Cyber-risks and Liabilities

March/April 2022

A Rising Security Threat: Malvertising

Malvertising—or malicious advertising—is a relatively new cyber-attack technique. The term comes from a combination of ‘malware’ and ‘advertising’. Cyber-criminals embed malware into the advertisements (ads) of well-known online publications. Trusting these legitimate sites, internet users load the webpage or click on the ad, allowing malware to be downloaded onto their device.

Recent attacks have occurred on high-profile websites such as The London Stock Exchange and Spotify, and it’s easy to see why. With millions of ads distributed daily, it’s difficult for organisations to vet each one. Therefore, website publishers must take steps to reduce the risk of malvertising. Consider these tips:

- **Review ad networks**—Before signing up for ads, inquire about their ad delivery paths and data security practices. Use trusted networks that have adequate malvertising prevention measures in place.

- **Run regular malware scans**—Don’t rely on your overall network security. Take additional security measures by running regular scans to ensure your website is malware-free.

- **Keep software up to date**—New vulnerabilities in website software are regularly uncovered, so it’s essential to check that your website is up to date and fully supported. Upgrade or apply service patches as soon as an update is received.

Additionally, employers and all website users should take steps to protect themselves:

- **Invest in an antivirus program**—A trustworthy antivirus program can go a long way in reducing your chances of encountering a malvertising attack. Once installed, remember to update your antivirus software often.

- **Turn on click-to-play plugin**—Through selecting the ‘click to play’ option in your browser, online content that requires plugins to play (eg Java, Adobe Reader) will be disabled unless manually allowed. This helps protect you from having a fraudulent website play content automatically and gives you more control.

- **Install an ad blocker**—By installing an ad blocker, you can prevent most malvertising attacks by ensuring that ads aren’t displayed in the first place. Be aware that some websites may not run properly when an ad blocker is enabled. However, you can choose to allow online ads from certain sites once you’ve properly examined the cyber-risk.

For more information on malvertising, contact us today.

MACKAY
Corporate Insurance Brokers

Password Security Tips

The National Crime Agency has recently recovered a database of 225 million login credentials from cyber-criminals, sharing the hacked passwords with the Have I Been Pwned (HIBP) security project. It's sensible for organisations to regularly check the HIBP website to see whether passwords have been compromised. Additionally, consider these tips:

- **Use strong passwords**. Employees should create passwords at least eight characters long, using a combination of upper- and lower-case letters, symbols and numbers. Passwords should be easy to remember but difficult to guess. A good rule of thumb is to make sure that somebody who knows the user well couldn't guess their password in 20 attempts.
- **Avoid reusing passwords**. Passwords shouldn't be reused, especially for more sensitive systems. For less important accounts, employers may wish to use a password manager tool, which creates and manages passwords in one system, helping to prevent 'password overload' in employees.
- **Be secure.** Ensure passwords aren't written down, shared with others or sent by email.

Additionally, organisations should consider implementing failed-login monitoring and account-lockout mechanisms to counteract brute force attacks.

For more information on password security, contact us today.

Combatting Social Engineering

Social engineering encompasses a broad range of activities to trick users into giving away sensitive information or making mistakes. Rather than looking for a software vulnerability, cyber-criminals exploit human vulnerabilities instead. According to a report by security firm Barracuda Network, an organisation is targeted by 700 social engineering attacks each year, on average. Types of attacks include:

- **Phishing**. Phishing attacks often involve an email or text message pretending to be from a trusted source asking for information (eg an email, supposedly from the bank, asking for security details).
- **Pretexting**. Criminals use pretext to gain attention before they discharge their cyber-attack (eg an internet survey that hooks the reader and then proceeds to ask for personal information).
- **Quid pro quo.** Criminals rely on people's sense of reciprocity, with attacks offering something in exchange for information (eg a cyber-criminal offering to urgently update a supposed security problem with the victim's software, pressuring the victim to act).

It's vital for organisations to know how to prevent social engineering attacks. Consider these tips:

- **Instil a positive security culture**. If an organisation falls victim to a social engineering attack, it must be quickly contained. Foster a culture where staff are encouraged to report incidents immediately.
- **Be suspicious.** Remind staff to always act with caution. It's essential to be suspicious of unsolicited communications and unknown people and to check whether emails have genuinely come from their stated recipient. Additionally, employees must think carefully before providing any sensitive information.
- **Train staff on social triggers.** Train staff on the tactics cyber-criminals use, including masquerading as trusted entities and creating a false sense of urgency to confuse victims.
- **Test training effectiveness.** Once staff have been trained, consider conducting a simulated phishing attack. The results will indicate who needs additional training and give a better analysis of cyber-risk.
- **Implement cyber-security measures.** Review technological cyber-security measures. These could include antivirus and anti-malware programs, regular software updates and penetration testing. Additionally, consider making two-factor authentication—requiring two forms of credentials—mandatory for staff to access services. This will create an additional layer of security against cyber-attacks.

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.