The New York Times
Wirecutter

The Best Security Key for Multi-Factor Authentication

By Max Eddy | January 5, 2024

Losing control of an online account to a digital intruder is a nightmare scenario. Multi-factor authentication (or MFA) is the best way to safeguard an account, because once MFA is enabled, an attacker won't be able to access it—even if they have your username and password. A physical security key is the most secure MFA option, since it's a dedicated authentication device and resistant to phishing. The Yubico Security Key C NFC is the best choice: It's affordable and will work with just about every site that supports security keys. If you're already familiar with security keys and need or want more-advanced features, the Yubico YubiKey 5C NFC is a pricier but worthwhile choice.

The Yubico Security Key C NFC is a well-made key that's compatible with nearly all sites and services that support security keys. Its USB-C connector and NFC support work with most modern desktops, laptops, and mobile devices, so you can log in securely anywhere. Combined with Yubico's excellent onboarding materials and customer support, this key is the best one for those seeking an easy-to-use security key to protect their online accounts.

Photo: Michael Hession

The Yubico YubiKey 5C NFC supports several additional authentication protocols, can work with an app to generate MFA codes, and can be configured to fill a variety of different roles, like logging into computers. It's impressive, but it's also more than what most people need.

Why you should trust us

Max Eddy is Wirecutter's senior staff writer for security, privacy, and software platforms. Prior to his time at Wirecutter, he covered security and privacy—including MFA security keys—at PCMag for 11 years. Additional reporting for this guide was contributed by Yael Grauer and Thorin Klosowski.

Who this is for

Passwords alone aren't enough to protect your online accounts. Frequent data breaches—along with relying on weak and recycled passwords instead of a password manager—make it easy for bad actors to take over online accounts. The solution is MFA, or multi-factor authentication, which is sometimes still called 2FA, or two-factor authentication. How MFA works: When you log in to a website, you have to present at least one other proof of your identity, such as a one-time-use code generated by an authenticator app or by putting your thumb on your phone's fingerprint reader.

Another way to log in is with a security key, which is a small hardware device. If a website supports security keys, you can enroll one for use with the account. The key cryptographically proves its legitimacy using the FIDO authentication protocol. Basically, instead of typing in a security code after entering your password, you plug the key into your computer (or tap it against a phone), and the site confirms your identity.

Compared with other forms of authentication, security keys have some major advantages. An authentication app generates a code on your phone, and it is easy enough to enter. But security keys save you the hassle of finding your phone, copying the code, and pasting it before the timer runs out. If you're frustrated by switching between apps to enter a security code, or if you often enter the code incorrectly, you'll appreciate the simplicity of security keys.

Security keys also work in scenarios where other MFA options fail. If your phone won't turn on, you can't generate authentication codes. If you're outside cell coverage, you can't receive SMS codes, making security keys an attractive choice for frequent travelers. Security keys require no data connection, and the best ones don't even need batteries. They're also more durable than phones, which have numerous fragile components.

The biggest advantage of security keys is that they are resistant to phishing attacks, said Bob Lord, senior technical adviser at the Cybersecurity and Infrastructure Security Agency (CISA). A phishing scam might trick you into entering your password and authenticator app code or a code sent via SMS, which can also be intercepted through SIM jacking. But security keys work only with sites where you've enrolled them.

More-advanced security keys can provide more than authentication. Some can store and replay credentials, be used to log in to computers, or offer biometric authentication so you can use your fingerprint to log in. These advanced features are most useful for those who are already familiar with multi-factor authentication, which is why we recommend a more-basic security key for most people.

But there are some major drawbacks to security keys. Unlike most MFA systems, they cost money—as little as $20 and as much as $95. Security keys can also be lost or damaged, and experts we spoke with recommended buying a second key as backup, effectively doubling the cost. Security keys are also not accepted by every site and service, so you will still need an authenticator app. But using a security key for even just a few important services—such as your primary email accounts, which can be used for password recovery—provides an overall security benefit.

