

CYBER SECURITY A YOUNG AND OLD TIPS

HOME SECURITY

- Consider changing WiFi SSID Name from default value
- Always have a WiFi password and make the password long and memorable
- Always use WPA2 or better WiFi security NOT WEP(WEP is crack-able)
- Consider disabling Remote Administration of the router – only make admin access accessible from inside your home network on WiFi or physically connected with a network cable
- Always change default 'admin' account password for your router. Websites list the defaults for each manufacturer!
- Always keep the router firmware up-to-date
- Always keep the firmware/software updates on any devices connecting to your WiFi turned on
- Always use modern supported Operating Systems (Windows 7/Windows 10/Ubuntu 16.04) etc – older unsupported Operating Systems increase the risk to your network.

MALWARE (Malicious Software)/Ransomware

- Be careful what websites you visit – some sites are booby trapped to infect your device
- Always keep your Anti-Virus Software up-to-date
- Backup on a portable drive anything you deem important from your computer – never leave the backup device connected and switched on as Ransomware can infect that too. Disconnect after backup.
- NEVER offer to pay up if you have ransomware – Reinstall from blank and restore your backups.
- Be wary of emails that ask you to click on links – the links may not always go where you think. "hover" the mouse over the link and it show you the web address that would be used if you click it.

SCAM CALLS

- Your bank will NEVER ask for your password to your online account
- Consider the TPS Service (Telephone Preference Service)
- Consider the BT 8500 phone to block scam calls 100% works!

BEING SAFE ONLINE – Web browsing

- Any website that expects you to "login" should be encrypted when you talk to it e.g. HTTPS at the start of the address HTTP (S means secure) - Look for a green padlock next or the words "Trusted" next to the website address

MOBILE PHONES

- Always enable the lock screen to protect your phone – password is better than 4 digit code!
- Enable device encryption – Apple/Android
- Consider using the Anti-theft features e.g. device tracking via GPS if lost and also enables remove lock/wiping of the phone
- Consider installing Anti-virus/malware bytes scanner

PRIVACY

- Use TOR browser – available for phone and PC's
- Review your Social Media settings for privacy e.g. Facebook/LinkedIn/Instagram/Google+
- NEVER use the SAME password for more than one login! If somebody breaches the easiest website that you use that password – the rest are then open too.
- Clean up emails – delete old emails- if your mailbox was hacked, it gives clues as to other aspects of your digital life