CYBER SECURITY ESSENTIALS FOR WORKING REMOTELY

GUIDANCE FOR PUBLIC PRACTITIONERS IN AUSTRALIA

This document provides cyber security guidance for members, and their clients, in light of the COVID-19 pandemic. Now more than ever its important to incorporate cyber security measures into your contingency planning and every day work practices as more people start to work from home, and the use of remote access technology increases. Below are the top 8 tips for keeping your data and systems safe and secure:

1. Good password security

Secure devices with good password hygiene and encryption on laptops. Strong passwords will not only protect your devices and systems being accessed if a mobile or laptop is lost or stolen, they also protect your business from hackers. Good password hygiene includes using long passwords with multi-characters and unique passwords for different systems and logins.

You can use a tool like a password manager to help you create and remember all your different passwords. Solutions such as LastPass provide a very flexible way of managing your passwords safely. Or a tip to remember passwords is to choose song lyrics and use the first letter of each word in the line. This way you can remember long strings of letters with ease. You could also try this with movie quotes or lines from poetry.

You may also wish to consider implementing multi-factor authentication (MFA) to improve security for employees working at home.

2. Keep mobile devices and laptops safe

Lost and stolen mobile devices and laptops are easy pickings for cyber criminals. The first line of defence is to look after these business assets: keep them secure and never leave them in cars etc. To give employees a chance of securing and recovering lost mobiles or tablets switch on the “Find My Device” mode.

3. Ensure up-to-date security protection is in place

Any devices that are owned by the business should be properly protected with antivirus, web filtering, firewalls, device encryption and other preventative software.

A virtual private network (VPN) allows you to create a secure connection to another network over the internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more. When you connect to a VPN, you usually launch a VPN client on your computer (or click a link on a special website), log in with your credentials, and your computer exchanges trusted keys with a remote server. Once both computers have verified each other as authentic, all your internet communication is encrypted and secured from eavesdropping.

If staff are using their own devices for remote working ensure that their systems, including VPN and firewalls, are up to date with the most recent security patches.

Your data security policy will need to either restrict staff from using their own devices for business critical activities, provide secure business-owned devices, or make personal data security protection as described above mandatory.

4. Be aware of cyber crime

Ensure all your staff are aware of cyber security and beware of COVID-19 themed phishing emails. Cybercriminals are exploiting the coronavirus outbreak using fake emails, scam messages and fake websites. They are pretending to represent people of authority and impersonating governments, health organisations, accountants and IT support providers.

The message may ask you to open a link to a new policy related to the coronavirus. If the link is opened, you may put your device at risk. Look for signs of a phishing email such as the email address, unexpected urgency or poor language and avoid clicking on any suspicious links.

Staff should be aware of cyber threats like phishing emails as well as information that should not be communicated in an email such as logins and passwords.

5. Use secure WiFi

Don't trust public or free WiFi, it can be vulnerable to malicious attack. Although this shouldn't be an issue if staff are working from home on a secure network, your data security policy should stipulate that employees should not use public WiFi for any sensitive, business critical activities.

6. Email encryption

Email is one of the most used digital technology by staff members working remotely and can open a backdoor to cyber criminals. Encryption and stringent management of business emails is essential. The installation of email encryption software can help but raising awareness of the vulnerabilities of email is important.

Check if your email provider supports email encryption or a method for your email client to be encrypted to protection the contents of your communications.

7. Negligence and accidental risks in the home

Even when your employees are working from home using your secure VPN, or remote desktop, there can be other risks that need to be considered. For example, cats have a habit of jumping on computer keyboards and young children might press a few keys when a laptop is unattended. Always screen lock when you step away from your computer or turn off your devices.

8. Assess risks & Update Policies

The final step for managing security and remote workers is to understand where your business is at risk. These risks should be communicated across the organisation so that all employees understand how their actions may compromise security and what steps they must take to protect company networks and systems.

Data security policies need to include the specific risks associated with remote working and put processes in place for working away from the office. The policy will also need to explain what actions need to take place if a remote worker believes they have exposed the business to a data security attack.

OTHER RESOURCES

- Podcast - Data security in the age of working from home
- Article - Password Protection in the Cloud Accounting Era
- Article- Top 5 Internet Security Software Packages
- Article - Improve Your Data Security and Keep the Hackers Out
- Article - Why Even Small Practices are Cyber Crime Targets
- Recorded webinar - Privacy, Data Breaches and Cyber Security
- Website – Stay Smart Online

NOTE: The information in this document is current as at 6 April 2020. However given the ongoing and uncertain nature of the COVID-19 pandemic, it is recommended that members use this document as a guide only. This publication covers technical and security issues in a general way. It is intended for information purposes only and should not be regarded as professional advice. Further advice should be obtained before taking action on any issue dealt with in this publication.