My Guide

Protect Yourself

in 8 steps

Australian Government

STAY SMART ONLINE

STAY SMART ONLINE

My Guide

Australian Government

Taking personal responsibility for online safety.

Welcome to the My Guide online security guide. This guide provides tips and techniques for you to stay secure when working or socialising online.

For most of us, the internet opens up new opportunities. We can shop, bank, research, work and connect when and where we want to. Unfortunately the online world also gives criminals opportunities to steal money, information or identities. For example, if you're not careful, you may find a loan being taken out in your name using stolen details.

So how do we reduce our risk of falling victim to online crimes? The Australian Government provides information and services to help you stay safe online. But protecting yourself properly means taking responsibility for your behaviour. My Guide helps you stay smart online so you can avoid falling victim to scammers.

My Guide has been developed by the Australian Government's Stay Smart Online initiative in collaboration with the New Zealand Department of Prime Minister and Cabinet, Australia Post, Australia and New Zealand Banking Group Limited, Commonwealth Bank, National Australia Bank, Westpac and Telstra.

My Guide covers eight key areas: privacy; backups and protection; surfing safely; suspicious messaging; passphrases; tablets and mobiles; online finances and payments; and reporting. We hope you will find this guide useful and welcome any feedback you may have.

STAY SMART ONLINE

My Guide

List of actions

Staying smart online is just as important for individuals as it is for businesses. The checklist below includes some actions you and your friends and family can take to safely connect, find news and information, shop and undertake other activities online.

1. Stop and think before you provide any photos or financial or personal information about yourself, your friends or your family.

2. Use strong, hard-to-guess passphrases and/or two-factor authentication where available to access your accounts.

3. When you receive an email, consider who is emailing you and what they are asking you to do. Call the business a suspect message claims to be from using contact details obtained from a website or other legitimate source.

4. (i) Minimise visits to unknown websites and avoid being enticed by the promise of sensational content through 'clickbait'.
   (ii) Look for the padlock symbol and 'https' in the browser address bar when visiting sites. This is particularly relevant when undertaking a transaction or entering personal information online.

5. (i) Access your bank's website by typing the address directly into your browser.
   (ii) Keep your computer up-to-date with anti-virus, anti-spyware and firewall software.
   (iii) Use the security measures (such as two-factor authentication) recommended by your bank.
   (iv) Always log out of the internet banking menu and closing your browser when you have completed a session.
   (v) Research for unknown retailers and their products and services.
   (vi) Deal primarily with trusted and reliable online retailers.

6. (i) Turn on the security features of your mobile devices.
   (ii) Set a password/phrase or PIN that must be entered to unlock the device.
   (iii) Install reputable security software.
   (iv) Read the user manual.
   (v) Use the most up-to-date operating systems.

7. (i) Regularly update applications (including anti-virus software and plugins) and operating systems to fix these vulnerabilities. Most vendors make automatic updates available.
   (ii) Back up your data regularly and retain the backup in a safe location, preferably protected or isolated from the device the data is being backed up from.
   You can:
   > Perform your own back-ups to a storage device such as a USB or external hard drive.
   > Back up regularly or set to do so automatically.
   > Back up to an online (cloud) service.

8. Report scams to: https://www.scamwatch.gov.au/report-a-scam

   Report online crimes to ACORN at: http://report.acorn.gov.au

   iDcare is Australia and New Zealand's national identity support service. iDcare can be contacted on 1300 432 273 for Australian residents and on 0800 201 415 for New Zealand residents.

STAY SMART ONLINE

My Guide

$229 million

the total amount lost to scams in Australia in 2015

Over 15,000

Reports of phishing scams were received in 2015, resulting in a total reported loss of $363,270

38%

of scam approaches occurred through email, over the internet or through a social network platform and accounted for 44 percent of losses.

*All statistics sourced from the report Targeting scams: report of the ACCC on scam activity 2015, published 16 May 2016, http://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2015

Privacy

Be wary of what you share

Privacy

Be wary of what you share.

