Episode Book

EPISODE #6590

Passkeys on YubiKeys, Hardware Wallets, and 1Password

PUBLISHED	14 November 2026 at 14:29 UTC
DURATION	22:12
LISTEN	myweirdprompts.com/episode/device-bound-synced-passkeys-15984/
HOSTS	Corn, Herman, Clive, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	omnivoice
PIPELINE	V5.26
SOURCES	25 cited by the research (listed at the end)
BOOK GENERATED	15 November 2026 at 11:16 UTC

SYNOPSIS

Passkeys aren't new—YubiKeys have supported them since mid-2018 under the FIDO2 standard. The real dividing line isn't hardware versus software, but whether a credential is copyable across a cloud account or bound to a single device. This conversation breaks down the FIDO Alliance's split between synced passkeys in managers like 1Password and device-bound keys, why attestation matters for high-assurance logins, and why Trezor handles FIDO2 better than Ledger's incomplete resident-key support.

TRANSCRIPT



Corn

Herman, a question before we start. If you own a credential you can hold in your hand, and a credential that lives in somebody's cloud, which one do you sleep better with?



Herman

That depends entirely on which cloud and whose hand. Which is, funnily enough, the whole of Daniel's prompt this week.



Corn

He uses passkeys synced in 1Password, likes them fine, but he wants to know whether a passkey can also live on actual hardware. A YubiKey, or even a hardware wallet doing FIDO authenticator duty. And if it can, whether that's a new thing or just FIDO2 with a fresh coat of marketing paint. His actual worry, underneath the jargon, is the gap between convenience and possession.



Herman

The short answer is yes, you can, and no, it's not new. But the distinction that matters isn't the one the naming suggests. That's the good part.



Corn

Then let's take the naming first, because I think it's where most of the confusion lives. Passkey sounds like a technology. It's a word.



Herman

It's a word for something very specific, though. A passkey is a WebAuthn, FIDO2 credential — a key pair where the private half is generated and held by something called an authenticator, and never leaves it. When you log in, the site sends a challenge, the authenticator signs it, the site checks the signature against the public half it stored at registration. The secret never crosses the wire. What makes a passkey a passkey specifically is that it's discoverable — sometimes called a resident credential. The key itself remembers which site it belongs to, so the site can offer you a username-less, password-less login.



Corn

And the YubiKey has been doing that since when?



Herman

Mid twenty eighteen, when the YubiKey 5 Series shipped. Yubico's own FAQ is almost refreshingly blunt about it. Passkeys, they say, "aren't a new thing. It's just a new name" for the passwordless FIDO2 credentials the key has created all along. They like the rebrand, and honestly, fair enough — "passkey" is a better word than "discoverable WebAuthn credential." Nobody was putting that on a billboard.



Corn

"Discoverable credential" does sound like something you'd find under the sofa.



Herman

Right, so the capability is about eight years old. A key from twenty nineteen does exactly what the word "passkey" describes. What actually changed is Apple and Google mainstreamed the term — Apple first floated it at WWDC in twenty twenty-one — and websites finally started implementing the passwordless flow at scale. The technology was waiting at the door the whole time.



Corn

So when someone says their YubiKey "now supports passkeys," the accurate version is their YubiKey supports what it supported in twenty eighteen, and the internet caught up.



Herman

That's the clean answer to Daniel's rebrand question. And the capacity is generous — a YubiKey stores up to a hundred passkeys. For a personal key, that's effectively unlimited.



Corn

I was going to ask how many accounts I'd need before that became a problem, but a hundred covers more than my entire password manager.



Herman

More than most people's entire password manager, yes.



Corn

The taxonomy, though — Daniel's real distinction. Synced versus device-bound.



Herman

The FIDO Alliance draws exactly two lines. Synced passkeys live in a credential manager — 1Password, Apple Passwords, Bitwarden, Google Password Manager, that crowd — and they're copied across your devices through the manager's cloud. Device-bound passkeys live on one device, typically a security key, and never get copied. You want to sign in on a new laptop, you plug the key in or tap it. That's the fork, and everything else in this discussion hangs off it.



Corn

One nuance before we go further, because I read the definitions and immediately abused them. Device-bound doesn't only mean hardware key.



