THE WALL STREET JOURNAL.
SUNDAY, MARCH 26, 2023

PERSONAL TECHNOLOGY

The Strongest Protection for Your Online Accounts? This Little Key

Passwords aren't enough to fend off hackers; these dongles are the best defense

By Nicole Nguyen

Strong passwords are very important, but they're not enough to protect you from cybercriminals.

Passwords can be leaked or guessed. The key to online security is protecting your account with a strong secondary measure, typically a single-use code. This is referred to as "two-factor authentication," or 2FA, as the nerds know it.

I've written about all the different types of 2FA, such as getting those codes sent via text message or generated in an authenticator app. Having any kind of second factor is better than none at all, but physical security keys—little dongles that you plug into a USB port or tap on your phone during account logins—offer the highest level of protection.

Security keys have been around for over a decade, but now they're in the spotlight: Apple recently introduced support for them as an optional, added protection for Apple ID accounts. Last month, Twitter removed text-message-based authentication as an option for nonpaying users, recommending instead an authenticator app or security key.

Some people are hesitant to use security keys because carrying around a physical object seems burdensome and they come with a $30-and-up added cost. Plus, what happens if they get lost?

I've used security keys since 2016 and think they are actually easier to manage than codes—especially with accounts that don't require frequent logins. They're not only convenient, but they can't be copied or faked by hackers, so they're safer, too.

PHOTO ILLUSTRATION BY RACHEL MENDELSON/THE WALL STREET JOURNAL, YUBICO

Here's how to weigh the benefits and common concerns of adding one or two of these to your keychain.

Which security key should I use?

Many internet services support the use of security keys, and you can use the same security key to unlock accounts on many different services. I recommend two from industry leader Yubico:

- YubiKey 5C NFC ($55) if you have a USB-C laptop or tablet
- YubiKey 5 NFC ($50) for devices with older USB ports

Other options include Google's Titan security keys ($30 and up). In addition

to working with laptops and tablets with USB ports, these keys are compatible with smartphones that have NFC wireless. Most smartphones these days have that, since it's the technology behind wireless payments such as Apple Pay.

Adam Marrè, chief information security officer at cybersecurity firm Arctic Wolf, recommends that your chosen key is certified by the FIDO Alliance, which governs the standards of these devices.

How do security keys work?

To add a key, look in the security settings of your major accounts (Facebook, Twitter, Google, etc.). During setup, it will prompt you to insert the key into your laptop or tablet's port or hold the key close to your phone for wireless contact.

Apple requires you to add two security keys to your Apple ID account, in case you lose one.

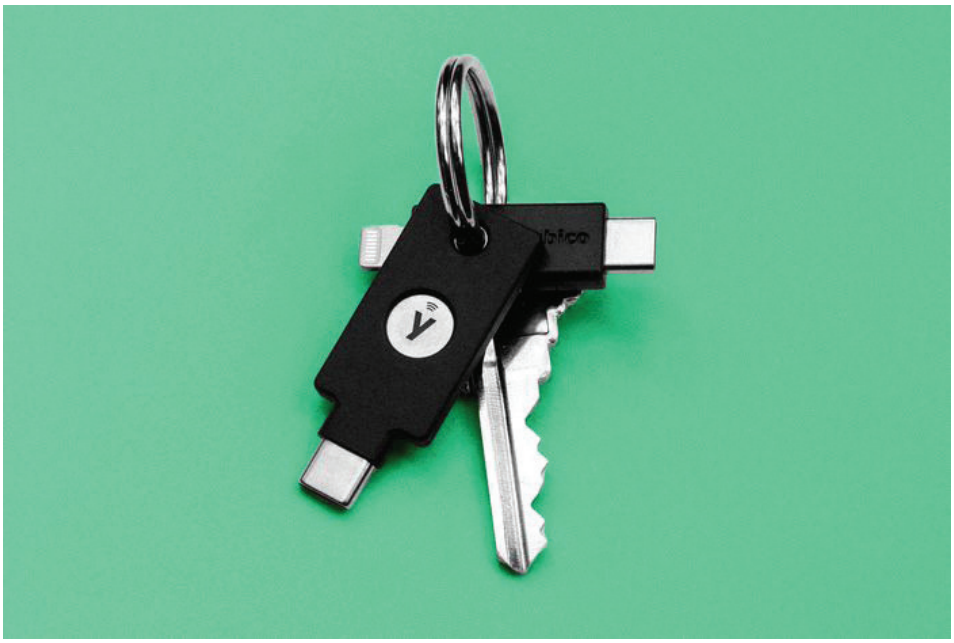
Typically, when you log in, you just go to the app or website where you've set up a key, enter your username and password as usual, then once again insert the key into the device or hold it close. (Some keys have a metal tab you have to press to activate.) At that point, the service should let you right in.

Why are they so secure?

Getting those two-factor login codes via text message is convenient, but if you are someone criminals are targeting, you could be the victim of SIM swapping. That's where thieves convince carriers to port your number to a new phone in their possession, and they use it along with your stolen password to hack your accounts.

Even if they don't go to all that trouble, criminals might try to trick you to hand them your codes, by calling you or spoofing a website you typically visit. At that point they can use the code for about 60 seconds to try to break in, said Ryan Noon, chief executive at security firm Material Security.

Security keys protect you in two ways: First, there's no code to steal, and second, they use a security protocol to verify the website's domain during login, so they won't work on fake sites.



Think of your security key as a house or car key: Always have a spare.

PHOTO ILLUSTRATION: RACHEL MENDELSON/THE WALL STREET JOURNAL, YUBICO

You can also add an authenticator app such as Authy to your most important accounts, to use only as a backup. But once you add these secure methods, you should consider removing the text-message code option.

In the rare case that someone snoops your passcode then steals your iPhone, beware: The perpetrator could still make Apple ID account changes using only the passcode, and even remove security keys from your account.

What happens if you lose your key?

The most important rule of security keys is to buy an extra one (or two).

"Think of your security key as you would a house or car key," said Derek Hanson, Yubico's vice president of solutions architecture. "It's always recommended that you have a spare."

If you lose a security key, remove it from your accounts immediately. You should have already registered your spare or an authenticator app as a backup to use in the meantime.

Where can you use a security key?

Start with your most valuable accounts: Google, Apple, Microsoft, your password manager, your social–media accounts and your government accounts.

When it comes to financial institutions, many banks don't offer security-key protection as an option, though most leading crypto exchanges do.

What comes after security keys?

Security professionals and tech companies widely agree that passkeys are the future. They're a new type of software option that combines the high security of a physical key with the convenience of biometrics such as your face or fingerprints. Passkeys are supported across the Android, iOS, Mac and Windows platforms, and some of your favorite sites already let you use them.

On several sites, such as Facebook and Dropbox, you can use a biometric passkey as a second factor.You can create a passkey on Facebook in security settings by following the app's instructions under the security-key option. Dropbox has a similar passkey setup. Once you're done, you'll use your face or fingerprint as a second factor, instead of a code or key.

Eventually, physical security keys could be what we keep safe in strong boxes, as backups for our biometric-enabled passkeys. Even then, you're probably going to want to have spares.