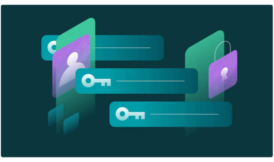
Passkeys Explained: What Is a Passkey and How Do Passkeys Work?

February 28, 2024 | Dashlane



**First published Nov. 11, 2022*

Passwordless authentication is becoming more mainstream as more people and platforms recognize how it improves security over traditional passwords. Big-name players like Microsoft, Google, and Apple are among those leading the charge. Bringing them all together is the FIDO (Fast IDentity Online) Alliance, an organization that works on passwordless technology and establishes standards for organizations to follow.

Digital Shadows researchers have found 6.7 billion unique logins—combinations of usernames and passwords—on the dark web. This treasure trove of logins puts a lot of consumers at risk, especially considering how many people reuse their passwords. When your passwords end up on the dark web, cybercriminals can use them to get into your accounts and steal your private data. That's why passkey-based authentication is becoming a fast-growing trend.

What is a passkey?

As simple as they are to use, passkeys can be difficult to understand. That's why we're breaking it down into varying concepts and levels, so you can leave this blog post knowing what a passkey is and how it's different from a password.

Explain it like I'm 5

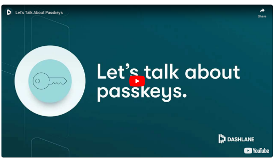
Passwords are a common way to log in to accounts, but if they get stolen (which they often do), anyone can use them to gain access. Passkeys are a way to log in without a password. They use your phone or another supported device to prove that you are who you say you are before letting you into your account. A lot of security happens behind the scenes, but the main benefit of passkeys is that they can't be stolen like passwords. Plus, there's nothing to remember, so you'll never forget them!

Explain it a bit more thoroughly

A passkey is a passwordless login, which is a password replacement that's more secure and easier to use. Passkeys are better than passwords because passkeys can't be phished or stolen. They're easy to set up and use, and you don't need to memorize them. Instead of having to create a password for your account, you enable an "authenticator" to generate a passkey. The authenticator can be your smartphone, another device, or a password manager that supports passkeys.

The authenticator still requires some form of user verification. This could be through entering a password or PIN or using biometrics (such as Face ID or Touch ID), which adds both security and convenience.

Your passkeys are stored securely in a vault, such as your device's keychain or your password manager. Since passkeys can sync across devices, they're seamless and convenient to use, and the overall user experience with passkeys is an improvement over passwords.



Explain the technical stuff

There are several reasons why passkeys are better than passwords. Passwords are a shared secret: The value is sent over the network to the server to be evaluated, meaning the server needs to store information about the password that could be valuable to an attacker. Passkeys, on the other hand, are based on public key cryptography, which ensures that the secret element of the credential isn't shared with the website and that no secrets are transferred between the user's device and the server.

In order for passkeys to work, an authenticator, such as a mobile device or password manager that supports passkeys, generates two cryptographic keys for each account you create. One key is public and stored on the site where you create the account, and the other is private and stored in your authenticator. When you sign in to your passkey-enabled account, your authenticator and the website communicate to authenticate your login without exchanging any actual secrets that a hacker could exploit.

Passkeys are created using the WebAuthn API that's widely implemented in all modern browsers and operating systems. Most of the complexity is hidden in the software. The user only needs to approve the creation or use of the passkey. User approval can take the form of an on-device biometric check using a fingerprint sensor or facial recognition or a local device password or PIN.

Passkeys can be either device-bound or synced between devices. Device-bound passkeys are typically ones that are created on a hardware key, such as a YubiKey or a Titan Security Key, while synced passkeys are typically managed by a password manager—either one that's built into your device's operating system or a standalone password manager such as Dashlane. Synced passkeys have the advantage of being available on any of your devices where the password manager is available.

> "Adopting passkeys was a no-brainer for us. It simplifies sign-ins, replaces the guesswork of traditional authentication methods with a reliable standard, and helps our users ditch the downsides of passwords. Simply put, it's a big win for both us and our users."
>
> **—Rew Islam, Director of Product Engineering and Innovation at Dashlane, on the Android Developers blog**

How are passkeys better than passwords?

One of the biggest benefits to the user is also one of the simplest: Passkeys, unlike passwords, don't need to be remembered each time you want to access your account (which can lead to password fatigue). Sure, password managers have removed some of that mental load, but creating, storing, and inputting passwords still takes some level of effort—and opens the door for potential vulnerability. With passkeys, logging in is basically effortless, and it's also much more secure.