Digital and online technologies are transforming our social and business lives. They enable us to connect more easily and complete tasks such as filling out forms for government agencies when and where we want to. However, many of the things we do online—banking, shopping, chatting with family and friends, or even making new friends—involve us giving out personal and financial information. Ensure you protect your personal information and privacy.

For example, if you use social media, read and understand any terms and conditions—particularly those relating to your personal information—and be aware of what you share. Remember photos or information can be hard to remove once posted. Be careful about sharing information that could compromise your security, such as date of birth, address or information about your children's schools.

Apply the same rigorous criteria when signing up for games online. The less information you make accessible publicly online, the lower the risk that criminals will be able to undertake identity theft activities such as taking out a loan in your name.

Action: Stop and think before you provide any photos or financial or personal information about yourself, your friends or your family.

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

Passphrases

Create strong passphrases
to be secure

Passphrases

Create strong passphrases to be secure.

In the same way as you apply sunscreen to protect your skin, you need to protect yourself from people who want to gain access to your accounts to misrepresent you or steal information. You should use passphrases for this purpose.

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 relatively easy to decipher.

Many businesses and organisations are making available two-factor or multi-factor authentication to help people become more secure.

Instead of using just a username and password to log in to an account (a username and password are typically regarded as one factor), you have to provide two factors—such as something you know (like a password) and something you have (like a one-time code sent to your mobile phone)—to gain access.

Actions: Use strong, hard-to-guess passphrases and/or two-factor authentication where available to access your accounts.

More information about protecting yourself online is available here: https://www.staysmartonline.gov.au

Suspicious Messaging

Treat any unexpected message with caution

Suspicious Messaging

Treat any unexpected message with caution.

Working with governments and organisations such as utilities online has enabled people to save time and effort. However, criminals are seeking to exploit these relationships to steal money and personal information.

A common method of doing so is to use phishing scams. These scams attempt to trick you into giving out information such as your bank account numbers, passwords/phrases and credit card numbers.

Phishing messages may include logos, disclaimers and other features from the business the message claims to be from. In recent years, many phishing messages have become hard to distinguish from legitimate emails. Phishing scams have also become more sophisticated. For example, spear phishing scams differ from ordinary phishing scams in that they use detailed information about a business to target its workers.

Actions: When you receive an email, consider who is emailing you and what they are asking you to do. If you are unsure, call the business a suspect message claims to be from using contact details obtained from a website or other legitimate source.

More information about recognising scam emails is available here: https://www.staysmartonline.gov.au/your-identity/recognise-scam-or-hoax-emails-and-websites

Surfing Safely

Avoid malware—keep to trusted websites

Surfing Safely

Avoid malware—keep to trusted websites.

Exploring the almost limitless horizons of the web is a hugely enjoyable activity for many people. However, this enjoyment may be spoiled by drive by downloads, one of the most insidious threats on the internet today. These downloads occur when you visit a compromised web page and often install themselves without notification on your computer or mobile device.

One way of minimising your risk is to manually type website addresses into your browser's address bar and check that the address displays properly with no added letters, numbers or symbols. Also keep an eye out for common types of domain name abuse such as replacing the letter O with zero or adding hyphens or bogus words to a legitimate address.

Actions: Minimise visits to unknown websites and avoid being enticed by the promise of sensational content through 'clickbait'

Look for the padlock symbol and 'https' in the browser address bar when visiting sites.

More information about recognising scam websites is available here: https://www.staysmartonline.gov.au/your-identity/recognise-scam-or-hoax-emails-and-websites

Online Finances and Payments

Keep financial details from prying eyes

Online Finances and Payments

Keep financial details from prying eyes.

Banking online is an easy and convenient activity. However, criminals are eager to steal your online banking details so they can drain your accounts. They use a variety of scams to do this, including using malicious code to exploit vulnerabilities in outdated or unpatched software to capture information.

Shopping online is another process that you need to be smart about. Be wary of websites that you have not visited before or that look suspicious or unprofessional. Scammers may have set them up to capture payments, harvest your personal information or deliver a virus or other malicious software to your computer.

