Cyber security tips for small business

Jane Richter

A cyber security incident can have devastating impacts on a small business. The Australian Cyber Security Centre (ACSC), as part of the Australian Signals Directorate (ASD), provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia.

Unfortunately, the team at the Australian Cyber Security Centre (ACSC) see the impact of cyber security incidents each and every day, on individuals, small businesses and large companies.

They recognise that many owners and operators of small businesses don't have the time or resources to dedicate to cyber security. However, there are simple measures that a small business can introduce to help prevent common cyber security incidents.

They have published a **Small Business Cyber Security Guide** that has been specifically designed for small businesses to understand, take action, and increase their cyber security resilience against ever-evolving cyber security threats. The language is clear, the actions are simple, and the guidance is tailored for small businesses.

For an overview of cyber security basics the Small Business Cyber Security Guide is an excellent place to start.

If you want to improve your cyber security further, you can find more information and advice on the ACSC website:

cyber.gov.au

Common Cyber threats

Malicious Software (Malware)

Malware is a blanket term for malicious software designed to cause harm including ransomware, viruses, spyware and trojans.

> Malware provides criminals with a way to access important information such as bank or credit card numbers and passwords. It can also take control of or spy on a user's computer. What criminals choose to do with this access and data includes:

- Fraud
- Identity theft
- Disrupting business
- Stealing sensitive data or intellectual property
- Siphoning computer resources for wider criminal activity

PROTECTING AGAINST MALWARE

Automatically update your operating system, software and apps to make sure the latest protection available is always installed on your devices

Regularly back up your important data to a separate location where malware cannot reach it

Train your staff to recognise suspicious links and attachments

Scam Messages (Phishing)

Scams can be 'dodgy' emails, messages, or calls designed to trick recipients out of money and data. Criminals will often use email, social media, phone calls, or text messages to try and scam Australian businesses.

These criminals might pretend to be an individual or organisation you think you know, or think you should trust. Their messages and calls attempt to trick businesses into performing specific actions, such as:

- Paying fraudulent invoices or changing payment details for legitimate invoices
- Revealing bank account details, passwords, and credit card numbers (sometimes known as 'phishing' scams, cybercriminals can mimic official branding and logos from banks and websites to seem legitimate)
- Giving remote access to your computer or server
- Opening an attachment, which may contain malware
- Purchasing gift cards and sending them to the scammer

Phishing scams are not limited to emails. They are increasingly sophisticated and harder to spot. Be cautious of urgent requests for money, changes to bank accounts, unexpected attachments, and requests to check or confirm login details.

Visit scamwatch.gov.au to report a scam.

PROTECTING AGAINST PHISHING

If you think a message or call might truly be from an organisation you trust (such as your bank or a supplier) find a contact method you can trust

Never open an attachment or click on a link in an email or SMS that is not from an organisation that you know you can trust

Check the actual email address that the email has been sent from as this will often reveal the sender is not who it seems

Ransomware

Ransonware is a specific type of malware that locks down your computer or files until a ransom is paid.

Ransomware works by locking up or encrypting your files so that you can no longer use or access them. Sometimes it can even stop your devices from working. Ransomware can infect your devices in the same way as other malware. For example:

- Visiting unsafe or suspicious websites
- Opening links, emails or files from unknown sources
- Having poor security on your network or devices (including servers)

Ransomware offers cybercriminals a low-risk, high-reward income. It is easy to develop and distribute. Ransoms are typically paid using an online digital currency or cryptocurrency such as Bitcoin, which is very difficult to trace. Also in cybercriminals' favour, most small businesses are unprepared to deal with ransomware attacks.

PROTECTING AGAINST RANSOMWARE

Ensure you have high quality, up-to-date security management software installed on every device

Regularly backup your important data

Automatically update your operating systems, software and apps

Photo credit: Anete Lusina

Other tips

- Ensure you have high quality security management software installed on all your devices
- Set your security system software to update automatically
- Ensure you have regular automatic back ups being made of your most important business data
- Where it is available, set up and use multi-factor authentication to access online programs and services
- Set all your passwords to be as secure as possible – use long passwords (at least 14 characters in length), include a mixture of upper case, lower case, numbers and special symbols
- Don't use the same password for more than one login
- Teach your staff to be security aware and to recognise potentially suspicious links or emails
- Include talks about the importance of cyber security in your team briefings and performance management discussions

The Department of Industry, Science, Energy and Resources has also developed an assessment tool to help improve cyber security skills among Australian small and medium businesses.

With the assessment tool, you can:

- identify the cyber security strengths of your business
- understand areas where your business can improve
- know how to improve your cyber security and where to find help

The assessment tool asks you questions about how you manage cyber security for your business. Based on your answers, it will determine your current cyber security maturity level. It will then provide you with guidance on how to improve.

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

What is Multi-Factor Authentication (MFA)?

This is a security measure that requires two or more proofs of identity to grant you access. MFA typically requires a combination of:

* something you know (password/passphrase, PIN, secret question)
* something you have (smartcard, physical token, authenticator app)
* something you are (fingerprint or other biometric)

Access the assessment tool at:

https://www.cyber.gov.au/acsc/small-and-medium-businesses/cyber-security-assessment-tool

Download the full Small Business Cyber Security Guide at:

https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide

For more resources, or to report a Cyber Crime, please visit:

https://www.cyber.gov.au/acsc/small-and-medium-businesses