Passkeys: What They Are and Why You Need Them ASAP

We tell you what passkeys are, and where you can use them to log in securely without exposing your email address or creating a password.

By Kim Key Updated June 3, 2024

(Shutterstock/BestForBest)

Table of Contents

I’m sick of passwords. They’re somehow both easily guessable and hard to remember, and keeping them out of the hands of criminals is tough. To solve that problem, the Fast Identity Online (FIDO) Alliance developed passkeys, a form of authentication technology. Passkeys eliminate the need to enter your email address or password into login fields all around the web.

Passkeys have plenty of benefits; for example, they cannot be guessed or shared. Passkeys are resistant to phishing attempts because they're unique to the sites they're created for, so they won't

work on fraudulent lookalike sites. Most importantly, in the age of near-constant data breaches, your passkeys cannot be stolen by hacking into a company's server or database, making the data extracted in such breaches less valuable to criminals.

We are encouraged to see many companies adopting passkeys. But what are they? Should you use them? Are they really more secure than traditional login credentials? Let's talk about it.

What Is a Passkey?

A passkey is a way to log in to apps and websites without using a username and password combination. It's a pair of cryptography keys generated by your device. A public key and a private key combine to create a passkey that unlocks your account.

Apps or websites store your unique public key. Your private key is only stored on your device, and after your device authenticates your identity, the two keys combine to grant you access to your account. We tell you how to put this into practice in our guide for setting up and using passkeys.

Usually, the device or software generating the passkeys uses a biometric authentication tool, such as FaceID or TouchID, to authenticate your identity. If a password manager is the passkey source, you can log in to the app using a strong master password instead of biometric authentication. Passkeys are unique to each app or website and stored in a password manager's vault or your device's keychain. Passkeys can sync across devices, making them a convenient choice.

(Credit: 1Password/PCMag)

Where Can You Use Passkeys?

You can use passkeys to log in to many websites, including Best Buy, eBay, Google, Kayak, and PayPal. Password management company 1Password maintains a community site where users can report websites that accept logins using passkeys. Currently, some of the sites on that list still require a traditional username and password for initial account creation and logins, but you can set up a passkey to use for future logins by visiting the Settings menu.

Swift passkey adoption by major apps and websites is encouraging, but it may take time for passkey adoption for websites owned by individuals or small companies. Some sites don't even support multi-factor authentication yet, so we may have to wait a while for the newest FIDO security standards to completely eradicate passwords.

Are Passkeys Really More Secure Than Passwords?

> "You have passkeys? That's fantastic. But there are things that criminals are going to do that are going to circumvent these kind of protections and we need to talk about how we can overcome that."
>
> Trevor Hilligoss, VP of SpyCloud Labs at SpyCloud

Allowing users to login using a passkey isn't the only update website owners need to ensure website security. Earlier this year, I got a chance to chat about passkey adoption and other cybersecurity trends with Trevor Hilligoss, a security researcher and vice president of SpyCloud Labs at SpyCloud. Hilligoss told me that widespread passkey adoption is "fantastic," but website owners really need to fix some other security holes, too. He noted that criminals can easily get around a passkey by stealing users' validated browser cookies using malware.

"You can use a passkey, you can use a password manager, you can use 'yourdog'sname2023', whatever. It doesn't really matter because authentication has already happened by using that cookie," Hilligoss said.

"Criminals are emulating an already authenticated session. So from the perspective of the website, it just sees that it's a valid cookie."

RECOMMENDED BY OUR EDITORS

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

How to Set Up Passkeys for Your Google Account

Hilligoss went on to explain that once a website, like say, your email service, validates the cookie, the criminal doesn't even need to log in using your credentials or authenticate their identity. The validated cookie, which lasts on a person's browser until it expires over a period of seconds or years, allows criminals to enter your accounts undetected and steal your data or money.

The onus is on website owners to find a solution for cookie hijacking. Hilligoss told me that the rest of us can protect ourselves from the cookie hijacking threat by using passkeys or strong and unique passwords wherever we can. He also said that some websites allow users to choose when their session tokens expire. You know the data privacy pop-up screens? Don't immediately tap "Accept." Instead, navigate to the "Cookies" or "User Data" sections and choose the shortest

available session duration. That way your cookies will expire automatically or whenever you close your browser window.

How Can I Keep Track of My Passkeys?

Many of the password managers I've reviewed for PCMag, such as Editor's Choice award winner Bitwarden, plus 1Password and Dashlane, can store and create passkeys for you. A password manager makes it easy to access both your old credentials and new passkeys when you log in.

If you don't use a password manager, it's not too late to try being more secure with your personal data. Android and iOS users can store their passkeys locally and access them using the keychain app on their mobile devices.

PC MAG

It's Surprisingly Easy to Be More Secure Online

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

FURTHER READING

Cybersecurity Checklist: Follow These Simple Steps to Break Bad Habits

BY KIM KEY

The Best Deal at the End of the Day: Best Price Ever on Samsung Galaxy Tablet A9+

BY JADE CHUNG-LEE

Amazon's Starlink Rival, Project Kuiper, Faces Another Delay

BY MICHAEL KAN

Best Desktop Deal Alienware, Lenovo

BY JADE CHUNG-LEE

About Kim Key

Security Analyst

As a PCMag security analyst, I report on security solutions such as password managers and parental control software, as well as privacy tools such as VPNs. Each week I send out the SecurityWatch newsletter filled with online security news and tips for keeping you and your family safe on the internet.

Before joining PCMag, I wrote about tech and video games for CNN, Fanbyte, Mashable, The New York Times, and TechRadar. I also worked at CNN International, where I did field producing and reporting on sports that are popular with worldwide audiences. Yes, I know the rules of cricket.

Read Kim's full bio

Read the latest from Kim Key

- Cybersecurity Checklist: Follow These Simple Steps to Break Bad Habits
- 10 Tips for Safer Online Shopping
- How to Work From Anywhere: A Primer for Digital Nomads
- How to Protect Your Data Online: Minimize, Monitor, and Manage
- Avoid Online Job Scams With These 7 Simple Tips

- More from Kim Key

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

askmen® EXTREMETECH IGN lifehacker Mashable Offers.com® RetailMeNot SPEEDTEST®

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