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.

Speak to a trusted advisor

Whether it's your accountant, your IT specialist, or us, know where to go for more guidance on your risks, vulnerabilities, and how to enhance your security online. Government agencies can provide more information:

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*.

For useful statistics on how cyber security affects small business, the **Australian Cyber Security Centre** (www.acsc.gov.au/publications.html) produces and regularly reviews statistics from cyber security incidents.

Contact the **Computer Emergency Response Team (CERT) Australia** (www.cert.gov.au/advice) to report suspicious activity or if you think you've been attacked.

1 It starts at the top

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

You should put at least one person in your business in charge of cyber security. It should be someone trusted in management with access to assets.

2 Get everyone on board

You need to have complicit **support from everyone** in the business from top to bottom to ensure your actions are employed.

Discuss cyber security regularly. Make it a day-to-day priority, just like locking your doors each night.

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 in the many ways to stay safe online. Encourage staff and customers to report incidents and anything that seems out of place.

4 Know your risks and vulnerabilities

When it comes to cyber-attacks, it's not a matter of if, but when. ***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 nature of the assets you need to protect.

Secure your Point of Sale systems, mobile devices, networks and stored data with recommended actions. Familiarise yourself with more 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]**
- **60% of small businesses who experience a significant cyber breach go out of business within the following 6 months.[2]**
- **22% of small businesses that were breached by the 2017 Ransomware attacks were so affected they could not continue operating.[3]**
- **33% of businesses with fewer than 100 employees don't take proactive measures against cyber security breaches.[4]**
- **87% of small businesses believe their business is safe from cyberattacks because they use antivirus software alone.[5]**
- **Cybercrime costs the Australian economy more than $1bn annually.[6]**

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

References

[1] smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html
[2] Testimony of Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College, before the U.S. House of Representatives Committee on Small Business (Apr. 22, 2015), available at docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00-20150422-SD003-U4.pdf.
[3] go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf
[4] 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
[5] www.myob.com/au/about/news/2017/cloud-security-the-silver-lining-for-smes
[6] 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/