Your Google account no longer needs a password for sign in

Google’s next step into a passwordless future is here with the announcement that passkeys – a new cryptographic keys solution that requires a preauthenticated device – are coming to Google accounts on all major platforms. Starting today, Google users can switch to passkeys and ditch their passwords and two-step verification codes entirely when signing in.

Passkeys are a safer, more convenient alternative to passwords being pushed by Google, Apple, Microsoft, and other tech companies aligned with the FIDO Alliance. They can replace traditional passwords and other sign-in systems like 2FA or SMS verification with a local PIN or a device’s own biometric authentication – such as a fingerprint or Face ID. This biometric data isn’t shared with Google (or any other third party), and passkeys only exist on your devices, which provides greater security and protection since there’s no password that could be stolen in a phishing attack.

Google accounts will request your passkey to sign in or verify your identity when it detects sensitive activity

When you add a passkey to a Google account, the platform will start prompting for it when you sign in or when it detects potentially suspicious activity that requires additional verification. Passkeys for Google accounts are stored on any compatible hardware – such as iPhones running iOS 16 and Android devices running Android 9 – and can be shared to other devices from the OS using services like iCloud or password managers like Dashlane and 1Password (expected to arrive in “early 2023”).

You can still use someone else’s device to temporarily gain access to your Google account. Selecting the “use a passkey from another device” option creates a one-time sign-in and won’t transfer the passkey over to the new hardware. As Google notes, you should never create passkeys on a shared device because anyone that can access and unlock that device would be able to access your Google account.

a:hover]:text-gray-63 [&>a:hover]:shadow-underline-black dark:[&>a:hover]:text-gray-bd dark:[&>a:hover]:shadow-underline-gray [&>a]:shadow-underline-gray-63 dark:[&>a]:text-gray-bd dark:[&>a]:shadow-underline-gray”>Image: Google
Users can immediately revoke passkeys in the Google account settings if they suspect that someone else can access the account or if they lose the only device that stored the passkey. Google says that users enrolled in its Advanced Protection Program, a free service that provides additional security protections against phishing and malicious apps, can choose to use passkeys in lieu of their usual physical security keys.

“We’re thrilled with Google’s announcement today as it dramatically moves the needle on passkey adoption due both to Google’s size, and to the breadth of the actual implementation – which essentially enables any Google account holder to use passkeys,” said Andrew Shikiar, executive director of FIDO Alliance, in a statement. “I also think that this implementation will serve as a great example for other service providers and stands to be a tipping point for the accelerated adoption of passkeys.”

It’s going to take a while for passkey support to be widely adopted, so Google accounts will continue supporting existing login methods like passwords for the foreseeable future. This gives folks who may not currently have access to a device that supports biometric authentication time to transition over to the new technology. It seems Google *is* planning to eventually transition entirely to passkeys, though, by encouraging users

to make the switch now and writing in its blog that it would scrutinize other sign-in methods “as passkeys gain broader support and familiarity.”

Today’s announcement follows smaller passkey implementations by Google. In December last year, Google’s Chrome browser gained passkey support, but passkey-supported sites and services are still relatively rare. That makes it difficult to go entirely password free just yet. 1Password has a page indicating which sites and services support passkeys, and hopefully the authentication tech will be more rapidly adopted now that companies like Google are more fully embracing a passwordless future.

https://www.theverge.com/2023/5/3/23709318/google-accounts-passkey-support-password-2fa-fido-security-phishing