Tips for Businesses to be Cyber Aware

COVID-19 gov.ky/coronavirus

STAY HOME CAYMAN SAVE LIVES

There has been a significant upsurge in cyber related fraud attempts as cyber attackers seek to take advantage of the chaos caused by the COVD-19 pandemic and the changes that businesses have had to make, particularly around remote working.

All of this means that as well as having to adjust to the new 'norms' arising from the COVD-19, businesses should also consider practical measures to protect and safeguard their digital platforms, online services and remote workers.

We have set out below, some "top tips" and practical guidance for businesses to implement at this time.

Regularly Backup Data
Ensure that you have a regular regime for backing up your data. This function is normally carried out by an IT person, but if you do not have such a resource, the most practical way of doing this is to copy the data onto a secure (password protected) external drive and to store in a safe or lockable cupboard. The frequency of taking backup, will depend on how critical the data is and the frequency by which the data changes.

Watch out "COVD-19" Fake Websites
Always be vigilant for fake websites that have been designed to give the impression that they are legitimate sources of information. Cyber attackers will use these fake websites to spread malicious software to compromise your computer. Remember to check the website address carefully for misspellings and oddly-placed letters or numbers. Always use a search engine to find official sources of information.

Watch out for Phishing Emails
Phishing emails have increased as cyber-attackers seek to exploit home-working at this time. Phishing emails are sent to encourage and persuade to compromise your personal or organisation's security by asking you to reveal passwords, personal information, and financial information, to transfer funds, to visit or click on malicious links or open malicious files. Always be suspicious of emails that ask for your personal information. Check the sender's email address. Is it exactly the same as the company's email address or similar? Look for bad spelling and grammar in the text of the email. If you are unsure, use a search engine to find the organisation to check the email address and telephone number.

Be Cautious when clicking on Email Attachments
You will need to be cautious, before opening Email attachments or clicking on Links from unknown persons or when it is unexpected. Cyber attackers often create PDF files, Word documents, Links containing Malicious and harmful software. Clicking on the attachment is likely to result in malicious software, being executed to run on your computers. From there it can spread to other computers on our network.

Ensure Computer Software is updated
Software vendors regularly release software updates to resolve security and other vulnerabilities. It is important that you ensure that the software on your computers are promptly updated with the latest vendor releases. If your software is out of date, it will not have the latest security patches and will be vulnerable to cyber-attack.

Secure use of Wi-Fi
Be cautious of using public Wi-Fi as there is no guarantee of it being secure, which could mean that whilst you are connected, everything you type into your keyboard goes across an insecure connection. If you have no alternative but to use public Wi-Fi, then you should ensure that you have a Virtual Private Network (VPN) client software installed on your computer for accessing public Wi-Fi. Your home Wi-Fi should always have a password enabled, so that unauthorised persons cannot gain access. You should also check with your Internet Service Provider, that the default password has been changed, if not, ask that they provide you with instructions on how to change this.

Use Strong Passwords and Multi-Factor Authentication
You should ensure that you implement good practice around your use of passwords. You should never use the same password to access your email or online service. The best practice is always use different passwords. The rule of thumb is that the longer the password, the more secure. Your passwords should contain a mixture of letters, words and numbers – always ensuring that it is memorable to you. If multi-factor authentication is available for accessing your email remotely or social media platforms, you should always enable this service. These features make it more difficult for cyber attackers to breach.

Using Video Conferencing
If you are using Zoom or other video conferencing service, you always require your meeting invites to enter a password to join and ensure that you don't have uninvited guests by doing a 'roll-call' of attendees before starting the meeting.

Local IT Provider
If you have a local IT Providers, then you may wish to ask them to support you with implementing these 'Top Tips' and to undertake a quick review and make further specific recommendations.

Always Report Suspicious Cyber or Computer Incidents
You should ensure that your remote working personnel are aware of the importance of reporting security incidents. Ensure you have practical measures in place for ease of reporting and designated responsible persons for leading your response and recovery to cyber security incidents.

Stay Safe, Well and Secure.

MINISTRY OF COMMERCE, PLANNING & INFRASTRUCTURE
CAYMAN ISLANDS GOVERNMENT

DATE: 06 MAY 2020