Podcast Transcript

EPISODE #244

# Goodbye 2FA: Why Passkeys are the Future of Security

Published January 16, 2026 • Runtime: 17:55

https://myweirdprompts.com/episode/passkey-future-security-adoption/

## EPISODE SYNOPSIS

In this episode of My Weird Prompts, Herman and Corn dive into the rapidly evolving world of digital security to answer a burning question: are passwords finally dead? From the staggering success rates of passkey adoption at Google and TikTok to the technical breakthroughs making these credentials portable across devices, the duo breaks down why the "two-factor dance" is becoming a thing of the past. Discover how the FIDO Alliance is solving the "lock-in" problem and why shifting to passkeys is the rare tech upgrade that actually makes your life easier while making it more secure.

## DANIEL'S PROMPT

**Daniel**

Everyone who takes security seriously has spent a lot of time over the past few years entering two-factor authentication codes. While 2FA is a great second layer of security, it can become tedious. The passkey movement seems to be gaining traction and is much more convenient, as it eliminates a lot of the friction associated with 2FA. Do you think passkeys will eventually replace two-factor authentication? It seems redundant to keep stacking layers like passwords, 2FA, and passkeys. What do you think is the future of authentication, and what system will we eventually settle on?

# TRANSCRIPT

**Corn**

Hey everyone, welcome back to My Weird Prompts. I am Corn, and I am sitting here in our living room in Jerusalem with my brother.

**Herman**

Herman Poppleberry, here and ready to dive into the digital weeds. Although, to be fair, these weeds are getting a lot more organized lately.

**Corn**

They really are. So, our housemate Daniel sent us a voice note this morning that hit on something I think we have all been feeling. He was talking about that collective sigh we all let out when we have to log into a new device and then go hunting for our phones to find a six digit code that expires in thirty seconds.

**Herman**

The classic two factor dance. It is the price we have paid for security over the last decade, but Daniel was asking if that price is finally coming down. He wanted to know if passkeys are actually going to kill off two factor authentication entirely, or if we are just adding yet another layer to the stack.

**Corn**

It is a great question because the friction is real. I mean, I have definitely abandoned a purchase or a sign up because I did not feel like getting up to find my phone for a text code. But before we get into the future, Herman, let's ground this. We are in early twenty twenty six now, and the landscape has shifted massively even in just the last twelve months. Where do things stand right now with passkey adoption?

**Herman**

It has been a huge year, Corn. If we look back at the FIDO Alliance Passkey Index that came out in October of twenty twenty five, the numbers are pretty staggering. They found that passkeys actually reduce sign in time by seventy three percent compared to traditional methods. We are talking about an average of eight point five seconds to log in versus over thirty one seconds for the old password and code combo.

**Corn**

That is a massive difference when you aggregate it across billions of logins. It is basically the difference between a minor annoyance and a seamless flow. But speed is one thing. What about reliability? Because the biggest headache with two factor is often the code not arriving or the app de syncing.

**Herman**

Exactly, and that is where the data really shines. That same index showed that passkey sign ins have a ninety three percent success rate. Compare that to about sixty three percent for other methods. That gap is where all the frustration lives. When you look at specific companies, Google has been reporting that passkey sign ins are four times more successful than passwords. Even TikTok, which you might not think of as a high security fortress, saw a ninety seven percent success rate once they implemented them.

**Corn**

Ninety seven percent is wild. But I want to push on Daniel's point about redundancy. If I have a passkey, do I still need a password? And if I do not have a password, is it even two factor anymore? It feels like we are collapsing the layers.

**Herman**

That is the beautiful technical trick of the passkey, Corn. It actually internalizes the multi factor requirement. When you use a passkey, you are using something you have, which is the physical device or the secure enclave on your chip, and something you are or know, like your fingerprint, face scan, or device pin. So the two factors are happening simultaneously in one gesture. You are not stacking them; you are integrating them.

**Corn**

So in that sense, the "two" in two factor authentication is still there, it is just hidden behind a single click. But let's talk about the friction of moving. One of the things that has held people back, and something we touched on briefly in episode two hundred sixteen when we were talking about security managers, is the fear of being locked in. If I save all my passkeys in my Apple keychain, am I stuck on an iPhone forever?