"They don't have to work everywhere, they don't have to do everything, but they will protect the biggest most precious things that you have online," said Derek Hanson, Yubico vice president of Solutions Architecture and Alliances.

What we heard repeatedly from the experts we spoke with is that any MFA is better than no MFA at all, so don't get discouraged if security keys sound like a huge hassle. If you're new to using MFA, authenticator apps are probably a better choice because they're widely accepted, free, and easy to use. But if the advantages of security keys sound intriguing, and you think you would actually make use of them, they are a great way to upgrade your online security.

How we picked and tested

We used the following criteria to evaluate the security keys we tested:

- **Price:** The up-front cost of security keys is likely a sticking point for most people, so a security key needs to be a good value to justify its existence on your key ring. Ideally, a security key should be inexpensive enough that you could buy more than one, because having a backup key is the most secure protection against losing access to your accounts. The cheapest key we tested was $20, and the most expensive was $95.

- **USB-C and NFC support:** We prefer security keys that are compatible with most devices, and that means support for USB-C and wireless Near Field Communication (NFC). Keys with NFC will work with most modern iOS and Android devices. For physical connections, we prefer USB-C because it's unlikely to be replaced anytime soon.

- **FIDO2/WebAuthn support:** This is the latest version of the protocol that powers security keys, and it also works with passwordless authentication systems and passkeys. The best keys are also compatible with the older, but still widely used, FIDO U2F protocol.

- **Performance:** Security keys shouldn't be harder to use than other forms of MFA, and a key should work correctly nearly every single time.

- **Company reputation:** You need to trust that your security key is, well, secure. Trustworthy companies are transparent about their practices and structure, and they have systems in place for researchers to submit potential vulnerabilities.

- **Design:** A good key should be able to survive for years on your keychain and wherever else it might end up. We also give preference to security keys that don't rely on moving parts or batteries.

- **Onboarding and customer support:** Security keys are fundamentally different from every other kind of MFA, and it's important that key makers help users get

Yubico Security Key C NFC

Photo: Michael Hession

started. We prefer services that have support materials, customer support, and a clear on-ramp for new security-key owners.

Based on this criteria, for this round of testing we looked at 12 security keys.

We enrolled each key with commonly used services and then logged in on Android, iOS, macOS, and Windows devices. We used both NFC and physical connectors on Android and iOS, when it was possible to do so. We also used these keys for passwordless authentication with a Microsoft account and for storing passkeys with a Google account. To test durability, we placed the security keys in a cloth bag filled with house keys and a fistful of loose change; then we shook it for 10 minutes. We also ran the keys through a washer and dryer and repeatedly ran them over with a car. After each durability test, we confirmed whether or not the keys could still be used for authentication.

Our pick: Yubico Security Key C NFC

The Yubico Security Key C NFC is the best security key for most people because it offers wide compatibility at a low price. It's the newer version of our previous top pick, and it supports newer authentication protocols. Design-wise, it's nearly identical to our upgrade pick, but it lacks that key's advanced features. However, unless you need to use it as a smart card or to generate MFA codes, the Security Key C NFC is capable enough, and it's also more affordable.

It can be used with almost any site that supports security keys. The refreshed Security Key C NFC supports the older—yet still widely used—FIDO U2F protocol. It also supports the newer FIDO2/WebAuthn protocol, which allows for passwordless authentication and passkey storage. That means you can probably use this security key well into the future.

It has reliable, multi-platform support. A security key that doesn't work well with all of your devices isn't worth buying. The Yubico Security Key C NFC got along well with the 15-inch MacBook Air, Pixel 7a, iPhone 14 Plus, and the Lenovo Windows 11 laptop we used for our latest round of testing.

It's durable enough to live on your keychain. The Security Key C NFC is extremely well made and pleasant to hold. The plastic enclosure is slightly textured, with a recessed, touch-sensitive disk on its surface that you tap during authentication. Although Yubico's products are light, they feel sturdy, and they didn't flex or creak when we tried to bend them. Many competing keys felt cheap, plastic-y, and hollow by comparison. The Security Key C NFC emerged from our shake test with minor scuffs, which were difficult to see even in good lighting. We've been using Yubico devices for years, and we can say with certainty that they can survive on keychains without issue.

