Passkeys vs Passwords

Free tech help for everyone

Author	Schnee Held
Github	@schneeheld

Read time	4 mins
Version	2026.v1
Pages	4

Passkeys vs Passwords

Passkeys vs Passwords — Overview

Passkeys and passwords both let you sign in, but they work very differently. Passkeys are cryptographic keys stored on your device, while passwords are shared secrets you type and that are stored on servers.

What a password is

A password is a confidential string that a user memorizes and enters manually. It is typically stored in hashed form on a website's server or within an organization's systems, and it may be reused across multiple services, which increases security risk. Passwords are vulnerable to phishing, breaches, guessing, and reuse-based attacks.

What a passkey is

A passkey is a cryptographic key pair that is generated on the user's device for a specific service or account. The private key remains securely stored on the device and never leaves it, while the corresponding public key is provided to and stored by the website or service. During authentication, the device uses the private key to cryptographically sign a challenge, which is then verified using the public key — meaning no shared secret is ever transmitted or exposed. Access to the private key is protected through local device authentication such as a fingerprint, Face ID, hardware security key, or device PIN, effectively combining possession of the device with user verification in a single step.

Key differences

Passkeys are unique per site, resistant to phishing, cannot be reused across services, and the private key never leaves your device. Passwords depend on security practices and user choices and are vulnerable to reuse, phishing, and database leaks.

Why passkeys are more secure

Passkeys protect against phishing websites, credential stuffing, password reuse, keylogging, and database breaches. Even if a service is compromised, attackers only get the public key, which is useless without the private key.

Where passkeys are stored

Passkeys may sync securely through systems such as iCloud Keychain, Google Password Manager, Microsoft Authenticator, or supported password managers, and can also be stored on hardware security keys.

Things to know

Passkeys are still rolling out across services. You should ensure you have backup or sync enabled. Some shared or multi-user device workflows may be tricky, and not all websites support passkeys yet — but adoption is growing quickly.

When to use passkeys

Use passkeys whenever a service supports them, especially for high-value accounts such as banking, email, and developer platforms. They provide strong security with a simpler sign-in experience.

Business & Usability Benefits

The FIDO Alliance’s 2025 Passkey Index — one of the first aggregated reports from real deployments — shows participating companies (e.g., Amazon, Google, PayPal, Microsoft) report:

93% login success rates with passkeys

73% reduction in sign-in time

Significant operational improvements like fewer help-desk incidents.

This provides quantitative evidence of business value from passkey adoption.

References

The Passkeys Revolution: How 2025 Became the Year Passwords Died
https://blog.magicauth.app/articles/passkeys-revolution-2025

Passkey use doubles year over year; Google, Amazon lead in authentications
https://www.scworld.com/news/passkey-use-doubles-year-over-year-google-amazon-lead-in-authentications

Microsoft - What is a passkey?
https://www.microsoft.com/en-us/security/business/security-101/what-is-passkey

Disclaimer: Portions of the material contained in this document were generated or assisted by the use of an artificial intelligence system. While reasonable efforts have been made to review, edit, and verify the accuracy and appropriateness of the information, the content may include automated output and should not be relied upon as professional, legal, technical, or factual advice. No representation or warranty, express or implied, is made as to the completeness, reliability, or suitability of the information for any particular purpose. The reader remains responsible for independently evaluating and verifying any information contained herein before relying on it or taking action based upon it.

IMPORTANT: The content should not be used in production environments, relied upon for decision-making, or implemented in real-world systems without appropriate expert review, testing, and validation. No representation or warranty, express or implied, is made as to the accuracy, reliability, suitability, or fitness of the information for any particular purpose. The reader remains solely responsible for independently evaluating, validating, and confirming any information contained herein before relying on it or taking action based upon it.