

Episode 9
MFA Stinks, Make It Stink Less:
Staying secure with less daily friction

Passwords get leaked.

MFA and monitoring are what stand between a major incident and a minor one.

WELCOME
to Clear Skies

Your Host:



Caroline Clark

Rob Gundling

President & Founder
Cloud 9 Computing Group



Tell Us More

How does your team prove it's really them?

- 📱 Text message code
- 🔢 Authenticator app
- 🔑 Passkey or security key
- ⌨️ Hardware token
- 🔒 Just a password
- 🤷 No idea

🔔 **Sign-in request from Clear Skies**

Every account my business relies on (email, banking, payroll, QuickBooks) has MFA turned on.

False **True**

Attackers Aren't Breaking In. They're Logging In.

97%+ of identity attacks are password attacks. The password is now the easy part.

WITHOUT MFA

Stolen password

= they're in. 🔓

No second step. Nothing in their way.

VS

WITH MFA

Stolen password

= still locked out. 🔒

MFA blocks 99%+ of identity attacks.

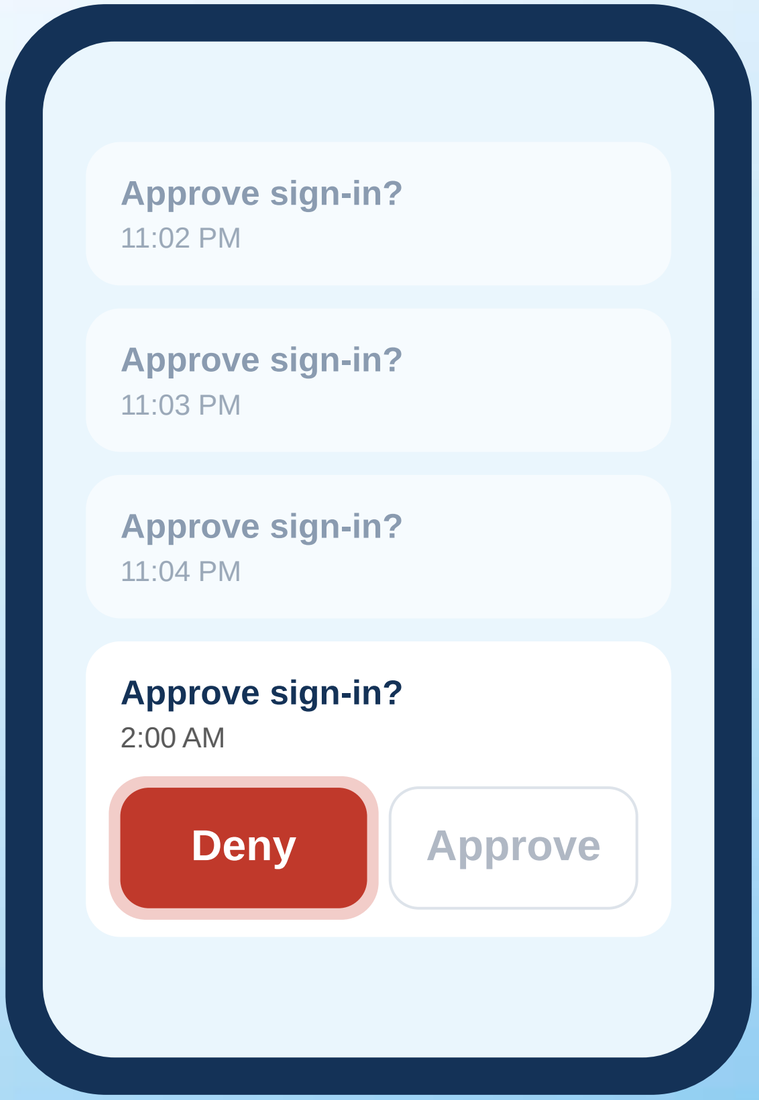
Source: Microsoft Digital Defense Report, October 2025

How Attackers Get Around MFA

Didn't start it?
Deny it.

Then tell IT. It means someone has your password.

