A Closer Look: A second layer of security online

8 September 2014, by Anick Jesdanun

In this June 16, 2013 file photo, Internet users browse the Internet in Hong Kong. Recent hacks exposing nude photographs of Jennifer Lawrence and other celebrities are prompting calls for people to fortify their online accounts with a second layer of security. (AP Photo/Kin Cheung, File)

Recent hacks exposing nude photographs of Jennifer Lawrence and other celebrities are prompting calls for people to fortify their online accounts with a second layer of security.

Thieves broke into the celebrity accounts at online storage services such as Apple's iCloud. Although Apple's systems weren't compromised, the hackers were able to figure out passwords and answers to personal security questions, according to the company.

In response, Apple urged users not only to set a strong password, but also to enable the second security layer, often known as two-step verification. It's a technique offered by most major services, including Google and Facebook. Amazon and its Cloud Drive service are notable exceptions.

Two-step verification typically works this way: When you log in from a new device, you must enter a code that is sent to your main phone. That way, a hacker who guesses your password would still need physical possession of the phone. You're usually able to bypass the check the next time you use that same device, on grounds that you've already proven that device is yours.

The catch is you need to turn the feature on. And it means occasionally getting off your couch to retrieve your phone when you're using a new Web browser, tablet or other gadget. But it beats having naked photos and other sensitive information stolen.

Here's a closer look at what the major services offer and how to enable two-step verification:

——

— APPLE ID

The Apple ID is the key to not just iCloud, but the Apple app store, iTunes, iMessage, Facetime and more.

To set up two-step verification, you need at least one phone that can receive texts. It doesn't have to be an iPhone.

Go to appleid.apple.com and log in with your Apple ID. Go to the "Password and Security" tab. Click "Get started..." under "Two-Step Verification."

In some cases, you have to wait. I had a three-day waiting period because I had just changed my password. Though the delay is inconvenient, it prevents hackers from enabling two-step verification on their own phones and then locking you out. Apple sends email to alert you that someone has tried to set this up, so you can stop it if the request wasn't from you.

After the waiting period, you need to enable one or more phones to receive the texts with the special codes. Having more than one helps if you lose your main one. That second phone can be a friend's. Don't enable too many, though, as that decreases security.

Once this is set up, you'll get a text with a four-digit code whenever you use a new device—say, one of the new iPhones expected to be announced Tuesday.

Before you're done, you're also given a 14-character recovery key as a backup to manage your account, in case you lose all your phones. This is in lieu of easy-to-guess security questions such as your pet's name. Keep this recovery key in a safe place —perhaps with your passport or birth certificate. If you lose it along with all your phones, you could be locked out of your account forever.

Apple CEO Tim Cook might use an event Tuesday to talk more about security in the upcoming iPhones and iOS software, but two-step verification is something everyone can do without waiting for Apple. That's especially important as Apple rolls out iCloud Drive and the ability to store a greater variety of documents online.

___

— GOOGLE ACCOUNT

The Google account is used for a variety of Google services, such as Gmail and Google Drive storage. Google also lets other services use its ID system so you don't need to create separate accounts and passwords for everything.

Start by going to the account settings, which you can get to from the top right of your Gmail page. Look for "2-Step Verification" under the security tab. You enter or choose a cellphone for receiving texts. If you have a landline phone, you can get Google's six-digit verification code as an automated recording instead. You can enable backup phones, too.

With Apple IDs, you're mostly dealing with Apple devices and Apple's websites, so everything just works. The Google account works with a greater variety of devices and websites, some of which don't know what to do with this verification code. One example is the Mail program on iPhones, iPads and Mac computers. Another is Microsoft's Outlook software.

Go to "App-specific passwords" to generate a one-time password for that specific app or service. Your regular password won't work.

You can also generate backup codes to use when you can't receive phone calls or texts, such as when traveling abroad. These get used in place of the six-digit code you'd normally get by text. You get 10 at a time to download or print out, and each can be used just once. You can also install the Google Authenticator app on Android, Apple and BlackBerry devices. The app generates codes you can use when you can't receive texts.

___

— MICROSOFT ACCOUNT

Microsoft accounts are used for email, OneDrive storage and more. You turn it on by going to the "Security & Password" tab of your account settings.

The process is much like Google's. You're given a seven-digit verification code via text. You can install an app to generate codes when you can't get texts, or you can have the code sent to an email address on file. You can create one-time passwords for devices and websites that don't support Microsoft's two-step verification system.

You don't get backup codes like Google's to print out and use in lieu of texts, but you can create a fallback recovery key like Apple's.

___

— AND THE REST ...

Facebook, Twitter and Dropbox are among the other services that offer two-step verification. They all basically work the same way. The differences are primarily in what they offer beyond receiving codes by text. Facebook, for instance, tries to steer

you toward its Code Generator app, with text used more as a backup. Also, Facebook calls it "Login Approvals" rather than two-step verification.

Even if you don't have naked photos in those accounts, turning this feature on is smart. It'll help keep others out of your private email, Facebook conversations and other sensitive data.

___

Apple ID: support.apple.com/kb/ht5570

Google: www.google.com/landing/2step

Microsoft: windows.microsoft.com/en-us/wi … tep-verification-faq

APA citation: A Closer Look: A second layer of security online (2014, September 8) retrieved 17 October 2021 from https://phys.org/news/2014-09-closer-layer-online.html