PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing.

Passkeys Are Here: We Just Have to Convince People to Use Them

A FIDO Alliance exec acknowledges that people can still balk at the concept of passkeys, but insists that password authentication is 'fundamentally flawed.'

By Rob Pegoraro Updated February 1, 2024

(Credit: Getty Images)

Passkeys promise to boil the login routine down to a single click or tap followed by a quick biometric confirmation of your in-person presence, but industry adoption of this concept can seem stalled at a simmering stage.

At a day-long conference on identity and authentication in D.C. last week, the head of a trade group behind the passkeys standard acknowledged that obstacles remain for this post-password authentication but emphasized how much things have warmed up for passkeys overall.

“From my point of view, 2023 was the year of the passkey,” said Andrew Shikiar, executive director and chief marketing officer of the FIDO Alliance, in an afternoon keynote. He cited a total of 8 billion user accounts that now allow passkey access, with more than 96% of active browsers and more than 98% of mobile devices supporting passkey authentication.

Shikiar allowed that people can still balk at the concept—“no one's not used a password”—but called password authentication “fundamentally flawed” because it allows for such human failings as password reuse across multiple sites and getting fooled by phishing scams.

Shikiar predicted that in 2024, the number of passkey-enabled accounts “will march towards 20 billion,” adding “I think we'll exceed that.”

A conversation with him afterwards, however, highlighted some lingering hang-ups despite real-world metrics showing how passkeys have streamlined the customer experience for companies that have adopted them.

Consider one example Shiakar cited in his keynote: Air New Zealand’s rollout last year of passkey support as what its site calls “Our Preferred Option” for account security. He said the airline saw a 30% opt-in rate over the first 24 hours, after which its login-abandonment rates dropped by 50%. (Google reported similar efficiency improvements from passkey adoption.)

US airlines, however, have yet to show any signs of detecting passkeys on their radar—their support for multi-factor authentication has barely gotten past security questions.

Shikiar suggested that Air New Zealand’s relatively small size helped it adopt passkeys faster: “They can move quickly because it's a smaller airline.”

But he acknowledged that the travel industry should jump on passkeys. That’s not so much because of the value of the transactions there but because of how often airlines and hotels require not just a username and password but also a last name—which, as Shiakar noted, breaks password managers that expect only the first two fields.

For example, Hyatt demands all three fields for its regular login. But activating its new passkey option reduces my login process to unlocking 1Password and clicking once to use the encrypted passkey saved in that password manager.

And while the tech industry has been much quicker to support passkeys, thanks in part to Google’s move to enable them for all consumer users last May, curious gaps in support persist.

For example, while Meta announced WhatsApp passkey support (at first only for Android) in October, it has yet to do the same for Facebook itself. And X, formerly Twitter, only rolled out passkey support (in its case, iOS only) last week, despite years of high-profile account takeovers.

It’s a strange online world where a Nintendo account can get better security than one of your primary social-media identities.

In other cases, a company or organization’s passkey support can be easy to miss because it doesn’t use that word to describe it or buries the entire option. The federal government’s login.gov portal, for example, offers an “Add face or touch unlock” option, while I was only able to find the passkey option on a PayPal business account because 1Password’s browser extension took me directly to it.

(Google’s Live Transcribe app, which I used during this interview, provided an unintentional demonstration of the poor visibility of passkeys when it consistently transcribed the word “passkey” as something else—for example, “basket,” “past skis,” “pasties,” and “paste,”)

Shikiar also shared some lessons learned about passkey uptake—specifically, about when companies can best make a passkey pitch to a customer. Short answer: When they have to change a security setting for one reason or another and have already navigated to those account settings.

RECOMMENDED BY OUR EDITORS

How to Set Up Passkeys for Your Google Account

Passkeys: What They Are and Why You Need Them ASAP

Shop Safely: How to Set Up Passkeys for Your Amazon Account

“No one enjoys going through security settings,” he said. “But if you're there, that's a good time to grab them.”

And that’s especially true if the customer has to reset a password, when adding a passkey can ensure that the customer doesn’t have to bother with passwords again.

Shikiar acknowledged concerns over what could happen if a passkey user loses the mobile device they use to authenticate a passkey login on another computer. In this common passkey scenario, the phone tells the browser on a desktop or laptop via an encrypted Bluetooth connection that the right user really is parked in front of the keyboard.

But he said that because all the major passkey implementations already offer end-to-end-encrypted synchronization of passkeys, losing a device is not a disaster as long as you retain access to the passkey-sync service—whether it’s Apple’s iCloud Keychain or such third-party password managers as 1Password, Bitwarden and Dashlane.

“All you need to do is recover your core account with that provider,” Shikiar said.

Companies that deploy passkeys, meanwhile, can apply more scrutiny to people still logging in with passwords. And once enough users enable passkeys, a user reverting from a passkey login back to a password can itself represent a warning sign of an account compromise.

“It's important to have higher numbers,” he said. “Because, you know, the end goal is you're getting rid of passwords.”

FURTHER READING

DOJ Charges Russian National for 'Cyberweapon' Attacks on Ukraine, US

BY KATE IRWIN

OpenAI to Clamp Down on Access for Users in China, Unsupported Regions

BY MICHAEL KAN

Hulu, 100K+ Other Websites May Be Exposed to Polyfill Malware

BY KATE IRWIN

Arkansas Sues Tei Chinese Shopping

BY MICHAEL KAN

About Rob Pegoraro

Contributor

Rob Pegoraro writes about interesting problems and possibilities in computers, gadgets, apps, services, telecom, and other things that beep or blink. He’s covered such developments as the evolution of the cell phone from 1G to 5G, the fall and rise of Apple, Google’s growth from obscure Yahoo rival to verb status, and the transformation of social media from CompuServe forums to Facebook’s billions of users. Pegoraro has met most of the founders of the internet and once received a single-word email reply from Steve Jobs.

Read Rob's full bio

Read the latest from Rob Pegoraro

- Supreme Court: The Feds Can Tell Social Media Platforms to Enforce Their Rules
- Cheap Netflix? Verizon Adds Streaming Bundles to Home Broadband Plans
- Your TV Probably Has a 'NextGen' Perk You've Never Heard Of
- 1Password Adds New Account Recovery and Device Addition Options
- Billionaire Frank McCourt Shares His Vision for a Decentralized, User-Owned TikTok
- More from Rob Pegoraro

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

Reviews Best Products Categories Brands Events Series Newsletters Encyclopedia Sitemap

About PCMag Careers Contact Us Press Center

ZIFF MEDIA GROUP askmen EXTREMETECH IGN lifehacker Mashable Offers.com RetailMeNot SPEEDTEST

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