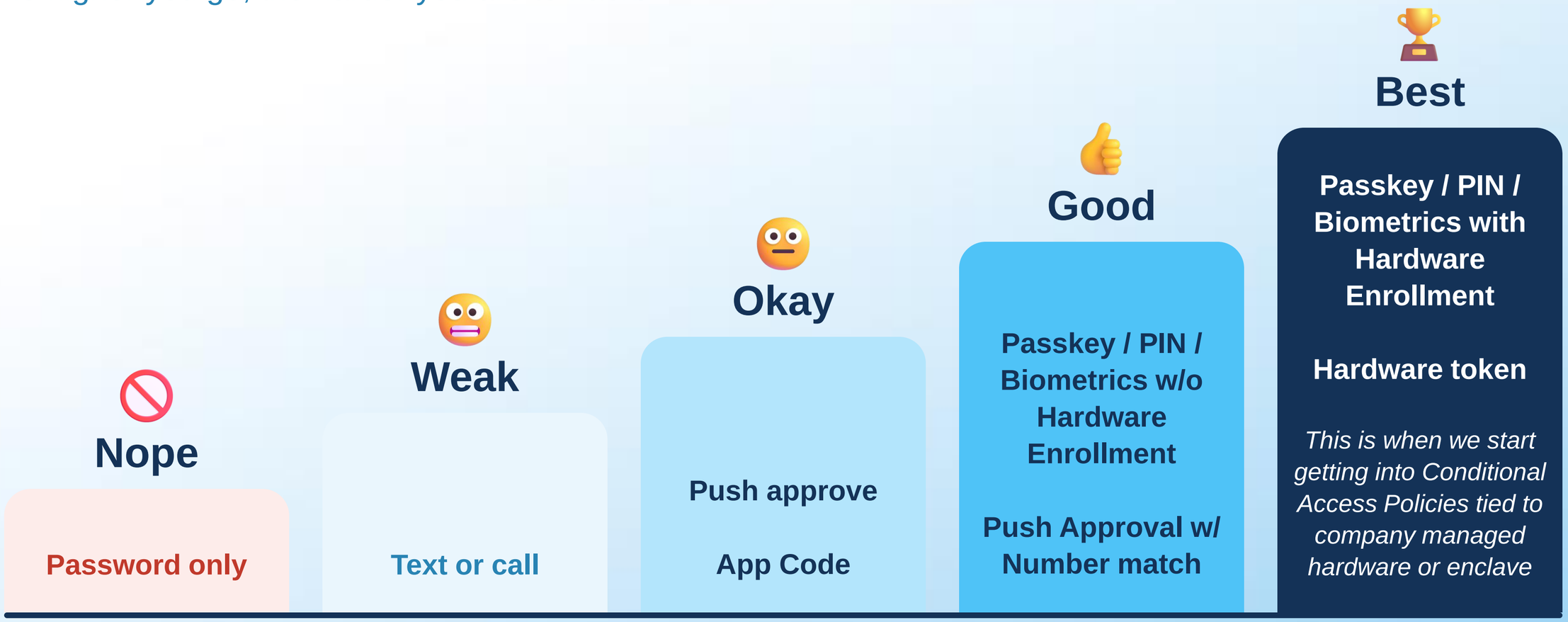
🔔 **Push Spam**	Prompt after prompt until you tap Approve
🎣 **Fake Logins**	Look-alike or proxy pages that pass your code along
📞 **Fake Calls**	Someone posing as IT asking for your code



Uber & Cisco (2022): push spam + a fake "IT support" contact. Sources: Uber; Cisco Talos; CISA/FBI (July 2025)

Not All MFA Is Created Equal

The higher you go, the harder you are to hack.



Only Conditional Access Policies tied to enrolled hardware fully stop fake login pages.

Modern MFA: Sign In With a PIN or a Key

No phone? No problem.

Both are phishing-resistant: there's no code for a fake sign-in page to steal.

A PIN on your computer



Windows Hello: unlock with a PIN, face, or fingerprint. The PIN never leaves your device.

A hardware security key



A small USB or tap-to-use key. Great for admins, finance, and anyone without a work phone.

Less secure → **Most secure**

📱 **Text code** | 🔢 **App code or tap** | 💻🔑 **PIN or key**

Sources: Microsoft Learn (Windows Hello for Business); CISA phishing-resistant MFA guidance

Only Your Devices Get In

Conditional Access: the right password isn't enough. It has to come from the right device.



A hacker can steal your password.

They can't fake your device.

Personal phone? Fine.

Company Portal walls off work stuff. IT can wipe that, not yours.

Security key

Plug it in or tap it to prove it's you.

Lost or stolen?

IT cuts that device off. Done.

🧱 **MFA + SSO + Conditional Access = easiest to manage, hardest to hack**

Why MFA gets a “bad rap” (and How to Fix It)

Sound familiar? Every one of these has a fix.

My phone died. Now I'm locked out.

THE FIX

Add a backup way to sign in

New phone. Now nothing works.

THE FIX

Call IT before you trade in the old phone

Why is it asking me AGAIN?

THE FIX

Number matching + a trusted work device

Ugh. The code expired. Again.

THE FIX

Use a passkey or PIN. No code, no timer.

Which app was this code in?

THE FIX

One app for every code, or one login with SSO →

💡 What's SSO?

Single sign-on. Log in once, and your connected work apps let you right in.

