Google

Passkeys: One step closer to a passwordless future

With the dramatic rise of state-sponsored cyberattacks and malicious actors online, we're more focused than ever on protecting people, businesses and governments by sharing our expertise, empowering society and continuously working to advance the state of the art in cybersecurity to help build a safer world for everyone.

Today passwords are essential to online safety, but threats like phishing continue to rise. Google has long recognised these issues and encouraged using authentication tools such as 2-Step Verification (2SV), Google Password Manager, security keys and now passkeys.

Challenge

Passwords have been used with computers for over 60 years, but, today, they're simply no longer sufficient in keeping users' and organisations' data safe. Phishing attacks continue to grow in their scale and sophistication by taking advantage of security weaknesses in passwords. For example:

- Over **60% of data breaches** in 2021 involved stolen credentials or phishing.[1]
- Data breaches caused by phishing cost organisations **$4.91 million on average** in 2022.[2]
- Phishing attacks grew **61%** in 2022, reaching 255 million in a six-month period.[3]

2-step-verification/2-factor-authentication (2SV/2FA) helps, but it could put strain on the user with additional friction and still doesn't fully protect against phishing attacks and targeted attacks like "SIM swaps" for SMS verification.

Solution

Partnering with the FIDO Alliance, we enabled support for passkeys - a simpler and more secure alternative to passwords, bringing phishing-resistant technology to billions of people worldwide. With passkeys, you can skip your password for an easier and more secure sign-in experience, using your fingerprint, face scan or screen lock.

Starting in early 2023, passkeys became available for personal Google Accounts along with the users of more than 9 million Google Workspace customers, as well as 3rd party sites and apps on Chrome and Android.

Simplest and fastest way to sign-in

Passkeys are **4x simpler** to use since they don't need to be remembered or typed. You just use your fingerprint, face scan, or screen lock to sign in across all your devices and platforms.[4]

Next-generation account security

Passkeys provide the strongest protection against threats like phishing. And since they're stored on your local device, they cannot be guessed or reused helping keep your information secure against attackers.

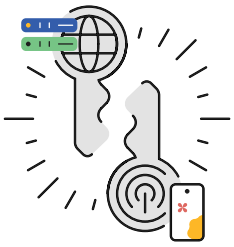
Privacy that's uniquely yours

Your passkey stays private on your personal device and is never shared with Google or any other 3rd party partners. You simply use your fingerprint, face scan, or screen lock to verify it is you accessing your private key.

Safer with Google

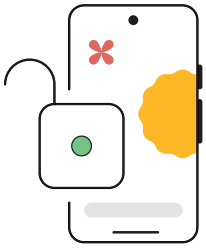
Google

Under the hood

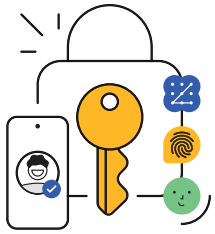


A passkey has two parts: a public key on the server for the website you're signing into and a corresponding private key on your devices.

When you sign in, the website checks to see if your public key matches up with your private key.



To verify that it does, you're simply asked to unlock your device.



You'll be signed in to your account, your private key and your biometrics will stay safely on your device, and they'll never be shared.

Enabling a safer ecosystem

Bringing passkeys to businesses and governments

Passkeys introduce meaningful security and usability benefits to users, and we're thrilled to be the first major public cloud provider to bring this technology to our customers — from small businesses and large enterprises to schools and governments.

Partnering for a passwordless, safer sign-in across the Internet

We partner with brands to enable passkeys across Chrome and Android platforms, providing easier, more secure sign-ins for their users. Multiple partners across industries such as ecommerce, financial tech, travel and others have already joined the passwordless journey with us, including 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal and Yahoo! Japan.

Our passwordless journey

Passkeys bring us much closer to the passwordless future we've been mapping out for over a decade.

2008	2011	2012	2013	2014	2017	2019	2023
Launched Google Password Manager for easier and safer sign-ins.	Enabled 2-Step Verification (2SV) for Google accounts.	Introduced phishing-resistant security key for Google employees.	Joined the FIDO Alliance to drive open standards for a passwordless world.	Expanded phishing-resistant security keys for everyone.	Introduced Advanced Protection Program (APP) for high-risk users.	Extended our FIDO support in Android for passwordless re-authentication across websites.	Enabled passkeys for Google Accounts, Workspace customers and 3rd party partners on Chrome and Android.

While passwords will continue to be part of our lives as we make the transition to passkeys, we are committed to helping people, and others in the industry, take this next leap to make signing in easier and safer with Google.

Sources: 1 - Verizon Data Breach Investigation report 2022 | 2 - IBM Cost of Data Breach report 2023
3 - CNBC's Cyber Report | 4 - Google Security Blog, May 2023

Safer with Google

Explore how Google helps keep everyone safe online at g.co/safety