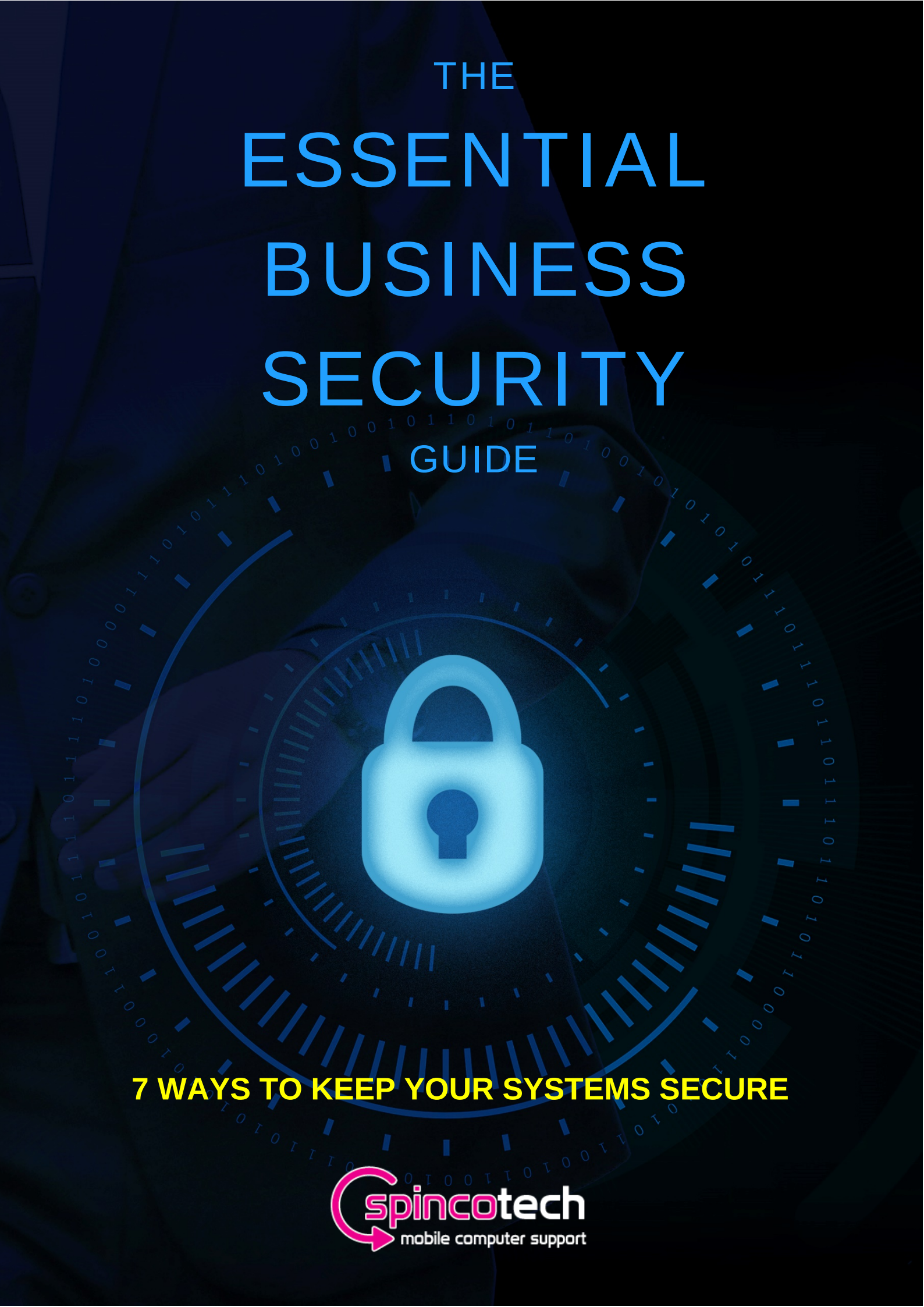
THE ESSENTIAL BUSINESS SECURITY GUIDE



7 WAYS TO KEEP YOUR SYSTEMS SECURE

spincotech
mobile computer support

Preview

Cyber-attacks on your business can be crippling, but there are easy ways to keep the bad guys out. Here are 7 simple changes to your employee routines are extremely effective at reducing the risk of malware or hacking.

Small Actions Can Make A BIG Difference

While having a team of IT professionals standing guard over every piece of micro-data is the dream, it's not exactly realistic. Even large corporations rely on their employees to take small, routine actions to protect against cyber-attack. Fortunately, the best tips are easy to follow and will help you avoid becoming a statistic.

