

Protecting Yourself Online – Eight Simple Tips

Many of us have openly welcomed the internet into our lives.

For most of us the internet is part of our daily routine for keeping in touch with friends and family, working, studying, playing games, shopping and paying bills.

While the internet offers us many benefits, there are also a range of safety and security risks associated with its use.

These include threats to the integrity of our identities, our privacy and the security of our electronic communications, in particular financial transactions, as well as exposure to offensive and illegal content and behaviour.

Whether you are new to using the internet or a regular user, here are **eight simple tips** you can take to protect yourself online.

1. Install and renew your security software and set it to scan regularly.
2. Turn on automatic updates on **all** your software, including your operating system and other applications.
3. Think carefully before you click on links and attachments, particularly in emails and on social networking sites.
4. Regularly adjust your privacy settings on social networking sites.
5. Report or talk to someone about anything online that makes you uncomfortable or threatened – download the Government’s Cybersafety Help Button.
6. Stop and think before you post any photos or financial or personal information about yourself, your friends or family.
7. Use strong passwords and change them at least twice a year.
8. Talk within your family about good online safety.

What these steps show is that protecting yourself online is about more than just how you set up and use your computer, mobile phone or any internet enabled device. It’s also about being smart in what you do and the choices you make while using the internet.

There are criminals who use the anonymity of the internet to run old and new scams. While many of these are scams that most people would spot a mile away if they were attempted in the ‘real’ world, online scams are very sophisticated and often harder to detect.

So it’s important to remember that while the technology may be new, the old wisdom still applies. If something you see online or which is sent to you seems suspicious or too good to be true, it probably is.

The booklet ***Protecting Yourself Online – What Everyone Needs to Know*** offers further information and advice. It will help you secure your computer, be smart online and be safe online.

The booklet is available online at www.ag.gov.au/cybersecurity. You can request hard copies of this publication from cybersecurity@ag.gov.au.

Where to go for more information

Cyber security

- www.staysmartonline.gov.au – for individuals and small business
- www.cert.gov.au – for large companies
- copies of the Australian Government's *Cyber Security Strategy* are available at www.ag.gov.au/cybersecurity
- www.icode.net.au for information on the Internet Industry Association's voluntary code of practice on cyber security (the icode)

Cyber safety

- www.cybersmart.gov.au
- www.thinkuknow.org.au
- cybersafety@acma.gov.au or phone 1800 880 176
- www.dbcde.gov.au/helpbutton

Identity security

- www.ag.gov.au/identitysecurity

Offensive content

- www.acma.gov.au

Online shopping

- www.accc.gov.au or phone 1300 302 502

Privacy

- www.privacy.gov.au

Scams and fraud

- www.scamwatch.gov.au
- SCAMwatch twitter – follow SCAMwatch on Twitter at http://twitter.com/SCAMwatch_gov or @SCAMwatch_gov

Spam

- www.spam.acma.gov.au
- phone the spam hotline on 1300 855 180
- spam SMS can be forwarded to 0429 999 888