CYBERCRIME

PROTECT YOUR BUSINESS

As technology evolves, the prevalence of cyber-attacks is growing among businesses. It is important to be vigilant with protecting your business online.

Manage email security and validate potential threats

Look to deter break-ins from opportunity theft by encrypting your business emails and communications. This will force a hacker to fight through another layer of protection, and that generally isn't worth their time when they can steal other information elsewhere without the hassle. Think of email encryption as the equivalent to locking your doors, the theory being that a thief is more likely to look for an unlocked door than bother breaking a window. While you're not entirely secure, every additional roadblock can help protect your information.

Enforce strict password policies

Train employees on the importance of using smarter passwords, which are crucial to upgrading cyber security. Use long passwords. Complex and difficult passwords may seem like a hassle to your employees, but they are vital to your online security. Remove authorities and access from old employees and consider refreshing passwords.

Passwords should never be the same across multiple platforms, and it's best to change them often e.g. every three months at a minimum. In addition, passwords should not be stored in the cloud or on sticky notes around the office. Consider using password management software.

You can further increase the security of your passwords by using two-factor authentication features, when applicable. These features make users enter an additional pin code that can be sent to your mobile device, and some require users to input their fingerprint to grant access, something that is difficult for hackers to replicate. Authentication that uses these extra steps can better secure your online accounts beyond the basic login identification and password requirements.

You should aim to fully understand how these security setting work to leverage the features to best protect your businesses assets and intellectual property.

Further train your employees on the warning signs

Every employee should be trained on understanding the warning signs of a harmful email or phishing scam. Phishing scams are attempts by scammers to trick you into giving out personal information such as your bank account numbers, passwords and credit card numbers. While email providers are continually improving their detection procedures and doing a better job at spotting these potential threats before you receive them, some of the trickier scams can still find their way into your inbox. These emails may be disguised as a trusted client's email or a recognisable brand, but these scams tend to have a few obvious clues.

This factsheet contains general guidelines for increasing security of your business and/or workplace.
No responsibility is accepted for any damage, injury or loss resulting from application of these guidelines.

Some red flags include:

- Emails that ask for personal or credit card information.
- Requests for immediate action regarding unfamiliar situations.
- Emails that include suspicious attachments.

If you think that you have received any of these emails, ask a colleague for another opinion but never forward or reply to the email. Inform your email service provider by reporting each email as spam. Also file a phishing complaint or block the domain from your email settings.

Emails that contain multiple spelling mistakes or suspicious links should also be carefully inspected before proceeding. Sometimes links within an email can appear to be normal but actually prompt an unwanted download where malicious software can be installed; always use caution and consider scanning your emails with a trusted anti-virus.

Protect your data. Take advantage of malware, spyware and firewall software programs

Ensure that each machine in your business has malware, spyware and firewall software installed to help catch and eliminate threats before they become problematic.

There are ways small businesses can better protect themselves or mitigate the potential impact of cyber-attacks;

- Testing your security systems.
- Protecting your network and applications.
- Encrypt sensitive data.
- Protect websites by using a secure communication protocol.

Do business with reputable vendors

Don’t provide a vendor with any financial or personal information before doing your homework. Once you’re sure they are reputable, you can proceed with your interaction. Like in the real World, identity theft is a method which criminals use to access and extort your finances and intellectual property.

This factsheet contains general guidelines for increasing security of your business and/or workplace.
No responsibility is accepted for any damage, injury or loss resulting from application of these guidelines.