The Answer

Advice, staff picks, mythbusting, and more. Let us help you.

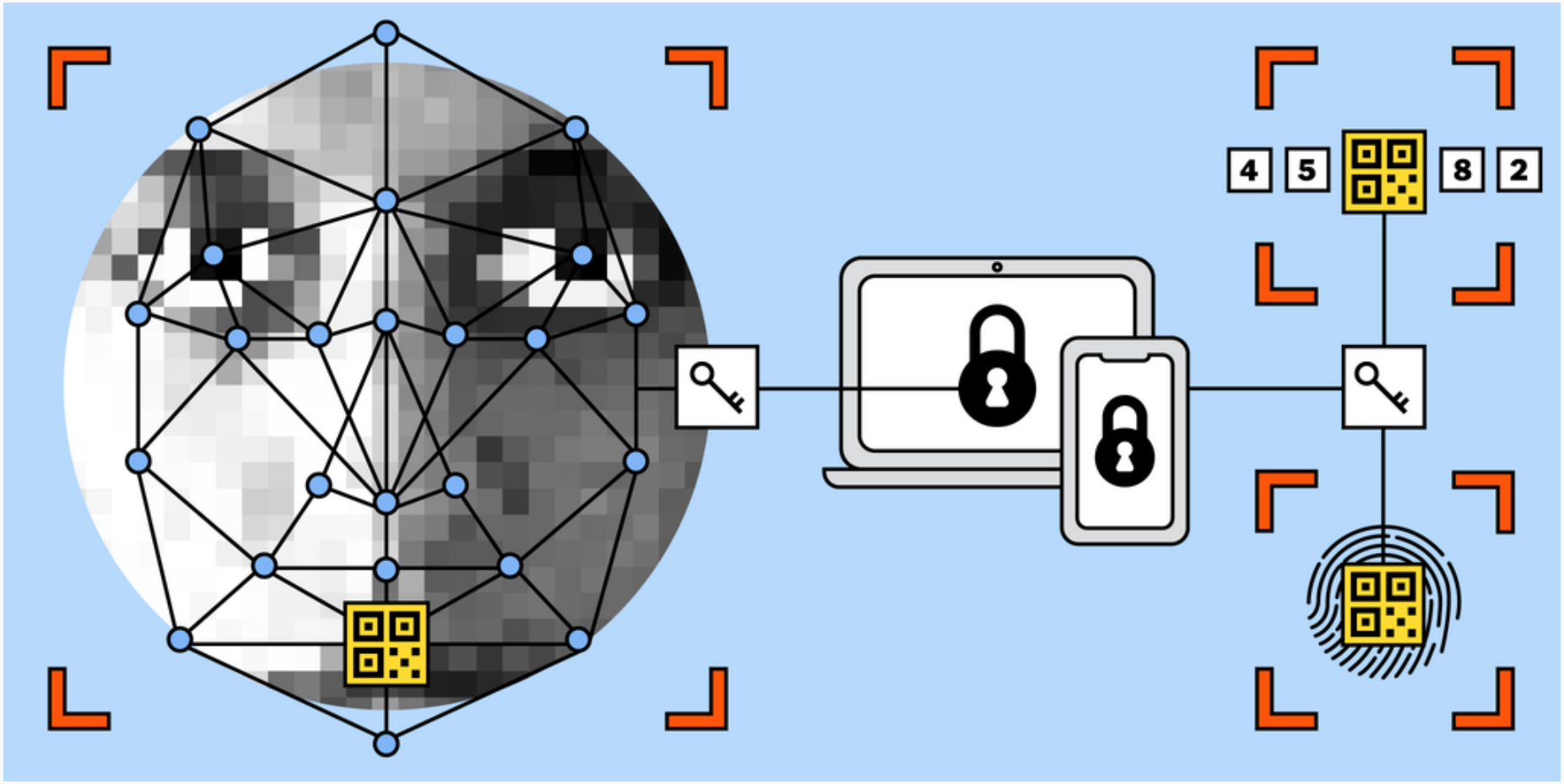

Illustration: Dana Davis

RIP, Passwords. Here's What's Coming Next.

