ARE YOU CYBER AWARE?

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Manyani Maseko | June 7, 2017

Take a moment to consider these 2 important questions:

1. How many time have you brought your own device to work and connected it to the server?
2. How many times have you taken your work devices home and connected them to your personal Wi-Fi?

If the answer is "*one time too many*", then I suggest you pay careful attention to this article. With the upsurge of cyber-attacks globally, it is crucial for all employees in a business to be fully aware of what a cyber-attack actually entails.

Cyber-attacks refer to malicious attacks by hackers which usually originate from an anonymous source which aims to alter, steal, damage and/or destroy a computer network or system. These attacks may exist in a variety of forms such as: phishing emails, spam, ransomware, malware, trojan horses etc. Just like day to day criminals, cyber criminals will look to attack the weakest areas of your business. You may think "*well that doesn't apply to my business, as I have installed a state of the art firewall*". However, it may not be your system that lets you down but rather your employees if they are not cyber aware.

The easiest method for cyber criminals to gain access to a network is usually through a phishing scam. Phishing is basically a fancy word for the attempts made by hackers to acquire sensitive information (Eg passwords, usernames and bank details) for malicious reasons, by disguising themselves as a trustworthy source in electronic communication.

Employees who are unaware of the true nature of a phishing email may accidentally click on the links provided in such email which only allows cyber criminals to delve deeper into an organisations business activities including any sensitive information. It is therefore imperative that all employees are trained in cyber awareness to avoid any potential damage to a business. This brings me back to my initial questions. Employees who connect their personal devices to their organisation's systems and/or take their organisation's devices home to connect to their personal hotspots run the risk of falling prey to a cyber-attack. Any device or system which is or is likely to be compromised due to cyber-attack will only give cyber criminals free access to your most sensitive information. This will not only be detrimental to a business in the monetary sense but from a reputational stance as well, if

made known to the public.

Intense training at all employee levels is therefore required by any organisation that wishes to protect its business from any cyber-attack. This could include:

- making sure that they are aware of the various types of cyber-attacks out there;
- ensuring that they understand the basis of a firewall and any anti-virus software installed on their devices;
- educating them on the various forms of security to use when conducting any activity related to work on their device or personal devices; and
- monitoring them to ensure that they are continuously vigilant of any possible cyber related threats.

So ultimately, the question that you should always remain is – ARE YOU CYBER AWARE?