**Herman**

That has been the billion dollar question, and honestly, it was a valid concern until very recently. But the FIDO Alliance has been working on two major pieces of the puzzle: the Credential Exchange Protocol, or CXP, and the Credential Exchange Format, known as CXF. They published a review draft of the format in March of twenty twenty five, and the goal is to make passkeys as portable as a CSV file of passwords used to be, but way more secure.

**Corn**

Right, because right now, moving from a password manager like Bitwarden to something else is relatively easy. But moving passkeys felt like trying to move a mountain because they are bound to the hardware or a specific cloud provider. How do CXP and CXF actually solve that without making the keys vulnerable?

**Herman**

It is all about a secure, encrypted handshake between the providers. Instead of just exporting a list of secrets that anyone could read, these protocols allow one manager to securely transfer the private key material to another without it ever being exposed in the clear. The big players like Apple, Google, and Microsoft are all at the table for this. It is in their interest because if people feel trapped, they will not adopt the tech in the first place.

**Corn**

That makes sense. It is that classic trade off between security and usability that we discussed way back in episode sixty five. But it feels like the balance is finally tipping toward usability. I noticed that Microsoft made a huge push recently. Did they not start making passkeys the default for new accounts?

**Herman**

They did. In May of last year, Microsoft announced that brand new consumer accounts would be "passwordless by default." You do not even create a password during sign up anymore. They give you the option to use the Microsoft Authenticator app, a passkey, or a physical security key. They actually reported that ninety eight percent of passkey login attempts were successful on their platform, compared to a much lower rate for passwords. It is a bold move to kill the password at birth, but it is working.

**Corn**

It is interesting to see who is leading and who is lagging. Google has had passkeys as the default for personal accounts since late twenty twenty three, but I read something weird about eBay. Did they not have some trouble with this recently?

**Herman**

Yeah, eBay is a fascinating case study in the "help desk" problem. Around March of twenty twenty five, there were reports that eBay actually removed passkey support in some regions, specifically for their classic web interface. The rumor was that they were hit with a massive spike in support calls from users who were confused or had locked themselves out. It just goes to show that even if the tech is perfect, the human element is messy. But by the end of twenty twenty five, they were already testing a re implementation. They realized they could not stay in the password era forever, especially with the cost of those support calls.

**Corn**

That is a great point. We often think about security in terms of preventing hacks, which passkeys are amazing at because they are phishing resistant by design. You cannot be tricked into giving away a passkey to a fake website because the browser and the hardware simply will not sign the challenge if the domain does not match. But for a company, the real ROI is probably in those help desk tickets.

**Herman**

Absolutely. The FIDO Index showed an eighty one percent reduction in login related help desk incidents for companies that fully embraced passkeys. Think about the millions of dollars spent every year on people calling in because they forgot their password or their SMS code did not arrive. Passkeys basically eliminate the "forgot password" button.

### Corn

I love the idea of a world without a "forgot password" button. But let's dig into the "what if" scenarios that Daniel's prompt brings up. If we settle on passkeys, what happens if I lose my phone? With a password and an authenticator app, I might have backup codes written in a safe. With a passkey, if it is synced to the cloud, I am okay, but what if it is "device bound"?

### Herman

This is where we need to distinguish between the two types of passkeys. Most consumers are using "synced passkeys." These are backed up to your iCloud or Google account. If you lose your phone, you just log into your new phone with your cloud account, and your passkeys are there. It is convenient, but for high security environments, like a bank's back end or a government agency, they use "device bound" passkeys. Those stay on the physical chip and never leave. If you lose that device, that specific key is gone.

### Corn

So for the average person, the synced version is the future. It is the perfect blend of "I can't be phished" and "I won't lose my access." But Daniel's point about stacking layers is still bothering me. I still see sites that ask for a password and then a passkey. That feels like the worst of both worlds.

### Herman

That is definitely a transition phase "anti pattern." It usually happens because a site has not fully committed to the passkey workflow. They are using the passkey as a second factor instead of a primary one. But as we move further into twenty twenty six, you are going to see that disappear. The ultimate goal is the "conditional UI" where you just click the username field, your device biometrics pop up, you touch the sensor, and you are in. No password, no code, no extra steps.