Herman

No, and this trips people up. Windows 10's built-in credential manager creates a device-bound passkey — bound to the machine, never synced. So the real dividing line isn't hardware versus software. It's copyable versus non-copyable. A YubiKey passkey can't be exported under normal circumstances; a synced passkey can be exported and imported by design, because that's how it reaches your other devices. One lives in exactly one place. The other is, by definition, in several.



Corn

Which reframes the security question entirely. It's not "is hardware more secure than software," it's "what does it mean that the credential can be copied."



Herman

Yes, and that's where the real substance sits, so let me park it for one moment and deal with the hardware wallet part of Daniel's question, because he asked about that specifically and the answer is messier than the YubiKey story.



Corn

He asked whether a hardware wallet can act as a FIDO authenticator. I assume someone in crypto decided it could, because of course they did.



Herman

The Trezor side is almost tidy. The Safe series — Safe 3, Safe 5, Safe 7 — and the Model T all support FIDO2 and passkeys. The old Model One is U2F only, which is the older, non-discoverable protocol — it can be a second factor but it can't do passwordless. So a Trezor bought in the last few years does the job.



Corn

Almost tidy. There's a but coming.



Herman

There is. The Safe 7 does FIDO2 over USB only — no Bluetooth — which matters if your plan was tapping your phone at a coffee shop. But that's a footnote compared to Ledger.



Corn

I've been looking forward to this.



Herman

Ledger ships a Security Key app that runs on the Nano line, the Gen5, the Stax and the Flex, and their developer docs cheerfully describe it as a FIDO2 hardware security key for services like GitHub and 1Password. But their own support page, updated this past July, says the app "currently does not support resident keys."



Corn

Resident keys being — the exact thing passkeys are.



Herman

Discoverable, resident, that's the credential. So a Ledger in its documented state can do FIDO2 second-factor and some WebAuthn flows, but not necessarily a true stored passkey. And the sources disagree — one site claims the modern discoverable-credential flow only works on the Stax and Flex line, Ledger's own help page lists the Nanos, and a third site just writes "not confirmed" and tells you to test it with the service you care about.



Corn

"Not confirmed" is my favorite row in any comparison table.



Herman

So the honest summary for Daniel: a Trezor can plausibly be your security key. A Ledger is a crypto wallet with a bolt-on app that, by its own documentation, is missing the one feature that makes a passkey a passkey. The "hardware key" category is not monolithic, and if he wants the hardware route he should buy the purpose-built thing.



Corn

I own a drawer of things that were almost the purpose-built thing.



Herman

We all do. The other half of the question — whether he should use both a synced passkey and a hardware key — Yubico has a nice line on that. A user who registers both has a stronger recovery story than a user who registered either alone. Complementary, not competing. But the reason they're complementary is worth unpacking, and that's the security argument.



Corn

Go there, because this is where the episode actually earns its length. What does the device-bound key give you that the synced passkey doesn't?



Herman

One word: attestation. When you register a credential from a real security key, the key can present an attestation certificate — cryptographic proof of who made it, what firmware it's running, what it's capable of. The site gets an identifier, the AAGUID, it can check against the FIDO metadata service. So a relying party can verify, mathematically, that the credential came from a genuine YubiKey rather than a piece of software claiming to be one.



Corn

And a synced passkey can't do that.



Herman

Microsoft's own Entra documentation says synced passkeys don't support attestation. So that's the one difference a server can actually check, rather than a philosophical difference about clouds.



Corn

Which is presumably why the high-security world cares. Banks, enterprises, that crowd.



Herman

Yubico's framing is that a high-assurance authenticator needs two different factors and a hard authenticator — the private key present on exactly one device, not copyable, not syncable. Their words on multi-device credentials are blunt: the fact that the private key can be exported and imported "disqualifies their use in high assurance scenarios." Their phrase for the hardware key is the gold standard — "no device, no access."



Corn

They also, and I want to make sure this lands because it's refreshingly honest for a company selling the gold standard, deflate their own product's competition. Yubico says copyable passkeys offer roughly the same security as Sign in with Google or Apple, plus an extra sync password.



Herman

Which is a remarkable sentence for Yubico to publish. They're saying: for most people, most of the time, the synced passkey is fine. You shouldn't force consumers to buy specialty hardware just to use your application — their words again. They're arguing against their own upsell, and I respect it.



Corn

A company that admits its premium product is unnecessary for most customers. Now that's phishing-resistant marketing.



