

[#AmazonPrimeDay](#)[#TopTravelTech](#)[Best Products](#)[Comparisons](#)[Reviews](#)[How-To](#)[News](#)[Deals](#)[Search](#)

PCMag editors select and review products [independently](#). If you buy through affiliate links, we may earn commissions, which help support our [testing](#).

[Home](#) > [How-To](#) > [Security](#) > [Password Managers](#)

How to Set Up Passkeys for Your Google Account

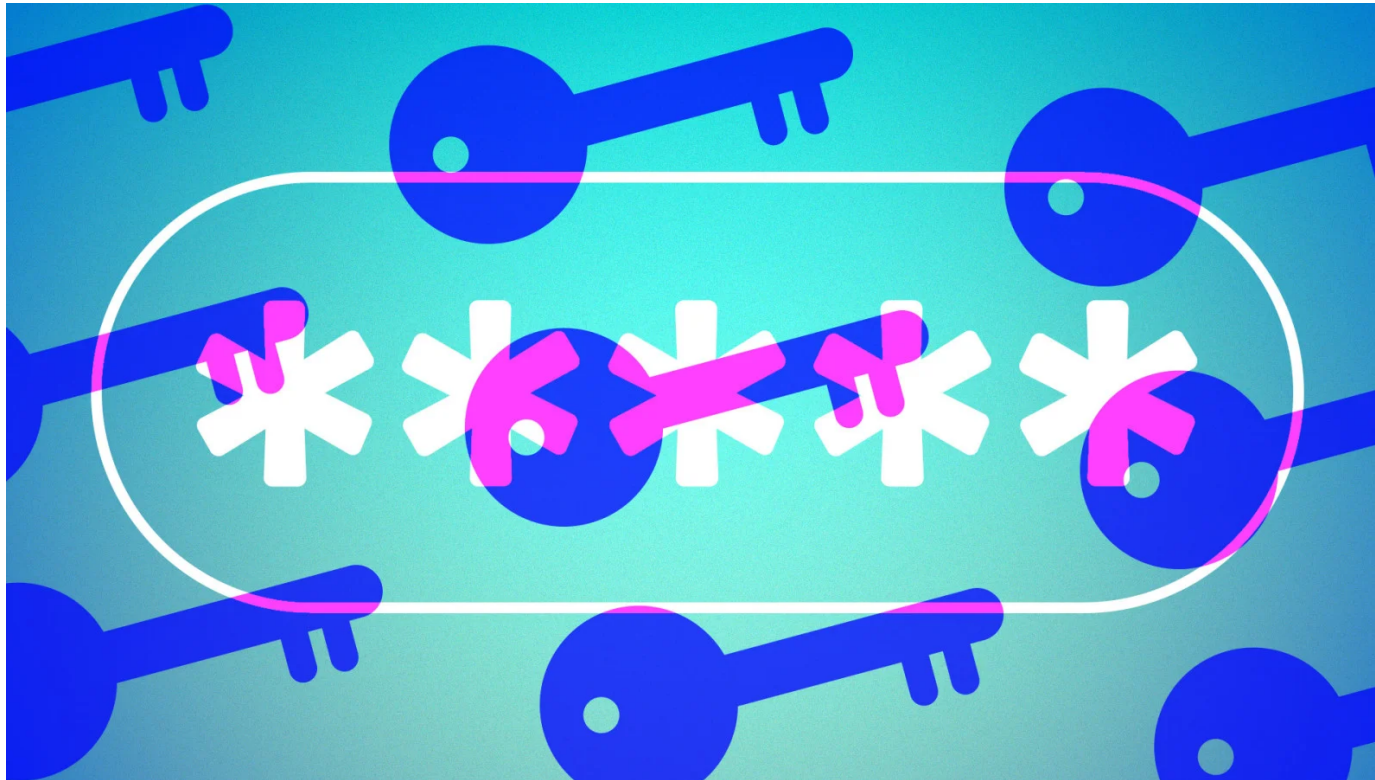
Passkeys are easier to use and more secure than passwords, but getting started with them isn't simple. We tell you how to set up and use passkeys for Google on all your devices.



By [Max Eddy](#)

May 15, 2023





(Credit: René Ramos)

Table of Contents



Passwords are an annoying and insecure reality of living with technology. Nobody likes them, but there has been no real alternative—until now. If they live up to their promise, passkeys can take the pain and the risk out of authentication with a simple, secure system built on trusted devices. Google is among the largest companies enabling passkeys, so you can now try this new technology when logging into your Google account.

What Are Passkeys?

Passkeys are intended to be more secure and easier to use than passwords. Instead of typing in a password (or letting a password manager do it) and verifying with a multi-factor authentication method, passkeys only require a trusted device and either biometric or PIN verification.

Part of why passkeys seem likely to replace passwords is that they're designed by a consortium called the FIDO Alliance and championed by Apple, Google, and Microsoft. These three companies have already baked support for passkeys into their browsers and ecosystems, which means that for the first time, there's a viable alternative to passwords. That said, passkeys have yet to see widespread adoption.

How Safe Are Passkeys?

For anyone who has worked hard to protect their passwords from phishing and brute-force guessing, this new technology might seem a little scary.

ADVERTISEMENT

You might wonder what happens if someone steals the device with your passkey. As passkeys can only be created on devices that require authentication to unlock, anyone who finds your device will first have to get inside it to impersonate you. While it's not impossible to bypass the biometric or PIN locks on devices, it's not easy work for a casual crook.

You may also worry about what happens if a site is breached or your device is attacked. Because they're made using [asymmetric key cryptography](#), a [data breach](#) doesn't expose any information an attacker could use to impersonate you. Even if your passkey was somehow extracted from your device, it wouldn't work without the device itself *and* your biometric or PIN authorization.

How Convenient Are Passkeys?

Even if you overcome these fears, there are also logistics to consider. How will you log in on a device that doesn't have a passkey? Fear not, you can use a device with a passkey to temporarily authorize another device that doesn't have a passkey on it. The connection is made securely over Bluetooth, but the passkey isn't transferred or copied. Instead, the receiving device is only authorized to log you in, and just for that one time.

**Part of why passkeys seem likely to
replace passwords is that they're
designed by a consortium called the FIDO**

Alliance and championed by Apple, Google, and Microsoft.

Depending on the platform you're on, passkeys can also sync between your devices. For example, when I created a passkey on my iPhone, an alert informed me it was saved to iCloud Keychain and available on my other Apple devices as well.

Does Your Device Support Passkeys?

Before you start, you should ensure the devices you want to create a passkey with are supported. [Google's documentation](#) lays out three important categories. You'll need at least Windows 10 (2015) or macOS Ventura (2022) for desktops and laptops. For mobile devices, you'll need at least [Android 9](#) (2018) or [iOS 16](#) (2022).

You can also use a [hardware security key](#) like the [Yubikey 5](#) to store your passkeys. The advantage is that your passkeys live on only one device you control, but it also means you'll lose all your passkeys if you lose your security key. Creating more passkeys on other devices or a backup security key is a good idea. Sites and services that use passkeys will have to provide some kind of fallback option for scenarios like this one, and it will probably mean dusting off your old password — or resetting it, if necessary. If you're using a security key, it needs to support FIDO2. Most modern keys support this standard, but older keys may not.

