Understanding Passkeys: A Simple, Practical Guide

Passkeys are a newer, more secure way to sign in to websites and apps, without ever typing a password. Instead of remembering a long string of characters, you simply unlock your device the same way you normally do.

How a Passkey Works

When you use a passkey, you don't enter a password. You just:

- Unlock your device using Face ID, fingerprint, or a PIN
- Your device then confirms to the website that it's really you

Behind the scenes, your device and the website use a pair of digital keys to verify your identify:

1. **When you create a passkey**
   - Your device generates two keys
     Private key: stays on your device and is never shared
     Public key: sent to the website and safe to store

2. **When you sign in**
   - Your device uses the private key
   - The website uses the public key
   - If the two match, you're signed in, no typing required

Important:

Your fingerprint, face data, or PIN, **never leaves your device.** The website never sees or stores it.

Why Passkeys Matter

Passkeys solve many of the problems that make passwords frustrating and insecure.

They're easier

- No passwords to remember
- No typing, especially helpful on phones or for anyone who finds typing difficult

They're safer

- Almost impossible to phish (fake login pages can't trick a passkey)
- Much harder for hackers to steal, because there's no password to leak
- Your biometric data stays on your device and isn't shared with websites

Passkeys vs Password

The table below shows how passkeys compare to traditional passwords in everyday use:

Feature	Passkeys	Passwords
Need to remember something	No	Yes
Typing required	No	Yes
Uses biometrics (Face ID / fingerprint)	Yes	No
Can be phished (tricked by fake wesites)	Extremely difficult	Very easy
Can be reused across different sites	No	Often yes (which is unsafe)
Stored on company servers	No secret stored	Yes, and often leaked
Works with password managers	Built into your device	Often needed
Accessibility-friendly	Very	Can be difficult
Overall security level	Very high	Medium to low

Passwords

Think of a password like a physical key you copy and hand out to every building you need to enter. If someone steals that key, they can get into all of those buildings.

Passkeys

A passkey works more like a secure ID badge stored on your phone. When you try to sign in, the website checks your device's "badge" to confirm it's really you. You don't have to remember anything, and nothing secret is shared.

Are Passwords Going Away?

- Not immediately, but the shift has already begun.
- Major companies like Apple, Google, and Microsoft are actively moving toward passkeys.
- Many websites now offer passkeys as the default sign-in option.

For the near future, you'll likely see:

- Passkeys as the primary way to sign in
- Passwords still available as a backup, at least for now