Be Connected

Introduction to internet safety

Let's help make sure we use the internet safely.

Computer and email security

Some of the main online risks include:

- **Viruses**, which spread from computer to computer through the Internet. Some are just a nuisance, others can also delete your data.
- **Trojans**, which are innocent looking programs that try to trick you into installing them.
- **Spyware**, programs that steal information like passwords or bank account details.

There are steps you can take to protect yourself and your computer from online threats.

1. Use **antivirus software**, which helps find, stop and remove viruses.
2. Use **anti-spyware software**, which helps stop your data being stolen.
3. Use a **firewall**, which helps protect your computer from unauthorised access from the internet.
4. Keep your internet security software up to date.
5. If you received antivirus software with a new computer, renew it when the trial runs out, or obtain free software such as AVG. Please note that Windows 10 comes with effective anti-virus software called Windows Defender. Windows will keep it up to date on your behalf.
6. If uncertain, get advice from **https://www.staysmartonline.gov.au/**.

Introduction to internet safety

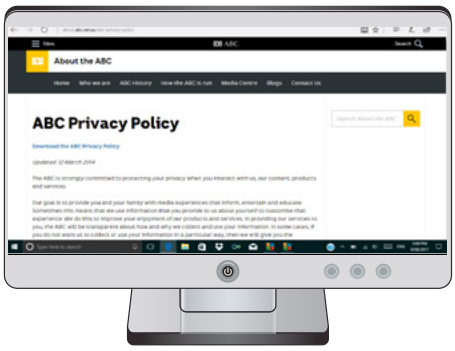
You should take extra care not to expose your computer to malicious software.

1. Think twice before opening emails - and especially email attachments - from people you don't know.
2. Deal with businesses online that you know to have a good reputation. Search for information about a company before you buy.
3. Make regular backups of all the information on your computer. If your computer does become infected, you will still have access to all your important data.

Protect yourself and your computer from online threats

Use of personal data on the internet

Sometimes it is necessary to provide personal information online, but there are limits to how much information you should share, and remain aware of your rights.



Laws govern the use of personal information by private companies in Australia

- Only provide information to legitimate companies if it's needed to verify your identity.
- Avoid posting personal information (date of birth, home address and so on) to public forums such as Facebook. Personal information can be used by criminals for identity theft.
- Laws govern the use of personal information by private companies. In Australia, that is the Privacy Act 1988.
- The Freedom of Information Act may apply to information you provide to government bodies.
- Reputable companies have policies on how they care for personal information. Read their privacy policies on their websites.
- For further information on consumer rights or up to date information on protecting yourself from scams, please visit the ACCC: **https://www.accc.gov.au/consumers.**

Introduction to internet safety

Online payment and secure areas

Beware of the information you share online

Buying things online can be convenient, and there are some quick checks to help ensure you pay safely.

1. Does the company you're dealing with have a good reputation? Check the company's privacy and return policies on its website. Use a search engine to find out more about the company.
2. Purchase using a credit card or PayPal. Both offer some form of buyer protection.
3. Just before entering your credit card information, check the **Address bar** of your browser. A secure site should be marked with a padlock and the website should start with **https:** (not just **http:**).

Child safety online

Children are less experienced in the world and so are more at risk from:

- Viewing explicit materials.
- Disclosure of personal information.
- Bullying and harassment.

Internet chatrooms and social media are places where approaches could be made. Never let your child meet up with anyone they've 'met' online unless they're accompanied by an adult.

There is protective action you can take top help children stay safe online.

1. Create the child's own user account for the computer.
2. Switch on parental controls for that user account.
3. For Google, turn **SafeSearch** on, and for Bing or Yahoo, set SafeSearch to '**strict**'.
4. Set YouTube to 'restricted', along with any other video sites.
5. Talk to your child about the dangers they could face online.

If a child has accidentally ended up in a dangerous situation online, report it to the Office of the eSafety Commissioner at:
https://www.esafety.gov.au/complaints-and-reporting.