The device you use will also need to meet some minimum security requirements. A laptop, desktop, or mobile device must have a lock feature enabled. That means you need to use biometrics or a PIN/password to open the device after it has been idle. You do *not* need a security key that supports biometrics, however.

ADVERTISEMENT

As noted above, passkeys can be used to authorize other devices with a Bluetooth connection. So, if you want to do that, you'll need a device with Bluetooth enabled.

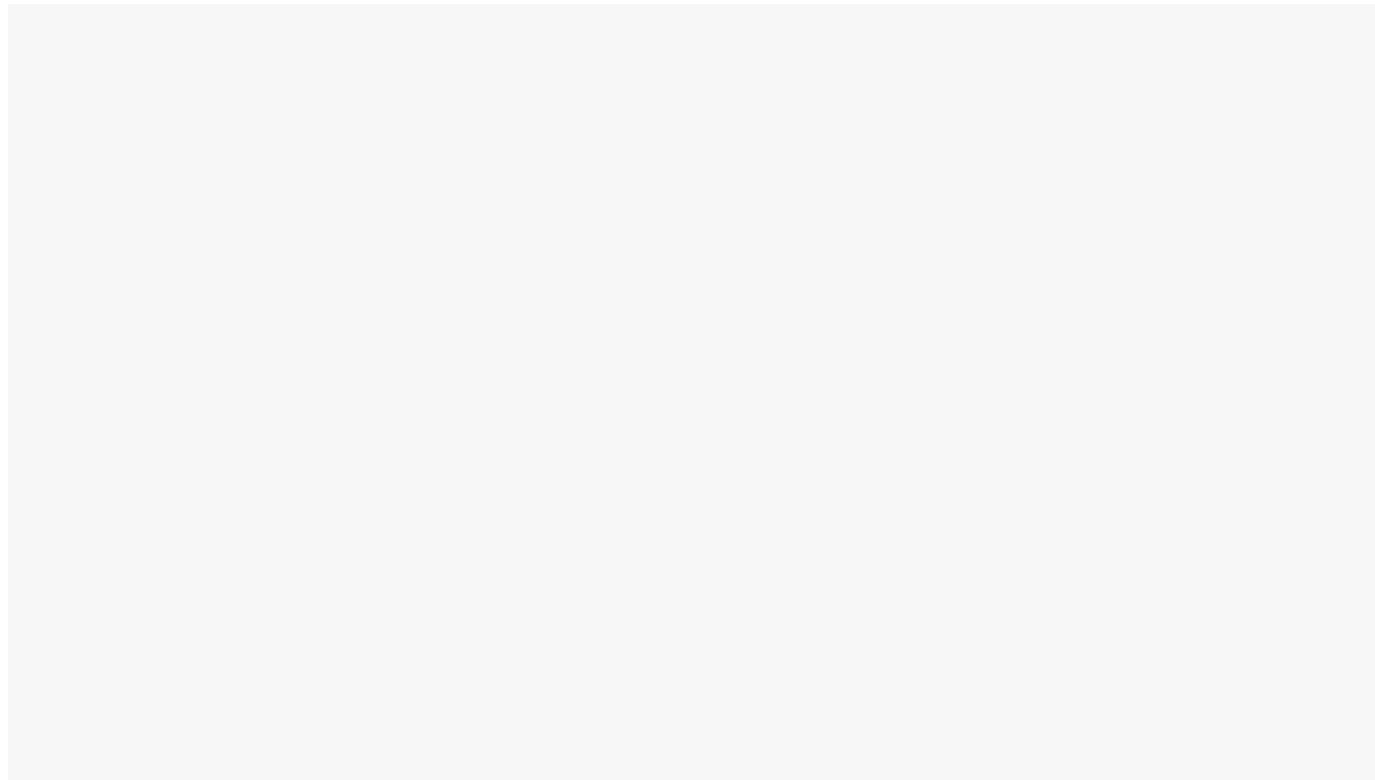
Finally, if you're using a browser—and you probably are—it will *also* need to support passkeys. Google's documentation says passkeys are supported in Chrome 109, Safari 16, or Edge 109. Noticeably absent is Firefox, although developer Mozilla says they are on the roadmap. In our testing, we found that other Chromium-based browsers may also support passkeys. We had no trouble creating and using a passkey with the latest version of Opera, for example.

Note that if your Google account is managed by an employer or other organization, passkeys aren't an option. However, you can use passkeys in place of security keys with Google's [Advanced Protection Program](#).

Getting Started With Passkeys

Google has created a special dashboard for viewing and managing the passkeys you've created to log in to your Google account. These are *only for your Google account*, not for all the passkeys for other sites and services on your device.

To view it, sign into Google normally (hopefully using multi-factor authentication and a password manager). Then click your icon in the upper right of the screen and click Manage Your Google Account. On the next screen, click Security in the left-hand column. In the section called How You Sign In To Google, you'll see several options, one of which should be passkeys.



Google lets you manage all the passkeys you've created to access your Google account (Credit: Google)

If you have an Android device, the top section of the passkeys screen is labeled Automatically Created Passkeys. That's right; if you've connected your Android device to your Google account, that device already has a passkey and can be used to log in to your Google account. If you see devices there you don't recognize or haven't used in a long time, click the Manage Devices link at the top of the screen (or visit the [Google device manager](#)) to unenroll them.

ADVERTISEMENT

The section called Passkeys You Created shows all the passkeys for your Google account, and some information about the platform the passkey was created on, the last time it was used, and the approximate location of its use. If you delete a passkey here, you de-authorize the device that created the key. That's handy if you accidentally created a passkey on a computer that wasn't yours, or if you're getting rid of a machine.

If you've already enrolled a hardware security key as a multi-factor device with your Google account, it will show up in the list below. It can get a little tricky here, though. In my testing, I wasn't able to use a previously enrolled key to create a new passkey or sign in with a passkey. When I unenrolled the key and then used it to create a passkey, it worked just fine.

