Review: Strong Passwords and Other Security Tips

ANICK JESDANUN, AP Technology Writer

NEW YORK (AP) — Rarely does a week go by without news of another hacking incident, whether it's Chinese hackers accused of breaking in to The New York Times' computer systems or Burger King finding its Twitter account taken over by pranksters.

Security threats aren't new and have long been part of online life. But the increased attention on them makes now a good time to review ways you can protect yourself. If nothing here feels new, that's good, as it means you've been doing the things you need to do to keep your accounts safe from hackers. Although there's no way to completely eliminate threats, minimizing them will go a long way.

One of the best things you can do is to make sure your password is strong.

If someone's able to guess the password to your email or Facebook account, that person can post or send embarrassing things on your behalf. Someone was able to access Burger King's Twitter account recently and changed its profile picture to a McDonald's logo. If a banking or Amazon account is involved, someone could pay bills or buy iPads under your name — with your money.

What's worse, getting a password to one account is often a stepping stone to a more serious breach. Someone can use your email or Facebook account to send spam and scam messages to your friends, for instance. And because many services let you reset your password by sending an email to your address on file, someone with access to your email account can reset passwords and gain access to all sorts of things. If the compromised password is one you use for work, someone can snoop around for files on your employer's network with trade secrets or customers' credit card numbers.

Here are ways you can keep your password strong to ward off that initial intrusion:

— Make your password long. The recommended minimum is eight characters, but

14 is better and 25 is even better than that. Some services have character limits on passwords, though.

— Use combinations of letters and numbers, upper and lower case and symbols such as the exclamation mark. Some services won't let you do all of that, but try to vary it as much as you can. "PaSsWoRd!43" is far better than "password43."

— Avoid words that are in dictionaries, even if you add numbers and symbols. There are programs that can crack passwords by going through databases of known words. One trick is to add numbers in the middle of a word — as in "pas123swor456d" instead of "password123456." Another is to think of a sentence and use just the first letter of each word — as in "tqbfjotld" for "the quick brown fox jumps over the lazy dog."

— Substitute characters. For instance, use the number zero instead of the letter O, or replace the S with a dollar sign.

— Avoid easy-to-guess words, even if they aren't in the dictionary. You shouldn't use your name, company name or hometown, for instance. Avoid pets and relatives' names, too. Likewise, avoid things that can be looked up, such as your birthday or ZIP code. But you might use that as part of a complex password. Try reversing your ZIP code or phone number and insert that into a string of letters. As a reminder, you should also avoid "password" as the password, or consecutive keys on the keyboard, such as "1234" or "qwerty."

— Never reuse passwords on other accounts — with two exceptions. Over the years, I've managed to create hundreds of accounts. Many are for one-time use, such as when a newspaper website requires me to register to read the full story. It's OK to use simple passwords and repeat them in those types of situations, as long as the password isn't unlocking features that involve credit cards or posting on a message board. That will let you focus on keeping passwords to the more essential accounts strong.

— The other exception is to log in using a centralized sign-on service such as Facebook Connect. Hulu, for instance, gives you the option of using your Facebook username and password instead of creating a separate one for the video site. This technically isn't reusing your password, but a matter of Hulu borrowing the log-in system Facebook already has in place. The account information isn't stored with Hulu. Facebook merely tells Hulu's computers that it's you. Of course, if you do this, it's even more important to keep your Facebook password secure.

— How do you keep track of these passwords? There are programs you can buy, if you're willing to put your trust in them. I use an Excel spreadsheet, but I encrypt it with its own password — a rather complex one. I am well aware that if the file gets compromised, all my services go with it. In fact, I once had it on a USB drive, which I had in a backpack that got stolen. I had to spend several hours changing passwords on all my accounts, just in case someone managed to break the password to that file. As a precaution, don't name that file "passwords." Name it something generic and boring.

— Ideally you'll have a system for creating and remembering passwords without needing the spreadsheet. For example, you might have a string that's constant, such as "?t7q1b9f8j2o0t0l1d!" (the acronym for "the quick brown fox jumps over the lazy dog" with my area code and ZIP code reversed and a few special characters put in). To vary it, you could add the first two letters of the website you are using to the front and the next four to the end. Or put the consonants in front and the vowels at the end, with every other letter capitalized and the letter O replaced with the number zero. So for Amazon, it would be "mZn?t7q1b9f8j2o0t0l1d!Aa0." Just try to guess that!

Of course, I'm not smart enough to have a system like that for myself.

Whatever system you adopt, it's good to change your password — and system — from time to time. And if there's reason to believe your password might have been compromised, change it immediately.

One other thing to be aware of: Many sites let you reset your password by answering a security question, such as the name of your pet or the name of your high school. Of course, these violate good password practices by requiring you to use something that can be easily looked up. Others ask for your favorite movie or hobby. That might not be easily looked up, but your tastes change over time.

Furthermore, because these questions get repeated from site to site, the answers you use violate the rule against repeating passwords.

I try to make these answers complex just like passwords, by adding numbers and special characters and making up responses. Unfortunately, some sites won't let you do that, and you'll be stopped if you try to enter a numeral when asked for a city name, for instance. These services will often send an email when a password gets reset this way, so be sure the address on file is current. Change your password and security questions immediately if you're notified of a reset you didn't initiate. You might want to contact the service as well.

While you're at it, make your username complex, too, if you're allowed to choose one. Banking sites typically do.

Some services such as Gmail even give you the option of using two passwords when you use a particular computer or device for the first time. If you have that feature turned on, the service will send a text message with a six-digit code to your phone when you try to use Gmail from an unrecognized device. You'd need to enter that for access, and then that code expires. It's optional, and it's a pain — but it could save you from grief later on. Hackers wouldn't be able to access the account without possessing your phone. Turn it on by going to the account's security settings.

Beyond passwords, here are a few other things to help you stay safe:

— Software flaws. Many break-ins result from flaws in the software program you

use, whether it's the Windows or Mac operating system, a Web browser or a video player. It's a good idea to let those programs automatically check for software updates, as those updates may contain fixes to known flaws. You can also check this government website to learn of the latest threats and fixes: http://us-cert.gov .

— Malicious software. Even if the software you're using is flawless, hackers may create a security opening by tricking you into installing a malicious program. That can happen if you click on a bad email attachment or link in your email. In rare cases, visiting a problematic website can cause the software to download. Should malicious software get on your computer, a hacker might be able to use the opening to look around for sensitive data, or record your keystrokes to capture your complex passwords. To minimize the threat, use caution when visiting unknown sites or opening mysterious email.

— Security software. Many companies sell anti-virus and other software to protect your computer from malicious software. There's a free one available at http://www.avg.com . Windows and Mac computers also come with firewalls to block some threats. Be sure it's turned on.

Think of these measures as layers of defense. If one gets breached, there's another to back you up. But eventually, the intruders will get through. Slow them down by making each layer as strong as possible.

—

Anick Jesdanun, deputy technology editor for The Associated Press, can be reached at njesdanun(at)ap.org.