BY MATT BURGESS SECURITY FEB 8, 2024 7:00 AM

I Stopped Using Passwords. It's Great—and a Total Mess

Passkeys are here to replace passwords. When they work, it's a seamless vision of the future. But don't ditch your old logins just yet.

ANIMATION: JACQUI VANLIEW; GETTY IMAGES

For two years, my Netflix password has been: tricke22ry-notiLonal-freely-soSak-lice-slacken. Yes, really. It is a strong, unique password, and it ticked

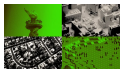
boxes for reducing the chances of me getting hacked. But for all its security protections, the password was a nightmare to type into an onscreen TV keyboard, and it constantly annoyed members of my family who shared my Netflix login. It's just the tip of my password suffering, though.

I use a password manager to generate and store all the login details for the 337 accounts I've made—from pizza delivery and airlines to social media and online shopping—over more than a decade online. However, using a password manager compulsively and having hundreds of strong passwords likely puts me in the minority: Many people use the same password across multiple accounts or use passwords that can easily be guessed.

The way we use passwords has been broken for a long time, but that's finally changing. Over the past year, it has become possible to ditch the password and move to passkeys instead. Passkeys are generated codes—created using public key cryptography—that are stored on your device or in your password manager and let you log in to websites and apps using your fingerprint, face recognition, or a PIN. They can't be guessed, leaked, or stolen, and they stop phishing attacks in their tracks, according to those behind the technology. Passkeys are widely considered to be more secure than passwords.

FEATURED VIDEO

MOST POPULAR



BACKCHANNEL

***SimCity* Isn't a Model of Reality. It's a Libertarian Toy Land**

BY KELLY CLANCY

GEAR

The Best Instant Coffees to Convince Your Friends Coffee Crystals Can Be...

BY JAINA GREY

POLITICS

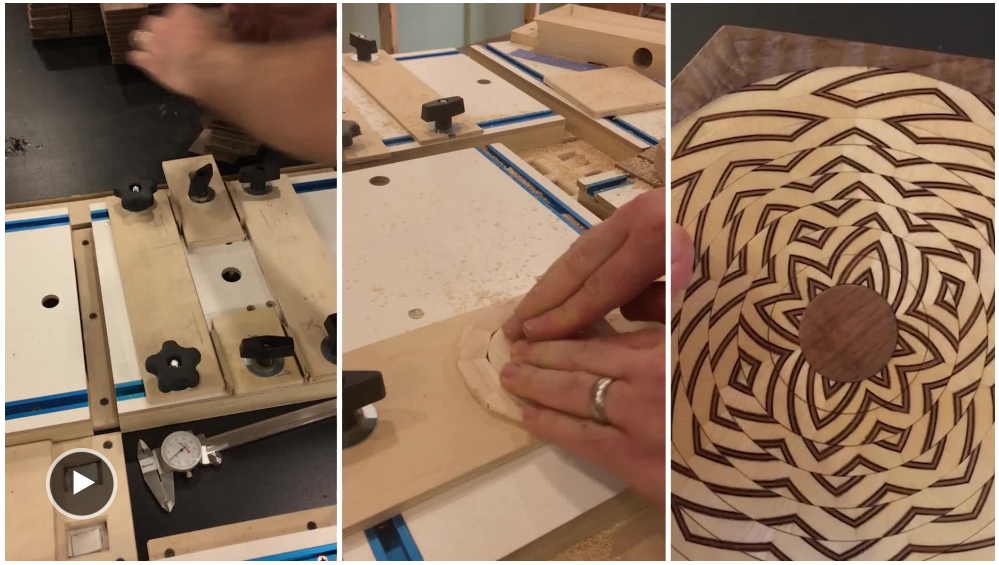
Trump–Biden Debate Conspiracies Have Already Flooded the...

BY DAVID GILBERT

GEAR

I Wore Meta Ray-Bans in Montreal to Test Their AI Translation Skills. It Did...

BY KATE KNIBBS



Google, Apple, Microsoft, Amazon, GitHub, PayPal, the UK's National Health Service, OnlyFans, Nintendo, and more than 100 websites have started supporting passkeys. More than 8 billion online accounts can set up passkeys right now, says Andrew Shikiar, the chief executive of the FIDO Alliance, an industry body that has developed the passkey over the past decade. So, I decided to kill my passwords.