Actions:

- Access your bank's website by typing the address directly into your browser
- Keeping your computer up-to-date with anti-virus, anti-spyware and firewall software
- Use the security measures (such as two-factor authentication) recommended by your bank
- Always log out of the internet banking menu and closing your browser when you have completed a session
- Research for unknown retailers and their products and services
- Deal primarily with trusted and reliable online retailers

More information about buying and selling online is available here:
https://www.staysmartonline.gov.au/buying-and-selling

Tablets and Mobiles

Stay secure while on the move

Tablets and Mobiles

Stay secure while on the move.

People today can use mobile devices to connect, shop, research and complete other tasks any time from any location. However, mobile devices like smartphones and tablets are small portable computers. Just like your computer at home they can be hacked, infected with a virus and, if unsecured, provide access to your personal information.

Actions:

- Turn on the security features of the device
- Set a password/phrase or PIN that must be entered to unlock the device
- Install reputable security software
- Read the user manual
- Use the most up-to-date operating systems

More information about mobile devices is available here:
https://www.staysmartonline.gov.au/mobile-devices

Backups and Protection

Back up and update for safety

Backups and Protection

Back up and update for safety.

New applications that make our lives easier and more fun are emerging constantly. However, hackers find weaknesses in these applications and the underlying operating systems that may provide access to data on your computer, smartphone or tablet. Your data may also be at risk from your computer hard disk becoming corrupted, or you leaving your mobile phone at a café, in a taxi or in another location.

Actions:

- Regularly update applications (including anti-virus software and plugins) and operating systems to fix these vulnerabilities. Most vendors make automatic updates available
- Back up your data regularly and retain the backup in a safe location, preferably protected or isolated from the device the data is being backed up from

You can:

- Perform your own back-ups to a storage device such as a USB or external hard drive
- Back up regularly or set to do so automatically
- Back up to an online (cloud) service

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

Reporting

Keep everyone safe
by reporting scams

Reporting

Keep everyone safe by reporting scams.

There are several government departments and agencies working to keep you safe online.

The Australian Cybercrime Online Reporting Network (ACORN) is a national online system that enables members of the public to securely report instances of cybercrime. ACORN is the national policing initiative of the Commonwealth, State and Territory governments.

The Australian Competition and Consumer Commission operates Scamwatch, a service that enables you to report scams.

If you believe you have experienced identity theft, iDcare—Australia and New Zealand's national identity support service—offers personalised support to individuals who are concerned about their personal information. Support is provided free of charge.

Contact your bank, mobile phone provider, and other key service providers so they can monitor your accounts for suspicious activity.

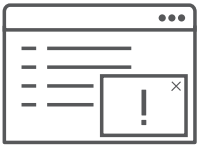
You can report online scams to Scamwatch here:
https://www.scamwatch.gov.au/report-a-scam

You can report cybercrimes to ACORN here:
http://report.acorn.gov.au

iDcare can be contacted on 1300 432 273 for Australian residents and on 0800 201 415 for New Zealand residents.

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

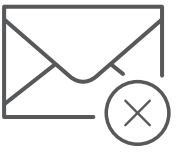
Malicious code that is hidden in a computer program or file that may appear to be useful, interesting, or at the very least harmless to you when using your computer. When this computer program or file is run, the malicious code is also triggered, resulting in the set up or installation of malware.

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

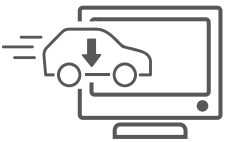
Unsolicited email. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or illegal services. Users are advised that if an offer in an email appears too good to be true then it probably is and should not be actioned in any way.

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

My 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.

iDcare—Australia and New Zealand's national identity support service—offers personalised support to individuals who are concerned about their personal information. Support is provided free of charge, iDcare can be contacted on 1300 432 273 for Australian residents and on 0800 201 415 for New Zealand residents.

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

My 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 - 978-0-9953944-1-4

STAY SMART ONLINE

My Guide

Australian Government