TASMAN

Cyber Safety

This month we will focus on cyber safety where cyberattacks are known to surge during the festive season especially those easy to guess and re-used passwords that cybercriminals can easily access.

Importance

Effective protection of business information is important to our business, both in the ability to preserve the data of the company and in reducing the risk of the occurrence of negative events and incidents.

Cyber Threats

Below are some of the cyber threats that may pose risk to the business, which our appointed IT provider investigates as part of their service to us.

Phishing – are fake messages trying to trick an individual into giving your financial or personal details. Some of the messages may look real, by using company logos and branding, and linking to authentic website. Phishing messages are common scams that you receive by email, text, message, social media or over the phone.

Pharming – is another common scam where the scammer puts a malicious code on your device that will take you to a fake version of a legitimate website. Pharming is like phishing as criminals rely on fake website and theft of personal details.

Malware – is a malicious software which spreads viruses. Trojans, worms, and spyware through email messages, bogus websites, pop-ups, and infected files. It works by installing software onto your computer, which then allows the cybercriminal to access your files. They can then use your information to authorise purchases on your credit card or open accounts in your name.

Ransomware – is a type of malware, often spread through phishing emails or bad app, which locks your computers content. The victim clicks on a link or downloads a file that allows the cybercriminal to demand a ransom to unlock your computer.

Invoice email scam – this scam involves scammers pretending to be legitimate suppliers advising changes to payment details. You may not realize until your business receives complaints from suppliers that payments did not occur.

Cybersecurity Measures

To prevent cyberattacks, all staff are encouraged to report unusual items to your manager and follow the recommended measures below.

Password requirements – the importance of having unique passwords for different logins and how often it needs to be updated.

Email standards – only open email attachments from trusted contacts and businesses, the importance of deleting and reporting suspicious looking emails and how to block, junk or spam or scam emails.

Handling of sensitive data – the importance of identifying sensitive data and destroying it when it is no longer required, storing physical files in a drawer or lockable cabinet.

Locking computers and devices – locking screens when they are left unattended is needed to be enforced.

Handling of removable devices – restricting the use of removable devices to prevent malware from being installed; and scanning all removable devices for viruses before they are justified to connect to your business systems.

Handling of technology – where employees can access their devices such as business laptop away from the workplace, how to report a theft or loss of the work device.

Summary

The best way to protect yourself and never get your identity stolen is to act now, and never share your personal details over the internet unless it is from a trusted source.

Stay Cyber Safe this Holiday Season!