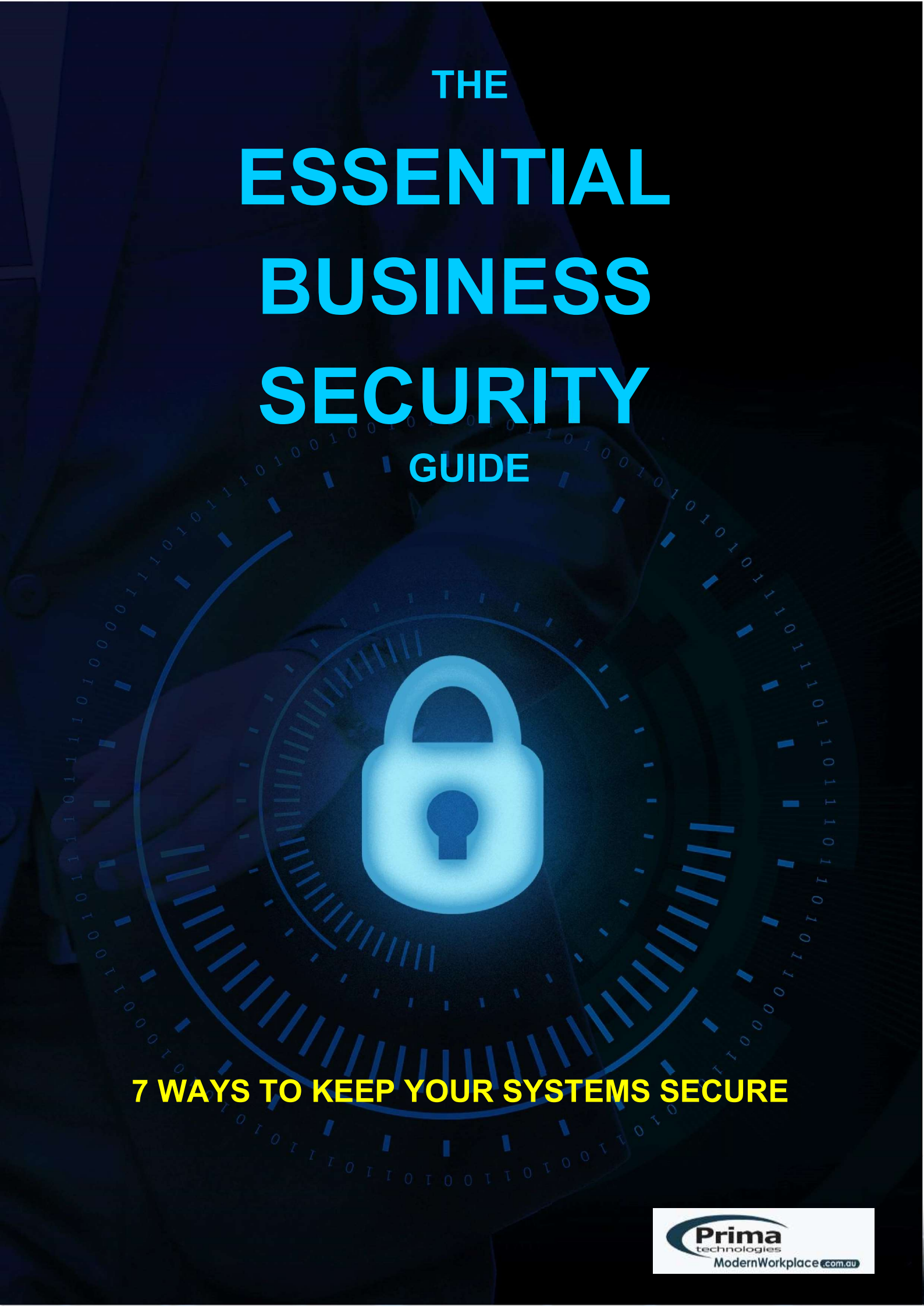
THE ESSENTIAL BUSINESS SECURITY GUIDE



7 WAYS TO KEEP YOUR SYSTEMS SECURE

Prima technologies
ModernWorkplace.com.au

Small Actions Can Make A BIG Difference

Cyber-attacks on your business can be crippling.

While your IT technician can configure strong security for your network, the weakest link is always the individual computer user.
Cybercriminals are constantly seeking ways to trick users into unknowingly giving them access to company data.
Here's some steps that you can take to stay safe.

