MY WEIRD PROMPTS

Podcast Transcript

EPISODE #305

Beyond the Password: The Rise of Invisible Security

Published January 26, 2026 • Runtime: 23:10

https://myweirdprompts.com/episode/passkeys-and-future-authentication/

EPISODE SYNOPSIS

As we move further into 2026, the friction of traditional two-factor authentication is reaching a breaking point for many users. In this episode of My Weird Prompts, Herman and Corn dive deep into the world of passkeys, hardware tokens, and the emerging "fourth factor" of security: behavioral biometrics. They discuss whether we are headed toward a more secure world or one where our every move is monitored for the sake of convenience. From heartbeat signatures to Zero Trust architecture, learn how the tech industry plans to kill the password once and for all while keeping the hackers at bay.

DANIEL'S PROMPT

Daniel

In a previous episode, we talked about passkeys and the industry move to make them more common. I’m happy to see them gaining momentum and I use them myself, but I think many people are tired of two-factor authentication. To me, however, two-factor authentication is a mandatory minimum standard, and I've been looking into different second-factor options beyond the password, such as biometrics like fingerprint readers, facial recognition, and voice. I’m wondering if passkeys will eventually solve the challenge of second-factor authentication for most people, or if we’ll see a move toward three-factor and four-factor authentication. In highly secure environments, what kind of layers will be added on top of passkeys? Will it be passkeys plus a biometric factor, or perhaps hardware like YubiKeys? What is the future of multi-factor authentication going to look like?

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, the man who probably has more security keys than actual keys on his keychain.

Herman

Herman Poppleberry, at your service. And you are not wrong, Corn. I think I have three different hardware keys just to get into my primary email account. But in my defense, the digital world is a wild place in January two thousand twenty-six.

Corn

It really is. And that is actually what we are diving into today. Our housemate Daniel sent us an audio prompt earlier about the state of authentication. He has been using passkeys, which we have touched on briefly in the past, but he is starting to feel that two-factor authentication fatigue that I think a lot of us are dealing with.

Herman

It is a real thing. That constant friction of getting a code, or tapping a notification, or scanning a thumbprint every time you just want to check your bank balance or log into a work portal. Daniel was asking if passkeys are the ultimate end-game that solves this for everyone, or if we are actually headed toward even more layers, like three-factor or four-factor authentication in high-security environments.

Corn

I love this question because it hits on that tension between convenience and security. We all want to be safe, but we do not want to feel like we are breaking into Fort Knox just to send an email. So, Herman, let's start with the basics for a minute. For anyone who might have missed the shift over the last year or two, where do passkeys stand right now? Are they actually replacing the traditional two-factor setup?

Herman

That is the big question. To understand the future, you have to understand that passkeys are a fundamentally different beast than passwords. When you use a passkey, you are using public-key cryptography. Your device creates a unique pair of keys, a public one that goes to the website and a private one that stays on your phone or computer. To log in, you just prove you are you, usually with a biometric like Face I-D or a fingerprint, and your device signs a challenge from the server.

Corn

Right, and the beauty of it is that there is no password to steal. A hacker can't phish a passkey because the key is tied to the specific domain of the website. But Daniel’s point is interesting. He uses passkeys, but he still feels like two-factor authentication is a mandatory minimum. Does a passkey count as one factor or two?

Herman

This is where the technical nuance gets really fun. Technically, a passkey often qualifies as two factors in a single gesture. It is something you have, which is the physical device holding the private key, and it is something you are, which is the biometric you used to unlock that device. Or, it could be something you know, if you use a P-I-N to unlock the device. So, in one quick tap, you have satisfied the multi-factor requirement that used to take two separate steps.

Corn

So, for the average person, passkeys are basically collapsing those two steps into one. That sounds like the solution to the fatigue Daniel was talking about. But he asked about the future. If passkeys become the baseline, do the high-security environments just move the goalposts? Are we going to see a world where you need a passkey plus a hardware key plus a retina scan?

