Small Business Guide

Second Edition

Protect your business in 5 minutes

Australian Government

Stay Smart Online

STAYSMARTONLINE

STAY SMART ONLINE

Small Business Guide

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

This information has been prepared by Enex TestLab for the Attorney-General's Department.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

ISBN 978-0-9953944-0-7

STAY SMART ONLINE

Small Business Guide

30%

of small businesses had experienced a cyber-crime incident in the year prior to mid-2015

109%

more security incidents were detected in Australia in 2015 compared to 2014

63%

of confirmed data breaches involved weak, default or stolen passwords

Sources: Mike Burgess, Telstra: Information security matters to small business too: https://exchange.telstra.com.au/2015/10/12/information-security-matters- small-business/.

PwC Global State of Information Security Survey 2016. http://www.pwc.com.au/press-room/2015/cyber-security-risks-oct15.html

Verizon 2016 Data Breach Investigations Report. http://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

STAY SMART ONLINE

Small Business Guide

Your business is your business

Every day we do things to safeguard ourselves and our businesses—we apply sunscreen to protect ourselves from the sun; we take out insurance for our health, homes, cars and business; and we watch the news to keep up-to-date on current issues and events. Just like putting on sunscreen when we go out on a sunny day, protecting our online information should become part of our normal day-to-day activities.

This short guide was developed to help you put in place some basic online security practices. It only takes a few minutes to read through the five easy steps, which will provide you with the basics on how to protect the information entrusted to you by your customers and suppliers.

Your business is *your* business—whether you're in business or managing someone else's business, you are responsible for its success. Stay Smart Online is the Australian Government's online safety and security information service, designed to help everyone understand the risks and simple steps that can be taken to protect personal and financial information when using the internet. Additional information about the Small Business Guide can be found at www.staysmartonline.gov.au/smallbusinessguide.

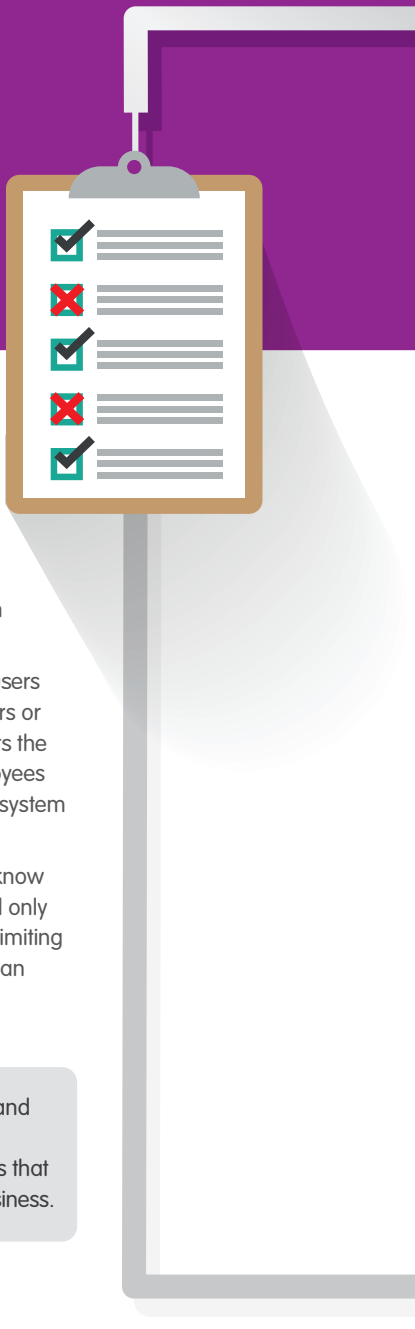
This Guide has been developed by the Australian Government's Stay Smart Online Initiative in collaboration with Australia Post, Australia and New Zealand Banking Group Limited, Commonwealth Bank, National Australia Bank, Westpac and Telstra.

Australian Government

Privacy

Keep friends close and information closer

Privacy



Keep friends close and information closer.

Take protecting your business seriously—do not share passphrases or keep sensitive business or customer data on computers outside your control.

Administrators need greater access privileges than normal users so they can undertake activities that may impact several users or business processes. Avoid software that gives standard users the same access privileges as administrators. In addition, employees should have individual access credentials for each business system (not shared credentials).

Your business information is a valuable commodity. Do you know who has access to your information? Your employees should only have access to the information they need to do their job. By limiting that access on a need-to-know basis, you reduce the risk of an 'insider' accidentally or maliciously releasing confidential information.

Action: Take responsibility for making your team understand information security, and include this in your business plan. Refer to the Implementation Guide available online for actions that help maintain the confidentiality of information within your business.

More information about privacy is available here:
https://www.staysmartonline.gov.au

Passphrases

Sunscreen protects us:
passphrases protect information

Passphrases

Sunscreen protects us: passphrases protect information.

Protecting yourself against too much sun is important. You should apply the same diligence online to protect your information from exposure and consequent loss or damage.

