Are Passwords Going Away? What You Need to Know About Passkeys

The future of logging in is already on your phone!

Let's be honest: passwords are not fun. They're hard to remember, annoying to reset, and, if you reuse them, leave us vulnerable to hackers. Even cybersecurity experts get overwhelmed trying to manage hundreds of passwords across multiple devices.

But a new technology called passkeys is changing the way we log in!

Passkeys are an exciting tech that many websites now use, and they're more secure than passwords. You can start using passkeys for your personal use today!

What is a passkey?

A passkey is a secure way to sign in to your online accounts without typing in a password.

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

Behind the scenes, passkeys are powered by a pair of cryptographic keys:

- A **public key**, which is stored by the service (like Google or Microsoft).
- A **private key**, which stays securely on your personal device.

Look, the tech is complicated, but using passkeys is easier than using passwords. And passkeys are very secure!

When you log in with a passkey, your device uses biometrics or a PIN to unlock your private key and respond to a security challenge from the server. If the two keys match, you're in – no password required.

It's like in movies where they must turn two keys at the same time, except one is invisible and lives on your phone.

Are passkeys safer than passwords?

Passkeys are much harder to hack or steal. Here's why:

- **No password to phish.** Since there's no password being typed in or transmitted, hackers can't steal it through phishing emails or fake login pages.
- **Biometrics or PIN required.** Even if someone steals your phone, they still need your fingerprint, face, or device PIN to use your passkey.

- **Private key stays on your device.** Your secret key never leaves your device, so it's not floating around on the internet or sitting on a company's vulnerable server.
- **No more reused or weak passwords.** Passkeys eliminate bad habits, like reusing passwords, that leave people exposed.

Who's accepting passkeys already?

The biggest names in tech are already rolling out passkeys:

- Google: You can now use passkeys to sign in to Gmail, YouTube, and other Google services.
- Apple: Passkeys are supported in iOS, macOS, and Safari.
- Microsoft: Passkeys are now available for Xbox, Microsoft 365, and more.
- Other brands: Websites like Amazon, Facebook, and eBay are also passkey-friendly.

If you're using a recent iPhone, Android phone, Mac, or Windows PC, you already have the hardware needed to start using passkeys.

How do I use a passkey?

Setting up a passkey is usually easy:

1. Log in to a service that supports passkeys.
2. Choose to create or save a passkey when prompted.
3. If you aren't prompted to create a passkey, check your Account Settings or contact the platform for help.
4. Verify your identity with biometrics like Face ID or a fingerprint, or your device PIN.

Your passkey will be stored on your device and can be synced across devices running the same operating system (for example, between your iPhone and iPad).

If you want to use a passkey on a different platform, like logging into your Google account on a Windows PC while your passkey is on an iPhone, you'll typically scan a QR code or approve the login from your device.

Are passkeys the same as MFA?

Not quite. Multifactor authentication (MFA) adds extra protection by requiring two or more login factors, usually a password and a one-time code or a biometric scan.

Passkeys go a step further. They replace passwords altogether. But they still use two strong factors:

- **Possession** – you have your device
- **Biometrics** – your fingerprint or face, or a PIN you know

In that sense, passkeys offer MFA-level security but with fewer steps and an easier user experience.

Are passwords going away?

Not overnight, and maybe not ever.

Most websites still use traditional logins, and people aren't ready to give up their password habits just yet. That's why we still recommend:

- Using long, complex, and unique passwords for every account.

- Turning on MFA wherever it’s available.
- Using a password manager to keep everything secure and organized.

But passkeys are the future. And now is a great time to try them out.

Passkeys are safer and easier

Passwords have had a good run, but they’ve also caused a lot of stress and security breaches. Passkeys offer a better way forward: easier logins, stronger protection, and fewer phishing threats.

If you're a Google, Apple, or Microsoft user, you can start using passkeys today.
