



Episode 7

Catch Scams Before They Catch You

*If it sounds urgent, secret, or too convincing to question —
look again.*



WELCOME to Clear Skies

Your Hosts:



Caroline Clark





Lanea Dunn

Technician at Cloud 9 - Cyber Security

What's the most convincing scam attempt you've ever seen or heard about?



Tell Us More

How confident are you that you could spot an AI deepfake voice or video?

- Very confident
- Somewhat confident
- Not at all confident
- Never thought about it

Scammers can clone someone's voice convincingly using just 3 seconds of audio.

- True
- False



Poll Results

Insights and feedback from today's live session.

“Scammers don’t need to hack your systems anymore — they just need to sound like your CEO for thirty seconds.”





What Exactly Is a Deepfake?

A deepfake is AI-generated audio, video, or imagery trained to convincingly imitate a real person — their voice, their face, even their mannerisms. What used to take a Hollywood studio now takes a laptop and a few seconds of sample audio.

One company every FIVE MINUTES is attacked by someone using Deepfakes.

Just 3 seconds of audio can produce an ~85% voice match to the real person (Research by McAfee Labs)

70% of people aren't confident they could tell a cloned voice from the real thing

3

deepfakes the average
person now
encounters online —
every single day.

*Source: 2026 deepfake fraud research
roundups*



The \$25 Million Video Call

What happened: A finance employee in Hong Kong joined a video call with who appeared to be his CFO and several colleagues. Every single participant was an AI-generated deepfake. Believing the call was real, he completed 15 wire transfers totaling roughly \$25.6 million — discovered only after a routine headquarters follow-up. The funds were never recovered.

\$3.05B

Business email compromise losses in 2025, up year over year

86%

of BEC losses moved by wire or ACH transfer — nearly impossible to claw back

22,000+

AI-enabled fraud complaints logged by the FBI in a single year, a brand-new category



Has This Happened to You?

Share what scams have targeted you, your business, or people you know.



Most people think scam awareness means catching bad grammar in a sketchy email. That's useful, but it's not the real unlock anymore.

*"If a request feels urgent, secret, or unusual — that's not an accident.
That's the scam."*

The unlock is realizing scammers now sound right, look right, and know just enough about you to seem completely legitimate. Verification has to move to a second, independent channel — every single time money, credentials, or sensitive data are on the line.



Red Flags to Watch For

-  **Urgency + secrecy** — “Act now,” “don’t tell anyone,” “keep this confidential” — pressure and isolation are the two most reliable scam signals.
-  **An unusual payment method** — Gift cards, wire transfers, cryptocurrency, or payment apps requested out of nowhere, especially for a “boss” or “vendor.”
-  **A sudden channel switch** — An email says to call an unfamiliar number, or a “colleague” moves the conversation from email to text or a new app.
-  **Small mismatches** — A voice that sounds slightly off, video with odd blinking or lag, or a sender domain that’s one letter off from the real one.
-  **A request to skip the process** — Bypassing normal approvals, dual sign-off, or your MSP/IT team “just this once” is exactly when to slow down.



How to Protect Yourself and Your Business

Practical steps to take this week:

Verify on a second channel

Call the person back on a number you already have on file, never the number or link in the suspicious message.

Set a safe word

Agree on a family or company verification phrase for any high-stakes ask involving money, credentials, or secrecy.

Slow down on purpose

Real urgency is rare. Manufactured urgency is the scam's main tool, give yourself permission to pause and check.

Turn on MFA everywhere

Multi-factor authentication stops most account takeovers even when a password or voice sample is compromised.

Report it immediately

Tell your IT/MSP team or bank right away, fast reporting is often the only way to stop or reverse a transfer.

Resources: reportfraud.ftc.gov • ic3.gov • cisa.gov/deepfakes



What's On Your Mind?

Let's open it up: questions, close calls, and the scam texts you almost fell for.



Thank You for Joining Us

Here's to staying sharp, staying skeptical, and staying one step ahead.

Thank you for being with us today.

