7 common misunderstandings about passkeys

PASSWORDLESS TIPS & ADVICE

by Nick Summers on Mar 16, 2023

Share this page

Almost everyone understands w they work. But passkeys? That's a different story.

Here at 1Password, we’re excited about passkeys, which let you create online accounts and securely sign in to them without entering a password.

But we know it’s early days, and the technology hasn’t gone mainstream (yet!)

Many people don’t know what a passkey is, or have heard an explanation that isn’t *quite* right. Here, we’re going to address some of the most common misconceptions so you can better understand how passkeys work, and use them with total confidence.

Misunderstanding: Behind every passkey is a password

Many of us use biometric authentication to unlock our devices and access our favorite online accounts. But in these scenarios, your biometrics don’t *eliminate* your password.

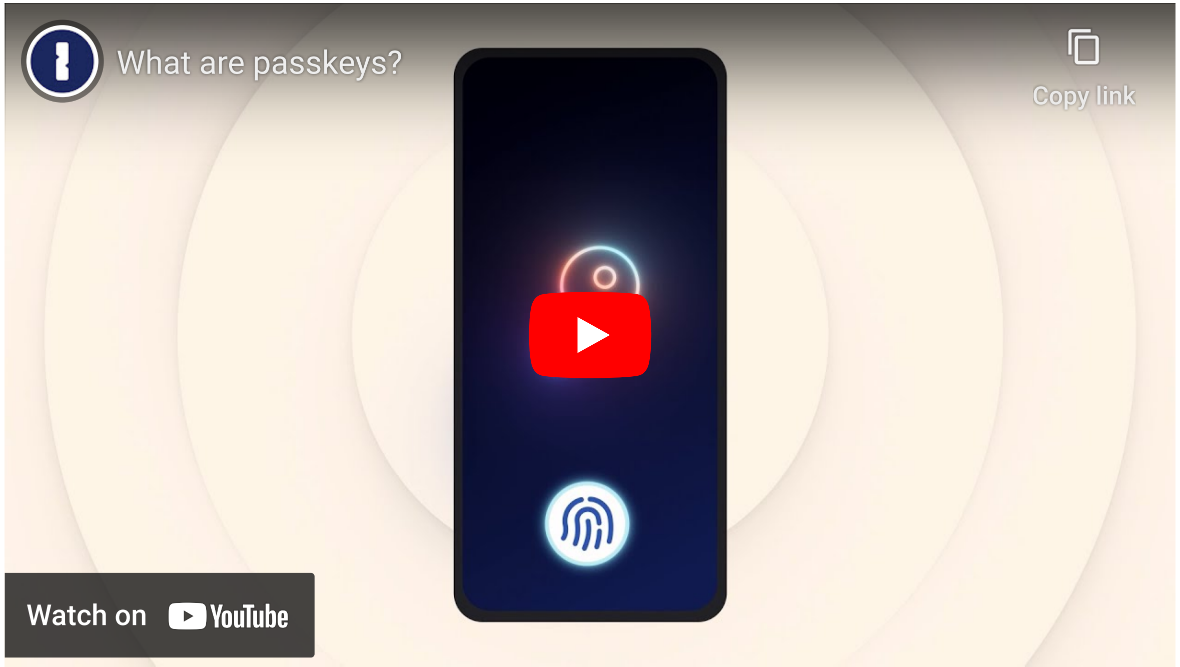
Passkeys, meanwhile, act as a *replacement* for traditional passwords.

Here’s a quick summary of how passkeys work:

Passkeys leverage an API called WebAuthn. Instead of a traditional password, WebAuthn uses public and private keys – otherwise known as public-key cryptography – to check that you are who you say you are. The advantage of this approach is that you never have to share your private key (hence the name), and the public key is useless to an attacker on its own.

Learn more about how passkeys work!

If there was a password behind every passkey, it would still be possible to “phish” the account owner. Passkeys are resistant to phishing because there’s no plaintext password or ‘secret’ that the user can be tricked into sharing, or that an attacker can try to intercept. This makes passkeys a more secure option than a traditional password.