Herman

I think we absolutely will, but maybe not in the way people expect. We are moving away from what I call synchronous friction toward asynchronous or continuous authentication. Think about it this way. Right now, authentication is a gate. You prove who you are at the door, and then the door stays open. In a three-factor or four-factor future, the gate might be easy to pass, but the house is constantly checking to make sure you are still the person who walked in.

Corn

That is a great analogy. So, instead of asking for a second or third factor at the start, the system is looking at other signals. What kind of factors are we talking about when we go beyond the standard three categories of something you know, have, and are?

Herman

Well, the industry is starting to lean heavily into what we call behavioral biometrics and environmental context. This would be the fourth factor. It is not just who you are, but how you behave. For example, the way you type on a keyboard, the cadence of your keystrokes, or the way you move your mouse. These patterns are surprisingly unique to individuals.

Corn

Wait, really? So if I am logged in and suddenly my typing speed changes or I start moving the mouse differently, the system could flag that?

Herman

Exactly. There are companies right now, and even some major banking apps in early twenty-six, that use these invisible signals. If the behavior doesn't match your historical profile, the system might trigger a step-up authentication. It might ask for that third factor, like a hardware key or a voice print, because the fourth factor, the behavior, didn't look right.

Corn

That is fascinating, but also a little bit "Big Brother"ish, isn't it? I can hear the privacy advocates cringing. If my computer is constantly monitoring how I move my mouse, that feels like a lot of data being collected.

Herman

You are spot on, and that is the big debate right now. The industry's counter-argument is that this data can be processed locally or anonymized into a mathematical representation of your movement rather than the raw data itself. But you are right, it is a trade-off. We are trading a bit of privacy and constant monitoring for the convenience of not having to type in a six-digit code every twenty minutes.

Corn

Let's talk about the hardware side of this. Daniel mentioned YubiKeys. For our listeners who aren't as nerdy as you, Herman, these are those little U-S-B sticks you plug in or tap against your phone. In a world of passkeys and biometrics, do these things have a future, or are they going to become like the floppy disks of security?

Herman

Oh, they are more relevant than ever. In fact, if you look at high-stakes environments, like government agencies, financial infrastructure, or even high-level software development, hardware keys are still the gold standard. The reason is simple: isolation. A passkey stored in your phone's secure enclave is very safe, but your phone is a general-purpose device. It is connected to the internet, it runs apps, it has a complex operating system. A YubiKey or a similar F-I-D-O-two token is a single-purpose device with a tiny attack surface. It does one thing and it does it with extreme security.

Corn

So for someone like Daniel, who wants that "mandatory minimum" of high security, a hardware key might be the third factor. You use a passkey on your laptop, which is your something you have and something you are, and then for your most sensitive accounts, you add a requirement for a physical hardware token.

Herman

Exactly. And we are seeing the hardware keys themselves evolve. Some of the newer ones coming out now have their own tiny fingerprint sensors on the key itself. So you have a factor on top of a factor on a dedicated device. It is like security inception.

Corn

I want to go back to the biometric piece. Daniel mentioned voice and facial recognition. We have seen facial recognition become pretty standard with things like Face I-D, but voice has always felt a bit hit-or-miss. I remember a few years ago, people were showing how you could trick voice authentication with a simple recording or a deepfake. Given where we are now with A-I, is voice even viable as a secure second or third factor anymore?

Herman

That is a very timely question, especially given how much we have talked about generative A-I lately. In fact, we did that whole episode on deepfakes recently, which really highlighted the risks. For a while, voice was actually being phased out because it was too easy to spoof with A-I clones. But there is a bit of a comeback happening with what is called liveness detection.

Corn

Liveness detection? Is that like the "prove you are a human" puzzles but for your voice?

Herman

Sort of. Instead of just listening to the sound of your voice, the system is looking for the physical characteristics of human speech that A-I has a hard time replicating in real-time. This includes things like the subtle sounds of breath, the way certain consonants interact with the acoustics of a room, or even asking the user to say a random string of words to ensure it isn't a pre-recorded clip. It is a constant arms race between the A-I that spoofs and the A-I that detects.