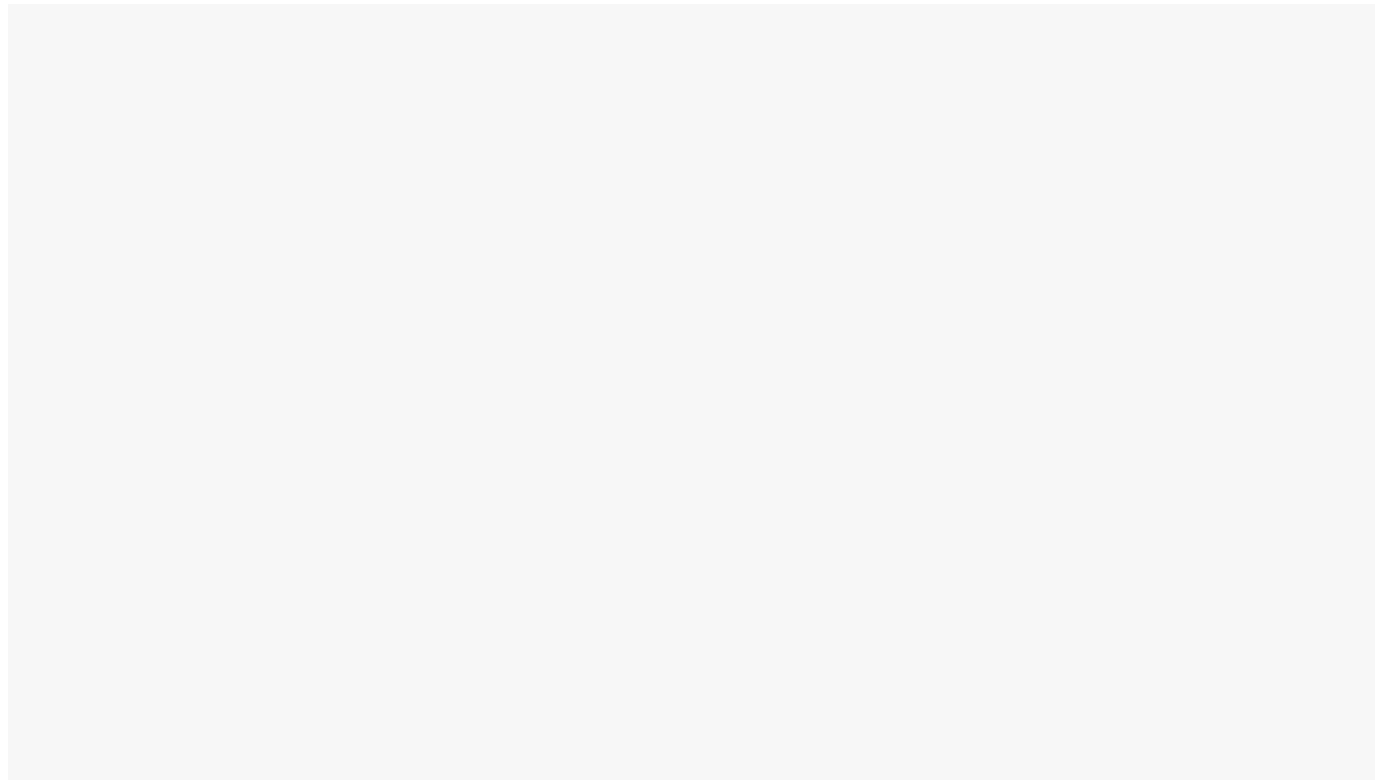
At the very bottom of the page is the most important part: a button that says Create A Passkey. This does exactly what it sounds like, and lets you create a passkey on a security key or the device you're using.

How to Create a Passkey for Google on Windows

First, make sure your Windows machine is set up to support passkeys. Most importantly, you'll need to enable Windows Hello before your PC can create a passkey. You can enable this feature in Windows settings.

Using either Microsoft Edge, Chrome, or a compatible Chromium-based browser, navigate to the Google passkey settings page and click the Create a Passkey button at the bottom of the screen. You can also use this short URL to start the process: <http://g.co/passkeys>.

You'll first be prompted to create a passkey, so just click Continue. Next, a Windows Security pop-up will appear. Then you use whatever Windows Hello method you use to unlock your PC. In my case, I entered my PIN and clicked OK.



Windows Hello must be enabled to create a passkey on Windows (Credit: Google/Microsoft)

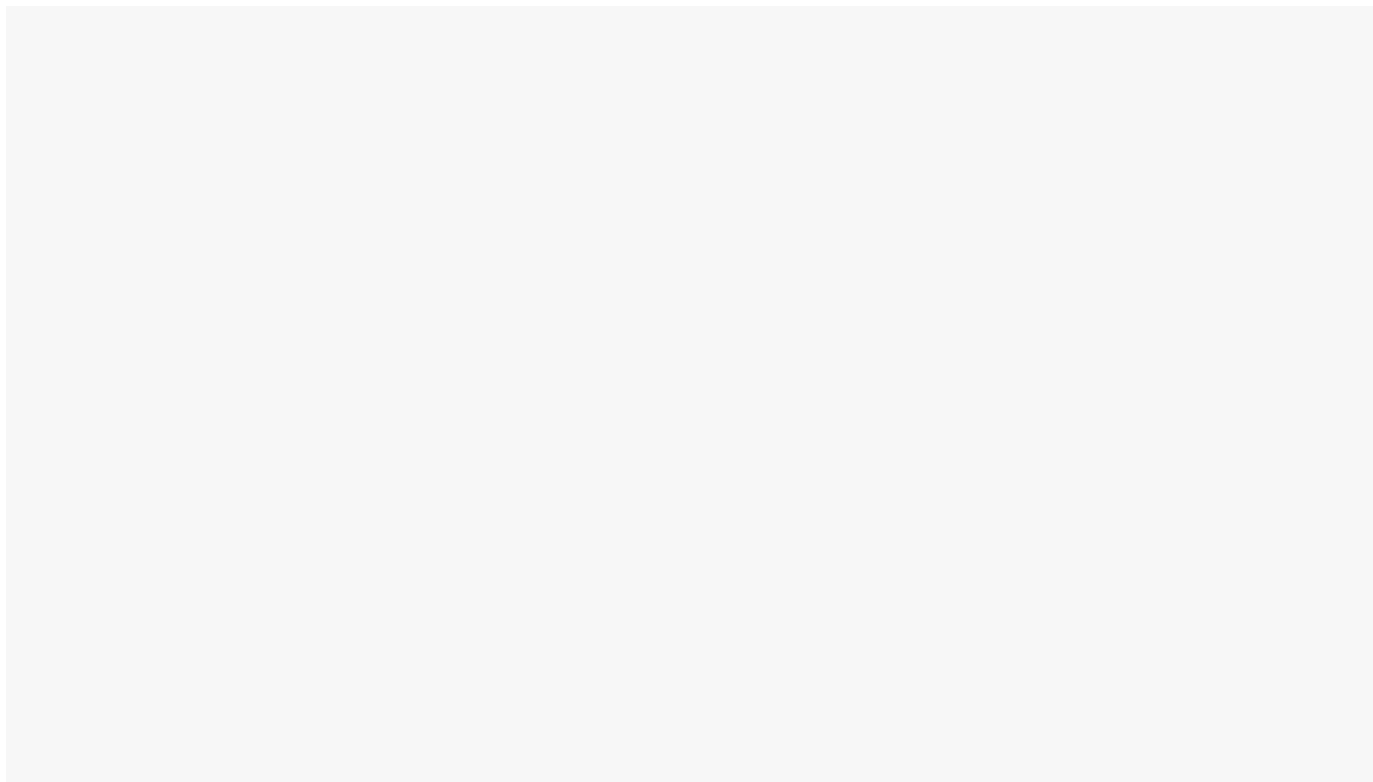
A passkey for Google is now stored on your Windows computer. Note that, currently, Microsoft does not sync Passkeys among devices—you have to manually create passkeys on all your other Windows machines. You can follow the steps above or use another device with a passkey for Google to authorize your other machine and then create a new passkey, as I explain below.

