Australian Government

STAY SMART ONLINE

Small Business Guide

PROTECT YOUR BUSINESS in 5 minutes

Passwords

Backups

Awareness

Confidentiality

Network and Device Security

STAY SMART ONLINE

Small Business Guide

Passwords

Backups

Awareness

Confidentiality

Network and Device Security

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 Department of Communications and the Arts.

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 9780642754745

STAY SMART ONLINE

Small Business Guide

Did you know?

60%

of businesses who experience a cyber attack, **go out of business within 6 months of the incident**

Average time to resolve a cyber attack is

23 days

Increases to 50 days

if the attack was an inside job

Effects of a cyber attack on business

business disruption

information loss

productivity loss

revenue loss

equipment damage

Sources: 2014 Cost of Cyber Crime Study: Australia, Ponemon Institute, and, Small Business Online Security Infographic, Stay Safe Online, National Cyber Security Alliance.

STAY SMART ONLINE

Small Business Guide

Passwords

Backups

Awareness

Confidentiality

Network and Device Security

Foreword

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.

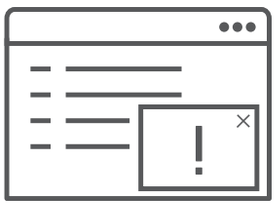
Your business is *your* business — whether you're in business or managing someone else's business, you are responsible for its success. Stay Smart Online is the Australian Government's online safety and security information service, designed to help everyone understand the risks and simple steps that 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

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 deliver the trick 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 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.

STAY SMART ONLINE

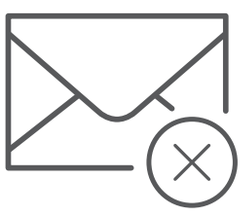
Common Online Threats

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.

Zombie or bot

A single compromised computer (a robot computer), called a zombie or a bot.

Water-holes

Malware placed on a legitimate website to compromise website or users.

Catfish

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

Passwords

Sunscreen protects us:
Passwords protect information.

Passwords

Sunscreen protects us: Passwords protect information.

Just as we all need a friendly reminder to protect ourselves from the sun, remembering to use strong passwords can protect your information.

If you're a small business, you need to educate your team to protect your business information held on computers and portable devices. Good passwords are 10 characters or more long, and include a mixture of numbers, letters, special characters, upper and lowercase. Longer passwords are stronger. Change them regularly, and never use the same password more than once.

Good passwords can prevent intruders from accessing critical information that can be used for fraud or to extort your business. Phones and other portable devices need Passwords, PINs or Pattern Locks in case they are lost or stolen. These should be changed regularly.

Action: Tell staff to create a password using a phrase and replacing some letters with characters and number. e.g. 'Be good, be wise' can be modified to B3g00db3w1$e

More details about passwords is available here:
https://www.communications.gov.au/what-we-do/internet/stay-smart-online/computers/set-and-use-strong-passwords

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 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 backup 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 details about backup are available here:
https://www.communications.gov.au/what-we-do/internet/stay-smart-online/computers/back-your-data

Awareness

All eyes open to stay secure.

Awareness

All eyes open to stay secure.

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.

Like keeping up with the daily news, the more that people are informed about online security, the more likely they are to apply that knowledge in your workplace to help protect your business.

Action: Ask everyone in your network to subscribe to the Australian Government's free Stay Smart Online Alert Service to keep on top of current security information by visiting: www.staysmartonline.gov.au/alert_service.

More information about online security is available here:
https://www.communications.gov.au/what-we-do/internet/stay-smart-online

Confidentiality

Keep friends close and information closer.

Confidentiality

Keep friends close and information closer.

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

Avoid using applications that do not allow you to apply separate administrator and user logins. Employees should have individual logins and passwords for each business system (not shared credentials).

Your business information is a valuable commodity. Do you know who has access to your information? 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. Consider using a password safe to store an encrypted copy of your passwords.

More information about confidentiality is available here:
https://www.communications.gov.au/what-we-do/internet/stay-smart-online/guide/business

Network and device security

Lock down your phones (and networks)!

Network and device security

Lock down your phones (and networks)!

You keep your home 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 may provide access to your sensitive business information? Insist staff keep them locked with a PIN in case of loss or theft. Ensure staff limit business information stored on them, including email.

Treat any network that your business does not control as insecure, particularly public Wi-Fi. It is good practice to assume that someone is eavesdropping on your information.

Action: Check that websites have a padlock symbol in the browser bar before entering information into them — this is the best indicator that your information is kept private as it is transmitted to and from the website.

More information about network and mobile device security is available here:

https://www.communications.gov.au/what-we-do/internet/stay-smart-online/mobile-devices

https://www.communications.gov.au/what-we-do/internet/stay-smart-online/computers/secure-your-computers

STAY SMART ONLINE

Small Business Guide

Passwords

Backups

Awareness

Confidentiality

Network and Device Security

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/privacy/privacy-resources/privacy-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

www.staysmartonline.gov.au/smallbusinessguide

Australian Government

Passwords

Backups

Awareness

Confidentiality

Network and Device Security