Why SSO is the multiplier

Prove it's you once. Every connected app trusts it.

EASIER

For your team

- **Sign in Less.** Fewer passwords, fewer prompts.
- **New hire?** Give access from one place.

SAFER

Against attackers

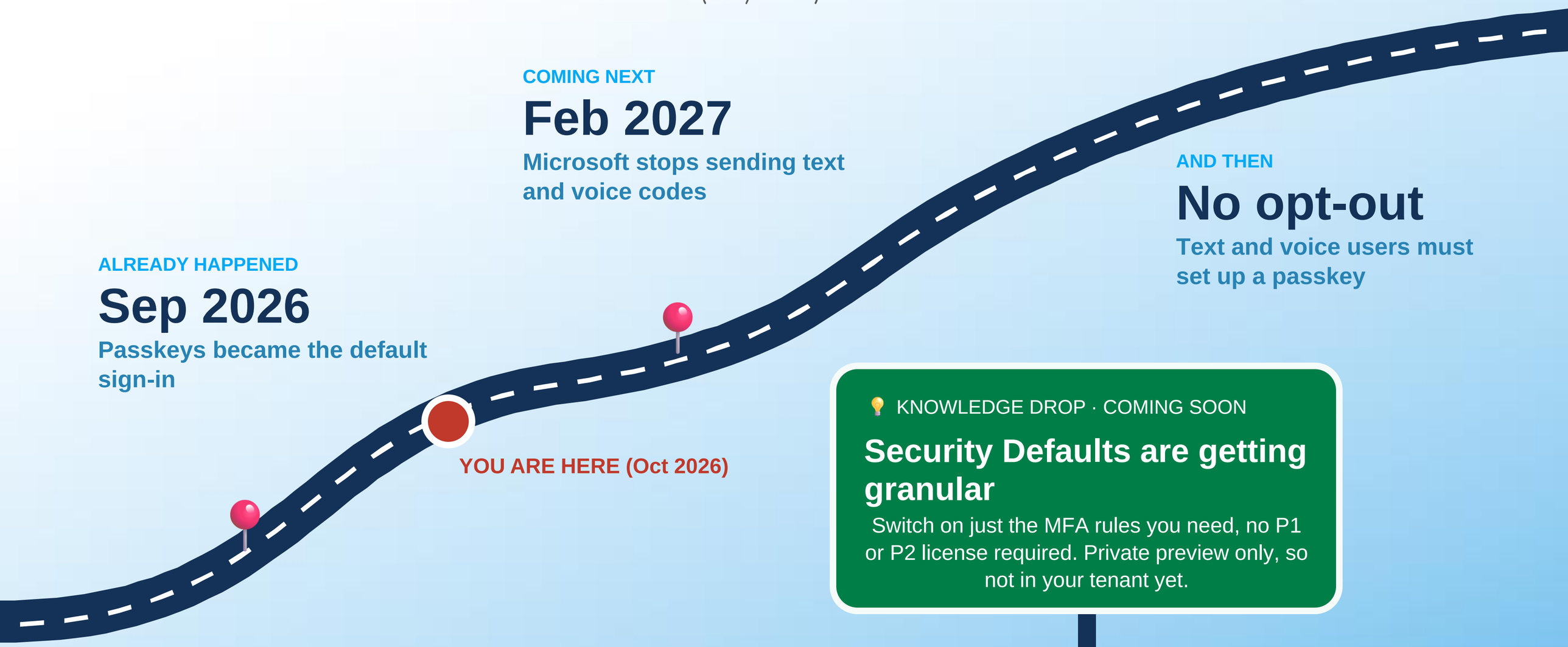
- **Only company devices get in.** Hard to fake.
- **Someone leaves or loses a device?** One switch.



⚙️ More setup up front: MFA + enrolled devices. **Every app you connect inherits that protection.**

Microsoft Is Making the Call for You

Source: Microsoft Entra announcement MC1426371 (July 2026)



ALREADY HAPPENED

Sep 2026

Passkeys became the default sign-in

YOU ARE HERE (Oct 2026)

COMING NEXT

Feb 2027

Microsoft stops sending text and voice codes

AND THEN

No opt-out

Text and voice users must set up a passkey

💡 KNOWLEDGE DROP · COMING SOON

Security Defaults are getting granular

Switch on just the MFA rules you need, no P1 or P2 license required. Private preview only, so not in your tenant yet.

Questions? Tap Approve.

Hot takes, horror stories, burning questions: bring 'em. Unlike that random 2 a.m. sign-in prompt, we'll approve every single one. 😉

(Yes, even your airport lockout story.)

Thank You for Joining Us

Questions? Follow up at communications@c9cg.com