FEATURE

Beyond passwords: How to set up passkeys with your Google account

You can still keep a password as a backup method of login.

By Alaina Yee
Senior Editor, PCWorld | MAY 10, 2023 6:01 AM PDT

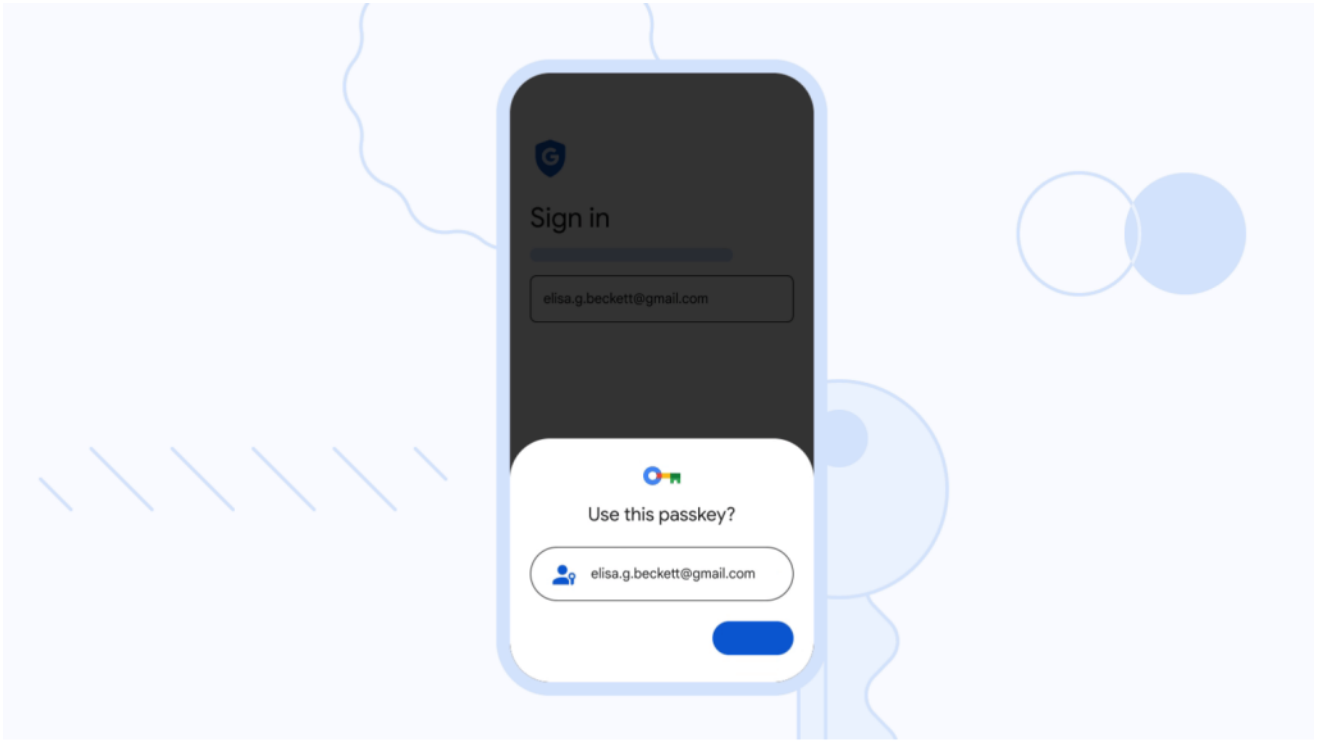


Image: Google

Passwords have one big flaw: If anyone guesses what your password is, you're left with no defense. It's why we use password managers and two-factor authentication to better safeguard our accounts.

Passkeys, on the other hand, are immune to this issue. In fact, this newer login method is both simpler and more secure. With just a smartphone, you can generate and store passkeys, and they don't require as much interaction or management. Once they're set up, you just approve login attempts with a PIN or biometrics (e.g., fingerprint or facial identification).