For the past month, I've been converting as many of my accounts as possible—around a dozen for now—to use passkeys and start the move away from the password for good. Spoiler: When passkeys work seamlessly, it's a glimpse of a more secure future for millions, if not billions, of people, and a reinvention of how we sign in to websites and services. But getting there for every account across the internet is still likely to prove a minefield and take some time.

Unlocking Passkeys

Put very simply, when you create a passkey, the website or app you're using generates two pieces of code. One is stored by the website or app; the other is saved on your device. When you log in, you prove it is you via a face scan,

fingerprint, PIN, or however you'd usually unlock your device, and the two pieces of saved code communicate with each other. That means that creating a passkey as a user is relatively simple. All you have to do is visit your account's security settings and go through the options to set up and save a passkey. In most cases, that's just a few clicks.

Logging in to my Coinbase account is the perfect example of how passkeys can work. To sign in to the cryptocurrency trading app—which I largely had forgotten I had an account with—it now just takes seconds. Opening the iPhone app, I can tap on the option to sign in with a passkey, which sits alongside the choice to enter my email address or sign in with an existing Apple or Google account. I tap the passkey option, and a popup appears to ask whether I want to "Use Face ID to Sign in?" and says it will use the passkey saved in my iCloud keychain. A quick face scan later, and I am logged in. No password, no username—under 20 seconds to sign in.

However, there are a few things that caused me problems setting up passkeys—my first attempt was disastrous. In that case, my work laptop wasn't running an operating system that supports passkeys. While waiting for it to update, the PayPal app kept glitching and wouldn't let me complete the passkey process. Then I couldn't create one specifically for TikTok as I used my work Google account to create the account. When I tried to set up a passkey for Amazon and needed to scan a QR code on my phone, I found that my password manager, Bitwarden, currently doesn't support passkeys on mobile.

Using passkeys likely means having a different mindset from how you think about passwords. There's nothing to remember when you log in, and you have to use something else to store your passkeys. Passkeys can be stored in Apple's, Google's or Microsoft's password manager systems; your browser; a dedicated password manager; or on a physical security key. I created a Google passkey on one USB key, and all I need to do to sign in is, essentially, plug it in. (All of

the devices I use professionally and personally are Apple, meaning I haven't tested passkeys between my iPhone and a Windows laptop, for instance.)

"The technology is mature, the front ends are still nascent," Shikiar from the FIDO Alliance says. Over the past year, the FIDO alliance has also been working on user experience guidelines, he says, making it more straightforward for people to sign up and use passkeys across systems. Gary Orenstein, the chief customer officer of password manager Bitwarden, says there are multiple groups involved in the creation and rollout of passkeys, so transitioning to a world where everything is seamless takes coordination. "The standards are at one level, user expectations are at a different level," he says. "The vendor implementations are at a third level, and they're merging, but it takes time."

Being able to save a passkey on essentially any device makes them more useful and means you aren't locked in to Google's, Microsoft's, or Apple's ecosystems. However, where you save a passkey is going to take some remembering. When setting up one passkey, I was asked by my password manager, browser, and the device operating system whether I wanted to save my passkey with each of them. Picking one spot and sticking to it is probably the best option.

Most of my work is done on my laptop—and it's rare that I download new apps or log out of apps on my phone—so I have been saving the majority of my passkeys in Bitwarden, which costs me $10 a year for a premium account alongside my hundreds of passwords. It works like this: When logging in to my Amazon account, I enter my username, and then Bitwarden's browser extension pops up asking whether I want to log in with my passkey for Amazon. I press confirm, and I am logged in. It also offers the option to use my device or a hardware key to log in, and if I select one of these options, it looks for passkeys stored on my laptop.

However, as mentioned, Bitwarden doesn't currently offer passkeys on mobile, meaning that to get the mobile-first Coinbase integration to work, I ended up saving that passkey to iCloud's Keychain instead. Orenstein, from Bitwarden,

says that making passkeys work on mobile is a priority for Bitwarden and more support should be rolling out in the coming months. The company has seen a “fantastic” adoption of passkeys so far, he says, but acknowledges people will have to get used to the change. “You still need an awareness about where it is,” Orenstein says. “I think, over time, as an industry, we can reduce the need for that awareness, hopefully to zero.”

