The internet has increasingly become part of our daily life, and so it is important for teens to adopt smart behaviours to protect personal and financial information online.

Here are some tips to help teens practice safe online behaviour:

- **Make sure your computer is secure**—install security software and turn on all automatic updates on all software, including your operating system and other applications.
- **Set strong passwords**, particularly for important online accounts and change them regularly—consider making a diary entry to remind yourself.
- **Stop and think before you share any personal or financial information**—about you, your friends or family. Don't disclose identity information (drivers licence, Medicare No, birth date, address) through email or online unless you have initiated the contact and you know the other person involved.
- **Don't give your email address out without needing to**. Think about why you are providing it, what the benefit is for you and whether it will mean you are sent emails you don't want.
- **Be very suspicious of emails from people you don’t know**, particularly if they promise you money, good health or a solution to all your problems. The same applies for websites. Remember, anything that looks too good to be true usually is.
- **Limit the amount and type of identity information you post on social networking sites**. Don't put sensitive, private or confidential information on your public profile.
- **When shopping online use a secure payment method such as PayPal, BPay, or your credit card**. Avoid money transfers and direct debit, as these can be open to abuse. Never send your bank or credit card details via email.
- **When using a public computer, don't submit or access any sensitive information online**. Public computers may have a keystroke logger installed which can capture your password, credit card number and bank details.
- **Deal with cyber bullying**. Don't respond to the bully, tell an adult you can trust (and your school and Internet Service Provider) and save any emails, online conversations, text messages of voicemails as evidence.
- **Secure your mobile phone**. Turn on security settings, turn off Bluetooth and GPS when not using it, use an encrypted network that requires a password when browsing online using WiFi, and be careful when downloading applications.

Visit [www.staysmart.online.gov.au](http://www.staysmart.online.gov.au) for further information on how to stay safe online.