Herman

The threat model is the real story, though. Ask what a synced passkey actually proves when you use it. Yubico's answer: it proves "there was access to a device which was logged into the user's cloud account." That's it. So the attack surface isn't the key anymore — it's the cloud account. You don't steal the credential, you compromise the account it syncs through.



Corn

Which means the hardening advice for a synced-passkey user isn't about passkeys at all. It's about the sync fabric.



Herman

The practical guidance people converged on this year is things like turning on Apple's Advanced Data Protection, adding a hardware key to your Apple ID, enrolling in Google's Advanced Protection Program if you're on Google — and cleaning up your recovery paths, because stale recovery emails and phone numbers are the soft underbelly. There's a line I liked from one of the checklists: if SIM-swap is possible, your recovery is only as strong as your carrier's support desk.



Corn

Somewhere, right now, a telecom support desk is being described as a load-bearing security component.



Herman

It's not wrong, though. That's the uncomfortable part.



Corn

Let's bring it back to Daniel specifically, because he told us his setup. Passkeys synced in 1Password. Can he layer the hardware key onto that, or does 1Password's passkey world close that door?



Herman

The door is open but it has a "beta" sign on it. Two separate things, actually. First, 1Password has supported YubiKeys and Titans as a second factor for your 1Password account for years — that's standard FIDO U2F, well-trodden. Second, and more recent: creating and unlocking a 1Password account with a passkey entered public beta at the end of twenty twenty-three, initially only for new individual accounts. Their staff confirmed you can add security keys to a passkey-unlock account. But it's still labelled beta, it's not compatible with Linux, and their own support doc has this quietly telling instruction: if 1Password asks you to save a passkey but you want to use a security key instead, select the little security key icon.



Corn

So the flow exists, and the flow is a small icon you have to know about.



Herman

Which is very nearly a metaphor for the entire passkey ecosystem — the capability is present, and the affordance is a pixel wide. But to be fair to 1Password, their forum people have been open about it. They've said they've absolutely heard the calls to unlock with a passkey stored on a security key. It's a real roadmap item, not a dismissal.



Corn

Before we get to the "should he use both" verdict, this feels like the moment for our regular guest with a travel tip that is really more of a warning. Take it away, Clive.

C

Clive

One-Star Getaways. In Ulaanbaatar I booked the Steppe Vista Panorama Guesthouse, which advertised a view of the mountains. The mountains were a mural, and the mural was peeling, so by my third night I was looking at a beige wall with a rumour of a peak on it. One star.

C

Clive

The kettle took nineteen minutes to boil and the pillow was a folded blanket with opinions. Warmly recommended for anyone seeking a disappointing trip this winter.



Corn

Nineteen minutes to boil. That kettle has the same relationship to boiling that Ledger has to resident keys.



Herman

You know, a mountain that's a peeling mural is at least honest about what's underneath.



Corn

It's November. There's a certain appeal to a beige wall in Ulaanbaatar.



Herman

You would book it. I've seen your bookmark folder.



Corn

So. Daniel's question, the practical half. He already has the synced passkeys. Does he add hardware, or is that the security equivalent of a peeling mural?



Herman

The answer is a qualified yes, and the shape matters more than the yes. The guidance that's converged on this year — and it's consistent across Yubico and the independent guides — is a division of labor. The synced passkey is your daily driver for the long tail of accounts, everything from the pizza place to the forum you barely use. The hardware key goes on your critical accounts — the number I keep seeing is five to eight of them. Your email, your password manager itself, your bank, your cloud accounts, whatever the short list is where the blast radius is your whole life.



Corn

Because the two defend against different things.



Herman

That's the reason it's not just redundancy. The synced passkey defends against losing your devices — new phone, dead laptop, it follows you. The hardware key defends against cloud account compromise — the attacker who owns your sync fabric owns every synced passkey in it, and can't touch the one on the key in your drawer. Each covers the other's hole. And then there's a second, simpler rule that everyone repeats because it's true: buy two keys.



Corn

Both before you rely on either.



Herman

Register both on every account before you make either one your primary. The buying guides are almost superstitious about this. Because a device-bound credential has the property Yubico brags about — no device, no access — which means lose the device, lose the account, unless the second key was already registered when you had the chance. That's the whole trap of the gold standard: it's only gold if you can still get in.



Corn

The gold standard has a recovery problem, and the thing that solves the recovery problem is the thing Yubico spent a decade telling people not to trust. There's something almost poetic about that.



