Tech Tips: Add 2nd layer of protection online

April 23 2014, by Anick Jesdanun

In this Wednesday, Feb. 27, 2013 photo illustration, hands type on a computer keyboard in Los Angeles. In the wake of the Heartbleed security threat, many security experts recommend a second layer of authentication _ typically in the form of a numeric code sent as a text message. You enter that code on the website to verify that it's really you and not a hacker who doesn't have your phone. (AP Photo/Damian Dovarganes, File)

If the Heartbleed security threat teaches us anything, it's that passwords don't offer total protection.

Browsers are supposed to keep passwords and other sensitive data safe, but a technical flaw in a widely used padlock security technology allows hackers to grab the information anyway. Even without this latest discovery, there have been countless disclosures of hackers breaking in to grab usernames and passwords, plus credit card numbers and more.

That's why many security experts recommend a second layer of authentication—typically in the form of a numeric code sent as a text message. If you're logging in to a website from your laptop, for example, you enter your password first. Then you type in the code you receive via text to verify that it's really you and not a hacker.

I've been using what's known as two-factor authentication or two-step verification on most of my accounts for more than a year, after seeing too many mysterious attempts to reset my Facebook password by someone who isn't me. The main exception was Gmail, but I enabled that recently after the discovery of Heartbleed. I was afraid the second authentication would be a pain to use, but things are going more smoothly than I expected after the initial setup.

The idea behind these double-layer passwords is to make it harder to use a password that's compromised or guessed. You're asked for a second piece of information that only you are supposed to know.

To balance security and convenience, you can typically bypass this check the next time you use the same Web browser or device. It won't help if someone steals your laptop, but it'll prevent others from using your password on their machines. If you're logging in at a library or other public computer, remember to reject the option to bypass that check next time.

The second piece of authentication could be your fingerprint or retina scan, though such biometric IDs are rarely used for consumer services.

Financial services typically ask for a security question, such as the name of your childhood pet, the first time you use a particular Web browser or device. That's better than nothing, though answers can sometimes be guessed or looked up. Some banks offer verification codes by text messaging, too.

I like that approach and use it for a variety of email and social networking services. To me, email accounts are the most sensitive because email can be used to reset passwords elsewhere. That includes my banks and shopping sites.

The two-step requirement is fairly simple to turn on. With Google, for instance, it's under the Security tab in your account settings. On Facebook, look for Login Approvals under Security in the settings. With Apple IDs, visit appleid.apple.com rather than the account settings on iTunes.

After you enable it, you'll typically have to sign in to your account again on various Web browsers and devices. After entering your username and password, a code will get set to your phone. You'll have to enter that to finish signing in. This has occasionally meant getting off my couch to grab my phone from the charger, but that's a small price for security.

What if you're somewhere without cellular access and can't receive texts?

Most services have backup mechanisms. Google, Facebook and Microsoft have apps that will let you receive verification codes even when you're offline. Google and Facebook also let you generate 10 backup codes that you can download or print to keep in your wallet. Each can be used only once.

You can also turn off the two-step requirement temporarily if you'll be

traveling without cellular access, though I don't recommend it. The reason I turned it on last year was because I was leaving the country and wouldn't be able to deal with further mysterious reset attempts.

Occasionally, you'll run into an app that won't accept the text code. Apple's Mail app on iPhones, iPads and Mac computers is one. Microsoft's Outlook software is another. If that happens, you'll have to go to your service's settings to generate a temporary password for that particular app. It's a pain, but I've rarely needed to do this.

There are several other challenges to making this work smoothly. For example, if you have a shared Twitter account, such as for your company or organization, two-step verification isn't very practical unless you also share your phone. There's a 12-character, hard-to-guess backup code you can use instead. But it's no security if you jot it down next to your main password.

The biggest problem, though, is losing your phone. Some services will let you provide a backup number, including a friend's cellphone or a landline phone. With Google, the code can be sent as a voice message instead of a text. Others offer a complex recovery code, which you'll have to jot down and keep in a safe place.

I know two-layer security is inconvenient. The first password is difficult enough to deal with. But think of the inconvenience involved should someone break into your account and shut you out. Consider the use of verification texts to be insurance.