Yubico offers easy onboarding and excellent customer support. Yubico packaging—which must be torn open and shows attempts from anyone trying to tamper with the key inside—includes a URL that leads to the company's onboarding materials. A visual menu helps people quickly identify their keys and find relevant setup materials, as well as instructional (albeit somewhat dated) videos. Yubico also lists which services are compatible with its keys, and this is very handy. We found that Yubico offers responsive customer support through its website. When we sent in a question, customer service responded in minutes with a thorough and thoughtful response.

Flaws but not dealbreakers

It doesn't have many advanced features. The Security Key C NFC does not support the Yubico OTP MFA protocol, though this isn't much of a loss because it's not widely used. This key also doesn't support TOTP storage, Smart Card/PIV, OpenPGP key storage, or any of the other neat tricks found in the YubiKey 5 series. But most people won't be able to take advantage of them anyway.

Yubico does not use open-source firmware or hardware. Open-source software can be examined for potential security

Yubico YubiKey 5C NFC *Photo: Michael Hession*

flaws, and open-source hardware should likewise be free of nasty surprise vulnerabilities. Yubico does, however, have an active vulnerability disclosure program.

You can't upgrade the firmware. Upgradable firmware is nice because it allows manufacturers to protect customers against recently discovered vulnerabilities and even add new features. A system for updating firmware, however, could potentially be exploited by attackers, though it would have to be a complex attack. In the past, Yubico has issued a recall when a problem was discovered with its product.

It has only one design. Although you can choose between USB-A and USB-C models, the Yubico Security Key line doesn't have the variety of designs and connectors found in the Yubico YubiKey 5 series or in Feitian's stable of products. If you have very specific needs related to the size and function of your key, you'll need to look at those options.

It's a good deal for one key but pricey for two. The most secure way to ensure you're never locked out of your accounts is to buy a backup key and enroll it everywhere you use your primary key. While the Yubico Security Key C NFC is comparably cheap, it's less of a compelling deal when you're buying a backup, too. One alternative is to use backup codes or another form of MFA as a backup. The experts we spoke with cautioned that attackers may attempt to fool you into using a backup MFA option that's phishable, so be careful if you go that route.

Upgrade pick: Yubico YubiKey 5C NFC

The Yubico YubiKey 5C NFC is the best security key for those who understand how to make the most of its numerous features, which include support for Yubico OTP and storing OpenPGP keys. This key is expensive—nearly double the price of our top pick—but it more than justifies that cost with its capabilities. Yubico rarely reduces prices, yet it sometimes offers discounts for purchasing more than one key. Whether or not you'll get your money's worth from the YubiKey 5C NFC depends on how you use it.

It supports numerous MFA options. The YubiKey 5C NFC and its YubiKey 5 series siblings are the most capable keys available. This key supports the most commonly used FIDO2/WebAuthn and FIDO U2F protocols, and it also supports Yubico OTP as well as OATH-HOTP and OATH-TOTP protocols. In addition to storing passkeys, the 5C NFC can also store one-time-use codes (TOTP) for 32 sites and services, accessed through Yubico's companion app.

If you don't know what all of those acronyms mean or why they're important, just know that they are other MFA systems. Not all of them are widely used, but supporting them makes the YubiKey 5C NFC extremely flexible. These keys are best suited for those who understand how to use these advanced features. For everyone else, the Security Key C NFC is the key to buy.

It provides more than just authentication. Experienced users can also configure the YubiKey 5C NFC to function as a smart card (PIV protocol), to securely log in to a computer, and to store OpenPGP keys for signing and encrypting information. You can also reconfigure the key's behavior using Yubico's desktop app. Again, these are advanced features intended for people who already know how to use them.

It offers Yubico's excellent design and customer support. Like our top pick, the YubiKey 5C NFC is well made and delivers comprehensive onboarding and support materials. But both are closed-source, and their firmware cannot be upgraded, which could be an issue for folks who value the transparency of open-source technology.