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.

Get everyone on board
You need to have support from everyone in the business. Just like locking your doors each night, make cyber security a day-to-day priority.

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.

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.

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
- Malware
- Ransomware
- Denial of service
- Watering hole attack

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.
