How Passkeys Work

Is No Password the Best Password? How Passkeys Work

The future of logging in may already be in your pocket.

We can admit: passwords are exhausting. You're told to create long, unique, and complex passwords for every account. Then you're expected to remember them all, avoid reusing them, and some websites even follow older advice by forcing you to update them regularly! No wonder so many people fall back on weak, easy-to-remember passwords, or they reuse the same ones over and over again.

But criminals know passwords are a weakness for many of us. Stolen passwords fuel data breaches, account takeovers, and phishing scams on the daily.

However, a newer technology called passkeys could finally help us all move beyond passwords, thereby making logging in both easier and more secure.

Major companies like Google, Apple, and Microsoft already support passkeys, and millions of people are using them without even realizing it.

What is a passkey?

A passkey is a way to sign in to an account without typing a password.

Instead of relying only on something you know, like a password, passkeys use something you have (your phone, tablet, or computer), something you are (your fingerprint or face), or something you know (your device PIN).

Before you get concerned about us getting too technical, take a breath! In practice, using a passkey feels very simple. You might unlock your phone with Face ID, tap your fingerprint sensor, or enter your device PIN — and that's it! You're signed in. No need to type in a password.

Under the hood, passkeys use advanced cryptography to keep your account secure.

When you create a passkey, your device generates two digital keys:

1. A public key, which is stored by the website or app
2. A private key, which stays securely on your device

The private key never leaves your device. When you log in, your device proves you're really you by securely matching those keys together.

The complicated part happens in the background! For users, passkeys are often easier than passwords.

Why are passkeys more secure?

Passkeys solve many of the biggest problems with passwords.

- **There's no password to steal.** A common phishing attack tricks people into typing passwords into fake websites. But with passkeys, there's usually no password to type.
- **Your secret key stays on your device.** With passwords, websites store information that can potentially be stolen in a data breach. With passkeys, the sensitive private key stays on your personal device instead of sitting on a server.
- **Biometrics for the win.** Even if someone steals your phone or laptop, they still typically need your fingerprint or face scan to use your passkey.
- **No more password reuse.** Password reuse remains one of the biggest cybersecurity risks. If one account is breached, attackers often try the same password on other accounts. Passkeys remove that temptation because there's no password to remember in the first place.

Who supports passkeys?

Many major platforms and websites already support passkeys.

Google: Google allows passkeys for Gmail, YouTube, Google Drive, and other Google services.

Apple: Apple supports passkeys across iPhones, iPads, Macs, and the Safari browser. Apple's Passwords app even stores your passkeys in one place, so you can check to see what accounts you have passkeys for.

Microsoft: Microsoft supports passkeys for Microsoft accounts, Xbox, and Microsoft 365.

Other services

Many other companies now support passkeys, including:

- Amazon
- eBay
- Facebook

If you use a modern smartphone or computer, you likely already have everything you need to start using passkeys.

How do you set up a passkey?

1. Setting up a passkey is usually quick and easy.
2. Sign in to a website or app that supports passkeys
3. Go to your account or security settings
4. Choose the option to create or save a passkey
5. Verify your identity using your fingerprint, face scan, or device PIN (we recommend biometrics instead of a PIN)

Once created, your passkey may sync across your devices via services such as iCloud Keychain or Google Password Manager.

That means if you create a passkey on your phone, you may also be able to use it on your tablet or laptop.

Can you use passkeys across different devices?

Usually, yes. For example, you might use an iPhone passkey to log in on a Windows computer. In many cases, the website will display a QR code that you scan with your phone to approve the login.

The process is designed to be secure while still keeping sign-ins convenient.

Are passkeys the same as multifactor authentication (MFA)?

Not exactly. MFA adds extra security to passwords by requiring additional verification steps, such as a one-time code or a fingerprint scan. Passkeys go further by replacing passwords entirely.

However, passkeys still rely on multiple layers of security, such as your physical device and your fingerprint or face.

That's why many experts consider passkeys resistant to phishing and similar threats that commonly bypass traditional passwords. In a way, passkeys sort of use multiple types of MFA factors that aren't passwords.

Are passwords going away?

Probably not overnight. Many websites still rely on passwords, and some services have not added passkey support yet. Passwords will likely remain part of online life for years to come.

Until passkeys take over the internet, our recommendations are still:

- Each password should be at least 16 characters long, unique, and a random string of characters
- Turn on MFA whenever possible
- Use a password manager to store strong passwords securely
- Keep your software updated
- Be suspicious of any unexpected, urgent inbound message to avoid phishing and scams

The shift toward passkeys is accelerating, especially as they improve both security and convenience.

Should you start using passkeys?

Yes! Passkeys make logging in faster, eliminate the need to remember passwords, and reduce the risks of phishing.

FAQs

Do I need a smartphone to use passkeys?

Usually, yes. Most passkeys are stored on smartphones, tablets, or computers that support biometric authentication or device PINs.

Can hackers steal passkeys?

Passkeys are designed to be much harder to steal than passwords because the private key stays on your device and isn't typed into websites.

What happens if I lose my phone?

Generally, this isn't a huge deal. Most passkeys can be recovered through your device ecosystem, such as your Apple, Google, or Microsoft account, especially if you use cloud syncing. Usually, the worst-case scenario would involve working with the platform to recover your account.

Should I still use a password manager?

Yes. Many websites still rely on passwords, so password managers remain an important tool for creating and storing strong, unique passwords. Many password managers even store passkeys!