

## Protecting your information

### Teenagers

Personal information is any information or combination of information that enables the identification of an individual.

Personal information is disclosed to, and used responsibly by, many legitimate online businesses to conduct business and online social interactions. However, if not managed carefully, it is possible for personal information to be accessed and misused for marketing, identity theft or for cyberbullying or cyberstalking.

The following tips can help teens manage their personal information safely and responsibly.

- Remind your teen that not everyone is who they claim to be. Although they may enjoy having many online friends, adding people that they don't know on 'friends lists' allows those people to learn all about them. This information could be used for scams, to steal their identity or worse.
- Talk to your teen about managing personal information on social networking sites. Encourage them not to put any personal information on their profiles. This includes their phone number, personal email address, home or school addresses, or the name of their school.
- Encourage your teen to be careful when they post photos that they are not accidentally providing clues to personal information such as their school uniform.
- Encourage your teen to set up a separate email account for use when signing up to games or websites. This account will be separate to all other personal accounts so they can disable it if it's misused. It should not include their names or other identifiers in the address.
- They might also like to set up a separate social networking account if they want to promote themselves or an interest and engage with like minded people that they don't know offline. They should ensure the site does not contain their personal information.
- Encourage your teen to read user agreements and privacy policies to determine how their personal information may be used when signing up to services as many organisations use information for their own marketing and some sell it to other marketing firms.
- Remind your teen that they should only disclose financial information on websites that they trust and that have secure payment facilities identified by a web address beginning with <https://> and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.
- Remind your teen that banking institutions will never email individuals asking for their user name or password. If they receive an email from an organisation claiming to represent a banking institution they should report the email to the bank and the Government's SCAMwatch website at [www.scamwatch.gov.au](http://www.scamwatch.gov.au) or their local consumer affairs agency. They should not respond and not click on any links provided.



# cyber(smart:)

## More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at [www.cybersmart.gov.au](http://www.cybersmart.gov.au). Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.