Succeed with Social Media

Brought to you by Crendon Insurance Brokers Ltd

Social Media Security

While the advantages of allowing access to social media sites outweigh the potential hazards for most organisations, social media use does pose a number of security risks for your company. Read on for a list of the most common risks associated with social media use and how to prevent compromising your organisation’s security.

Mobile Applications

Risk: As smartphones and other mobile devices become more prevalent, the number of people who access social media on their mobile devices is expected to grow greatly. This brings unique challenges to organisations that issue company phones or allow employee phones to connect to their wireless networks.

Mobile devices are susceptible to attacks from malicious downloaded applications (apps) and if the phone has access to your network, your company’s security could be at risk.

How to prevent it: Instituting a policy that bans employees from downloading any third-party apps on company phones may lower your exposure, but it may also negate most of the advantages of supplying your employees with smartphones. Alternatively, you could provide a list of pre-approved apps that employees are allowed to download to their employer-supplied smartphones and to approve more upon request.

You may also wish to implement a policy that prohibits employees from accessing your company’s wireless network with their personal smartphones, as it could cause a breach in security. Another option is to create a separate wireless network that is intended specifically for employee smartphone use. This will allow employees to use their smartphones as they choose without placing your organisation’s other networks at risk.

> ‘
>
> **Social media use can pose a number of security risks for your organisation.**
>
> ’

Social Engineering

Risk: Email has long been a favoured medium for scam artists to steal people’s identity or money. Now many of these con artists are setting up false social media accounts and targeting individuals they think will give them the personal or corporate information required to exploit employees or employers.

New research suggests that individuals are far more likely to trust a person who contacts them on a social networking site rather than through email. This poses a threat for many organisations as there have been incidents where employees are

The content of this document is of general interest and is not intended to apply to specific circumstances. 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. Further, laws may have changed since first publication and the reader is cautioned accordingly.

Crendon Insurance Brokers

tricked into offering up propriety information, trade secrets or access to company networks.

How to prevent it: Employee education is essential for thwarting any social engineering attempt. Do not assume that all employees know better than to give up the username or password to their accounts until the requestor provides sufficient credentials. Offer in-depth IT training and keep employees informed of the latest scams and phishing attempts.

Social Networking Sites

Risk: While social networking sites such as Facebook®, Twitter™, Google+ and LinkedIn are all secure sites, any third-party content contained on those sites has the potential to contain malicious software. Every link, application or advertisement could breach your security if accessed on a computer connected to your organisation's network.

Due to link-shortening services, which are especially popular on Twitter, it is not always clear where a link is taking you. These condensed links can direct employees to malicious Internet sites that extract personal and corporate data.

How to prevent it: Employee education is the best defence against these types of attacks. During IT training, be sure to teach employees not to use applications, such as games, on any social media site or to click on advertisements while on a work computer.

Also consider introducing your employees to a URL decoder that can expand shortened links. This will allow them to see where the link will take them before they click on it.

> ‘
>
> **Social networking sites are secure, but third-party content is not.**
>
> ’

Other Preventive Steps

Here are a few other tips to prevent a security breach:

- If you don't have one already, develop a social media policy.
- Tell employees to utilise the security functions of social networking sites to their fullest extent. This may prevent their accounts from getting hacked and protect the organisation by extension.
- Protecting your office's digital security is a priority, but make sure this protection extends to those employees outside the office. Those working from home need to be informed about digital threats and to take similar steps to protect their home networks.