What are Passkeys?

A passkey is a secure, password-free way to log in to accounts using your device (phone, tablet or computer). Instead of typing a password, you authenticate using biometrics (fingerprint/face) or your device PIN.

How Passkeys Work

When a passkey is created, two cryptographic keys are generated:

- **Public key** - stored by the website/app
- **Private key** - securely stored on your device

During login:

- Your device verifies your identity (biometric or PIN)
- It sends a secure response to the website

The private key never leaves your device, making it highly secure.

Why Passkeys are More Secure

- Cannot be guessed, reused or stolen like passwords
- Phishing-resistant (won't work on fake websites)
- No sensitive data is shared or stored on servers
- Built-in multi-factor authentication (device + biometric)

Benefits for Users

- No passwords to remember
- Faster, easier login
- Works across devices (when synced via Apple, Google, Microsoft)
- Biometric data stays private on the device

Key Takeaway

Passkeys are a safer, simpler alternative to passwords and are designed to reduce fraud, eliminate password fatigue, and improve the login experience.

Passkeys FAQs

How do I get a passkey?

Open any online service or application that supports passkeys and click the option to create a passkey. Simply follow these prompts, which generally involve biometric authentication.

What is the difference between a password and a passkey?

Regular passwords are created by the user in a string of characters, passkeys are generated through cryptographic keys created and securely stored on your device. Passkeys are immune to phishing or data breaches compared to passwords.

Can passkeys be hacked?

Passkeys are virtually unhackable. The private key never leaves your device, and this requires biometric authentication, making them completely immune to phishing and breaches.

What are the disadvantages of passkeys?

Some possible drawbacks of the use of passkeys include limited adoption, their access depends on devices, and difficulty in recovery in case all the devices are lost.

What if I lose my phone?

Recovery options are available with most platforms offering the feature, such as using another device tied to the account or using a recovery code. It is highly recommended that you set up backup devices or even use an alternative way of recovering to get access to your various accounts.

Can I still use a password if I have a passkey?

Correct, most of the time you would still be able to use your password even after setting up a passkey. Most services that support passkeys, still support passwords for compatibility reasons and as an alternative form of authentication.

Will passkeys replace passwords entirely?

Passwords have been around a long time and will not be going away anytime soon. People are comfortable and familiar with them. Still, weak or reused passwords can put both people and the companies they work for at risk, which is why strong support for passkeys is increasing.

Microsoft, Google and Apple are all pushing to "kill the password." All are moving toward passkeys as the primary and best supported authentication method for accounts. Where those three go, everyone else is most likely to follow.