SCAMS & FRAUD

Physical Security Keys Can Offer Extra Protection from Scammers

The pros and cons of using hardware keys to secure your digital life

By Matt Alderton, AARP
Published March 05, 2024 • EN ESPAÑOL

PAUL SPELLA /GETTY 20

Although a determined criminal will always find a way inside a home — by breaking a window, say — locked doors have long been the first line of defense against burglaries. Without a key, gaining entry is much more difficult, conspicuous and time-consuming.

The same kind of deterrence that keeps your physical possessions safe can help you safeguard your digital valuables.

That's the principle behind hardware security keys. Designed to protect you from cybercriminals, they are the equivalent of a physical house key for your electronic identity. Knowing what they are and how to use them can help you decide if security keys are right for you.

What is a hardware security key?

In the simplest terms, a hardware security key is a small device that you connect to your computer or mobile device to securely access online accounts.

It's "basically a little dongle that you can connect to your USB port — it comes in USB-A or USB-C format — or that you can tap on your device, if your security key and your device support NFC, which is near-field communication," explains Santiago Del Portillo, global sales engineer at Kensington, which sells security keys under the brand name VeriMark.

Security keys are used as a second factor in multifactor authentication (MFA). "What hackers have discovered over the last two decades is that people are pretty lazy and tend to use the same passwords everywhere," says Steve Won, chief product officer at password management software company 1Password. "The concept of multifactor authentication is: Even if you use the same password, let's have a safeguard — something the attacker's not going to have."

You've probably used MFA before: To log into an account, you must provide your username and password, then complete a second action proving your identity, like answering a security question or entering a one-time passcode that's sent via text message. In other words, you have to unlock two doors to access your account. In lieu of other methods, a hardware security key unlocks the second door, literally and figuratively.

"A security key is really a physical way of verifying presence," says Craig Lurey, cofounder and chief technology officer of Keeper Security, a maker of password management software for individuals and businesses. "It's a way of proving that you're in possession of something that ... an attacker wouldn't be able to present."

The advantages of hardware security keys

Lurey considers security keys the pinnacle of digital security: "Security is all about layers," he notes. "If someone's going to attack you ... how many things will they have to overcome to be successful?" The keys "add an extra layer of security, and every time you add a layer, it makes it harder and harder to attack you."

Some layers are more permeable than others. Because they can be exposed in data breaches and easily cracked — attackers use sophisticated software to guess usernames and passwords at scale until they find a match — passwords alone are the weakest possible defense.

"A password is better than no password, obviously, but what's even better is SMS-based MFA," Won says, referring to those one-time passcodes you receive by text. He estimates that this second level of authentication "makes things 20 percent to 30 percent harder for an attacker."

But even one-time passcodes issued by text are weak, argues Ronnie Manning, chief marketing officer at Yubico, which makes security keys called YubiKeys. "An SMS code that's sent to your phone is ... not secure," he says, citing as examples SIM swapping attacks and social engineering attacks, including phishing attacks. With SIM swapping, attackers intercept text messages by gaining control of a victim's mobile number. With phishing, criminals make contact through a website, email, text message or phone call while pretending to be someone their victim trusts, such as a loved one in need or a bank employee trying to complete a transaction. They subsequently convince the victim to share sensitive information — including, potentially, one-time passcodes issued via email or text message.

Security keys are resistant to both SIM swapping and phishing attacks "because even if a hacker has access to your username and password, they still need the physical security key to gain access to your account," Del Portillo says.

The disadvantages of using hardware security keys

Although hardware security keys offer an extra layer security, they come with at least five potential drawbacks worth considering:

- **Inconvenience:** Perhaps the biggest downside to hardware security keys is what makes them so secure in the first place — you can't log in without them.

  "Having a physical key for online services is just like having a physical key for your car. If you want to go somewhere, you have to go get your key," says Derek Hanson, vice president of solutions architecture and alliances at Yubico.

  You typically won't need to fetch your key every time you log into a website, however. Instead, you only need it the first time you log into an account from a new device. After that, the device is trusted. You also can opt for a "nano-sized" security key that's designed to stay in your device on a semi-permanent basis for uninterrupted access to your accounts.

- **Loss:** Like car keys and house keys, physical security keys can be misplaced, lost or stolen. "But we find that people are usually way more worried about losing keys than they need to be," Hanson says. "They tend to put their security key on their key ring with their car key and their house key, so it's with something important. People don't tend to lose those keys. And if they do, it's not for very long."

  It's a good idea to have a backup security key just in case, Manning says. With a backup, you can log into your accounts and remove lost or stolen keys as authentication methods. If you lose your only key, you can typically recover access to your accounts, but will need to contact the services you use about how to do so.

- **Complexity:** Although most models come with easy-to-follow instructions, security keys do require some initial configuration.

  "Some users are not very well-versed ... in IT or technology, so for them it's very complex compared to traditional methods of authentication like a PIN or password," Del Portillo says.

- **Compatibility:** While security keys typically work with many apps and services — Yubico's YubiKeys, for example, work with more than 900 of them, according to Manning — some institutions, including most banks, don't support them, Lurey points out. "The stuff you really want to protect with a hardware key isn't necessarily supported," he notes.

  Echoes Del Portillo, "There are different technologies out there for security keys, and that means your security key is probably compatible with some services and not compatible with others. So you have to make sure you do your research on which services you're going to use and which security keys they support."

- **Cost:** Security keys typically sell for between $30 and $80 per key, Del Portillo says. If you want to have a primary key and several backups, that adds up.

Where to buy and how to use a hardware security key

Yubico's YubiKeys and Kensington's VeriMark security keys are just two options among many. Other manufacturers include Feitian, Nitrokey, Solo, Thetis and Google, which released the latest version of its popular Titan security key last year. Although you can find some models at retailers like Walmart and Office Depot, as well as online retailers like Amazon, you'll have the most choice if you buy directly from manufacturers' websites.

During the initial setup, you'll need to register your primary security key as well as any backups with the apps and services you want to access with your key; you must register each key individually with each account you want to protect. After that, using your security key is easy:

- When you log into an account, you'll enter your username and password as usual.
- Depending on what security key and device you're using, you'll then validate your identity when prompted either by inserting your security key into your USB drive or touching it to your device.
- You'll then tap the security key in a designated touch-sensitive spot to prove that you're a human who's physically interacting with the key instead of a hacker who's trying to access it remotely.
- Instead of a touch-based contact, some models might have a biometric sensor that detects your fingerprint for even greater security.

Best practices when using a security key

Manning recommends:

- Using the key to lock down core accounts, like your Apple ID if you're a Mac user or your Google account if you're an Android user, then using those accounts to log into secondary services like Facebook or Doordash. When you protect root accounts, that protection extends automatically to other connected services.
- Also using a password manager, like 1Password, Keeper, Dashlane or Bitwarden, that repels phishing attacks by creating and storing unique usernames and passwords for every service you use and automatically enters them when needed. Using a security key to access your password manager's vault will prevent hackers from stealing and sharing your login credentials.

Matt Alderton is a contributing writer who specializes in health and wellness, travel and technology. His work has also appeared in USA Today, Forbes *and* The Washington Post.

HAVE YOU SEEN THIS SCAM?
- Call the AARP Fraud Watch Network Helpline at **877-908-3360** or report it with the **AARP Scam Tracking Map**.
- Get **Watchdog Alerts** for tips on avoiding such scams.

Report a Scam
Sign Up for Watchdog Alerts