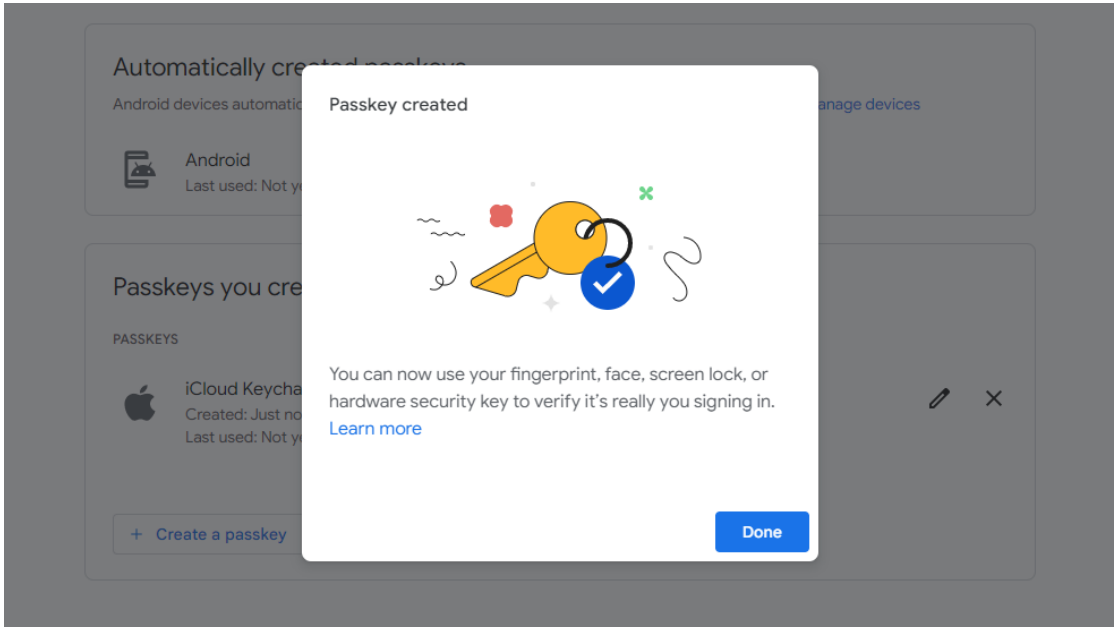
If that sounds exciting, you're in luck. Passkey support beginning to pick up steam, and Google is the latest big corporation to let you log into an account with a passkey. Here's how to get started.

How to set up passkeys for your Google account

On PC, you'll begin by heading to the web version of Google's account management. If you plan to set up a phone or tablet, it must be nearby the computer you'll be using. The PC also must have Bluetooth and run Windows 10 or 11, and you must use Chrome (version 109 or newer) or another Chromium browser like Edge (version 109 or newer).

1. Head to *myaccount.google.com*.
2. On the left side of the page, click on *Security*.
3. Under *How you sign into Google*, click on *Passkeys*. If you don't see this option, you'll need first to click on *Use your phone to sign in* and link your account to a device like a phone or tablet.
4. Click on the blue *Use passkeys* button.

You'll now see a management screen for your passkeys. If you have any Android devices already logged into your Google account, they'll automatically be available for passkey setup. You just have to log into your account to complete the process.



When you've manually set up a passkey successfully, you'll see this confirmation screen.

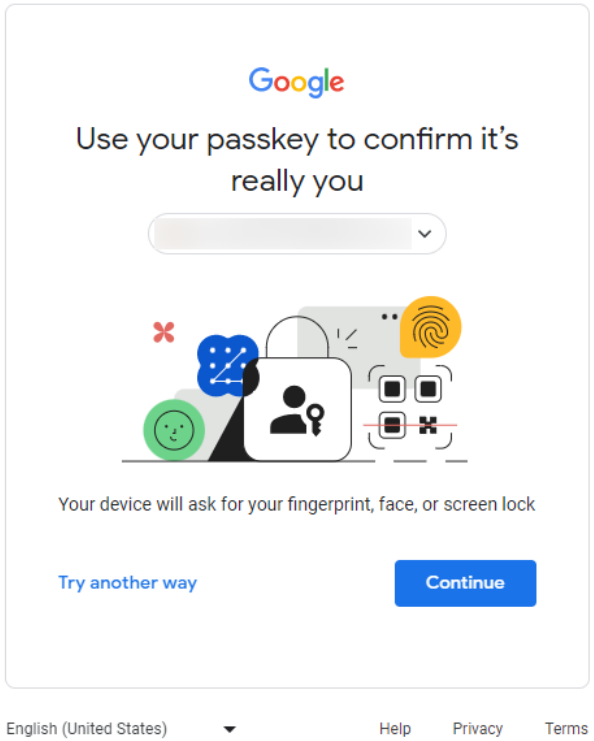
Image: PCWorld

To manually create a passkey, click the white *Create a passkey* button. If you're on an incompatible PC, you'll see a dialog box with a blue button to *Use another device*. You can choose to set up a device like a phone or tablet by scanning a QR code, or a security key. (For setting up passkeys in a compatible password manager, use the QR code method.)

