Get cyber secure

Three quick steps to serenity

Adopt these protections within your business…

Prevention – *Protect your assets*

- **Back-up regularly** to protect against loss.
- **Patch applications** by installing security updates.
- **Use complex passwords** and use two-step authentication.
- **Limit access** to administrator accounts and sensitive information.

Well-being – *Do things safely*

- **Communicate safe practice** and talk about cyber security frequently.
- **Browse safe sites** and ensure your staff do too.
- Only allow **applications you trust** on your computers.

Response – *Report and recover from an attack*

- If you think an attack has happened, **tell staff** and **tell the authorities**.
- **Restore backups** from before the incident.
- Consider cyber insurance.

Familiarise yourself with the ***Stay Smart Online*** guide (www.staysmartonline.gov.au/protect-your-business) for simple tips for protecting your business.

The recommended place to go for a comprehensive list of practical actions to make your computers, networks and systems more secure is the **Australian Signals Directorate's (ASD) *Essential Eight*** (asd.gov.au/infosec/mitigationstrategies.htm) which aim to prevent malware from running, and to limit the extent of incident and recover data.

Report a breach to the **Australian Cybercrime Online Reporting Network (ACORN)** (www.acorn.gov.au).

If a data breach has serious consequences, you may be required to report it to the Australian Information Commissioner, www.oaic.gov.au.

1 It starts at the top

It starts and finishes with people in **management**.

Put at least one person in your business in charge of cyber security. Someone in management with access to your data and assets.

2 Get everyone on board

You need to have **support from everyone** in the business. From top to bottom.

Just like locking your doors each night, make cyber security a day-to-day priority.

3 It's a hands-on effort

There is **no single-fix** for cyber security. You can't solely rely on antivirus software to keep you safe from attacks.

Educate yourself, staff and customers. Encourage staff and customers to report incidents and anything that seems out of place.

4 Know your risks and vulnerabilities

If you **use the internet**, you are **at risk**.

Understand the ways your business can be attacked.

Perform regular checks and audits of your online '*footprint*' so you can prioritise your risks.

5 Protect your business

The right approach for you **depends on your business**, the people in it, and the information you need to protect.

Secure your Point of Sale systems, mobile devices, networks and stored data learn advanced techniques to become cyber secure.

Cyber security is a big problem for small business

This is how it affects your business…

- **Small business is the target of 43% of all cybercrimes.[1]**
- **22% of small businesses that were breached by the 2017 Ransomware attacks were so affected they could not continue operating.[2]**
- **33% of businesses with fewer than 100 employees don't take proactive measures against cyber security breaches.[3]**
- **87% of small businesses believe their business is safe from cyberattacks because they use antivirus software alone.[4]**
- **Cybercrime costs the Australian economy more than $1bn annually.[5]**

Cyberattacks

Know what you are at risk from…

Email phishing

Attempts to trick you by sending hoax emails, getting you to click on a dangerous link, or providing personal or financial information to an unauthorised source.

Malware

Malicious or intrusive software, including viruses, worms, Trojans, ransomware, spyware and adware.

Ransomware

Hijacking your files and locking you out of your system, then ransoming access back to you.

Denial of service

Using a network of computers to send requests to your system and overload it and make it unavailable.

Watering hole attack

Setting up a fake (or compromised) website you are known to go to, then using it to infect visiting users.

The Small Business Cyber Security Best Practice Guide

For more detailed information on how to protect your business, check out our *Cyber Security Best Practice Research Report* at www.asbfeo.gov.au/cybersecurity

Australian Government

Australian Small Business and Family Enterprise Ombudsman

The Small Business Cyber Security Best Practice Guide

Canberra
Level 2
15 Moore Street
Canberra ACT
GPO Box 1791
Canberra City ACT 2601

T 1300 650 460
E info@asbfeo.gov.au

Twitter : @ASBFEO
Facebook: @ASBFEO
LinkedIn: Australian Small Business and Family Enterprise Ombudsman
YouTube : Australian Small Business and Family Enterprise Ombudsman

Written enquiries may be sent to:

Manager
Communications and Marketing
Australian Small Business and Family Enterprise Ombudsman
02 6263 1500
media@asbfeo.gov.au

References

[1] smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html
[2] go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf
[3] www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf https://www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
[4] www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
[5] acumeninsurance.com.au/2017/03/14/cybercrime-costs-the-australian-economy-over-4-5-billion-annually-and-is-now-in-the-top-5-risks-faced-by-businesses/