

**CYBERSECURITY ESSENTIALS  
FOR SMALL BUSINESS**



**5 MUST-DO BASICS FOR  
EVERY SMALL BUSINESS**

**Intro.**

# SMALL BUSINESSES ARE BIG TARGETS.



Unfortunately, cybercriminals love small businesses. You're connected to sensitive data, often lack IT support, and make quick decisions under pressure — the perfect recipe for risk.

The good news? You don't need to be a tech wizard to take control. This guide gives you five fast, practical tips to protect your people, devices, and data today.

Simple actions can make a massive difference.



**Why Cyber  
—Security Matters.**

# IT'S NOT JUST BIG CORPORATES AT RISK.



Your business is vulnerable to:

- Phishing scams that trick staff into clicking malicious links or paying fake invoices.
- Ransomware attacks that lock your data and demand a payout.
- Compromised devices that let attackers snoop or steal login credentials.

Beyond financial loss, a cyber breach can damage your reputation, violate compliance rules, and shake your customers' trust.



# The Essentials Checklist.

# 5 MUST-DO BASICS FOR EVERY SMALL BUSINESS.

- **Use strong passwords & a password manager.**  
Avoid reusing passwords. Use tools like LastPass or 1Password to store them securely.
- **Enable 2FA (Two-Factor Authentication).** Wherever possible — email, banking, and cloud services. It's one of the easiest ways to stop unauthorised access.
- **Update software regularly.** Keep your systems, apps, and plugins up to date. Patches close security holes.
- **Back up your data.** Use cloud-based backups and test them regularly. If ransomware hits, backups can save you.
- **Train your team.** Most breaches start with human error. A few minutes of education can prevent massive damage.



# Common Mistakes We See.

# REAL STORIES FROM AUSSIE BUSINESSES

## **\$18,000 Invoice Scam**

A staff member received an email from a fake supplier. It looked real. They paid it. It wasn't.

**How to prevent it:** Set up internal approval processes and verify unusual requests by phone.

## **Remote Access Tool Left Running**

A business let a "tech support" scammer access their PC with AnyDesk. They didn't realise the session was still open.

**How to prevent it:** Disable logins and reset passwords immediately after offboarding.



**Get Your Free  
Cybersecurity Audit.**

# LET THE EXPERTS CHECK FOR WEAK SPOTS.



We'll remotely assess your systems, identify common risks, and give you a clear, jargon-free action plan.

## **Includes:**

- Basic device and software checks
- Password security review
- Scam risk and access point assessment
- Recommendations you can action fast

Book now at: <https://www.buzzageek.com.au/cybersecurity-audit>



**About Buzz A Geek.**

# YOUR IT SUPPORT & CYBERSECURITY PARTNER.



Buzz A Geek helps Australian small businesses stay safe, supported, and productive with:

- On-demand tech support (remote & onsite)
- Cybersecurity services & audits
- Backup & cloud setup
- Staff training & device management

Need help now? Visit [buzzageek.com.au](https://buzzageek.com.au) or call 1300 738 570

We're geeks you can trust.

