QBE

How to protect your business *from cyber crime*

SME Cyber Security Guide

Cyber crime costs Australian businesses an estimated **$29 billion** a year

Source: **Microsoft, 2018**

It's no secret that cyber crime is a growing problem for businesses of all sizes. And with most of us working remotely right now, you might be wondering if your work from home set up is secure. QBE Group Chief Information Security Officer, Andrew Dell shares the simple steps you can take to protect your business regardless of where you and your team are working.

What is cyber crime?

Identity theft and romance scams are common forms of online attacks against individuals – and may spring to mind when you think about cyber crime. For a business however, the threat comes from criminals gaining unauthorised access to systems or data, for financial gain.

7 ways to ramp up your online security

A careless password, out-of-date software running on a computer, or an innocent click on a scam email is all it takes to open the door to a serious data breach. Here are a few simple ways to help secure your business and keep your information safe.

Step 1

Keep your software up-to-date

Cyber criminals often target security holes in outdated software - so making sure all your devices, operating systems, and applications are up-to-date is key.

The notifications that let you know that an update is available for a program shouldn't be ignored. Always click 'update now' or schedule as soon as you can. Lots of devices and applications have an 'auto-update' feature. If it's available, enable it.

It's also a good idea to check all devices manually, to make sure the operating system and application software is the latest version. And don't forget other devices, like network internet routers, may also need to be updated.

Step 2

Use strong and unique passwords with "multi-factor" protection

Most security breaches and cyber-attacks involve stolen or weak passwords. So, it's important to use strong unique passwords, alongside multi-factor protection. A password manager can help you keep track of these securely.

Passwords

Use a strong, different password for each account. A strong password is generally one that has a minimum of 12 characters and isn't easy to guess. To make a password easier to remember, a great idea is to create a 'passphrase' rather than a word. If you can incorporate special characters, even better. Something like '101yellowbottleZonthew@ll!' is easy to remember and hard to crack.

Weak passwords are passwords that can be guessed by a person or computer easily and include names of family members, home addresses, or anything with the word password in it.

Multi-factor protection

It's also a good idea to use multi-factor protection (sometimes known as "two-factor authentication" or 2FA), for accessing your key systems and accounts and to add an extra layer of defence. Using it means that instead of just using a username and password to log into your account, you also need to provide something extra to prove it's you (like a unique code texted to your phone).

Lots of sites and services use it, such as most banks, Google Apps, Office 365 and LinkedIn to name a few.

You can find out more about using 2FA on the government's Stay Smart Online website **here**.

Password managers

A password manager is a software app that you can use to generate strong and unique passwords for your online accounts. It stores them securely so that you don't have to remember each password – just a master one which is protected with 2FA.

There are a number of password manager solutions available, here are just a few:

- Dashlane (Windows, Mac, iOS, Android) – **dashlane.com**
- LastPass (Windows, Mac, iOS, Android) – **lastpass.com**
- KeePass (Windows Mac, Android) – **keepass.info**
- 1Password (Windows, Mac, iOS, Android) – **1Password.com**

Each of these products has a range of features and pricing options, from free to a small annual charge, so it's best to review and chose a solution that best suits your needs.

Step 3
Install anti-virus security software

Viruses, malicious code and spyware can provide cyber criminals with remote access to your devices and keystrokes or can corrupt or delete your files. Installing a strong security software solution on your computer systems can help protect you.

So the software can do its job, make sure it's set up to run automatically when your computer starts and ensure malware scans run daily. By using a security software solution, you're much better protected but remember, these products need to be kept up-to-date in order to stop threats.

There's a huge range of providers to choose from, including big players **Norton** and **McAfee**. For more information on anti-virus software, check out this article from **Stay Smart Online**.

Step 4
Set up a Business VPN

To make sure your employees are the only ones who can access your network and information, it's a good idea to use a business VPN (Virtual Private Network) service.