Herman

Yubico themselves published that a user with both has a stronger recovery story than either alone. So even the vendor whose entire business is the hardware key says the answer is both.



Corn

To circle back to Daniel's framing one more time — his question "is a passkey on a YubiKey something new" has a clean answer, which is no, same credential, rebranded, and Yubico will tell you so themselves. His other question, "should I use both," also has a clean answer, which is yes, for different jobs. The rebrand is the story. The capability sat there since twenty eighteen waiting for everyone else.



Herman

And there's a sense in which the industry has barely started using what's there. The 5.8 firmware Yubico shipped this summer adds things like Secure Payment Confirmation and enterprise attestation — the direction is passkeys authorizing actions, not just logging you in.



Hilbert

Not actions. Approvals. There's a difference and Corn will get there in a minute.



Corn

I might, now.



Hilbert

I've got a drawer of these keys. The one I bought in twenty nineteen already did what the word passkey describes, and I registered it on my main email that same week. Never once had to use it. The login flow has never once asked for the key, so far as I can tell the credential sits there like a fire extinguisher behind glass. I assume it still works. I haven't checked.



Herman

You haven't tested the backup at all?



Hilbert

The backup key is still in the original packaging. Sealed.



Corn

Sealed.



Hilbert

You open it, you've used it up. That's how I think of it and I'm not going to be talked out of it at this desk.



Herman

Herman Poppleberry here, formally registering my objection as a retired physician. An untested backup isn't a backup, it's a hope.



Hilbert

It's a good hope. The primary key's worn to the shape of my pocket and works every time. The email one, the sealed one — that's for the day everything else is gone. Herman, you explained attestation beautifully earlier, by the way, and I don't care about any of it. What I care about is that the key is a thing I can lose and find. I've lost that drawer twice and found it twice. A synced passkey you can only lose in a way nobody can see coming.



Corn

The unopened backup is doing a lot of load-bearing work in your recovery plan.



Hilbert

It's doing exactly as much work as it was doing in twenty nineteen. That's the point of it. The people who make these keys do careful work. I'll say that much.



Corn

He's not wrong about the losing-it-invisibly part, you know. That's the one line in the whole synced-passkey pitch nobody puts on the box. When your cloud account goes, there's no drawer to find. It's just gone, quietly, from everywhere at once.



Herman

And the industry's answer to that is exactly the split Daniel's already positioned for — synced for reach, hardware for the accounts that would end you. He's got the synced half running today. The gap between him and the qualified yes is one purchase order and an evening of registering.



Corn

Which raises the question I'd leave him with. The capability has been there since twenty eighteen. Yubico has now shipped firmware that lets a passkey authorize payments and signatures, not just logins. The real open question isn't whether hardware keys support passkeys — they always did — it's whether anyone on the other side of the transaction will ever actually demand the assurance a hardware key provides. Right now almost no site checks attestation. Convenience is winning by default, because nobody's asking for the gold standard. The hardware is ahead of the demand.



Herman

And if passkeys do become authorization tokens — approving a payment rather than proving a login — the copyable versus device-bound distinction stops being a security nicety. You can argue about who synced your login. Approving a wire transfer is a different animal.



Corn

Then the split becomes the whole argument.



Herman

Which is why I'd tell Daniel to buy the keys now, while it's still a choice and not a requirement.



Corn

He'll do it. The man has a password manager and opinions about it. He's halfway to the drawer already.



Herman

Our producer is Hilbert Flumingtop, who has a sealed backup and no regrets.



Corn

If this was your kind of episode, go back for episode twenty, Architectural AI; episode three, Safetensors or something else; and episode two forty-four, Goodbye 2FA. This has been My Weird Prompts. If today's episode earned a place in your podcast rotation, a review on Spotify helps other people find the show.



