

Use common sense when shopping online

and trust your instincts. If the website looks suspicious or if it is offering bargains which look too good to be true, use your common sense and don't continue. Only purchase via secure webpages and always print and keep a copy of the transaction.

Beware of email and offers from unknown sources.

Be cautious about opening emails if you don't recognise the sender. If a stranger makes you an offer that seems too good to be true, then it probably is.

Ensure your wireless internet connections are secure.

If you are using wireless internet:

- change the default password from the manufacturer
- ensure you have encryption turned 'on' in your wireless software settings—this will make it very hard for anyone who somehow manages to intercept your transmitted data to make sense of it.

Be careful about the amount of information you share on social networking sites.

Remember, anything you put on the internet—whether it is your name and address, or personal photos and videos—stays online forever, and you never know how someone might use it.



For more information

For more information about how to keep yourself and your family secure online, visit the Australian Government's Stay Smart Online website www.staysmartonline.gov.au

You can also subscribe to the Stay Smart Online Alert Service. You'll be sent regular emails to help keep you up-to-date with the latest e-security risks and provide useful advice about how to avoid them.

For more information about the types of online scams, visit Scamwatch,

www.scamwatch.gov.au

To learn more about how to protect yourself against identity theft, visit Protect your ID,

www.protectfinancialid.org.au

Always remember the five simple steps that need to be followed

1. Install, update and use your security software.
2. Use strong passwords and change them regularly.
3. Be careful when sharing personal information online.
4. Think before you click—if it looks too good to be true, it probably is!
5. Be smart and stay informed—visit www.staysmartonline.gov.au, and sign up for the new Stay Smart Online Alert Service.

0000340001.009



Australian Government

Department of Broadband,
Communications and the Digital Economy

E-security for your home

www.staysmartonline.gov.au



Online risks

These days, just about everyone is online. We use the internet for banking, to buy tickets, book holidays and to keep up with friends and family. But as we become more familiar with the internet, we also need to protect ourselves from e-security risks.

Some of the risks can lead to:

- Identity theft—thieves can steal personal information about you, from your name and address to your credit card number. This information can be used to purchase things in your name or even steal your identity in the real world.
- Your computer being infected with malicious software such as spyware and viruses, which can steal your financial information as well as slow down your computer.
- Being defrauded by online scams.
- Thieves using your wireless connection to steal your monthly download limit.

Fortunately, there are some simple measures you can take to improve the security of your computer, yourself and your family while you are online. There are **some things you need to have** and **some things you need to do**.

What you need to have

Just as you have locks for your doors and seatbelts in your car, there are some simple things to install and activate on your computer to help keep yourself and your family secure when online.

Security software can identify and block malicious software, like viruses, worms, trojans or spyware attempting to access your computer. Different packages have different levels of coverage—some software only block viruses, while others offer more comprehensive protection against a wider range of threats.

You can buy security software packages from computer and office supply stores and many can be downloaded from the internet.

The most important thing is to keep software up-to-date, so make sure to switch on 'auto updates' function when you install your software.

A **firewall** is software or hardware that monitors information going in and out of your computer. It is important to have a firewall installed to ensure that you can control what is being installed on your computer.

A firewall may have been installed on your computer when you bought it. Make sure it's switched on. Some security software packages also include firewalls.

You can also choose **smart settings for your internet browser**, which add another layer of security. Depending on the security level you choose, your internet browser can alert you when you are visiting unsecure webpages, or help to block unwanted pop-ups.

The higher your levels are set the more secure your internet access will be, but you may have fewer options and functions available.

What you need to do

Get into some simple habits to help keep you and your family secure online.

Use strong passwords and change them regularly. A strong password should:

- have at least eight characters—14 or more is even better
- use a mix of upper and lower case letters, numbers and symbols e.g. a very secure password would be something like this: j>kb*D-94x.

Keep your software up-to-date. Software manufacturers routinely identify vulnerabilities in their products and issue 'patches' to address them, which can help to protect your computer. You can set your computer to check for updates regularly.

Make sure your online banking is secure. Always log out from your internet banking session when you have finished. For the latest information, keep up-to-date with security advice from your financial institution.

