How to Spot **AI Voice Scams**

The advancement of artificial intelligence (AI) has created many opportunities for both individuals and organisations, but this technology may also help criminals develop new methods for stealing. AI voice scams are a rising threat and generally entail a perpetrator using software programs to impersonate someone in an attempt to extort another party. Alarmingly, such software is now so sophisticated that 95% of people were unable to tell a fake AI-generated voice from a real one in recent research by software company McAfee.

The CEO of a UK-based energy firm thought they were speaking to the chief executive of a partner company, who asked them to send funds to a supplier over the phone. The AI voice scam was so convincing that the employee transferred approximately £200,000 to criminals, according to the organisation's insurance firm, Euler Hermes Group SA.

Common Types of AI Voice Scams

Bank fraud—Criminals use AI-generated voice clones to impersonate bank representatives to fool victims into sharing sensitive information such as banking details and account passwords.

Social media impersonations—Criminals create fake social media profiles and impersonate celebrities or other well-known individuals to exploit those that interact with fake accounts.

Technical support scams—Criminals impersonate technical support representatives from well-known security organisations to install malware or trick victims into paying for fake "computer fix" services.

Voice phishing—Criminals pretend to be a trusted contact (eg an employee's manager) and trick victims into sharing sensitive information over the phone.

AI-Voice Scam Avoidance Tips

To mitigate the risk of AI-voice scams, share the following tips with employees:

- **Be social media savvy.** Employees should avoid providing scammers with access to voice recordings by adjusting their social media privacy settings. Additionally, they should act cautiously when choosing who to follow online, whether personally or professionally.
- **Ask questions.** Employees should ask suspicious callers questions that only the person they may be impersonating would know the answer to. Additionally, they could consider establishing a code word to use with friends, family and colleagues.
- **Look for inconsistencies.** Employees should consider if the supposed caller is different from how they usually act or uses words they wouldn't normally use.
- **Hang up.** If something doesn't feel right, employees should hang up and phone the caller back on their regular phone number or the one advertised on the company's website.

Contact us today for further cyber-security resources.

RISK SOLUTIONS