At first, websites and apps will likely offer passkeys **alongside** traditional password authentication. That way you'll have a choice, and can use both methods in tandem if you wish.

Misunderstanding: You need Bluetooth to log in to an account with a passkey

Some articles have implied that a Bluetooth connection is required to successfully authenticate and sign in to accounts using passkeys.

That's simply not true.

When you create a passkey, the website will ask you to confirm your authenticator. This could be your phone, tablet, PC … or, in the not so distant future, 1Password. The next time you want to sign in, your device will ask you to authenticate using your face or fingerprint as a security measure, but that's it.

Bluetooth only plays a role if you create a passkey using one of the solutions offered by Apple, Microsoft, or Google, and then need to access that same passkey **from a device that sits in a different company's ecosystem.**

For example, let's say you create an online account with a passkey using Google's password manager on your Android phone. And then you want to access that same account on your Windows PC.

In this scenario, you’ll normally be prompted to authenticate using your Android phone.

Bluetooth is required to check that your Windows PC and Android phone are physically close to each other. (This is to prevent phishing.) But passkeys don’t rely on Bluetooth’s security properties to secure the actual sign-in process.

That’s why if you’re using the same device, or a solution that syncs your passkeys between devices, you don’t need a bluetooth connection.

> Remember: passkey support is coming to 1Password! This will let you sync your passkeys across all of your devices – no Bluetooth required!

Misunderstanding: You only need a single passkey to access all your online accounts

A single passkey isn’t a master key that can unlock *all* of your online accounts. You’ll still need to create a passkey for each online account.

That might sound a little tedious, but in practice passkeys are incredibly convenient to create, store, and use. That’s because:

- **You don’t have to create anything manually.** Your authenticator will generate a passkey – which contains a public and private key pair – on your behalf.

- **Every passkey is strong by default.** So you don’t have to worry about whether your private key is long or random enough.

- **You don’t have to remember or type out your passkeys.** Your private key is stored on your device, and retrieved automatically when you want to sign in to your account. A copy of your public key is stored with the account provider so you never have to type it out. Instead, your passkey is processed seamlessly in the background when you select ‘Sign in’.

Misunderstanding: If someone steals your phone, they can instantly access your passkeys

Your phone is a safe place to store your passkeys. For starters, most hackers won’t travel to wherever you are because pickpocketing is neither cheap nor time effective. Instead, attackers will likely try other tactics that don’t require them to leave their computer.

If someone *did* manage to steal your phone, it would still be difficult for them to find and exploit your passkeys. That's because they would need to unlock your device first. If you've secured your phone with biometrics, or an alternative method that's difficult to guess – like a strong and unique password – an attacker will have a hard time breaking in and accessing your passkeys.

> **Your passkeys are well protected, even if a hacker managed to steal your phone.**

Your confidential passkey data (e.g. the private half of every key pair) is also stored in a Trusted Platform Module (TPM) that is virtually impenetrable.

The bottom line is that you can rest easy knowing that your passkeys are well protected, even if a hacker managed to steal your phone.

Misunderstanding: You can't sign in to your accounts if you don't have the device that contains your passkeys

What happens if you arrive at work and realize you've forgotten the phone that has all your passkeys? Will you be locked out of all your online accounts? Not necessarily.

Google, Apple, and Microsoft will sync your passkeys across devices using their respective cloud-based storage services. So if you create a passkey using an iPhone, you can access the same passkey on your other Apple devices via iCloud.

Okay, but what happens if you've forgotten your iPhone, but need to use a Windows PC in a public library? In this scenario, you should be given a second option to sign in. For example, a website might send you a "magic link" — a one-time link that lets you instantly sign in — to your chosen email address.

Passkey support is also coming to 1Password! (Sign up to our passwordless newsletter for updates!) This will let you access your passkeys on all your devices, regardless of which operating system they run, and any major web browser. That way, there's no need to worry if you leave your phone at home one day.

