

Demystifying Passkeys

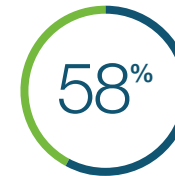
The path to passwordless starts here

Phishing threats are always evolving. Advancements in AI have made it possible for cyber criminals to launch more sophisticated attacks at a larger scale, making it even harder for the average person to discern phishing attempts from genuine communication.



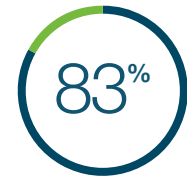
Between Q4 2022 and Q4 2023, there was a **1,265% increase in malicious phishing emails** and a **967% rise in credential phishing** that was most likely due to AI use.

[Source](#)



58% of organizations suffered account takeovers in 2023, of which **79%** came from credentials obtained through phishing.

[Source](#)



83% of organizations who experienced a phishing attack had a form of multi-factor authentication (MFA) in place that cyber criminals bypassed.

[Source](#)

Passwords remain the most common form of user authentication, but offer weak security that is easily compromised. Many organizations have implemented multi-factor authentication (MFA) as a secondary line of defense, but not all MFA is created equal and many of these solutions can be surpassed by hackers and offer poor user experience. A better, more secure solution is needed.

What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences.

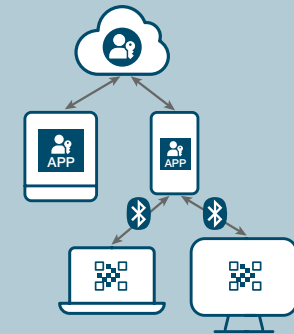
Synced or device-bound: What's the difference?

There are three different types of passkey implementations that you can roll out across your organization. It is important to choose the right passkey approach based on your required security and risk posture.

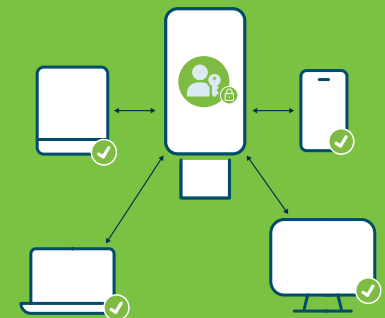
Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.





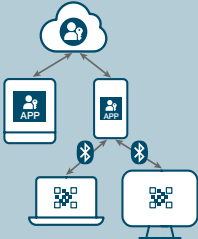
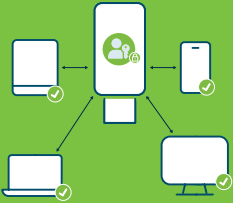
Device-bound passkeys on general purpose devices such as smartphones, laptops and tablets offer enterprises greater control of their FIDO credentials compared to synced passkeys but are still backed by a password and offer weak security.



Device-bound passkeys on modern FIDO hardware security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach organizations can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across regulated industries.



How to choose the right passkey approach?

<p>If you need</p> 	<p>Synched passkeys</p> 	<p>Device-bound passkeys on general-purpose devices</p> 	<p>Device-bound passkeys on hardware security keys</p> 
Synched/shareable between devices	Unmanaged syncing	Managed syncing	No syncing between devices
Works across Apple/Google/Microsoft	May not work	Works across all platforms	Works across all platforms
User registration/onboarding	Weak; backed by password	Weak; app backed by password	Most secure as user registration not reliant on a password
Credential recovery	Easy to recover	Time to replace phone and costly	Fastest with a backup key
Compliance and audit	Authenticator Assurance Level 2 (AAL2) No attestation; unsure if user controls passkey	Authenticator Assurance Level 2 (AAL2) Supports software attestation	Authenticator Assurance Level 3 (AAL3) Supports hardware attestation
Risk/Costs	Perceived as “free”; high IT/helpdesk costs and higher risk exposure is costly	Perceived as cheaper than HW; but risk exposure gaps can be costly in long run	Perceived as higher cost upfront; but less costly due to lowered breach risk and reduced IT burden
Works across enterprise scenarios	Not in mobile-restricted, shared workstations	Not in mobile-restricted, shared workstations	Works across all enterprise scenarios

Phishing-resistant users create phishing-resistant enterprises

Every move away from passwords, no matter how small, is a move in the right direction. Adopting device-bound passkeys on modern FIDO hardware security keys such as the YubiKey protects users across locations, devices, and business units without sacrificing on security or experience. And when users are well-protected and productive, so is the business.

Build your bridge to passwordless with the most secure solution on the market. [Learn how to get started here.](#)



Contact us
yubi.co/contact

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries.

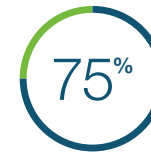
For more information, visit: www.yubico.com © 2024 Yubico

Why choose the YubiKey for your passkey implementation?



99% reduction of risk of credential theft and account takeovers while delivering 203% ROI

[Source](#)



75% reduction of password reset related help desk costs

[Source](#)



30% reduction of cyber insurance premiums

[Source](#)



Provide secure user access at scale on any device with the best user experience



Deploy the most secure passkey strategy: device-bound that is purpose-built for security, FIPS 140-2 validated and AAL3 compliant



Go at your own pace. The YubiKey offers a bridge to modern passwordless with multi-protocol support for Smart Card/PIV, FIDO2/ WebAuthn, FIDO U2F, OTP and OpenPGP on a single key

yubico