[ADVERTISEMENT](#)

How to Create a Passkey for Google on macOS

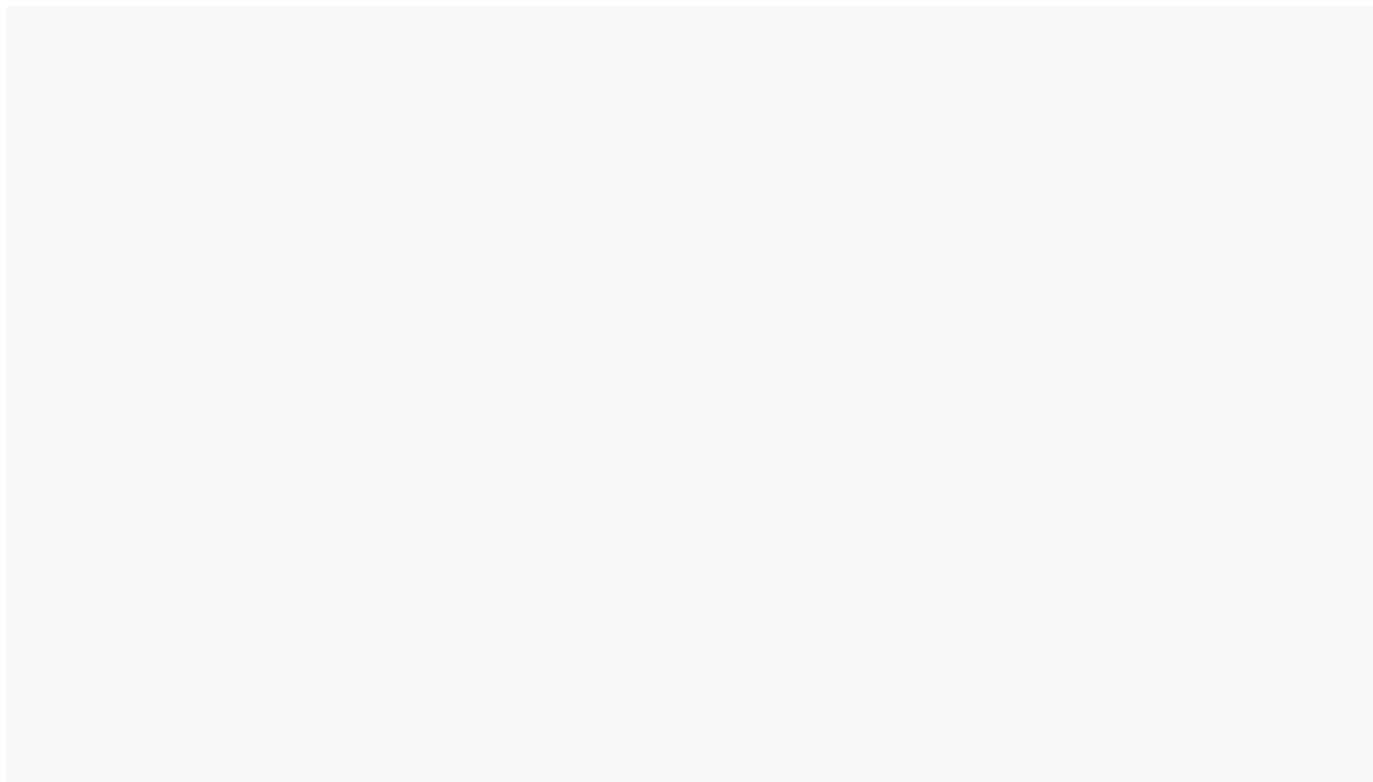
You can use either Chrome, a supported Chromium-based browser, or Safari to create a passkey on macOS. Be sure that your computer is using the latest version of macOS and that you have enabled either a biometric lock or password to secure your machine.

Navigate to the Passkey setting above and click the Create A Passkey button. Or use the Google short URL <https://g.co/passkeys>.



The first screen when creating a passkey on Google Chrome for macOS (Credit: Google)

You'll be prompted to create a passkey on your Mac. Once you press the Continue button, you verify the Google account for which you want to create a passkey. Next, you authorize the creation of a passkey with whatever mechanism you use to unlock your Mac. In my case, I used the MacBook Pro's fingerprint scanner.



macOS generating a prompt to enter a fingerprint or password (Credit: Google)

The passkey is now safely stored on your Mac, and a new entry will appear on the Google passkey settings page.

[ADVERTISEMENT](#)

How to Create a Passkey for Google on Android

To create a passkey on your Android device, you don't need to do anything. If you're already logged into your Google account then Google has already generated a passkey on your device. You can use it immediately to sign in to Google securely and authorize other devices as well.

As I noted above, because this is automatic you may have passkeys on devices you don't use or even own anymore. Be sure to look in the Google passkeys settings page and remove any devices you no longer use.

RECOMMENDED BY OUR EDITORS

Google: Passkeys Log You In Much Faster Than Passwords (Trust Us)

