Cyber-risks and Liabilities

May/June 2022

Spotting and Reporting Phishing Attacks

A phishing incident is a type of social engineering attack that involves a cyber-criminal using scam emails, text messages or phone calls to deceive a victim. Phishing attacks exploit people, aiming to trick individuals into doing the wrong thing, such as clicking a suspicious link that downloads malware or steals personal information. Despite a high level of scam awareness, people still frequently fall victim to phishing incidents. According to the Department for Digital, Culture, Media & Sport, 83 per cent of cyber-security breaches in 2021 stemmed from phishing attacks. As such, it's essential for your organisation to remain vigilant.

A well-trained workforce is the first line of defence against phishing attacks. It's vital that employees don't make themselves an easy target. Remind staff to be careful when sharing personal and company information online, as cyber-criminals can use this information to tailor an attack. Consider creating a digital footprint policy describing what staff can and can't disclose online. Additionally, train staff to spot and report phishing attacks by looking out for the following 'red flags':

- **Urgency**—Messages that ask for immediate responses are often scams designed to pressurise recipients into making quick decisions before fully analysing the facts.

- **Emotion**—Cyber-criminals regularly make false claims of support or use threatening language to instil fear into recipients.

- **Scarcity**—Some scam messages try to lure victims by offering things in short supply (eg deals on expensive goods or services).

- **Current events**—Cyber-criminals may exploit big events or current news stories to make their scams seem more relevant.

- **Authority**—Scammers might claim to be someone official (eg a bank or government worker). Therefore, it's important to carefully check the sender's details on all messages received. Often, a scam message will be sent from a public email domain rather than an official business address. If in doubt, it's best to cross-reference the sender's details against those displayed on the official company website.

No matter how rigorous your phishing training is, employees may still occasionally fall victim to these attacks. Remind staff to immediately report suspicious emails and messages to the IT department. Additionally, adopt a multilayered approach to phishing defences. Organisational measures should include implementing email filtering and blocking mechanisms, utilising two-factor authentication and making sure only supported software and devices are in use.

For more information on phishing attack prevention, contact us today.

MACKAY
Corporate Insurance Brokers

Organisations Urged to Reconsider Russian Technology Risks

The National Cyber Security Centre (NCSC) previously published guidance related to the use of cloud-enabled products when the supply chain includes hostile nation states, such as Russia. Government national security departments were advised to ensure they weren't using Russian products, like Kaspersky antivirus software. The NCSC is expanding this guidance amid the Russian invasion of Ukraine. The following organisations should reconsider the risks involved in using Russian software:

- Public sector organisations not covered by the original 2017 NCSC guidance
- Organisations providing services to Ukraine
- High-profile organisations that—if compromised—could represent a public relations 'win' for Russia
- Organisations providing services related to critical national infrastructure
- Organisations doing work that could be seen as being counter to Russia's interests, making them retaliatory targets

Furthermore, because the Ukraine invasion has increased cyber-threats in general, the NCSC recommends that all organisations ensure they have the fundamentals of cyber-security in place to protect their devices, networks and systems.

For more information, visit the NCSC website.

Safe Disposal of Hardware and Devices

Failing to securely dispose of IT hardware could result in sensitive information falling into the hands of cyber-criminals. Hardware and devices are likely to retain sensitive data, even when powered down. Therefore, it's vital for your organisation to carefully consider how best to decommission or dispose of IT equipment. The chosen method will depend on how sensitive the data is and whether the hardware needs reusing. Consider the following disposal options:

- **Leverage physical destruction**. When media is physically destroyed, the data contained won't be recoverable without using advanced equipment. Before destruction, determine whether removing the media will invalidate any warranty on the device itself. Remember, if you wish to reuse the device, you will need to replace the destroyed media with a new storage facility.
- **Utilise deletion software.** Software can be used to overwrite data, allowing the media to be reused once overwritten. It's recommended to overwrite data more than once to ensure success. Consequently, large drives may take a long time to overwrite. Additionally, a full format—erasing files and recreating the data structures and file system—can provide further assurance that data can't be recovered.
- **Restore the device to factory settings.** If a device doesn't have accessible storage media, the device itself may offer a function to 'restore to factory settings'. This will return the device to the state in which it was bought. Before considering this option, check with the device manufacturer to decide whether it's sufficiently secure for your needs.
- **Send the device to a specialist.** If the stored data on a device is sensitive, consider using a specialist. There are many organisations that will securely delete data from a range of devices and media types. However, be sure to perform a 'restore to factory settings' reset before sending your device. This will provide a degree of protection prior to the specialist's more detailed deletion.
- **Don't forget about cloud data.** Securely deleting data from the cloud or other remote storage services cannot be achieved with overwriting software. Contact your cloud provider to check how this data can be deleted securely.

Finally, don't disregard faulty devices. Even if a device won't turn on, the data can still be retrieved. Dispose of faulty devices just as carefully as those that work correctly.

For more cyber-security tips, contact us today.

The content of this publication is of general interest and is not intended to apply to specific circumstances or jurisdiction. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice from their own legal counsel. Further, the law may have changed since first publication and the reader is cautioned accordingly.