Cyber Security for Home Workers

The global increase in cyber attacks during the COVID19 epidemic is well reported and with a significant population working from home for the first time, companies and their data are increasingly vulnerable to threats. Cyber attacks cost companies money, market share, and reputation and can be especially damaging during times of crisis. We are already seeing in the media that cyber criminals are using the crisis to target home-workers. Here are some tips from us on how you can better protect your data from home.

Advice for Employees:

- Secure your home Wi-Fi Network:
  - Change the default password for you home wireless router
  - Ensure your wireless network is password protected
  - Ensure your router's firmware is up to date
  - https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

- Where at all possible, only conduct work on company devices and do not transfer business or customer data through your own devices.

- Ensure all internet-facing devices have the most current updates and patches installed. This includes personal mobile devices, laptops and desktop as well as any smart home devices (personal assistants, appliances, etc.)

- Be wary of malicious emails and websites; Do not click on links or open attachments in emails from untrusted senders.

- Carefully inspect any new URL before visiting: If in doubt, use an online URL checker before connecting such as https://isitphishing.org

- If you suspect you may have inadvertently opened a malicious email attachment, or otherwise been the victim of a cyber attack, notify your employer immediately.

- Help raise awareness of others in your household and encourage them to educate and protect themselves against cyber risk.

- Use unique passwords for all your work and personal services; A reputable password manager can be used to manage this job for you.

- Adhere to standard privacy controls at home as if you were in the office e.g. lock the screen when away from your desk.

- Regularly visit https://haveibeenpwned.com and check if any of your email addresses have been involved in a known cyber breach

- Only use software and apps sanctioned by your employer. Based on recent media reports with concerns relating to Zoom app, we recommend you use only approved Video Conference apps and software.

Advice for Employers:

- Provide additional *information security training* to your employees including how to recognise malicious emails and report suspected or identified incidents or breaches. Off-the-shelf training packages are readily available and can be purchased from third-party vendors. Consider making this training freely available to others within your employees' households as they will usually be operating from the same network and could inadvertently support a breach.

- Make it safe and easy for employees to report breaches without fear of punishment; Mistakes happen and are best managed through targeted training and support

- Remote access to company networks should only be provided via a *secure VPN connection*

- *Two-factor or multi-factor authentication* should be deployed as an additional security layer when users attempt to access the company network

- Employee devices should be equipped with a corporate *Mobile Device Management* solution to enforce appropriate security controls and securely house and encrypt sensitive information such as company files and emails.

- Implement additional network monitoring and consider *Anomalous Activity Tracking Software.* Where these are already present, ensure they are appropriately calibrated for your newly dispersed workforce

- Carefully risk assess any new software before approving installation. There may be a temptation to rush the process in order to have your staff operating remotely as quickly as possible, however poorly designed or maintained software can introduce new vulnerabilities. For instance, recent media scrutiny about Zoom Video Conferencing app seem to have merit, and this app should be avoided due to privacy concerns.

Cyber Security Self-Assessment

- Download the Zurich Risk Advisor app and complete the cyber risk self-assessment module for your business https://www.zurich.com.au/general-insurance-for-business/products/risk-management-tools/zurich-risk-advisor.html