No More Passwords: How to Set Up Apple's Passkeys for Easy Sign-ins

Try Passkeys, But Keep Your Password Manager

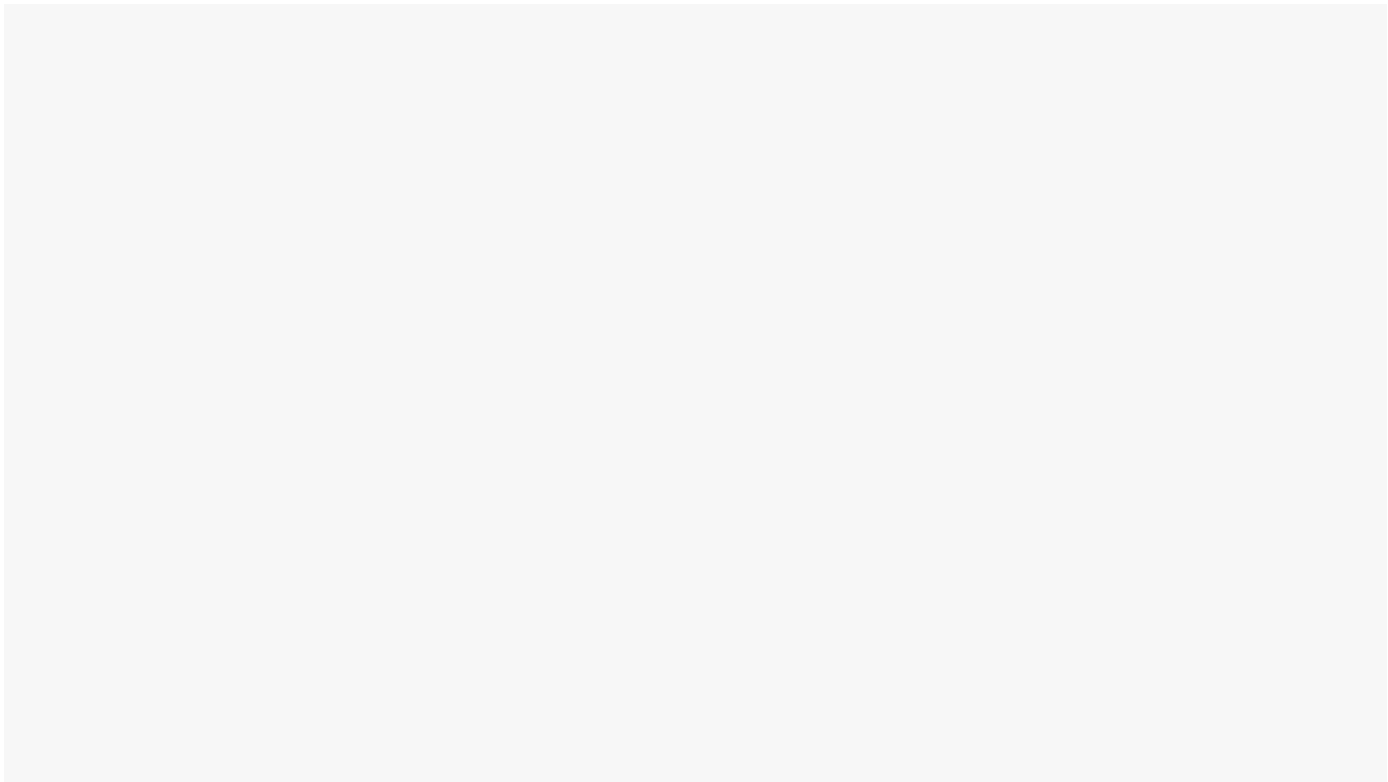
ADVERTISEMENT

How to Create a Passkey for Google on iOS

Using either the Chrome (or compatible Chromium-based browser) or Safari browsers on iOS, navigate to the Google passkey settings and tap the Create a Passkey button or use the short <http://g.co/passkeys>. You'll be prompted to create a passkey and tap Continue. Now, iOS takes over and alerts you that your passkey will be added to your iCloud Keychain and sync to all of your devices. Tap the button at the bottom, and then perform whatever ritual you use to unlock your device. For me, I entered my PIN code. That's it! Your passkey is created and stored.

Note that you can also use your passkey to log in to Google in other apps. For example, I created a passkey in Safari and then used it to log in to Chrome for iOS.

How to Create a Passkey for Google on Your Security Key

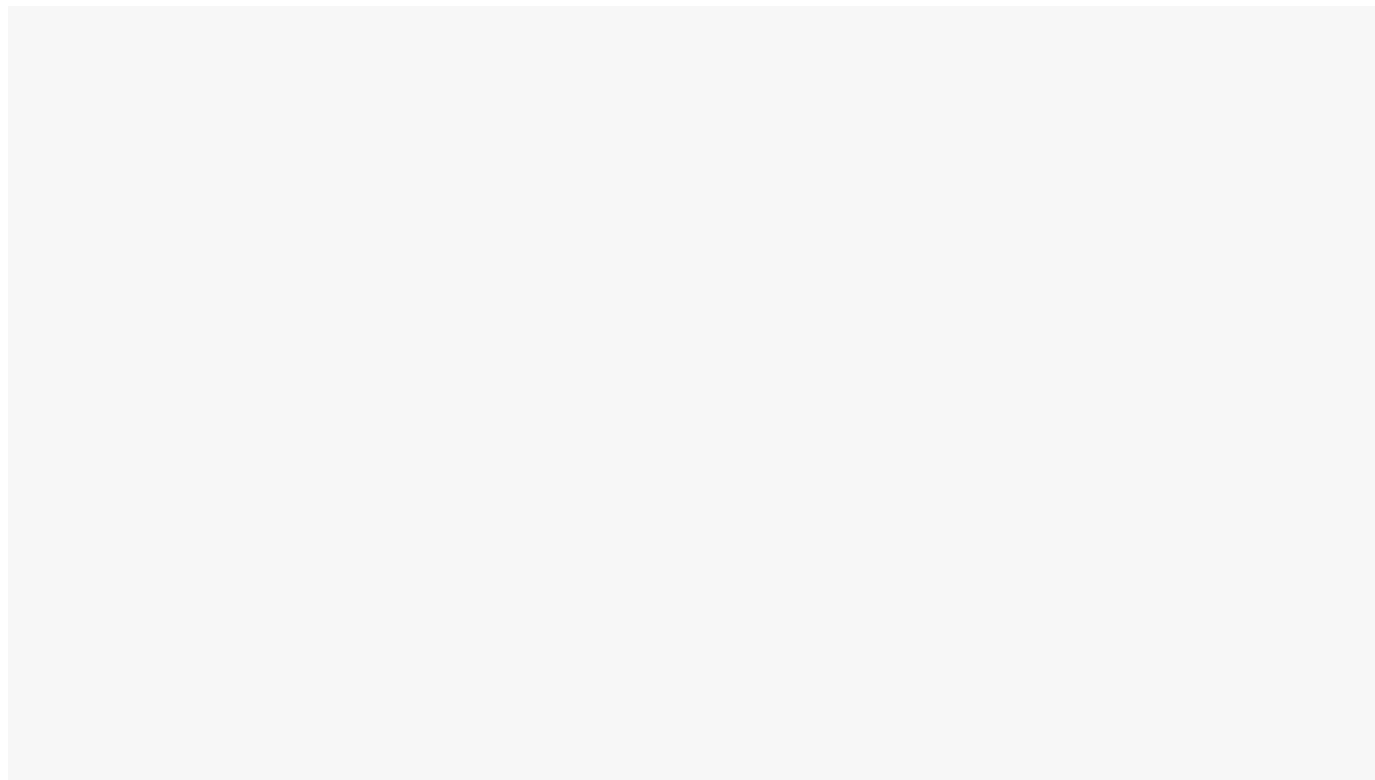


You can use a hardware security key like the Yubikey to store your passkeys (Credit: Max Eddy)

Before you start, make sure your security key supports FIDO2. Older keys won't work. Also, check to see if you have already enrolled your security key with Google as a multi-factor authentication device. In my testing, I found I couldn't use a security key I had already enrolled for multi-factor authentication to create a passkey. However, I simply unenrolled the key and then created a passkey on it. Weirdly, I separately had to reenroll the key again for use as a multi-factor authentication device. If you need to do this trick, I strongly suggest having another multi-factor authentication method available or creating a passkey on another device first, to ensure you have a safe and reliable means to log in.