A business VPN extends your private office network, and secures connectivity using encryption so that it can't be intercepted. It means users can send and receive data across shared or public networks securely, as if their computer devices were directly connected to your private company network. Once again, there are plenty of providers including **NordVPN Teams** and **Perimeter 81**.

Step 5

Educate your staff

Whether you have two employees or 50, it's important to educate them on how to minimise risks, and what to watch out for.

Make sure your employees know how to spot suspicious emails with malicious links or attachments. It's also wise to make sure they know which sites they can visit on their work devices, and the dangers of visiting risky websites like movie sharing, torrents and pirated software sites.

Step 6

Encrypt your data and backup

Encrypting data

Whatever your line of business, protecting your financial and customer data will be a priority. Encryption tools jumble your sensitive data, making it useless to a potential thief. There are plenty of encryption software products on the market.

Some operating systems have encryption tools built in, to protect your local drives:

- **On a PC running Windows 10 Pro**, open 'File Explorer' and right-click the drive you want to encrypt. Then select 'Turn on BitLocker' from the menu that appears.
- **On a Mac, open 'System Preferences'** and click on 'Security and Privacy'. Go to 'FireVault' and turn the setting to ON. Your local firewall can be turned on here too.

Backing up data

Backing up your data securely is critical to keeping your business safe from ransomware attacks (where attackers try to hold information hostage and extort money) and other disastrous events.

To protect your business, identify what your most important data is, and back it up on a regular basis to another location. Put a recurring reminder in your calendar to back up your data religiously, even if it's to a simple 1TB hard drive. In fact, a portable drive stored securely at a different address is a great idea, in case your office is subjected to robbery, fire or a ransomware attack.

There are also a number of **cloud based backup solutions** for small businesses available.

Step 7

Maintain your security hygiene

Just as you maintain your company records, it's important to keep your security measures up-to-date. Do an audit of your IT set up at least every year, to ensure each device is secure. If it's a little out of your depth or you don't have the time, hire an IT specialist.

Simply put, it's all about being sensible, proactive and maintaining the security measures you have in place. By doing so, you dramatically reduce your businesses' chances to falling prey to cyber crime.

And if you're looking for more information on small business cyber protection, you can find more resources from the Australian Government **here**.

Cyber security term glossary

There's a lot of jargon when it comes to cyber security, so here's a glossary of the most common terms.

Botnets – Networks of infected computers that perform tasks without the user's permission

Brandjacking – Fake websites or emails that look like they're from a well-known organisation

Data breach – Where data is copied, transmitted, viewed or stolen by a cyber criminal

Emotet malware – A sophisticated trojan that steals data and loads malware on a device

Firewall – A security barrier between your internal files and the internet that filters traffic

GDPR – The EU General Data Protection Regulation, which businesses need to comply with

Malware – Short for malicious software, which gives hackers remote access to your systems, or causes extensive damage to data and systems

2FA – Second Factor authentication , which provides an additional layer of protection to your accounts

Pharming – A technique that redirects users to websites without them knowing

Phishing – Scam emails containing malicious links or attachments, designed to obtain user credentials, or to install malicious software

Ransomware – A form of malware that locks your computer and files until a ransom is paid (often in cryptocurrency)

Spyware – Another form of malware that records your keystrokes, usernames / passwords, and steals information

SSL – Secure Socket Layer which encrypts internet traffic – a must for eCommerce sites (shown as https:)

Trojan – Malware disguised as legitimate software often used to gain unauthorised access to a system

Virus – Malware that when executed replicates itself by modifying other computer programs and infecting other available systems.

VPN – Virtual Private Network, a way of securing connectivity to your business when working remotely

The advice in this document is general in nature and has been prepared without taking into account your objectives, financial situation or needs. You must decide whether or not it is appropriate, in light of your own circumstances, to act on this advice.

Like to know more?

Read more from QBE about protecting and running your small business here including:

- **Employer guide: Working from home, support for your employees**
- **Employer guide: Your duty of care**
- **Six productivity tips for working as a remote team**

QBE Insurance (Australia) Ltd. All rights reserved. ABN 78 003 191 035 | AFSL 239545.