insight

Small Business Cyber Security Guide

People and Procedures

Key Areas

Businesses, no matter how small, need to be aware of and consciously apply cyber security measures at every level.

Given small businesses often lack the resources for dedicated IT staff, this section addresses how you can manage who can access, and who can control your business' information, and the training of your staff.

Your internal processes and your workforce are the last, and one of the most important lines of defence in protecting your business from cyber security threats.

insight

Access Control

WHAT?

A process to regulate who can access what within your business' computing environment

Access control is a way to limit access to a computing system. It allows business owners to:

- Decide who they would like to give access privileges to
- Determine which roles require what access
- Enforce staff access control limits.

WHY?

To minimise risk of unauthorised access to important information

Many small businesses employ internal staff or outsource work to external suppliers e.g. website hosting companies.

Access control systems help you protect your business by allowing you to limit staff and supplier access to your computer:

- Networks
- Files
- Applications
- Sensitive data.

WHO?

Principle of least privilege

Depending on the nature of your business, the principle of least privilege is the safest approach for most small businesses. It gives users the bare minimum permissions they need to perform their work. This also reduces the risk of an 'insider' accidentally or maliciously endangering your business.

Quick wins

- ☐ Restrict administrator privileges
- ☐ Do not share passphrases
- ☐ Remember to revoke accounts

insight

Passphrases

WHAT?

Using a phrase or sentence, not one word, as your password

A passphrase is similar to a password. It is used to verify access to a computer system, program or service. Passphrases are most effective when they are:

- **Used with multi-factor authentication** - see page 12
- **Unique** - not a famous phrase or lyric, and not re-used
- **Longer** - phrases are generally longer than words
- **Complex** - naturally occurring in a sentence with uppercase, symbols and punctuation
- **Easy to remember** - saves you being locked out.

WHAT?

Greater security & more convenience

- **Harder to crack** against common password attacks
- **Easier to remember** than random characters
- **Meets password requirements easily** – upper and lower-case lettering, symbols and punctuation

Brute Force Attacks and **Dictionary Attacks**
both generate millions of password/passphrase attempts per second.

WHERE?

For all fixed and mobile devices

Passphrases will significantly increase security across all of your business' devices. See below for a comparison of password vs passphrase security.

PASSWORD/ PASSPHRASE	TIME TO CRACK		EASY TO REMEMBER	COMMENTS
	Brute Force Attack	Dictionary Attack		
password123	Instantly Less than AU$0.01	Instantly Less than AU$0.01	Very Easy (too easy)	One of the most commonly used passwords on the planet.
Spaghetti95!	48 hours AU$587.50	Less than half an hour AU$6.10	Easy	Some complexity in the most common areas, and very short length. Easy to remember, but easy to crack.
5paghetti!95	24 hours AU$293.70	Less than 1 hour AU$12.20	Somewhat Easy	Not much more complexity than above with character substitution, and still short length. Easy to remember, but easy to crack.
A&d8J+1!	2.5 hours AU$30.60	2.5 hours AU$30.60	Very Difficult	Mildly complex, but shorter than the above passwords. Hard to remember, easy to crack (against BFA).
I don't like pineapple on my pizza!	More than 1 Year More than AU$107,222.40	More than 40 days More than AU$11,750.40	Easy	Excellent character length (35 characters). Complexity is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember, and very difficult to crack.

insight

Employee Training

WHAT?

Education to protect your staff and business against cyber threats

A cyber security incident response plan can help to change the habits and behaviours of staff and create a sense of shared accountability in keeping your small business safe.

Your cyber security incident response plan teaches staff how to:

- Recognise
- Avoid
- Report
- Remove
- Recover

WHY?

Employees can be the first and last line of defence against cyber threats

Employees make mistakes. As business owners, you have a legal responsibility to keep your business and customer information safe. That's why having a cyber security training program is vital.

WHEN?

Regular cyber security awareness and training

Cyber security is continuously evolving. Keeping everybody up to date could be the difference between whether or not a criminal accesses your money or data.

Quick wins

- ☐ Incorporate, update and regularly repeat
- ☐ Create a cyber security incident response plan
- ☐ Reward employees who find threats
- ☐ Create a cyber security culture

People and Procedures Checklist

- ☐ **Establish an Access Control System to determine who should have access to what**
  - ☐ Restrict administrator privileges to an 'as-required' basis
  - ☐ Do not share passphrases e.g. individual logins
  - ☐ Remember to revoke accounts when employees leave the business
- ☐ **Use strong passphrases**
  - ☐ Use with Multi-factor authentication
  - ☐ Longer
  - ☐ Complex
  - ☐ Unique
  - ☐ Easy to remember
- ☐ **Incorporate, update and regularly repeat cyber security training and awareness amongst your employees**
- ☐ **Create a cyber security incident response plan**
- ☐ **Reward employees who find threats**
- ☐ **Create a cyber security culture and encourage regular discussions**
- ☐ **Always be cautious of emails with the following**
  - ☐ Requests for money, especially if urgent or overdue
  - ☐ Bank account changes
  - ☐ Attachments, especially from unknown or suspicious email addresses
  - ☐ Requests to check or confirm login details