PUBLISHED JANUARY 11, 2023

Thorin Klosowski

Save

Sign up for Wirecutter's newsletters to get independent reviews, expert advice, and the very best deals sent straight to your inbox.

Thinking of new passwords and then keeping them organized and secure is a pain, even with a password manager. But Apple, Google, and Microsoft are working together to support a new way for people to log in to accounts without using passwords at all. Their solution is called a passkey, and though this new sign-in method isn't yet widespread, it is now rolling out—and it promises to make creating new accounts online and logging in to them securely a lot easier. Here's what you need to know.

What is a passkey?

The system for using a passkey in the real world is very much a work in progress, but the goal is for you to be able to log in to every account the same way you unlock your phone, with biometrics or a PIN. It might be best to think of a passkey as a

“password 2.0”—a passkey is functionally the same as the username-and-password combination you’re used to, just without, well, an actual password. Instead, each account you have is linked to a key on a device, such as an iPhone or Android phone.

On a technical level, your device uses what’s known as asymmetric cryptography (or public key cryptography) to register a public “key,” which is then stored on a website for which you have an account alongside a private key that’s stored only on your device; your device creates a new private key for each site you register. When you log in to the website, it checks with your device to see if the two keys match. To grant the website access to that key, you have to authenticate with whatever means you use to unlock your device, such as a fingerprint, your face, or a PIN. If you’re logging in on a device other than the one you used to create the passkey—say, you’re logging in on a Windows laptop for an account whose passkey you created on your iPhone—the device where you created the passkey needs to be physically near the device you’re using to log in, something that the system checks through the scanning of a QR code and the use of Bluetooth Low Energy.

All of this sounds complicated, but the end goal is for the experience of logging in with a passkey to be easier than doing so with a username and password, and for it to work almost like shopping using a credit card, “where the experience is more or

less the same everywhere you go," said Derek Hanson, Yubico's vice president of solutions architecture and alliances.

Passkeys are based on standards developed by the major tech companies. Apple, Google, and Microsoft, along with other tech giants, are working with the FIDO Alliance on passkeys, which are based on what's known as the WebAuthn standard. You don't need to remember any of that in order to use passkeys. What's important is that passkeys should work more or less the same across platforms and will be supported for years to come. "Standards equal security," said Alex Weinert, Microsoft's director of identity security. He added that the scrutiny that the standards provide also makes the company more confident about passkeys' widespread adoption.

Why is a passkey more secure than a username and password?

Passkeys solve two of the biggest problems with passwords: data breaches and phishing. Passkeys aren't reused across sites like passwords often are, so stolen credentials do less damage. And since one side of the key is linked to the web-based service itself, it can protect against phishing attempts, because your device should recognize a phishing website as a fake. Passkeys aren't perfect, but they are expected to be an improvement over the status quo.

“There’s no password attacks when there’s no password present,” Microsoft’s Weinert said. “I’m hugely hopeful about the ability for this to get us to a new era in terms of end-user security.”

In the long run, passkeys will be easier and safer for website operators, too, as they will no longer need to store passwords, which means they won’t need to worry about password-database breaches (though they’ll still need to secure the rest of the data they collect).

A username-and-password combo isn’t the only type of login you can use to access websites and apps, of course: Apple, Google, and other tech companies let you use your credentials for their respective services to sign in on websites across the internet. Yubico’s Hanson noted that from a security perspective, “Sign in with Apple” or “Sign in with Google” offers roughly the same security as passkeys stored by Apple, Google, or Microsoft.

How to set up passkeys

For passkeys to be a login option, they need to be both offered by the website you want to log in to and supported by the operating system, browser, or password manager you use. As of late 2022, 1Password’s tracker listed about two dozen sites that support passkeys, but the experts we spoke with all had hopes for continued adoption over the next year. That seems

increasingly likely, too, as Shopify, a popular web-store backend for independent shops, in December 2022 announced a new plugin for shop owners to implement passkey support easily.