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 all over their accounts, it can mean the hack becomes life-altering.

Make sure to follow recommended password guidelines:

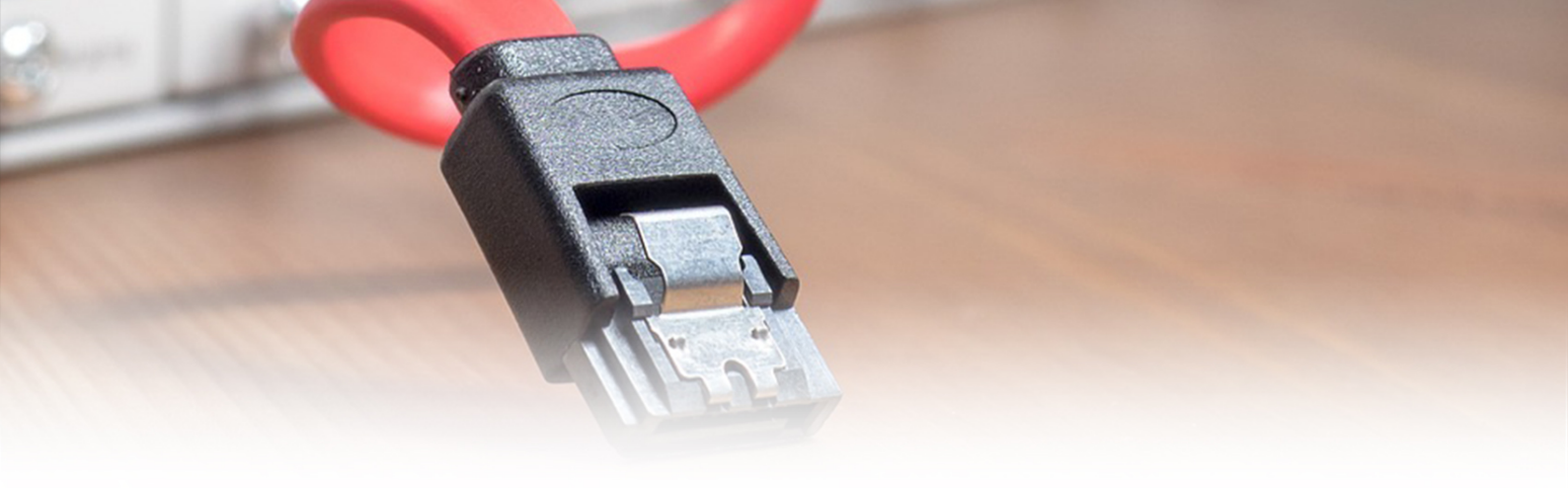
- At least 8 characters
- Include both upper & lower-case letters
- Include numbers
- Include symbols
- Avoid words that appear in the dictionary
- Avoid letters and numbers in sequence.

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

Never write passwords down on a post-it!

2. 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.



3. Be Careful With Your Data

It goes without saying that you should be careful not to share sensitive data, but did you know hackers will often steal an entire computer? It's true. After all, it's so much easier to steal someone's laptop than it is to write a virus. Physically secure your laptops, USB drives, servers etc to make them hard to steal. Place secure locks on your server rooms and ensure any off-site backups are treated like digital gold.

When sensitive data is no longer needed, you should destroy it.

4. Lock it Down

What does a hacker like even more than an easy password? **No** password! Even if you're only away from your machine for a few minutes, always lock it using the shortcut: **Windows Key** + **L**

This keeps all your apps running, all your tasks open, but locks the system until your password 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.

As delays can end up costing thousands, encourage users to report problems as soon as possible. Early detection/attention helps limit damage. Be sure everyone knows how to respond and what actions to take. The simpler the process, the more likely they'll follow it.

5. 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.

6. 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.

7. Heads-up Handling

Simple guidelines can save a lot of problems - make sure everyone knows how to store devices when not in use, and what to do if one is lost or stolen. Also set in place procedures around who is in charge of system updates, patches and updates, and when this maintenance will occur. Quite often the problem can be narrowed down to thinking someone else will take care of devices and that updates happen ‘magically’.

If you would like some help with your business security, to lock down computers and protect you from cyber-attacks, give us a call.

Call us on 07 855 2169.

Phone: (07) 855 2169
Email: help@spincotech.co.nz
Web: www.spincotech.co.nz
Facebook: **facebook.com/spincotechnology**