Avoiding F(AI)kes: *Practices for Verifying Communications With People You Trust*

The Elections Group

It's late on election night. Your phone rings. The caller ID shows an internal office extension. The voice is familiar; it's your boss.

"I know you went home, but the last results file you posted has errors and the press and candidates are at my heels. I'm still at the office with the vendor and we need to fix it now. What's the log-in information?" she asks.

You give it to her – not knowing that the voice you are hearing is generated by an artificial intelligence tool.

AI is an accelerator for many election threats, particularly in the public-facing information environment. However, as the example suggests, AI can be used in new ways to wreak havoc inside an organization if trusted relationships are not verified.

Generative AI tools that can be used to create compelling and conversational impersonations present a new and sophisticated threat. **Developing general awareness, training and internal policies can help secure your systems.**

General Awareness: *Your First Line of Defense*

Talk with employees so they are aware of AI-driven phishing attacks and confident in how to respond.

- ☐ Make sure employees are aware of generative AI (deepfakes, synthetic media, etc.) as a subject matter.

- ☐ Review audio and video examples of impersonations to develop good personal radars of the characteristics of each.
  - ○ Audio may include slurred phrases or unnatural tone and pacing. You can often spot a chatbot simply by engaging in normal conversation, especially if it purports to be someone you know. Chatbots are good at churning out content and facts, but don't converse naturally.
  - ○ Video might include lip movement ("lip flaps") that does not sync perfectly with the audio. Many synthetic videos also do not change their orientation – they only face forward and make only slight movements.

- ☐ Develop instincts to pause before you respond to unusual requests from a familiar voice.
  - ○ Give pause and ask yourself whether a co-worker would normally call and ask for a password.
  - ○ Why would they need sensitive or personal information over the phone, especially if that's not how you normally converse.
  - ○ Consider what information is a person likely to already know – and why they would need to have it repeated to them over the phone.

Possible Authentication Practices

You and your staff still need to be able to speak and exchange information over the phone, text, and video conferencing. Authentication practices are ways to ensure that you are interacting with the actual person presenting themselves online, over the phone, over video chat, etc. Whatever method or methods you deploy, make sure your team is informed of these new protocols.

A simple and effective practice is to establish a "safe" or code word before sharing secure, confidential, or sensitive information with a teammate over the phone or online. Share this safe word in person and then request it during your remote conversations. You can change safe words routinely.

Other authentication practices include:

- ☐ A simple verification method is the call-back method. Callers can misrepresent the phone number from which they are calling. If you are suspicious of the caller, simply terminate the call and call your coworker back at their regular phone number.
- ☐ Use knowledge-based authentication (KBA). Ask staff a personal question only a legitimate person would know. You can also use predetermined security questions established in your office – similar to security questions for online banking.
- ☐ Two-factor authentication works as well with humans as it does with computers. Use authentication apps or send verification codes to staff via text message.
- ☐ Look for behavioral authentication. Voice synthesizers might mimic your voice range, but not necessarily your speech patterns and behavior. Video bots are often very static in their head movements. Ask the caller to raise their hand or make a polite gesture.
- ☐ Using out-of-band authentication. Whatever channel you use to communicate, use something else for verification (email, video conference, text, etc.).
- ☐ Using physical tokens that generate a code the user must provide during the call. In a video call, this can be as simple as having a person hold their employee ID up to the camera – an action current generative AI tools would not be able to produce in real time.

These practices are recommended in the context of sharing secure, confidential, or privileged information. While implementing robust verification policies is critical for security, it's also important to balance these measures with the need for a positive and seamless user experience.

Other Resources:

- ☐ CISA
- ☐ The German Marshall Fund's Alliance for Securing Democracy
- ☐ The Brennan Center for Justice

The Elections Group