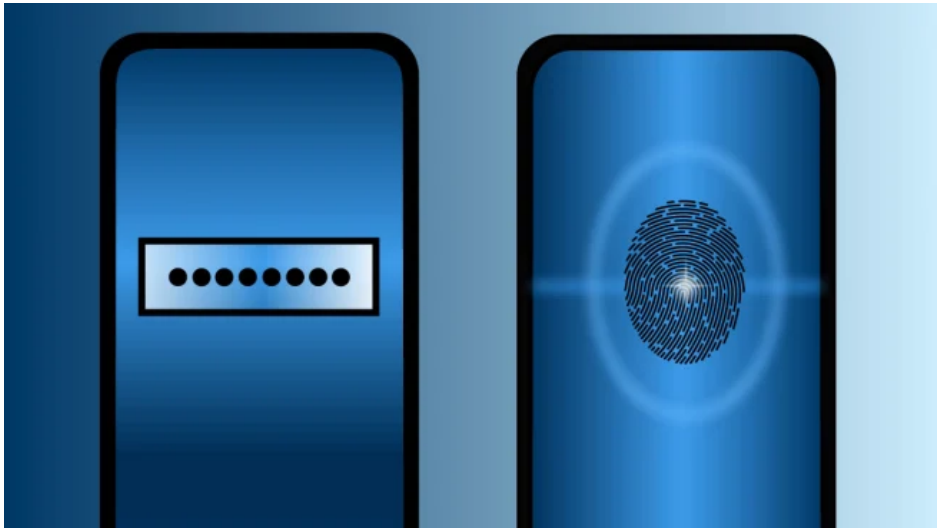
Should You Use Passkeys Instead of Passwords?

Google and Apple have rolled out passkeys, but the technology isn't yet seamless across all browsers, operating systems, and devices

By Amira Dhalla and Yael Grauer

May 24, 2023



Passkeys, a password-free way of logging in, offer better protection against phishing and malicious websites than traditional passwords do.

Illustration: Lacey Browne/Consumer Reports

For years, security experts have emphasized the importance of creating strong and unique passwords. But even the most complex passwords are vulnerable to phishing, where unsuspecting users are tricked into disclosing their passwords or entering them at a fraudulent look-alike website controlled by the attackers. Even using an authentication app like Authenticator or Authy isn't foolproof–you could still be tricked into entering your one-time password on a fake log-in page.

Because of the risks of passwords, the tech industry has been eager to create a password-free future. Passkeys–developed by Apple, Google, Microsoft, and others–are an alternative to passwords, and they provide robust protection against phishing attacks and website breaches. The launch of passkeys for Google accounts is the latest step to improving safety on digital accounts and ownership of your personal information.

MORE ON PRIVACY & SECURITY

Tips for Better Passwords

CR's Password Manager Ratings

Consumer Reports Security Planner

Why It's Smart to Use Authentication Apps for Multifactor Security

30-Second Privacy Fixes: Simple Ways to Protect Your Data

Physical security keys, which can distinguish between legitimate websites and look-alikes, are another technology that many security pros recommend. But passkeys might appeal to more people, because they are free, and you don't need to carry them around.

Passkeys can be used on phones, tablets, or computers, and implemented across devices. The technology still isn't as widespread and convenient to use as it could be. However, it's not too early to consider using it for at least some of your accounts as passkeys continue to be integrated and standardized across services.

How Passkeys Work

Passkeys use public-key encryption for security, which means that one key is stored on your device, and the other is with the service on which

your account is held. Passkeys can also be synced to the cloud, and your key can be copied from one device, such as your phone or laptop, to another.

Passkeys require some form of authentication before they can be used. That might be the passcode you use to unlock your screen, or a form of biometric authentication such as a face scan or a fingerprint. That biometric data stays local on your own device—it's not shared with the services you use.

Using a passkey means you can't accidentally enter your personal log-in on a malicious site or give it to a phishing account, making passkeys more secure than a traditional password.

What happens if you lose your phone—do you also lose access to your online accounts? This should not be a problem, as long as you've connected your passkey across multiple devices. And you can revoke a passkey for your Google account in your password settings, or from your Mac and iCloud keychain.