Misunderstanding: You'll lose access to your accounts if you lose the device that contains your passkeys

It's natural to worry about what would happen if you broke your phone. Or what would happen if you left your laptop in a public place, like a cafe, and went back only to discover it had vanished.

As we've already covered, it's possible to sync your passkeys between devices. Apple, Google, and Microsoft will offer to sync your passkeys within their respective ecosystems. And, later this year, you'll be able to use 1Password to create, store, and seamlessly sync passkeys.

> **The simpler and less stressful option is to sync your passkeys between devices.**

If you don’t opt in to syncing *and* lose the device that contains your passkeys … your passkeys will be lost. But don’t worry! You’ll still have other options to access your accounts, like magic links. Once you’ve successfully signed in, the site or app should then give you the option to create a new passkey.

The simpler and less stressful option is to sync your passkeys between devices. With 1Password, you’ll soon be able to create, save, and access passkeys on any piece of hardware, alongside your passwords, credit cards, and other digital secrets.

Misunderstanding: Your passkeys are vulnerable if your biometrics are compromised

Unlike a password, you can’t change your face or fingerprint. (Not easily, anyway!) With this in mind, you might be worried about the possibility of someone stealing your biometric data, and then using that to wreak havoc with your passkeys.

Researchers have proven that *some* Android phones can be fooled by a high-quality photo of the device’s owner. This has led to more Android devices with depth-sensing cameras and 3D mapping technology similar to the iPhone.

Depth mapping allows your device to turn a photo of your face into a mathematical representation that's only ever stored locally, and never transmitted over the internet. For example, your Apple device stores biometric data encrypted with a key made available only to the Secure Enclave — a component built specifically to safeguard and process sensitive data.

> **An attacker would need physical access to your device *and* a flawless representation of your face or fingerprint.**

Apps that offer biometric authentication never have direct access to that data. Instead, a request is sent to the Secure Enclave. It verifies your identity by ensuring the stored mathematical representation of your face matches the one currently being presented.

So, what does all this mean?

A theoretical attacker needs physical access to your device **and** a flawless representation of your face or fingerprint. Obtaining both is incredibly difficult.

The chances of someone breaking into the Secure Enclave area also extremely slim. And even if they did, they wouldn't find a picture of your actual face.

Passkeys: An exciting future

The bottom line is that passkeys are safe and convenient for the vast majority of people. That’s why we’re so excited about this new kind of login credential, and are working hard to make passkeys simple enough for everyone to use in their daily lives.

Of course, 1Password will continue to protect your traditional passwords. But we look forward to helping you create, store, and sync passkeys too, so you can live an even simpler, more secure life online.

Subscribe to our passwordless newsletter

Read the latest passkey announcements by 1Password, as well as helpful guides, explainers, and community chatter about passwordless authentication.

Subscribe to Beyond Passwords

Nick Summers
Content Marketing Manager

Tweet about this post

Continue Reading

What are passkeys and how do they work?

TIPS & ADVICE PASSWORDLESS

by Nick Summers Nov 7, 2022

Passkeys and the future of authentication: Q&A with Andrew Shikiar, CMO of FIDO Alliance

PASSWORDLESS PODCAST

by Stacey Harris Mar 1, 2023

Families
Teams
Business
Small Business
Enterprise
Integrations
Watchtower
Developers

Password Generator
Username Generator
Security
Privacy
Customers
Password Manager
Resources
Webinars
1Password University
Secrets Management

Forum
Contact Us
Locations
Europe
Canada
United States

Partnerships
Affiliate
Press
Gift Cards
We’re Hiring!
Podcast
Newsletter
Legal Center
Passage by 1Password

iOS
Windows
Android
Linux
Web Browser
Command Line
Browser extensions

Terms of Service - Privacy Policy - Cookie Policy - Accessibility
4711 Yonge St, 10th Floor, Toronto, Ontario, M2N 6K8, Canada. 🇨🇦

Find us on