Security Tools

It's important to secure your computer properly-otherwise you may be putting yourself and possibly your family and friends at risk.

If malicious software infects your computer it can stop it working properly, can delete or corrupt your files and can allow others to access your computer and your confidential information.

Having up-to-date security software installed and activated, securing your internet connections and services and understanding and managing the emails and files you do receive or download can help reduce the risks.

Backing-up your data can also help you recover your information if a virus destroys your files, or your computer is stolen or damaged.

Protecting your children from harm is just as important online as it is in the real world. As a parent or carer, you can play an important role in helping children have safe and positive experiences online.

The internet offers an exciting world of experiences for children and the whole family. It can be entertaining, educational and rewarding. However, using the internet also involves risks and challenges.

Children might be exposed to content that is sexually explicit, violent, prohibited or even illegal. They may also experience cyber bullying or be at risk from contact by strangers.

Children may - unknowingly or deliberately - share personal information without realising they may be subject to identity theft, or that they are leaving behind content that might not reflect well on them in the future.

By taking an active role in talking with you kids about the risks and answering their questions or concerns about something that they find on the Internet you can help them stay safer online.

Tips

- Know what your children are doing online.
- Get to know the technologies your children are using
- Discuss the risks with your children and agree on some rules for internet use.
- Tell your children if they are uncomfortable talking to you they can contact the Cybersmart Online Helpline (Kids Helpline) www.cybersmart.gov.au
- Place the computer in a family area of the home
- Install an internet content filter
- Make sure your children now not to share personal information or photos.
- Report inappropriate, harmful or criminal activities that occur online or via a mobile device to www.thinkuknow.org.au

- Report offensive content to the Australian Communications and Media Authority (ACMA). phone 1800 880 176

With proper planning and the implementation of some basic precautions, it is possible to limit becoming a victim of telecommunications fraud. Below are some quick tips that are recommended to help protect you.

Broadband Service
With the variety of ways to access the internet such as wireless networks there are additional safety precautions you should to consider rather than the physical security of your modem.

Tips to consider:

- Disable any remote access on your modem/router
- Regularly change your routers username and passwords (particularly once you have set up for the first time)
- Ensure your passwords are something that only you will know and use a combination of characters such as upper case, lower case, symbols and numbers
- Disable broadcasting the name of your connection
- Only allow specific devices that you have authorised connect to your internet
- If you are going away or not using your internet connection for an extended period of time switch off your router
- Ensure all you anti-virus software is up to date
- Have a firewall installed on your modem/router
- Install an Ad-Ware application to protect your computer against malicious software
- Before opening any email attachment ensure you are familiar with their source
- Understand the dangers of pirated software and file sharing
- Stay informed about the current techniques of cyber criminals and the latest scams

VoIP Service
As VoIP uses the internet the implementation of some simple security measures can allow customers to enjoy the benefits of VoIP without compromising on security.

Tips to consider:

- Ensure your home or office network security software is up to date
- Use complex passwords for your router and change them regularly
- Ensure you have anti-virus and anti-malware installed on your computers
- Protect your site with a hardware based firewall
- Minimise access to your PBX or Voice Box
- Never place your device in a De-Militarised Zone (DMZ) of your router
- Done give out sensitive information such as usernames and passwords
- Stay informed about developments and improvements in VOIP security options

For further information about online security and safety visit the Australian Government website http://www.staysmartonline.gov.au/