How to Get Started With Passkeys

A handful of services are rolling out passkeys. Android devices may automatically create passkeys when you log in to your Google account. You can start using passkeys for personal Google accounts by going to this page and selecting "start using passkeys." You need Windows 10 or up to use passkeys on a PC, and Windows 11, version 22H2 or newer to access features such as synchronization. Some browsers might not support passkeys, so you may need to switch to a supported browser to set up a passkey for your Google account.

Apple requires you to use a traditional password to log in to your Apple ID, but creating a passkey on an Apple device will let you sign in with that passkey on any Apple device, as long as your device runs iOS 16 or macOS Ventura or newer, and you are using iCloud Keychain.

You can already use passkeys with dozens of companies, such as Best Buy, Hyatt, and PayPal. See this full directory of passkeys. For more information on setup, check out the Freedom of the Press Foundation's guide to passkeys, or the following instructions for major platforms:

- Passkeys on a Google account
- Passkeys for Chrome and Android
- Passkeys on a Mac
- Passkeys on an iPhone
- Passkeys on an iPad

Sharing Your Passkey

What about the accounts we share with others? You might think that passkeys would make this harder, but Apple allows you to AirDrop a shared passkey with people in physical proximity to you, so you can share accounts with trusted individuals much like you can do for passwords in Apple.

If you need to borrow a friend's phone or use a shared computer, Google lets you scan a one-time QR code from your phone, which will give you access to your account on the borrowed or shared device without storing your passkey on it. The device you're borrowing just needs to be nearby. (The technology checks to see if the two devices are in Bluetooth range of each other, to protect against remote attacks.)

Passkey Limitations

Currently, passkeys are available only on select websites, apps, and services. Keeping track of where you can use them can be challenging. For example, if you use a passkey to log in to an app on your phone, you'll still need a password on your laptop if you want to use a browser that doesn't yet work with passkeys.

Getting passkeys set up on your various devices can be tricky because things don't always sync seamlessly. For example, you can share passkeys across Apple devices using iCloud Keychain, and you can share them across Android and Chrome devices using Google Password manager. But there is not yet a seamless and easy way to share passkeys across iPhone and Android devices or across Windows devices.

The technology has other quirks, too. You can use passkeys with Apple's Safari browser, but if you are on a MacBook, you may have to use the Chrome browser to set up a Google passkey. (Check this table to see if you can use passkeys on your preferred operating systems, browsers, and devices.)

The user experience around passkeys "can definitely be improved based on availability of the services and lack of consistency around how exactly you get the keys on your devices," says Martin Shelton, principal researcher at Freedom of the Press Foundation. "That said, I also believe it's really exciting technology because it could—pending availability—make it a lot easier for people to stop typing their password on malicious websites."

Passkeys are still in their early stages. Given that they're not yet available for all services, operating systems, and devices, it's too soon to switch away from using passwords for all your online security. But you can start experimenting with passkeys on accounts where it makes sense for you.

Either way, you'll still want to use a password manager to keep your passwords safe. Some password managers even allow you to store passkeys, and more are working on this feature.

You can also store passkeys on a security key. That passkey can't be copied from the security key. That can make it more secure, but it's important to register these passkeys on multiple keys kept in different locations if you do decide to use them.

Amira Dhalla

Amira Dhalla is a digital privacy and security expert at Consumer Reports. She has been with CR since 2019, producing reports and tools to improve cybersecurity and privacy in the marketplace, as well as tackling discriminatory technologies, deceptive design, trust and safety, and more. Follow her on X.

Yael Grauer

Yael Grauer is an investigative tech reporter covering digital privacy and security. She manages Security Planner, a free, easy-to-use guide to staying safer online. She has covered surveillance, online privacy and security, data brokers, dark patterns, clandestine trackers, security vulnerabilities, VPNs, hacking, and digital freedom for the Atlantic, Wired, Vice, The Intercept, Slate, Ars Technica, OneZero, Wirecutter, Business Insider, Popular Science, and other publications.

Trending in Digital Security

How to Turn Off Smart TV Snooping Features

How to Wipe a Computer Clean of Personal Data

Best Smartwatch for Your Kid

Best Photo Scanning and Video Digitizing Services

SHOW COMMENTS (0) | *commenting powered by Facebook*

Be the first to comment