



# AI & Deepfake Awareness



Hi there

**Have you ever wondered how easy it would be for someone to impersonate you online?**

With just a single photo and a few seconds of audio, someone can create a convincing digital version of you that's nearly impossible to tell from the real thing. And cybercriminals are already using this technology to target people just like you.

## The New Face of Fraud



### Deepfakes are getting harder to spot 🤖

Today, about 7 out of 10 deepfakes look real enough to fool the average person. That means a video call, a voicemail, or even a short clip online might not be what it seems. Imagine your boss asking you for a wire transfer on Zoom, or a loved one calling you from the hospital in urgent need of money. These situations feel real, but they may actually be a scammer using deepfake technology. That's why it's so important to slow down, double-check, and verify before taking action.

### One photo can become your "digital double" 📸

It doesn't take advanced tools or weeks of work — just one clear photo of you online can be enough to build a realistic talking version of your face. In under an hour, someone could make a deepfake of you giving instructions, resigning from a job, or saying things you'd never say. The photos we casually share on LinkedIn, Instagram, or other platforms can give attackers the keys to impersonate us.

### Just 3 seconds of your voice is enough 🗣️

Your voicemail greeting, a short social media clip, or even a few words captured in the background of a video can be cloned into a voice that sounds exactly like you. From there, a scammer could make "you" authorize a payment, confess to something you didn't do, or damage your reputation. Every public word you've spoken online can be turned into material for fraud.



## How to Protect Yourself

Deepfakes aren't science fiction anymore — they're here. The good news is that awareness is the first step in protecting yourself. Whenever something feels rushed, emotional, or urgent, pause and verify. A real request will wait; a fake one counts on you moving too fast.



### Pause before reacting 🛑

Deepfake scams rely on panic and urgency. If something feels rushed or emotional, stop and give yourself a few minutes to think before responding.

### Request a live interaction 🗣️

Ask the person to do something spontaneous in real-time, like wave their hand, say a random word you choose, or turn their head to show their profile. Deepfakes struggle with unexpected requests.

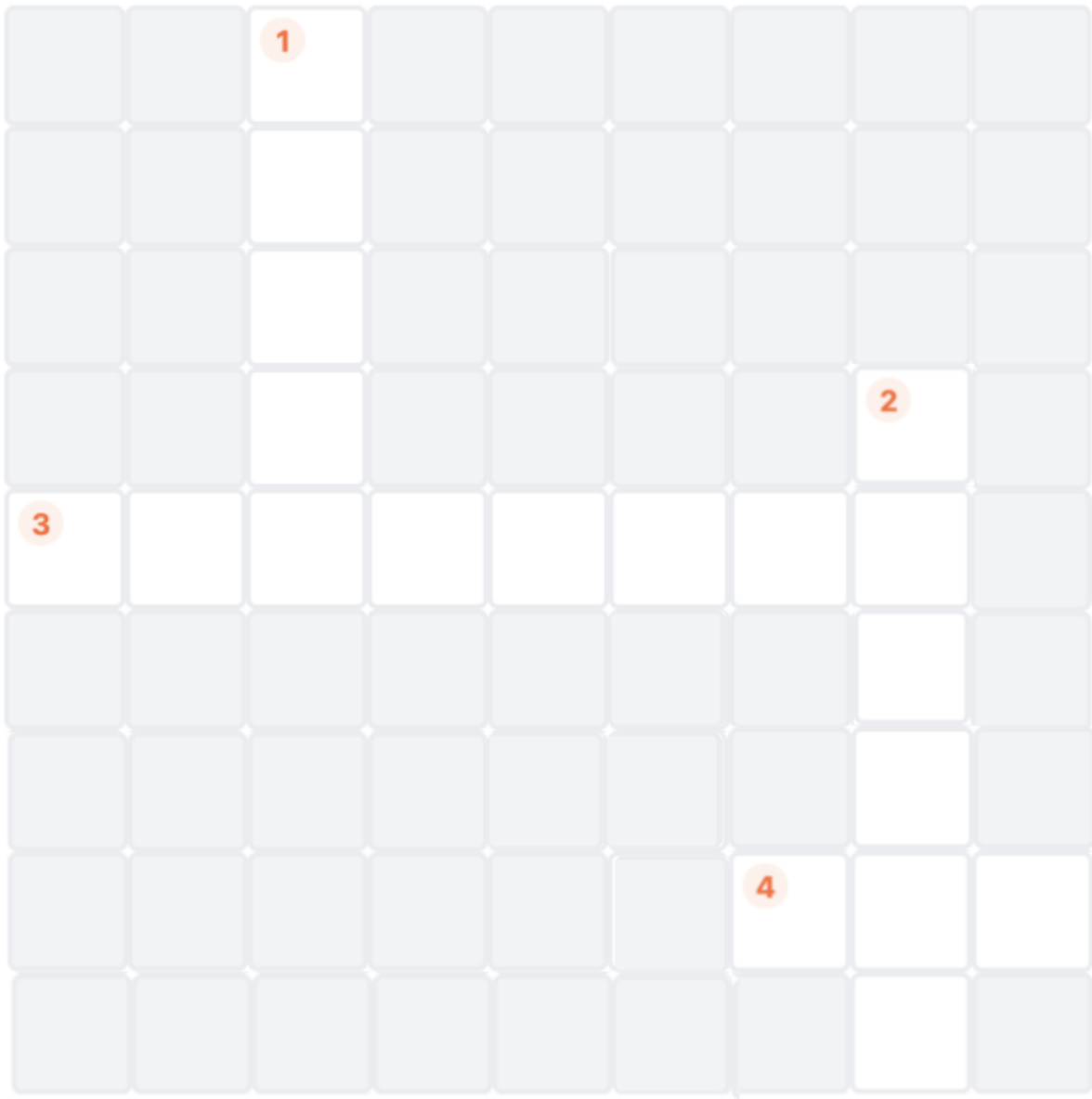
### Verify through another channel 📞

If you get a strange request on Zoom, WhatsApp, or email, confirm it through a different method — like a direct phone call, text, or in-person check. Real people won't mind the extra step.



## Let's Play a Game!

Use the clues below to complete this cybersecurity crossword puzzle.



### Across

- Technology that creates fake but convincing images, voices, or videos
- Extra step you can take to secure accounts (abbreviation)

### Down

- Only a few seconds of this is enough to clone your identity
- Always do this through another channel to confirm strange requests

Answers: 1. Voice, 2. Verify, 3. Deepfake, 4. MFA



As deepfake technology evolves, so must our awareness. Stay curious, stay cautious, and keep learning.

Your organization is partnering with Adaptive Security to offer you industry-leading security training.



902 Broadway, Floor 8  
New York, NY 10010