Cyber-risks and Liabilities

July/August 2023

Tips for Avoiding Vishing Scams

Cyber-criminals 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 organisations, corporate executives or technical support personnel—to convince victims to share personal and sensitive information, such as National Insurance numbers, credit card information or account passwords.

It is critical for organisations 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 cyber-security 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 name and contacting the organisation 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 information secure.

Managing Supply Chain Risks

It's common to rely on multiple service providers to do business. However, a complex supply chain can substantially increase cyber-risk. Specifically, just one vulnerability within a supply chain could allow a cyber-criminal to gain access to a whole host of organisations. In fact, thousands of organisations—including British Airways, healthcare company Boots and the BBC—suffered a data breach after a file transfer system within their supply chain was compromised in June 2023. Yet only 13% of businesses review the risks posed by their immediate suppliers, and even less (8%) scrutinise their wider supply chain, according to the government's 2023 Cyber Security Breaches Survey.

To help address this gap, the National Cyber Security Centre (NCSC) has released two free e-learning packages relating to supply chain management, as follows:

- **Module 1: Mapping your supply chain risk**—This e-learning module explores the what, why and how of supply chain mapping to help organisations improve their cyber-security.
- **Module 2: Gaining confidence in your supply chain**—This e-learning module describes the practical steps that organisations can take as they review their supply chain.

For further information, visit the NCSC website.

Protect Your Organisation Against Malware

One of the most prevalent types of cyber-crimes comes from malicious software, more commonly known as malware. Malware can exist in many forms, such as ransomware, spyware and viruses. Once malware infiltrates a device or system, cyber-criminals can gain access to critical information. For instance, Royal Mail fell victim to a ransomware attack in January 2023 after hackers encrypted Royal Mail's international export systems and demanded a huge ransom payment in exchange for the decryption key. The attack resulted in severe disruption to international export services and significant consumer delays.

To avoid a similar fate, protecting your organisation against malware is vital. Consider the following tips for doing so:

- Frequently back up data and devices.
- Utilise antivirus, anti-malware and anti-phishing software.
- Use a firewall on company devices.
- Keep company software up to date.
- Train employees to be cautious about downloading any files or attachments.
- Use an ad blocker.
- Try to avoid using public Wi-Fi when travelling.
- Turn off Wi-Fi, GPS and Bluetooth settings when they are not being used.
- Be wary of emails and text messages containing links.
- Never share personal information, such as any security question answers, that hackers could use to access accounts.
- Purchase robust cyber-liability insurance to cover the cost of malware attacks or other losses incurred from breaches.

Although malware and other cyber-attacks are a constant threat, by ensuring you have sufficient cover and the necessary risk-mitigation tools, you can go a long way in protecting your organisation from these and other perils.

Contact us today for further guidance and insurance solutions.