If you decide you don't like passkeys and want to remove them, you can delete manually added ones by clicking the X button. For automatically added devices, you must remove that phone or tablet from your account.

How to use a passkey to log into your Google account

Once you've set up passkeys for your Google account, they become your default login method. After you enter your user name, you'll see a screen prompting you to use your passkey. Click on the blue *Continue* button.



Once you setup passkeys, they become the default login method.

Image: PCWorld

If you've used a phone or tablet (which most people will), you'll see another prompt asking if you want to sign in using the passkey on that device. Click continue, then switch to your phone to verify the request with your PIN or biometrics. You'll then be logged in—if two-factor authentication is enabled on your Google account, it'll only be necessary when logging in with your password. A passkey is considered to already be both something you know (the private encryption key stored on the device) and something you have (the phone). In other words, it's two factors already combined into one system.

How passkeys work

At first glance, passkeys may seem less secure due to their simplicity. It can look like a phone's facial recognition, fingerprint, or PIN becomes the only thing protecting the Google account.

Passkeys use public-key encryption, also known as asymmetrical encryption, for login authentication. When you create a passkey, a public key and a private key are generated. The public key gets shared with the website (in this case, Google), while you hang on to the private key. You need both to sign into your account—whenever you try to log on, the website will ask for proof that you're you. If you approve the request, your device will use your secret key to create a digital signature to send to the website, which the website will unencrypt using the public key you gave it. Your PIN (or biometrics) safeguards use of your private key, rather than serving as the full authentication process.

Sync your passkey to the cloud and you can more easily use it across devices (or pick up where you left off, if your primary device is lost or stolen).

Image: Google

This process offers better protection against website breaches, since no one can guess your private key based on the public key. Passkeys are also tied to the website they're generated for, so they can't be captured by fake phishing sites like passwords can.

Passkeys can also be saved in several different ways—not just to your device, but also to hardware security keys, a compatible PC, and the cloud. For cloud backups, you can use a password manager like Dashlane or NordPass, or save them to your operating system (Windows; macOS & iOS). You can control how widely you spread your collection.

Other sites that use passkeys

Google isn't the only major site that supports passkey login—Apple beat them to the punch late last summer. You can find more websites (like Best Buy) on this list hosted by password manager 1Password. Password managers will also be more widely adopting passkey support in the coming months, too. Overall, expect passkeys to become more common as the year rolls on.

Author: Alaina Yee, Senior Editor, PCWorld

A 14-year veteran of technology and video games journalism, Alaina Yee covers a variety of topics for PCWorld. Since joining the team in 2016, she's written about CPUs, Windows, PC building, Chrome, Raspberry Pi, and much more—while also serving as PCWorld's resident bargain hunter (#slickdeals). Currently her focus is on security, helping people understand how best to protect themselves online. Her work has previously appeared in PC Gamer, IGN, Maximum PC, and Official Xbox Magazine.

Recent stories by Alaina Yee:

- Data breaches are everywhere—but you still need to pay attention to them
- Why are tech companies so willfully bad at privacy?

- Best antivirus software 2024: Keep your PC safe from malware, spyware, and more

PCWorld

PCWorld helps you navigate the PC ecosystem to find the products you want and the advice you need to get the job done.

POLICIES

Privacy Policy
Cookie Policy
Copyright Notice
European Privacy Settings
Member Preferences
Editorial independence
Licensing & Eprints
California: Do not Sell my Personal Info

ABOUT

About Us
Advertise
Ad Choice
Contact Us
Foundry Careers
GamePro
Smart Answers

PCWORLD CATEGORIES

Business
Laptop
Mobile
PC Hardware
Deals

SUBSCRIBE

Digital Magazine - Subscribe
Digital Magazine - Info
Gift Subscription
Newsletters

FOUNDRY

Explore the Foundry Network +