accounts.

Fortunately, the latest iPhones and Samsung Galaxy phones have fingerprint IDs that make it easier to unlock phones. Instead of typing in the four-digit passcode each time, you can tap your finger on the home button.

Apple now allows other app developers to use that fingerprint ID, too. So you can unlock banking apps with just a tap of your finger. In its upcoming Android update, called M, Google is also promising to make it easier for app makers to incorporate fingerprint ID. And Microsoft plans support for biometrics—such as a fingerprint or iris scan—in the upcoming Windows 10 system.

—

DOUBLE SECURITY

Major services including Apple, Google, Facebook, Microsoft and Dropbox offer a second layer of authentication, typically in the form of a numeric code sent as a text message. After you enter your regular password, you type in the code you receive on your phone to verify that it's really you. A hacker wouldn't have access to your phone.

You need to go into the account settings to turn it on this feature, which

goes by such names as two-factor authentication or two-step verification.

It's a hassle, but it keeps your accounts safer. Just assume that your password will get compromised at some point. This extra layer will keep the hacker from doing anything with it.

___

EVEN SAFER ...

When given a choice, sign in with your mobile number rather than your email address. It's much easier to hack into an email account to reset passwords. Of course, you'll have to trust the service not to use your mobile number for marketing. In many cases, I still use my email—with the two-step verification.

Also be careful when creating security questions to reset passwords. Your dog's name? Your first school? These are things someone might find on your social-media page or elsewhere online. I make up answers and make them as strong as my regular passwords.

I won't repeat my tips on creating strong passwords, but you can find them here: passwords" target="_blank">bigstory.ap.org/article/7-ways … ronger-passwords