How to use a passkey to sign into your Google account

Passwords have always been a necessary evil, giving you the choice of either using one that is too simple (so you can easily remember it) or one obscure enough to be secure but complicated enough to require a password manager.

Until now, the best way to keep your accounts secure was to partner a password with two-factor authorization (2FA). But now, Google is offering another choice: using a passkey – a secure credential tied to the PIN or biometric authentication your device already uses. The passkey only exists on your device, not in the cloud, making it even safer.

Want to give it a try? Here's how.

Currently, you can create a passkey on any compatible hardware, including laptops / desktops with Windows 10 or macOS Ventura (or later) running Chrome 109, Safari 16, or Edge 109 or later. If you're setting up a passkey on a mobile phone or tablet, it must run iOS 16 or Android 9 (or later). You can also use it with any hardware security key that supports the FIDO2 protocol.

You will also need to have a screen lock enabled, and if you want to use your phone to sign into another device, such as a laptop, you will also need to have Bluetooth turned on.

Finally, if you have a Google Workspace account through a school or employer, you won't be able to set up a passkey for that account. (You can, however, use it for any personal Google account.)

a:hover]:text-black [&>a:hover]:shadow-underline-black

dark:[&>a:hover]:text-gray-e9 dark:[&>a:hover]:shadow-underline-gray-63 [&>a]:shadow-underline-gray-13 dark:[&>a]:shadow-underline-gray-63″>*You can only delete passkeys you've created.*

If the passkey was automatically created by Google, you can't delete it — instead, you have to sign that device out of the account.

Yes. If you want, you can go back to using passwords and 2FA as before. (Note: the passkeys will still be part of the account; they just won't be used.)

https://www.theverge.com/23712758/google-passkey-password-2fa-security-how-to