The Password’s Long Goodbye

You may not have set up any passkeys yet, but it’s only a matter of time. Tech companies are starting to make passkeys the default, and more businesses are adopting them. In the past couple of weeks, X has started allowing some people to use passkeys, and WhatsApp is bringing them to iPhones and iPads after previously rolling out passkey support for Android devices.

Leona Lassak, Blase Ur, and Maximilian Golla, three academics from Germany and the US who have researched the adoption of passkeys, say that businesses they’ve interviewed are generally positive about the adoption of passkeys and the extra security it will bring. However, it will likely take some time until the majority of websites, apps, and companies are using passkeys for everything. “I don’t think we will have a big bang in the next few months,” Lassak says. “It’s going to be a slow process, which on the way will then also catch other and smaller entities.”

As a result, passwords will still be around for a while. It’ll be a long time until I have converted my remaining 320-ish accounts to be using passkeys. And for the time being at least, those accounts where I do have passkeys will still have existing passwords that I can fall back on. “Passkeys is having fewer passwords, but not necessarily no passwords,” says Golla.

Experts recommend setting up a few passkeys whenever you come across them on your online accounts, rather than necessarily trying to change them all at once. There are guides to what websites are using passkeys already, and Google, Microsoft, and Apple all have straightforward explanations on how to create passkeys. And there are plenty of benefits to getting started now.

“They are a true password replacement that eliminate the threat of phishing, eliminate the hassle of password resets, and eliminate the liability that service providers have when they’re managing thousands, tens of thousands, or tens of millions, or billions of passwords,” Shikiar says. “It really is an entirely new way of doing user authentication.”

You Might Also Like ...

- Navigate election season with our WIRED Politics Lab **newsletter** and podcast
- Don’t think breakdancing is an Olympic sport? The world champ agrees (kinda)
- How researchers cracked an 11-year-old password to a $3M crypto wallet
- The uncanny rise of the world’s first AI beauty pageant
- **Give your back a break:** Here are the best office chairs we’ve tested

Matt Burgess is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and now lives in London. Send tips to Matt_Burgess@wired.com.

SENIOR WRITER

TOPICS PASSWORDS SECURITY PHISHING HACKERS

READ MORE

The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever

The number of alleged hacks targeting the customers of cloud storage firm Snowflake appears to be snowballing into one of the biggest data breaches of all time.

MATT BURGESS

Apple Is Coming for Your Password Manager

Plus: A media executive is charged in an alleged money-laundering scheme, a ransomware attack disrupts care at London hospitals, and Google's former CEO has a secretive drone project up his sleeve.

ANDREW COUTS

A US Company Enabled a North Korean Scam That Raised Money for WMDs

Wyoming's secretary of state has proposed ways of "preventing fraud and abuse of corporate filings by commercial registered agents" in the aftermath of the scheme's exposure.

WILLIAM TURTON

Microsoft's Recall Feature Is Even More Hackable Than You Thought

A new discovery that the AI-enabled feature's historical data can be accessed even by hackers without administrator privileges only contributes to the growing sense that the feature is a "dumpster fire."

ANDY GREENBERG

Inside the Biggest FBI Sting Operation in History

When a drug kingpin named Microsoft tried to seize control of an encrypted phone company for criminals, he was playing right into its real owners' hands.

JOSEPH COX

AI Is Your Coworker Now. Can You Trust It?

Generative AI tools such as OpenAI's ChatGPT and Microsoft's Copilot are becoming part of everyday business life. But they come with privacy and security considerations you should know about.

KATE O'FLAHERTY

The Age of the Drone Police Is Here

A WIRED investigation, based on more than 22 million flight coordinates, reveals the complicated truth about the first full-blown police drone program in the US—and why your city could be next.

DHRUV MEHROTRA

The Lords of Silicon Valley Are Thrilled to Present a 'Handheld Iron Dome'

ZeroMark wants to build a system that will let soldiers easily shoot a drone out of the sky with the weapons they're already carrying—and venture capital firm a16z is betting the startup can pull it off.

MATTHEW GAULT

WIRED

WIRED is where tomorrow is realized. It is the essential source of information and ideas that make sense of a world in constant transformation. The WIRED conversation illuminates how technology is changing every aspect of our lives—from culture to business, science to design. The breakthroughs and innovations that we uncover lead to new ways of thinking, new connections, and new industries.