If you are running a small business, you need to educate your team to protect your business information held on desktop computers and mobile devices such as smartphones and tablets. Using strong passphrases is the online equivalent of applying a strong sunscreen.

Put simply, passphrases are a series of words that are longer, easier to remember and harder to guess than traditional passwords. However, you should avoid using passphrases drawn from dictionaries or that may be relatively easy to decipher.

Passphrases can help prevent criminals from accessing critical information that can be used for fraud or to extort your business. They should be used for all fixed and mobile devices, and where possible, in combination with other security measures such as firewalls and antivirus software.

Encouraging your workers to use two factor authentication is another way of improving security. Instead of using just a username and password to log in to an account (a username and password are typically regarded as one factor), your workers have to provide two factors—such as something they know (like a password) and something they have (like a one-time code sent to their mobile phone)—to gain access.

Action: Tell your employees to create passphrases for their online accounts. Advise them to use two-factor authentication or verification for additional protection.

More information about small business security is available here:
https://www.staysmartonline.gov.au/business-owners/protect-your-business

Awareness

All eyes open to stay secure

Awareness

All eyes open to stay secure.

Like keeping up with the news, the more aware people are about online security, the more capable they are of applying that knowledge to protect your business.

Staying smart online is not just about you and your team, it's about insisting your business partners and suppliers, and even your family and friends, stay up-to-date with the latest scams, spam and internet threats.

Being aware also means knowing the right questions to ask. As a business owner, you need to be able to have an informed discussion with your IT provider to ensure they can meet your needs. There are some questions at the end of this guide to help you.

Awareness also extends to being on the lookout for suspicious messages, including:

- phishing emails or text messages (these messages try to lure you into providing your passwords, online banking details or other sensitive information),
- spam (unsolicited advertising or promotional messages), and fake telemarketing calls requesting personal or financial information.

You should always be suspicious of unsolicited messages or phone calls requesting personal or financial information. If you have any doubt regarding the legitimacy of a phone call or message, contact the organisation to confirm it by using a phone number, address or form sourced from its legitimate website.

If you have provided your details to a suspicious caller or sender, immediately change your passwords and associated information. You should also alert service providers such as your bank and ask them to monitor your accounts for unusual activity.

Action: Look for the padlock symbol in your browser address bar and 'https' at the start of the website address when visiting sites. Also manually type website addresses into your browser's address bar and check that the address displays properly with no added letters, numbers or symbols.

More information about awareness is available here:
https://www.staysmartonline.gov.au

Network and device security

Lock down your computers (and networks)!

Network and device security

Lock down your computers (and networks)!

You keep your home and office free of pests—do the same for your business systems. Having antivirus software that is updated regularly is a good start, as well as setting your systems to automatically update software.

Did you know that mobile phones and tablets may provide access to your sensitive business information? Insist workers lock them with PINs in case of loss or theft and limit business information stored on them. Treat any network that your business does not control as insecure, particularly public Wi-Fi. Educate your workers to be wary of plugging unknown USB drives into their computers as these drives may contain viruses.

You can also improve the safety of your business by using separate computers at home for work and personal activities. This reduces the risk of your work files being infected by you or other members of your family as you or they browse the web, play games or undertake other activities online.

In recent years, criminals and malicious individuals have turned to extortion as a way of obtaining money from businesses. Extortion techniques include tricking workers into infecting computers with ransomware that encrypts files so the criminals can demand payment (usually in digital currencies such as bitcoin) for the decryption key.

Action: Keep your security software up to date and back up your data to devices or locations isolated from your corporate network.

More information about computers and network security is available from https://www.staysmartonline.gov.au/computers

Backups

Insure your data: back it up!

Backups

Insure your data: back it up!

You insure your house, health, car, life and physical business assets, but can you replace your lost or damaged business data? Not backing up your data can cost you your business.

What is business data? It includes accounting files, invoicing and quoting systems, letters and emails, information and resources, and even your website files.

Regularly backing up your data or setting devices to automatically back up can help you quickly recover from a cyber attack, hard disk failure or another disastrous event.

Back up your data to a removable storage device such as a hard drive. Do not back up to your computer as it may become compromised too.

Action: Take your backup offsite or store it securely, like other important documents. Test your backup system regularly to ensure that it restores all information correctly.

More information about backing up your data is available here:
https://www.staysmartonline.gov.au/computers/back-your-data

STAY SMART ONLINE

Common Online Threats

Adware

Software that is covertly installed on your computer and designed to deliver advertisements or other content which encourages you to purchase goods or services.

Spyware

Software that is covertly installed on a computing device and takes information from it without your consent or the knowledge of the user.

Virus

Malware designed to infect and corrupt a computer and to copy itself. Viruses can disrupt programs installed on a computer.

Scam

A commonly used term to describe a confidence trick, relying on email or a website to obtain sensitive information or deliver malicious content (such as malware) to unsuspecting users.

Malicious software (malware)

A catch-all term used to describe software designed to be installed into a computer system for the purpose of causing harm to you or others. This would include viruses, spyware, trojans, worms, etc.

