Security Basics For All Devices!

If you instigate these basic security procedures on your mobile phone, tablet and computer, it will help keep these devices 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. It is worth putting the effort in to instigate these suggestions.

Most of the suggestions below are universally applicable across most make and models of phones, tablets laptops,, computers and modems. 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, tablets, computers & modems off completely when not in use, greatly limits the time available for someone to break into the device. **(Note: Some modems need to stay on to maintain VIOP phone services.)**

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 computer, laptop, smart phone and tablet, settings.

This will significantly improve security and safety by limiting the number of remote access doorways into your device. **Use the *"Flight Mode"* setting to turn multiple wireless services off at once. You will find more important information on Wifi and device safety here, http://sccc.org.au/wifi/microwave-safety-chart.pdf**

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 web cam 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, NBN, a software firm like Microsoft, the taxation office, Insurance firm etc. **IT IS IMPORTANT TO EDUCATE ALL YOUR FAMILY THAT THESE ARE DEFINITELY HACKS AND SCAMS!** If you think it may be legitimate, hang up and *independently* look up the organisation's official phone number, and call them directly.

If you are unsure how to implement any of the suggestions, please attend a club meeting, and get help. http://sccc.org.au/

√   **Security Check list, (Relatively easy to implement)**

🟧   **Anti-virus program installed, up to date and working.   (Go To Page 2 ->)**

- **Spyware / Malware program up to date and working.**

- **Download and run this free [Inspectre tool](#) to check if your Windows computer is protected from the serious Meltdown and Spectre hardware flaws.**

- **Keep your devices up to date with the latest operating system, software, firmware, and driver updates.**

- **Only use complicated passwords.** Passwords should be at least 8 to 12 characters long, plus be made up of random upper case, lower case, symbols and numbers. You should not use dictionary words or a simple number sequence. 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. Securely store this book away from your devices.

- **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.**

- ***Surveillance for profit is the new oil.* Reclaim your personal privacy, under "Privacy Settings" on your smart devices, computer, or app, turn off all data sharing services you do not want!**

- **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 free secure [Open DNS](#) address like 208.67.222.222 or 208.67.220.220 to your device's Ethernet and Wifi settings.**

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.

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. **(Send a copy to your friends and relatives)**