



Passkeys are **not simply another form of 2FA**; they're a different authentication model. By replacing passwords with public-key cryptography and using your device's built-in biometric or PIN verification, they provide a login experience that is both more secure and more convenient. Hopefully, they'll provide another layer of protection against Identity Theft and fraud.

Not because two-factor authentication (2FA) is "failing," rather, passkeys are increasingly replacing **password + 2FA** because they eliminate the password altogether while providing security that is at least as strong as, and often stronger than, traditional 2FA.

## Traditional Login

Password  
Usually Requires 2FA  
Vulnerable to Phishing  
Users forget Passwords  
Can be Intercepted

## Passkey Login

No Password  
Usually not needed  
Phishing - resistant  
Nothing to forget  
Cryptographic Authentication



Most successful cyberattacks don't actually defeat the "second factor". They steal or guess the password first.

Common methods include:

- Phishing emails
- Fake login websites
- Credential stuffing using breached passwords
- Malware
- Password reuse

**Passkeys remove passwords entirely.**



## Are passkeys replacing all forms of 2FA?

Not entirely, organizations still use 2FA in many situations:

- Legacy systems
- Banking
- Government portals
- Enterprise applications
- VPN access
- Healthcare systems



Many services now offer both:

- Password + 2FA
- Passkey

**Users can choose either.**

## What happens if I lose my phone?

A desktop is probably hard to lose but your mobile device less so. It's a common concern. Modern passkey systems are designed with recovery options:

- Passkeys sync securely across your devices via services like iCloud Keychain or Google Password Manager (depending on your settings).
- You can register multiple devices.
- You can keep a hardware security key as a backup.
- Many services also provide account recovery processes.

**Recovery can still be more involved than resetting a password, but it avoids many of the security weaknesses of password-based systems.**

## So what does the future look like?

Major technology companies—including Apple, Google, Microsoft, Amazon, PayPal, and many banks and online services—have adopted or are rolling out passkey support. The long-term trend is toward passwordless authentication, with passkeys becoming the default login method where practical.



Call us at 877 308 9169

Learn more at our website:

<https://idresolution.net/>