Worm

A self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Ransomware

'Ransom Software' is a type of malware which handicaps computer functionality, for example, through browser hijacking or encrypting personal data, and offers to restore the functionality for a fee, which is extortion. Paying the fee does not guarantee removal of the ransomware, which can lay dormant ready for attack in the future.

Phishing (email/website)

Fraudulent email messages or web sites used to deliver malicious content (such as malware); or gain access to personal information for illegal purposes such as transferring funds or purchasing goods over the internet.

Trojan horse

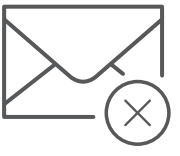
Malicious code that is hidden in a computer program or file that may appear to be useful, interesting, or at the very least harmless to you when using your computer. When this computer program or file is run, the malicious code is also triggered, resulting in the set up or installation of malware.

CryptoLocker

A particularly malicious type of ransomware which, once installed on your computer, encrypts and locks all of the files on the infected computer including documents, photos, music and video. A pop up window will then display on the computer screen requesting payment of a ransom in return for a CryptoLocker key to unlock the encrypted files. Paying the ransom does not guarantee removal of the CryptoLocker.

Keylogger

A keylogger is a program that records the keystrokes on a computer. It does this by monitoring a user's input and keeping a log of all keys that are pressed. The log may be saved to a file or even sent to another machine over a network or the Internet. Keylogger programs are often deemed spyware because they usually run without the user knowing it.



Spam

Unsolicited email. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or illegal services. Users are advised that if an offer in an email appears too good to be true then it probably is and should not be actioned in any way.

Scareware

Malware that causes frightening messages to appear (for example, that your computer is infected with malware or that you are guilty of a crime), and attempts to extort money from you to resolve the alleged issue. Similar to ransomware.

Man-in-the-middle

A man-in-the-middle attacker inserts themselves between two parties who are communicating with each other online, so they can disable or alter those communications.

Drive-by download

A drive by download occurs when a user's computer is infected with malware simply by visiting a compromised website.

Zombie or bot

A single compromised computer (a robot computer), called a zombie or a bot. Once infected, these computers can be used for malicious activity without the knowledge of the user.

Water-holes

Malware placed on a legitimate website that attempts to compromise visitors' computers.

Catfish

Internet predators who create fake online identities to lure people into emotional or romantic relationships for personal or financial gain.

STAY SMART ONLINE

Small Business Guide

How to ensure your website is secure

A lot of small businesses have a website, but many don't have the knowledge to feel confident they are setting it up or maintaining it correctly. This section provides a list of basic security features and questions you should discuss with your website developer when building and maintaining your site.

How is security embedded into the design of the site, and what are the key features relevant to protecting your information?
Best practice secure web design should be applied through the definition, development and deployment of your site.

Have all vulnerabilities been identified and remediated on the application and infrastructure platforms?
Has the site and supporting infrastructure been independently verified not to be high risk?

How is the resilience of the site assessed and improved?
What are the availability and recovery features of the site and hosting provider? Do they meet your business requirements?

Who are the people that control the content and access to your site?
Do you know exactly who can access your site? Access should be limited to individuals who need to perform administration or content deployment.

Do you use unique credentials for each of your clients' sites?
Do you make sure that each of your clients is protected from unauthorised access?

What are the administrative access points to your site?
Is it a simple administration logon to the site or is it through a content management system? Ensure you know how the site is managed.

Is there strong authentication methods used to access your site?
Your site should have strong authentication controls in place, such as two-factor authentication for administrators, or at a minimum very strong passphrases.

How is change control managed on your site?
What are the processes in place to manage changes to your site? There should be a process to get approval before making changes and also there needs to be plans in place to "roll back" changes if they impact the functionality of the site.

How are security events and alerts monitored?
What are the processes in place to detect suspicious event and alerts on your site and support infrastructure, and what happens if they are proven to be related to a security incident?

How are security incidents managed?
Once a security incident has been declared, what is the process to manage, resolve and learn from the incident?

If externally hosted, where is your information actually located i.e. which country?
Once live, where will your site and information be hosted?

Who owns the IP on your site and how can you gain access to it?
Will you have any data sovereignty issues in the event of an incident or trying to recover your information?

STAY SMART ONLINE

Small Business Guide

More information

More information about how to protect your personal and business information can be found at www.staysmartonline.gov.au.

Detailed information about scams, including phishing scams, and how to report them is available at SCAMwatch www.scamwatch.gov.au or call 1300 795 995.

To report a cybercrime, visit the Australian Cybercrime Online Reporting Network at www.acorn.gov.au or call your local police.

Information about small business privacy requirements is available at www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10

The Australian Government's Digital Business website can assist you with simple, practical tips on how to get your business or organisation online and take advantage of the opportunities that the internet can bring. Visit www.digitalbusiness.gov.au.

Stay Smart Online recommends that if your computer network is compromised, seek immediate technical advice that is relevant to your personal circumstances.

STAY SMART ONLINE

Small Business Guide

Second Edition

https://www.staysmartonline.gov.au/smallbusinessguide

Australian Government