Security Basics

If you instigate these basic security procedures on your devices and computers, it will help keep the devices and computers much more secure!

Recently I came across a number of people in the local community who have suffered greatly because they did not understand how to set up basic device security. As a result their health was severely affected, because of the stress created by the significant financial losses they incurred. So it is worth putting the effort in to instigating these suggestions.

The more services you have turned on in your device or computer, the more doorways are available for a hacker to break in!

Turning your mobile phones, modems, tablets, and computers off completely went not in use, greatly limits the time available for someone to break into the device.

Only have the device's wireless, bluetooth, nearby device scanning**,** data, and GPS/Location functions turned on, when necessary. Remember there can be more than one wireless type built into a device, WiFi as well as bluetooth and GPS etc. You can turn these functions off in the laptop, smart phone and tablet, settings. This will significantly improve security by limiting the number of remote access doorways into your device. **Use *"Flight Mode",* to turn multiple wireless services off at once.**

Turn off unused services like your microphone and cover web cam if not in use. These devices can be used to listen in or see what you are doing. People have been blackmailed by hackers who have recorded embarrassing or sensitive information of users by recording the microphone and webcam feed.

Have an up to date anti-virus and spyware / malware program installed on your computer, plus make sure the device firewall is turned on.

Where possible, only download and install well known programs from the software creators sites, and not from third party sites. This will greatly reduce the potential chances of a program being hacked before download. Free and paid software can be hackware. Do a search engine investigation to make sure it is safe to use before installing.

Don't save all your passwords on devices, this only becomes a honey pot for hackers to get all your passwords.

Never allow anyone to access your computer remotely unless they are well known to you and you have asked them to. **Ignore those web page pop ups asking you to ring a number to fix alleged security issue!**

Ignore any unsolicited phone calls or emails claiming to be from your bank, Telsra, a software firm like Microsoft, the taxation office, Insurance firm etc. **THESE ARE DEFINITLY HACKS AND SCAMS!**

Security Check List

√ Tick (Relatively easy to implement)

- **Anti-virus program installed, up to date and working**
- **Spyware / Malware program up to date and working.**
- **Keep your devices up to date with the latest operating system, software, and driver updates.**
- **Only use complicated passwords.** Passwords should be at lest 8 to 12 characters long, plus be made up of upper case, lower case, symbols and numbers. They should also be random, and do not use dictionary words. Use different passwords for different services.

Having a password book would be a good idea, so if you forget a password you can look it up. Stored this book away form your device.

- **Turn off *Wifi* in your device and modem when not in use. Most modern devices and modems have a physical or software WiFi on / off switch.**
- **Turn off the *Blue Tooth* service when not in use.**
- **Turn off *GPS / location services* when not in use.**
- **Turn off *smart phone and tablet data services* when not in use.** Ever wondered why your prepaid plan keeps running out of money very quickly? This could be the reason.
- **Cover your computer or laptop web camera when not in use.**
- **Cover your smart phone and tablet web camera when not in use.**
- **Turn off your device microphone when not in use.**
- **In the *network connection settings* turn off file and printer sharing, if you don't use it.**
- **Turn off the "Remote Access" service in your device, if you are not using it.**
- **Turn off file synchronising if not in use. This feature allows you to synchronise files, photos, contacts etc., and settings amongst multiple devices.**

√ Tick (A bit more skill level will be needed to implement these tasks.)

- **Change the factory set default user password that allows you to access your ADSL or NBN modem, to one you have created. Read the device manual to find out how to do this.**
- **Change the factory set default pass key and SSID (Wifi station name) of your ADSL or NBN modem, to one you have created. Read the device manual to find out how to do this. Newer NBN modems can have 2.4G and 5G Wifi turned on, turn one of both off, if not in use.**
- **Add a secure DNS address like 208.67.222.222 to your device's Ethernet and Wifi settings.**
- **Under the *"Privacy Settings"* in Windows Eight and Ten, turn of all the Windows service activities you don't use.**

It is import to understand that if you are using a device for banking or financial transactions, it is a requirement to have an up to date virus checker installed and the firewall turned on, or you may be in breach of your Internet banking terms of use agreement.

If you are unsure how to implement any of the above suggestions, please attend a club meeting, and get help. I hope this information has helped you. More information on this subject can be found at the club web site, under the *"Computer Security"* heading here.
http://sccc.org.au/site-index

Peter Daley
President,
Sunshine Coast Computer Club Inc.