### Corn

It feels like we are approaching a "single factor experience" with "multi factor security." But what about the people who do not have biometric hardware? Are they going to be left behind?

**Herman**

Not necessarily. Remember, a passkey can also be protected by a device pin. So if you are on an older laptop without a fingerprint reader, your "something you know" is the pin you use to unlock the laptop itself. The security still comes from the fact that the private key is stored in the hardware's secure element. It is still way better than a password that can be stolen from a server database.

**Corn**

That is a key distinction. Passwords are a shared secret. Both you and the server know it. If the server gets hacked, your secret is gone. With passkeys, the server only has your public key. They can hack the server all they want; they will never get your private key because it is not there. It is a fundamental shift in the architecture of trust.

**Herman**

It really is. And to Daniel's question about what we will eventually settle on, I think the answer is a "passkey first" world where the password is a legacy fallback that eventually gets turned off for good. We are seeing this with the "Passkey Pledge" that dozens of organizations have taken. They are committing to making passkeys the primary way people interact with their services.

**Corn**

So, if you are listening to this and you haven't enabled passkeys on your main accounts yet, specifically things like Google, Microsoft, Amazon, or your password manager, you are basically living in the past. But I want to pivot to the practical side for a second. Herman, for someone who is ready to make the switch, what is the best strategy? Do you just go through every account one by one?

**Herman**

That is one way, but a better strategy is to use a modern password manager that supports passkey storage. That way, you get the benefit of the passkey security, but you also have a centralized place to manage them, and you are not tied to just one ecosystem like Android or iOS. Most of the big names like 1Password and Bitwarden have excellent passkey support now. When you log into a site, it will often prompt you to "upgrade to a passkey." Just say yes.

### Corn

It is one of those rare moments in tech where the more secure option is actually the easier one. Usually, security means more locks and more keys. Here, it is like replacing a bunch of rusty padlocks with a high tech smart lock that recognizes your face.

### Herman

Exactly. And the "phishing resistance" cannot be overstated. We talked about high altitude surveillance and balloons in episode two hundred thirty nine, and how governments plan for the end in episode two hundred forty two. In those high stakes worlds, the weakest link is always a human being getting tricked into giving up a credential. Passkeys basically remove that human error from the equation. You cannot give away what you do not know.

### Corn

That is a powerful thought. You cannot give away what you do not know. It makes me think about the future of "agentic" authentication, where maybe our AI assistants handle the handshakes for us. But that is probably a rabbit hole for another day.

### Herman

Oh, I have thoughts on that, but let's stick to the current reality. One thing to watch out for in twenty twenty six is the "passkey recovery" process. Since there is no password to reset, how you regain access to your "vault" if you lose everything is the new critical path. Most providers are using "recovery sets" or "trusted contacts" to handle this. It is a different mental model for users.

### Corn

Right, instead of "what was my first pet's name," it is "who are the three people I trust to vouch for me." It is more human, in a way. So, to wrap up Daniel's question: yes, passkeys are the replacement. The "stacking" of layers is a temporary transition. Eventually, the password and the six digit code will go the way of the rotary phone.

**Herman**

I think that is a safe bet. We are seeing the infrastructure mature, the portability issues are being solved by FIDO's new standards, and the business case is just too strong for companies to ignore. The "password era" is officially in its twilight.

**Corn**

Well, on that note, I think I am going to go check my accounts and see how many more passwords I can kill today. Daniel, thanks for the prompt. It is always good to step back and look at these things we do every day and realize that the friction we just "accept" might actually be on its way out.

**Herman**

Definitely. And hey, if you are out there listening and you have found a site that is doing passkeys particularly well or particularly poorly, let us know. We love those real world examples.

**Corn**

We really do. And if you have been enjoying the show, whether you are a new listener or you have been with us for all two hundred forty four episodes, we would really appreciate a quick review on your podcast app or Spotify. It genuinely helps other curious people find us.

**Herman**

It makes a huge difference. You can find all our past episodes and a contact form at our website, myweirdprompts.com. We are also on Spotify, obviously.

**Corn**

Thanks for joining us today. This has been My Weird Prompts. I am Corn.

**Herman**

And I am Herman Poppleberry. Keep asking the weird questions, everyone.

**Corn**

We will see you next time. Bye.

**Herman**

Goodbye!