CYBER INSIGHTS

Northern Insurance Brokers

NAVACORD®

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.

Specifically, if criminals can find a recording of someone's voice, such as through a video posted on social media, they may be able to "spoof" that person's voice and use it for nefarious purposes. Alarmingly, fraudsters may need just three seconds of audio to mimic their victim's voice.

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 impressions - 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 pose as your company's technical support, claiming your computer has issues. They offer a remote solution, pretending to conduct diagnostic tests.

Voice phishing - Criminals pretend to be a trusted contact (e.g., 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 co-workers.
- **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.

If you have questions specific to your business, or would like additional information, please reach out to your Northern Insurance Advisor.

LET US HELP YOU MANAGE YOUR RISK

Sault Ste. Marie
Sudbury

northernins.ca
contact@northernins.ca
1.888.525.4662