Here is how the setup process works on a website when you're using a supported device and web browser:

1. Enter your email address.
2. An option to create a passkey appears. If the device you're on has a PIN or a biometric login (as on an iPhone or Android device), you get the option to set up a passkey there. If the device you're on doesn't have a PIN or biometric option, you can either use a password or "save on another device." For example, if you're using a Windows PC but want to save a passkey to your Android phone, on the PC you'll see a QR code that you can scan with your phone.
3. Your account is created, and in the future you'll need the device you created the passkey on to log in to that account.

It sounds simple enough, but in my experience, I've found that the process can be confusing. When I attempted to test it by creating a Kayak account, I repeatedly got stuck waiting for a verification email that never showed up. Eventually, I managed to log in, and the passkey worked seamlessly on an iPhone. But when I tried to create a passkey on my Mac, I was locked in a loop where the site repeatedly asked me to enter my email address; I soon realized that I had to select the option to scan a

QR code with my phone because my Mac mini doesn't have Face ID or Touch ID, and I needed to authenticate on a device that does. At no point in the login process was that made clear.

Other sites, like that of Best Buy, take a different approach. Unlike Kayak, Best Buy's site requires that you create an account with a standard username and password first, after which you can add a passkey for logging in. Although this arrangement doesn't protect against data breaches, it can help to protect against phishing, and unlike my experience with Kayak, this process worked consistently for me on Best Buy's site. Several experts we spoke to suggested that having a password backup will frequently be the case as passkeys gain adoption.

What happens if you lose your phone or laptop?

Within a device family, passkeys are synced to whatever cloud storage method your device uses, such as iCloud Keychain on Mac and iPhone or Google Password Manager on Android and ChromeOS, so if you lose your device, they should be stored there, and you should be able to restore your passkeys to a new device. Because passkeys are end-to-end encrypted, companies like Apple or Google cannot access them.

If you need a higher level of security on certain accounts, using a physical security key, which doesn't sync online, may be a

better option than using your mobile device.

What happens if you want to switch between devices?

If you create a passkey on an iPhone, for example, and then want to use that passkey on another device, such as a Windows laptop, on the second device's screen you'll see a prompt to scan a QR code, which you can do with your iPhone; once you then approve the login, you'll be on your way. This approach is called multi-device authentication.

However, if you're permanently switching, such as migrating from an iPhone to an Android phone, the process is currently unclear. At the moment you have no way to transfer passkeys from one platform to another, but it is a problem that companies are working on. Mark Risher, Google's product management director overseeing Android, said that Google is working with the FIDO Alliance to design ways to transfer credentials between platforms: "With regards to transfers in particular, it's a top priority for us, so we're exploring a few options that allow portability but don't open a new channel for attackers to grab 'the keys to the kingdom.'"

What if you want to share a passkey with someone?

On iOS, you can share a passkey over AirDrop. If, say, Netflix suddenly switched over to passkeys, you still would be able to share your account with family members as long as they're also iPhone owners. Google didn't respond to our request with any information about how it might handle this issue for Android users.

Will passkeys replace password managers?

Passkeys aren't necessarily replacements for password managers. It will be a long time before every website supports passkeys, so you'll still need traditional passwords for years to come. But both 1Password and Dashlane have announced passkey support, and other password managers are likely to follow. 1Password's plans seem comprehensive, as the company is not only allowing you to store passkeys within its password manager, which lets you easily access them across different devices and share them with family, but is also working on tools for you to export your passkeys to other password managers if you leave the 1Password service. Implemented well, password managers could provide better passkey portability between ecosystems than the operating-system-level options do.

Does this mean law enforcement could more easily access your passwords?

Passkeys provide excellent protection against online attacks on the services you use, but the situation is complicated if you're more concerned about law enforcement gaining physical access to your device.