(SMEs make up 58% of cyber-attack victims (Verizon 2018 report [1])

1. Be A Password Pro

Most people dislike using passwords and tend to choose overly simple ones like ‘password’ or their pet’s name. These short, guessable passwords are easily hacked, and since the user has repeated the same password in many applications and sites, if one of them is hacked then the hacker can access everything else.

Make sure to follow recommended password guidelines:

- At least 8 characters
- Include both upper & lower-case letters, numbers & symbols
- Avoid words that appear in the dictionary

Never write passwords down on a post-it!

The downside is that the passwords become hard to remember! We recommend using a password manager tool to keep secure track of them all.

A good password manager will not only log you in automatically but will also automatically include your second factor authorisation saving you login time and effort.

Go Password-less

Because passwords are inherently insecure there is a push for secure, password-less solutions.
Biometric identification creates a unique identifier that is securely stored locally only on the device that you are using.
Biometric identification such as fingerprint or facial recognition is becoming more common.
Windows Hello in Windows 10 utilises this technology.

Make sure that you use this technology when logging in to Windows by creating a PIN. It's faster than keying your password when logging in and is more secure.

2. MFA Is Not An Option

Because of the massive increase in cybercrime the use of only a login password is getting more and more risky.
It has become critically important to add another factor of identification. Examples are, a pass code sent by text to your phone, a random number generated by your authenticator app or using a physical device such as a Yubi Key.

Some people are put off by the perceived inconvenience of MFA (sometimes called 2FA). However, many apps and portals that provide an MFA option also give you the opportunity to select 'trust this device for xx days'.
When Microsoft 365 is secured by MFA the computer that you are registered on becomes a 'trusted machine', at least for the time that your IT provider has set, and you hardly ever notice that you are protected.

If you are away from your machine for a few minutes, always lock it using the shortcut: Windows Key + L

3. Lock it Down

This keeps all your apps running, all your tasks open, but locks the system until your password or PIN is entered again. Make locking your system a habit, especially in public places and you'll enjoy greater privacy as well as more robust security.

Enable screen saver password protection so that a password (or PIN) is needed to resume your work:

In Windows 10 go to settings, personalisation –

lock screen.

On the right side, scroll down and click on 'screen saver settings'. Select 'On resume, display lock screen'.

4. Be careful with Personal Devices

Remote working is becoming more popular, but with that comes an increased risk as employees connect their personal laptops and phones to the business network.

As they download files and navigate through your systems, it may open up doors for hackers or introduce malware.
Check with IT to ensure that you are complying with BYOD (bring your own device) policies.
If you access Office 365 email on your phone it should be connected correctly to your organisation so that if it is lost or stolen, company data and emails can be remotely wiped.
Download and use the Microsoft Outlook app to be fully compliant.

5. Think About That Click

It's important to be wary of clicking links on webpages or in emails. Quite often cybercriminals will either send 'phishing' emails to gain access to your systems, or spoof legitimate websites. Take a second to hover over links and make sure the link is pointing where it should, and that websites are secure.

Before you click, consider the following:

- Do I know what clicking that link will do?
- Does it look right?
- Do I trust the sender/website?

Many phishing emails and fake websites can be stopped at server level, but when one sneaks through you want to be sure nobody will fall for it.

6. Distrust Unknown Devices

This could be a USB thumb drive you found in the parking lot, abandoned in the drawer or even something handed out at a convention. These harmless looking devices could contain malware. You'd hope your anti-virus would detect it before any damage is done, but history suggests it's not worth the risk. The Iranian nuclear program was sabotaged by a virus called Stuxnet not too long ago after an employee found the USB drive in a parking lot and plugged it in.

7. Be Aware of Security Basics

Does your organisation have written IT policies for staff?

Do you know what to do if a device is lost or stolen?

Do you know if security updates for Microsoft and other software are regularly maintained? (In Windows select ‘settings’, ‘update and security’ to check).

Always ask if you have any doubt about an email.

If you use Microsoft 365, ask your IT provider what the companies security score is. 65% or over is good, if under 35%, they definitely need to fix it fast.

There is a huge increase in dangerous text messages. Stay alert to any message tempting you to tap to find out what that purchase that you didn’t make is all about, or any of the other techniques used to try and trick you.

Prima Technologies

Mount Warren Park
Qld 4207 Australia

Phone: **1300 795105**
Email: **graeme@primatechnologies.com.au**
Web: **primatechnologies.com.au**
Facebook: **facebook.com/primatechnologiesM365**