

## 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** - 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.

**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** - Criminals pretend to be a trusted contact (e.g., an employee's manager) and trick victims into sharing sensitive information over the phone.
- **Ask questions** - Criminals pretend to be a trusted contact (e.g., an employee's manager) and trick victims into sharing sensitive information over the phone.
- **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** - Criminals pretend to be a trusted contact (e.g., an employee's manager) and trick victims into sharing sensitive information over the phone.

---

**If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.**

---

™@Local Touch. National Strength. Navacord and Navacord logo are Trademarks of Navacord. The information contained herein is general in nature and general insurance description only. The information is not intended to be insurance advice; nor does it amend, modify or supplement any insurance policy. Consult your actual policy or your broker for details regarding terms, conditions, coverage, exclusions, products, services and programs which may be available to you.

**LET US HELP YOU  
MANAGE YOUR RISK**

Edmonton: 1.800.665.5243  
Calgary: 1.866.845.8330  
Kelowna: 1.800.665.5243

lloydsadd.com  
info@lloydsadd.com