CYBER INSIGHTS

LloydSadd INSURANCE BROKERS

NAVACORD®

Tips for Avoiding Vishing Scams

Cybercriminals are constantly developing new techniques to target and attack unsuspecting victims. One of these more recent methods is voice phishing, more commonly known as "vishing."

With these attacks, scammers will use fraudulent phone numbers to impersonate institutions and people of authority—such as financial establishments, government organizations, corporate executives or technical support personnel—to convince victims to share personal and sensitive information, such as PINs, social insurance numbers, credit card information or account passwords.

It is critical for organizations and their employees to understand how to avoid falling victim to these types of scams because they could result in company information being stolen. Share the following cybersecurity tips with employees to help them detect and avoid vishing scams:

- **Be suspicious of callers requesting private information.** Instruct employees to never give out personal information such as usernames, passwords or banking details. Even if they are reasonably certain of the legitimacy of the caller, they should double-check by asking for a contact name and reach out to the organization using an official channel, such as the phone number listed on its website.
- **Practise caution when receiving calls from unknown numbers.** Employees should be hesitant to answer calls from unknown numbers. Instead, they should let these calls go to voicemail.
- **Understand scare tactics.** Vishing scammers will often use fear to get victims to react. For example, they may say an account has been hacked and a password is needed to verify their identity. Inform employees of these tricks so they can avoid falling victim to them.
- **Listen for audio quality.** One way to notice a spam caller is by paying attention to the audio quality. If the caller's tone is robotic or has an unnatural speech pattern, encourage employees to hang up.
- **Use spam protection features.** Many phone brands and network providers offer built-in anti-spam features that can filter, block and report unwanted calls. Employees can look into setting up this protection on their personal devices.

Employees often have access to sensitive data, making them vulnerable to vishing. However, ensuring they know how to take the proper precautions can help keep their information secure.

If you have questions specific to your business, or would like additional information on vishing scams, please reach out to your local advisor.