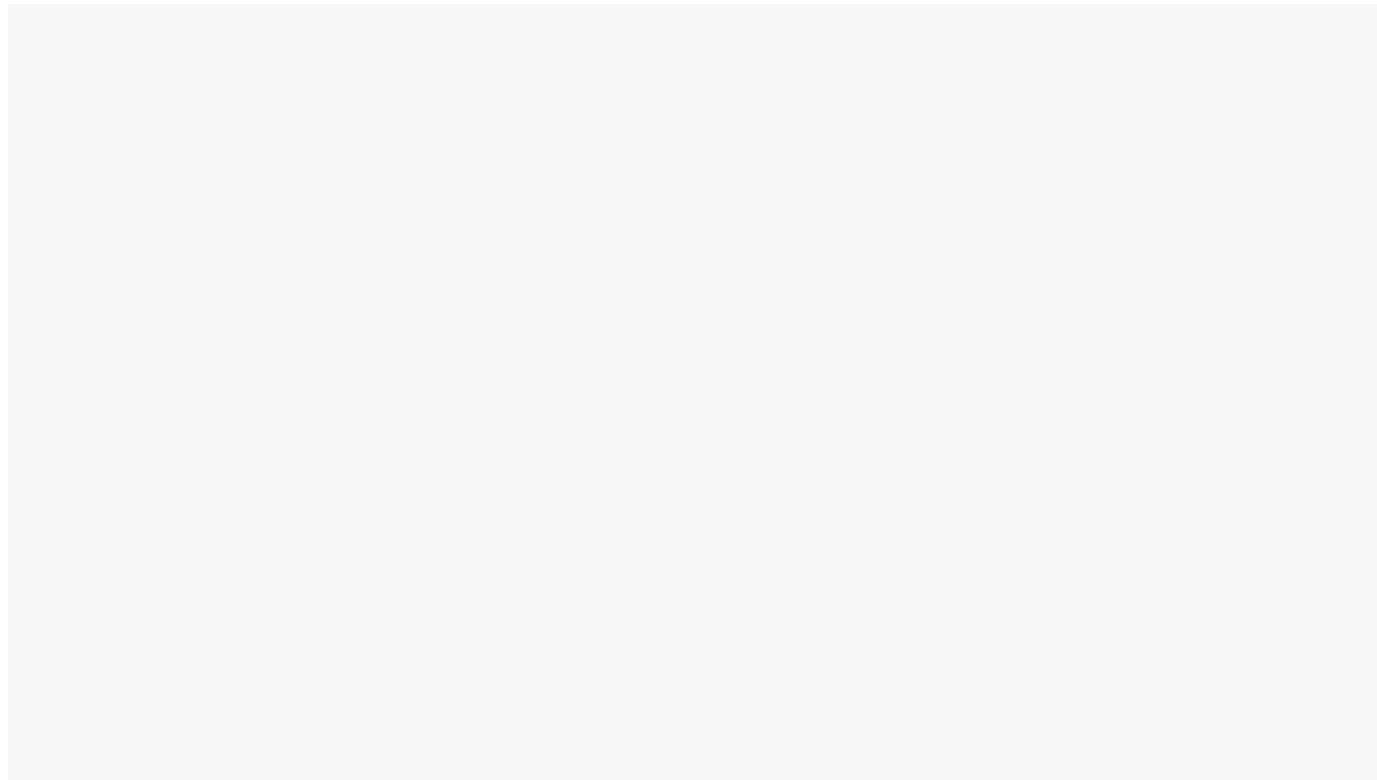
ADVERTISEMENT

Using a supported browser, navigate to the Google passkeys settings page and press the Create a Passkey button or use the short URL: <http://g.co/passkeys>. When prompted to create a passkey do *not* click Continue. Instead, click the Use Another Device link just to the left. From the list that appears, select the USB security key.



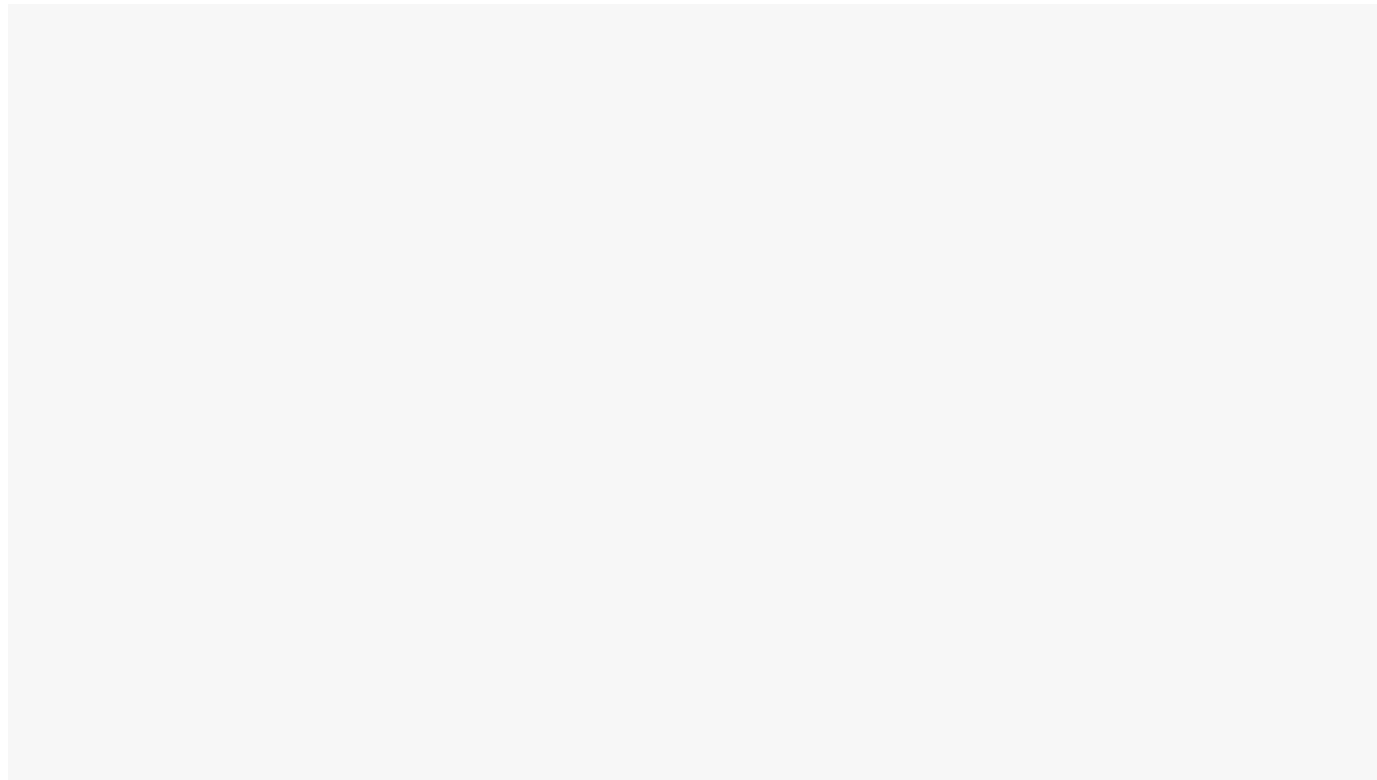
Clicking Use Another Device provides several options for creating a passkey in Chrome (Credit: Google)

You'll then be prompted to plug in your security key and tap its touch-sensitive button. If you have already created a PIN for your security key you'll have to enter it now. Otherwise, you'll be prompted to set a PIN for the key.



If you've never used your security key for any kind of passwordless entry, you'll have to assign it a PIN (Credit: Google)

You'll tap the key again, and then press Allow on the following screen that asks permission to access your security key. A window will then appear confirming the passkey was successfully created on your security key.



The passkey will remain on this security key (Credit: Google)

Remember: the passkey you've just created *only* exists on your security key, not the machine you were using.