Herman

We'll be back soon. See you then.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Yubico [primary]**
   Passkey Frequently Asked Questions, docs.yubico.com (retrieved 2026-11-14; no publish date shown)
   https://docs.yubico.com/hardware/yubikey-guidance/best-practices/all-faq-passkeys.html

2. **Yubico [primary]**
   Passkey use cases, developers.yubico.com (retrieved 2026-11-14)
   https://developers.yubico.com/Passkeys/Passkey_use_cases.html

3. **Yubico [primary]**
   FIDO2 Passwordless Authentication | YubiKey (retrieved 2026-11-14)
   https://www.yubico.com/authentication-standards/fido2/

4. **Yubico [primary]**
   Yubico Extends Passkeys Beyond Trusted Authentication to Verified Authorization with Launch of YubiKey 5.8, press release, 2026-07-21
   https://www.yubico.com/press-releases/yubico-extends-passkeys-beyond-trusted-authentication-to-verified-authorization-with-launch-of-yubikey-5-8/

5. **Yubico [primary]**
   5.8 Firmware Specifics, YubiKey Technical Manual (retrieved 2026-11-14)
   https://docs.yubico.com/hardware/yubikey/yk-tech-manual/yk5-firmware-5.8.html

6. **Yubico [primary]**
   What's New YubiKey 5.8 Datasheet (retrieved 2026-11-14)
   https://www.yubico.com/resource/whats-new-yubikey-5-8-datasheet/

7. **FIDO Alliance [primary]**
   FIDO Passkeys: Passwordless Authentication (published 2024-10-11)
   https://fidoalliance.org/passkeys/

8. **FIDO Alliance [primary]**
   White Paper: FIDO Deploying Passkeys in the Enterprise, Introduction
   https://fidoalliance.org/white-paper-fido-deploying-passkeys-in-the-enterprise-introduction/

9. **FIDO Alliance [primary]**
   White Paper: FIDO Authentication for Moderate Assurance Use Cases
   https://fidoalliance.org/white-paper-fido-authentication-for-moderate-assurance-use-cases/

10. **1Password Support [primary]**
    Unlock 1Password with a passkey (beta) (retrieved 2026-11-14)
    https://support.1password.com/passkeys/

11. **1Password Support [primary]**
    Use your security key as a second factor for your 1Password account (retrieved 2026-11-14)
    https://support.1password.com/security-key/

12. **1Password [primary]**
    Passkeys in 1Password: The Future of Passwordless Authentication product page (retrieved 2026-11-14)
    https://1password.com/product/passkeys

13. **1Password Blog [primary]**
Mitch Cohen, Now in beta: Create and unlock a 1Password account with a passkey, 2023-12-14
https://1password.com/blog/unlock-1password-individual-passkey-beta

14. **Ledger Support [primary]**
Ledger Security Key app, last updated 2026-07-09
https://support.ledger.com/article/12350325732893-zd

15. **Ledger Developers [primary]**
Security Key (retrieved 2026-11-14)
https://developers.ledger.com/docs/ai-tools/hardware-security/security-key

16. **Trezor [primary]**
Using your Trezor as a security key (FIDO2 & U2F) (retrieved 2026-11-14)
https://trezor.io/guides/bonus-tools/using-your-trezor-as-a-security-key-fido-2-and-u2f

17. **GitHub Docs [primary]**
Managing your passkeys (retrieved 2026-11-14)
https://docs.github.com/en/authentication/authenticating-with-a-passkey/managing-your-passkeys

18. **Microsoft Learn [primary]**
Enable synced passkeys in Microsoft Entra ID (retrieved 2026-11-14)
https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-synced-passkeys

19. **Yubico**
The passkey spectrum: Importance of user choice in digital security journeys, by Patryk Les and Luke Walker, 2026-05-19
https://www.yubico.com/blog/the-passkey-spectrum-importance-of-user-choice-in-digital-security-journeys/

20. **Passkey Central**
Passkey Types (retrieved 2026-11-14) [primary-adjacent, FIDO-aligned]
https://www.passkeycentral.org/introduction-to-passkeys/passkey-types

21. **Wikipedia**
Passkey (authentication), last edited 2026-11-07
https://en.wikipedia.org/wiki/Passkey

22. **Wikipedia**
WebAuthn, last edited 2026-11-09
https://en.wikipedia.org/wiki/WebAuthn

23. **Wikipedia**
FIDO Alliance, last edited 2026-11-14
https://en.wikipedia.org/wiki/FIDO_Alliance

24. **1Password Community**
Unlocking 1password with passkey on yubikey, 1P_Dave reply 2024-03-07
https://www.1password.community/1password-at-home-31/unlocking-1password-with-passkey-on-yubikey-20667

25. **1Password Community**
Can I store the passkey for my 1Password account on a Yubikey?, 1p_jac reply 2023-12-07
https://www.1password.community/1password-at-home-31/can-i-store-the-passkey-for-my-1password-account-on-a-yubikey-20587