Corn

It feels like we are in this loop where the technology gets more advanced to catch the hackers, which then makes the hackers get more advanced. Does this ever end? Or are we just going to be adding factors until we are doing a full physical exam just to log into Netflix?

Herman

You know, it is funny you say that. There is actually research into using heart rate patterns or even E-K-G signatures as a biometric factor. Your heart has a unique electrical signature. Imagine a world where your smartwatch is constantly authenticating you to your laptop based on your heartbeat. That would be a "continuous" third factor. As long as the watch is on your wrist and detects your specific heart rhythm, your devices stay unlocked. If you take the watch off, or if someone else puts it on, the connection breaks instantly.

Corn

Now that is a future I can get behind. It is invisible. It is the opposite of the friction Daniel is worried about. But it also relies on us being constantly "on the grid" with our wearable tech. If my watch dies, am I locked out of my life?

Herman

That is the "fallback" problem. Every security system needs a way out when the primary method fails. And usually, the fallback is the weakest link. If you have this incredibly secure heartbeat-plus-passkey system, but the fallback is "answer your mother's maiden name," then the whole thing is only as strong as that security question. This is why the industry is trying to push toward "account recovery" that uses your social circle or other verified hardware rather than old-school questions.

Corn

We have talked a lot about the technical side, but I want to touch on the human element. Daniel mentioned he is tired of two-factor authentication. I think a lot of people feel that way. If we move to three-factor or four-factor, even if it is "invisible," isn't there a risk that people will just find workarounds because it feels too intrusive?

Herman

Absolutely. We call it "security bypass behavior." If a system is too annoying, people will find the path of least resistance. They will leave their devices unlocked, they will share passwords, or they will choose the least secure options available just to save time. The goal for the next few years is to reach "Zero Trust" architecture without making the user feel the weight of it.

Corn

Zero Trust. We have mentioned that before. Can you give us a quick refresher on how that fits into this multi-factor future?

Herman

Sure. The old way of thinking was "Trust, but verify." Once you were in the network, you were trusted. Zero Trust is "Never trust, always verify." Every single request to access a file or an app is treated as a potential threat. To make that work without driving people crazy, you need those invisible factors we talked about. Location, device health, time of day, behavioral patterns. If I am logging in from my house in Jerusalem at ten A-M on my usual laptop, that is a low-risk scenario. The system might only ask for one factor. But if I suddenly try to access sensitive files at three A-M from a server in a different country, the system is going to demand three or four factors before it lets me in.

Corn

So it is dynamic. The number of factors you need changes based on the risk of what you are doing. I like that. It makes sense that checking my grocery list shouldn't require the same security as transferring ten thousand dollars.

Herman

Exactly. And that is really the answer to Daniel’s question. The future isn't just "more factors" across the board. It is "smarter factors" that scale up and down based on the situation. Passkeys are the foundation because they remove the biggest vulnerability, which is the password. Everything else, the biometrics, the hardware keys, the behavioral analysis, those are the layers we add when the stakes are high.

Corn

So, for someone like Daniel, or any of our listeners who are feeling the fatigue, what is the practical takeaway here? If they want to be as secure as possible without losing their minds, what should their setup look like right now, in early twenty-six?

Herman

Number one, move everything you can to passkeys. If a site offers it, take it. It is a massive upgrade over passwords. Number two, for your "crown jewel" accounts, your primary email and your main bank account, use a hardware key as your second factor. It is a bit of an initial setup headache, but once it is done, it is incredibly fast and nearly unhackable. And number three, embrace the biometrics on your devices. Use the fingerprint reader, use the face scan. It is much more secure than a four-digit P-I-N that someone can shoulder-surf while you are on the bus.

Corn

That is solid advice. I actually moved my primary email to a hardware key last month, and I was surprised at how much less I worry about it now. There is a certain peace of mind that comes with knowing someone would literally have to break into my house and steal a physical object to get into my account.