ADVERTISEMENT

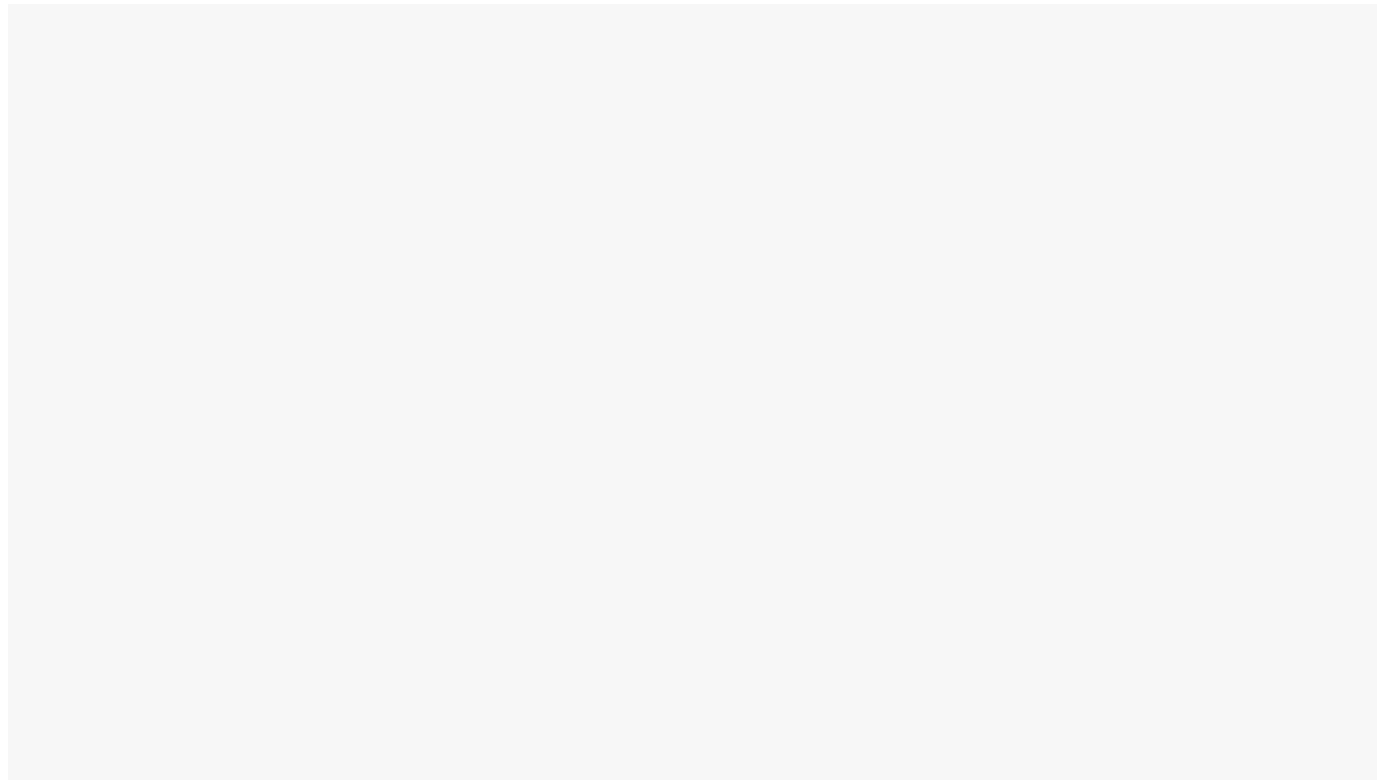
How to Use a Passkey on Another Device to Log In to Google

To log in to Google on one device using a passkey stored on another, you'll first have to create a passkey using one of the methods above. You'll also need to have Bluetooth enabled on both devices—the one with your passkey, and the one you wish to authorize with your passkey. If one of your devices does not support Bluetooth, this won't work. The device that contains your passkey also needs a functioning camera.

Note that if you created your passkey on a security key, you can just plug the key into the device and log in. You can then create a new passkey on the device you're logging in with if you wish.

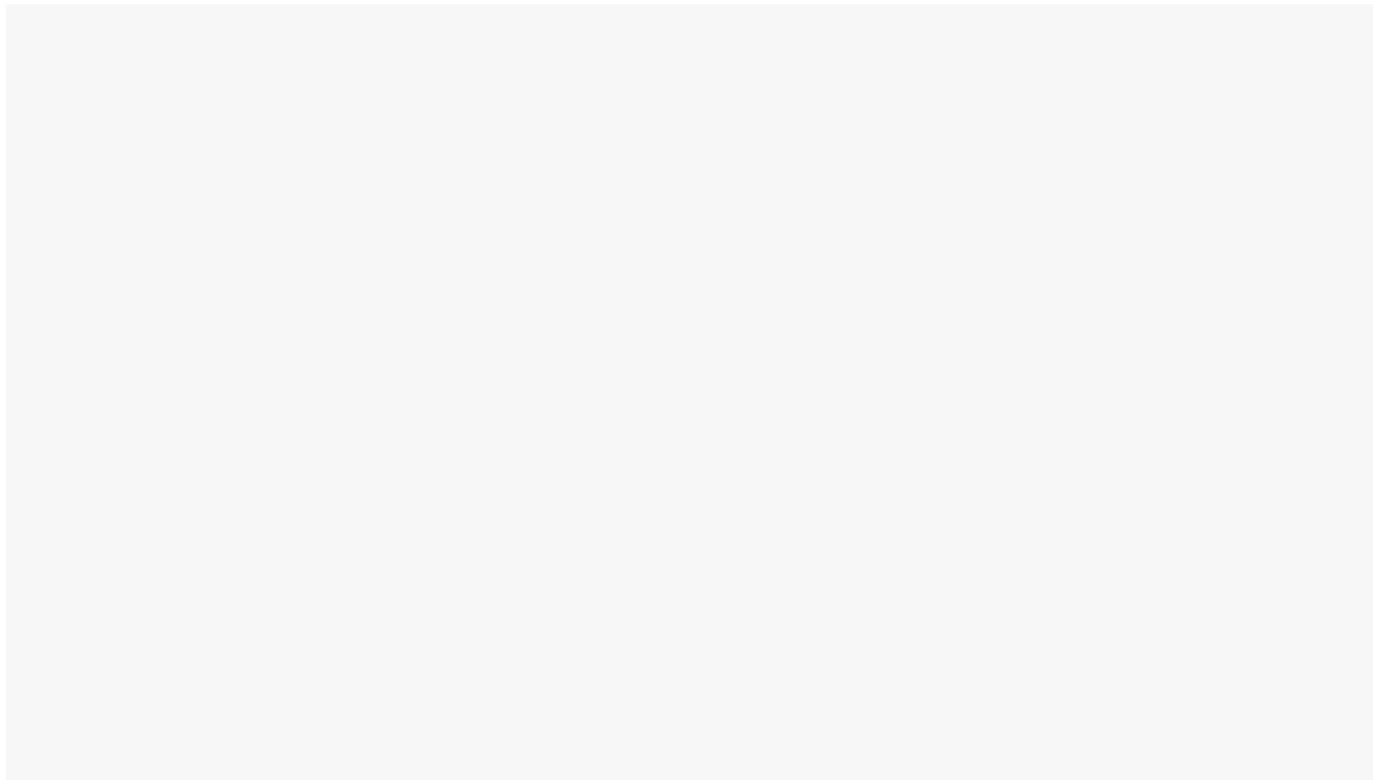
When you begin logging into Google, the site will generate a prompt saying that you have a passkey on another device and provide options for logging in. Depending on which device and browser you're using, this will look different and have different options. Select the device that has your passkey and continue.

If you're authorizing Google Chrome with an Android device, a push notification will appear on your phone.