Your device's password or PIN is (or should be) stored in your brain. In the US, the Fifth Amendment, which gives people the right not to be witnesses against themselves, is often invoked when law enforcement attempts to get a suspect to unlock a device. Using your face or fingerprint to unlock a device may not always fall under Fifth Amendment protections, and Electronic Frontier Foundation attorney Andrew Crocker said that, so far, "courts have given more Fifth Amendment protection to the use of a passcode to unlock the device." Passkeys could be similarly protected, Crocker added.

Crocker also pointed out that although a warrant grants access to the contents of a phone, it should not mean that law enforcement is entitled to search the contents of a website account just because the passkey for that site is stored on the phone. For example, a warrant to search your phone does not give police authorization to search your Facebook account just because you have the Facebook app installed on your phone. But because of how passkeys work, this situation can still be problematic. Since you're using the same form of authorization for both your phone and each service, if law enforcement agents gain access to your device, it could give them access to the

associated services, as well, even if they do not have legal authorization for such access.

The EFF recommends using a PIN instead of biometric unlocks for your device if you're concerned about potential law enforcement access. Since passkeys also support a PIN, they should have the same protections. Storing your passkeys on a physical security key could be another solution, since you can always leave that security key at home.

When can you start using passkeys to log in to your accounts?

Passkeys aren't available on many sites, and platforms are still rolling out support. Here's how and where you can use passkeys right now:

- **Passkeys created on Android (in beta):** Can be used on that Android device and other Android devices synced to the same Google account, as well as on Macs, Windows PCs (in Edge or Chrome), and iPhones using cross-device authentication (scanning the QR code).

- **Passkeys created in Google Chrome:** Can be used on Windows 11, Mac, Android, and iOS (Chromebooks and Windows 10 are not currently supported). They sync through the operating system, namely through Google Password Manager on Android and Keychain on iOS and Mac. Currently Windows doesn't support sync.

- **Passkeys created on iPhone or iPad:** Can be used on that iOS device and other Apple devices logged in with the same Apple ID, as well as on Windows (in Edge or Chrome), ChromeOS, or Ubuntu devices using cross-device authentication (scanning the QR code).
- **Passkeys created on Windows:** Can be used only on the same Windows device that created them.
- **Passkeys created on macOS:** Can be used on other Macs or iOS devices logged in with the same Apple ID.
- **Passkeys saved to security keys:** Can be used on iOS, macOS, Windows, and Ubuntu.

1Password has a list of sites, alongside those of Best Buy and Kayak, that have added passkey support. If you want to check out how passkeys work without messing around with a real login, head to this demo site created by the security company Hanko.

Passkeys will take a while to become ubiquitous, but experts predict that they are the future. The login process will standardize over time, and passkeys are expected to be implemented more seamlessly over the next year or so. When they work correctly, it feels a little like magic: The login process is smooth and fast, and account creation is less cumbersome than it is with usernames and passwords. There's no real downside to trying out a passkey login when you come across

one, and if you're willing to put up with a little troubleshooting, you'll be on the edge of what feels like an inevitable change.

This article was edited by Caitlin McGarry and Signe Brewster.

Further reading

The Best In-Wall Smart Light Switch and Dimmer

A smart dimmer works like a regular switch but makes it easy to put lights on a schedule, automate them with other devices, and control them remotely.

The Gadgets We Bring on Every Trip

You don't have to be a digital nomad to travel like one. Here are a few gadgets and accessories to make travel as painless as possible.

Urban Gardening Starter Kit

These are the tools and supplies you need to start a container garden in a small area.

The Best Password Managers

Everyone should use a password manager, and after researching dozens and testing six, we recommend **1Password** because it's secure and easy to use.

The New York Times
Wirecutter

Wirecutter is the product recommendation service from The New York Times. Our journalists combine independent research with (occasionally) over-the-top testing so you can make quick and confident buying decisions. Whether it's finding great products or discovering helpful advice, we'll help you get it right (the first time).

Deals
Lists
Blog
Newsletters
Make a Donation

About Wirecutter
Our team
Staff demographics
Jobs at Wirecutter
Contact Us
How to pitch

Privacy Policy
Terms of Use
Cookie Policy
Partnerships & Advertising
Licensing & Reprints
RSS