Herman

It is a different kind of security. It turns a digital problem back into a physical one, and humans are generally much better at managing physical security. We know how to lock doors and keep track of our keys. We aren't as good at managing thousands of unique, complex strings of characters in our heads.

Corn

You know, thinking about what you said earlier about heartbeats and E-K-G signatures, it makes me wonder about the long-term implications of our bodies becoming the keys. If my biometric data is the lock, and that data gets compromised, I can't exactly change my heartbeat or my fingerprints.

Herman

That is the big one. That is the nightmare scenario for security experts. If a database of biometric templates is stolen, you can't "reset" your face. This is why the F-I-D-O standards are so important. They ensure that your biometric data never actually leaves your device. The website doesn't get your fingerprint; it only gets a digital signature that says, "Yes, the person with the correct fingerprint is here." That distinction is vital. As long as the biometrics stay local to the hardware, the risk is contained.

Corn

That makes me feel a bit better. It is about keeping the "secret" in your hand, not in the cloud. I think that is a distinction a lot of people don't realize. They think when they scan their face for a website, that website now "has" their face in a database somewhere.

Herman

Right, and that is almost never the case with modern standards. If you are using a reputable service that follows the WebAuthn protocols, your face stays on your phone.

Corn

So, looking ahead, say five years from now, to twenty-thirty-one. Do you think passwords will be completely gone? Or will they still be lingering around like those old legacy systems that just won't die?

Herman

I think for the top one thousand websites, passwords will be a relic of the past. But the long tail of the internet is very long. There are millions of small forums, local business sites, and old databases that will still be using "Password one-two-three" for a long time. The challenge will be how we bridge that gap. Password managers are already becoming "credential managers" that handle both passwords and passkeys, and I think that is how we will live for the next decade. A hybrid world.

Corn

It is like the transition from horses to cars. For a while, you had both on the road, and the infrastructure had to accommodate both. Eventually, the horses became a niche hobby, and the cars took over.

Herman

Exactly. And right now, we are in that period where the first Model T is rolling off the line, but a lot of people are still comfortable with their horse and carriage. Passkeys are the Model T. They are faster, safer, and eventually, they will be the only way people want to travel.

Corn

Well, I hope Daniel feels a bit more optimistic about the future of authentication now. It sounds like the friction we are feeling today is part of a transition toward a much smoother, and ironically more secure, future.

Herman

I think so. It is that "awkward teenage phase" of technology. We are moving away from the old ways, but the new ways haven't quite become invisible yet. But we are getting there. The fact that we can even have this conversation about heartbeat authentication and behavioral biometrics shows how far we have come from the days of "What was the name of your first pet?"

Corn

Oh man, don't even get me started on security questions. "What was the make of your first car?" Well, I have had four, and I can't remember which one I told this random website ten years ago.

Herman

Precisely. That is a "something you know" that you have actually forgotten, which is the worst kind of factor.

Corn

Well, I think we have gone deep enough into the weeds of authentication for one day. Herman, thank you for being our resident security expert, as always.

Herman

My pleasure, Corn. It is a topic that affects every single one of us, whether we realize it or not.

Corn

And to our listeners, thanks for joining us on this deep dive. If you are enjoying these explorations into the weird and wonderful prompts that Daniel sends our way, we would love it if you could leave us a review on your favorite podcast app. Whether it is Spotify, Apple Podcasts, or anywhere else, those ratings really do help other curious minds find the show.

Herman

They really do. And if you have your own weird prompts or questions about the future of tech, or anything else for that matter, you can always get in touch with us through the contact form at myweirdprompts.com. We love hearing what is on your mind.

Corn

You can also find our full archive and the R-S-S feed there if you want to catch up on any of our previous two hundred ninety-three episodes. This has been My Weird Prompts.

Herman

Thanks for listening. We will catch you in the next one.

Corn

Stay curious, everyone. Bye for now.