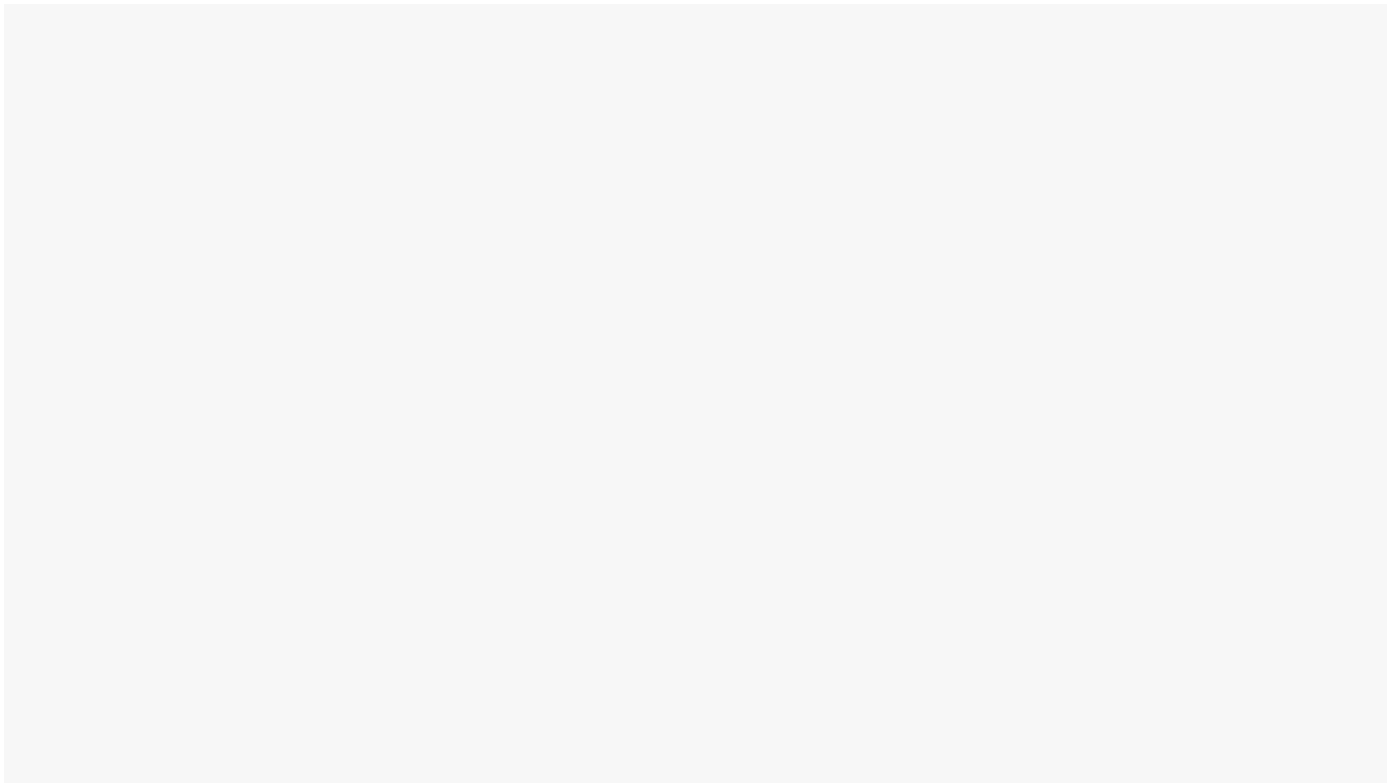
If your Android device has a passkey on it, the Chrome browser can send a push notification asking for authorization
(Credit: Google)

If you're using some other combination of devices, a QR code will appear on the one you're trying to authorize. Scan the code with the device that already has your passkey, and then use whatever means you use to unlock that device.



Scanning the QR code connects the two devices via Bluetooth (Credit: Apple/Google)

Next, you get can create a new passkey on the device you just authorized. Be sure you don't create a passkey on a shared device or one you don't own. If you regret your choice, simply use the Google passkey settings page to de-authorize the device.



A newly authorized device can create its own passkey (Credit: Google)

ADVERTISEMENT

Passkeys Might Just Be the Future

Passkeys may seem strange and intimidating, but after doing the research and testing for this article, I'm pleasantly surprised to find how seamless and smooth the experience is. We're a long way from finally freeing ourselves from the misery of passwords, but passkeys are our best bet to do it.



What Is Two-Factor Authentication?

Like What You're Reading?

Sign up for **SecurityWatch** newsletter for our top privacy and security stories delivered right to your inbox.

Enter your email

 Sign Up

This newsletter may contain advertising, deals, or affiliate links. Subscribing to a newsletter indicates your consent to our [Terms of Use](#) and [Privacy Policy](#). You may unsubscribe from the newsletters at any time.

FURTHER READING

How to Change Password Managers on iPhone

BY EDWARD MENDELSON

How to Master Google Password Manager

BY ERIC GRIFFITH

How to Switch to a New Password Manager

BY KIM KEY

3 Simple Tricks for Strong Passwords

BY NEIL J. RUBENKING



About Max Eddy
Lead Security Analyst



Since my start in 2008, I've covered a wide variety of topics from space missions to fax service reviews. At PCMag, much of my work has been focused on security and privacy services, as well as a video game or two. I also write the occasional security columns, focused on making information security practical for normal people. I helped organize the Ziff Davis Creators Guild union and currently serve as its Unit Chair.

Read Max's full bio

Read the latest from Max Eddy

- [Why You Need a VPN, and How to Choose the Right One](#)
- [How to Set Up and Use a VPN](#)
- [VPN vs. Proxy: What's the Difference?](#)
- [6 Tips to Watch Porn Online Safely](#)
- [How to Set Up a VPN in Windows 11](#)
- [More from Max Eddy](#)

PCMag Newsletters

Our Best Stories in Your Inbox →

Follow PCMag



HONEST, OBJECTIVE, LAB-TESTED REVIEWS

PCMag.com is a leading authority on technology, delivering lab-based, independent reviews of the latest products and services. Our expert industry analysis and practical solutions help you make better buying decisions and get more from technology.

[How We Test](#)[Editorial Principles](#)[Reviews](#)[Best Products](#)[Categories](#)[Brands](#)[Events](#)[Series](#)[Newsletters](#)[Encyclopedia](#)[Sitemap](#)[About PCMag](#)[Careers](#)[Contact Us](#)[Press Center](#)[askmen[®]](#)[EXTREME TECH](#)[IGN[™]](#)[life hacker](#)[Mashable](#)[Offers.com[®]](#)[RetailMeNot](#)[SPEEDTEST[™]](#)

PCMag supports Group Black and its mission to increase greater diversity in media voices and media ownerships.

© 1996-2024 ZIFF DAVIS, LLC., A ZIFF DAVIS COMPANY. ALL RIGHTS RESERVED.

PCMag, PCMag.com and PC Magazine are among the federally registered trademarks of Ziff Davis and may not be used by third parties without explicit permission. The display of third-party trademarks and trade names on this site does not necessarily indicate any affiliation or the endorsement of PCMag. If you click an affiliate link and buy a product or service, we may be paid a fee by that merchant.