The extra security comes in the form of phishing-resistance. To understand why, let's look at how a phishing attack works. During a phishing attack, the attacker sends the victim a message that prompts them to visit a website with the hope that they will enter their login information. The website the user will be prompted to visit isn't legitimate, but it will likely appear legitimate to the user. Users who try to sign in to the phishing site will give away their username and password, allowing the attacker to access their account.

This simply can't happen with passkeys. Passkeys eliminate the need for users to enter their passwords, and they can't be used on malicious websites because they're technically bound to the original website for which they were created. Even if a user visits a phishing site, their passkey won't be prompted and won't try to sign the user in. Therefore, the attacker can't steal their passkey like they can steal their password. Similar to passwords, certain 2-factor authentication (2FA) credentials are also vulnerable to phishing attacks, which means even a password with a 2FA credential isn't as secure as a passkey.

While no authentication method is completely foolproof, passkeys are better all around: They're easy to use, phishing-resistant, and can't be guessed or forgotten.

Will passkeys replace passwords?

In short, yes—eventually. Passkeys are simply a better option, and we've already seen more widespread adoption and advancements in the last six months.

The FIDO Alliance has been working on passwordless authentication standards for some time. The most important development, however, came somewhat recently when the technology consortium announced it had proposed a method to store cryptographic keys so they can sync between devices. (In fact, FIDO calls passkeys multi-device FIDO credentials.) This paves the way for the wider adoption of passkeys that we're already beginning to see.

How does Dashlane make it easier to manage passkeys?

Third-party passkey providers like Dashlane make it possible to use your passkeys to access services from across different devices. This offers flexibility and convenience because you aren't locked into a specific platform like Apple or Microsoft. You can keep your passkeys in Dashlane and sign in to services on any device using the Dashlane extension or app.

It's possible to use passkeys without a third-party passkey provider, but it's not nearly as streamlined or accessible. For example, if you save a passkey for ebay.com natively on your Windows computer, you can't use that passkey to sign in to ebay.com on your iPhone. Or, if you save your passkeys on a Windows computer and then lose that device, you can't retrieve your passkeys or gain access to the services that used them. Saving your passkeys in Dashlane ensures easy access and use from anywhere across all your devices and platforms.

How do I start using passkeys?

If you're sold on the security and convenience of passkeys and want to try it out for yourself, a growing number of websites support passkey use. We've also curated a few of our favorites below that exemplify great implementation and popular usage.

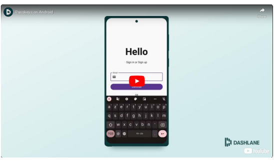
1. Google
2. GitHub
3. Uber
4. Kayak
5. Amazon

Dashlane makes it easy to create and store your passkeys for the above sites and more—if you've got the Dashlane extension, just start the passkey login process on any of those sites, and Dashlane will do the rest! Check out our videos below to see how simple it is to use passkeys on your web and mobile devices.

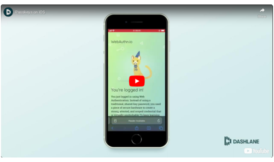
Create a passkey using the extension

0:00

Create a passkey on Android



Create a passkey on iOS



As you start to create and use more passkeys across websites, you'll find that you need passwords less and less. But don't worry—even if you create a passkey for a site you already have a password for, Dashlane will keep both safe in your vault. You can still use your password to log in wherever you need to.

Dashlane was the first password manager to offer an in-browser passkey solution that allows users to automatically log in across websites without a password. And thanks to our patented zero-knowledge architecture, you benefit from yet another security layer because no one except you can access your logins (not even us).

Passkeys are a simpler and more secure way to log in. Learn more about how passkeys work and how Dashlane streamlines access.

FIDO | FIDO ALLIANCE | PASSKEY | PASSKEYS | PASSWORDLESS | PASSWORDLESS AUTHENTICATION

SHARE

Dashlane

Dashlane is a web and mobile app that simplifies password management for people and businesses. We empower organizations to protect company and employee data, while helping everyone easily log in to the accounts they need—anytime, anywhere.

READ MORE

YOU MAY ALSO LIKE

Benefits of Artificial Intelligence in Cybersecurity
High data capacity, learning capabilities, impressive threat detection, and an improved UX make AI in cybersecurity a valuable asset.
READ MORE

Why Security Teams Are Important
Security teams are essential for keeping organizations protected from cyberattacks. Learn what to consider when building your own.
READ MORE

Passkeys are Here: 3 Authenticate 2023 Takeaways
As a board member of the FIDO Alliance, Dashlane attended the Authenticate 2023 conference on passkeys and passwordless authentication.
READ MORE