1. Safe Online Behaviour

There are a significant number of ways in which you can improve the security of your devices, such as computers, smartphones and tablets, and protect yourself and your information.

Click on the www.getsafeonline.org weblink to learn more about the topics listed below.

1. Protecting your computer

Antivirus, viruses & spyware - A basic understanding of computer viruses and spyware.

Backups - Regularly back up your files to protect your data.

Downloading & file sharing - Use trusted websites. Ensure you have effective and updated antivirus/antispyware software and firewall running before you start downloading.

Firewalls - A firewall protects you against**:**

- Hackers breaking into your computer
- Worms – types of viruses that spread from computer to computer over the internet
- Some outgoing traffic originating from a virus infection

Online gaming - Online gaming is growing in popularity. Make sure you do it safely.

Passwords - Always use a password. Choose a password with a combination of upper and lower case letters, numbers and keyboard symbols such as @ # $ % ^ & * ( ) _ +. (for example SP1D3Rm@n – a variation of spiderman, with letters, numbers, upper and lower case). However, be aware that some of these punctuation marks may be difficult to enter on foreign keyboards. Choose a password containing at least eight characters, although it should be noted that longer passwords are harder for criminals to guess or break.

Physical security - A few physical security measures to help combat cyber crime.

Ransomware - Beware malware that holds you to ransom.

Safe computer disposal - How to dispose of computer hardware safely.

Safe internet use - The risks of visiting malicious, criminal or inappropriate websites include:

- Viruses and spyware (collectively known as malware)
- Phishing, designed to obtain your personal and/or financial information and possibly steal your identity

- Fraud from - fake shopping, banking, charity, dating, social networking, gaming, gambling and other websites
- Copyright infringement – copying or downloading copyright protected software, videos, music, photos or documents
- Exposure to unexpected inappropriate content

Safe Linux use - Advice on how you should use a Linux system safely online.

Searching the internet – Risks from searching the internet and advice to do this safely.

Skype & internet calls - Use the internet to make calls safely.

Software updates - Criminals will exploit vulnerabilities in software that may have been patched by the provider in more up-to-date versions, so not keeping your software current can result in serious issues, affecting both your computer and your own personal security. These include:

- Viruses, spyware and other malware
- Cyber-criminal attacks
- Crashing, freezing and generally poor performance

As well as resolving security issues, software updates frequently contain improvements and new features.

Spam & scam email - A few simple rules about dealing with spam and scam emails.

Update your browser - Run the latest version of your chosen browser.

Webmail - Using the internet to send and receive email safely.

Windows updates - Everything you need to know about operating system updates.

Wireless networks & hotspots - Simple rules on setting up and using wireless networks and hotspots.

2. Protecting yourself

Accepting terms & conditions - Terms and conditions are legally binding. Make sure you read them.

Buying & selling vehicles - Buying or selling ... protect yourself and your money.

Computer use in public places - Using computers, smartphones or tablets in public places safely.

eCards - Be sure you know what you're sending or receiving.

Fraud - There are many words used to describe fraud, for example scam, con, confidence trick, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink. Online fraud can be perpetrated via spyware and other malware or sometimes more elaborately in conjunction with other channels such as email, telephone calls or letters.

Holiday & travel booking - Risks and online booking advice.

Job searching - Advice on how to keep your online job hunting safe and secure.

Money muling - Transferring the proceeds of crime overseas is a criminal offence.

Price comparison websites - Be careful and make sure you really are getting the best deal.

Privacy - Maintain privacy and avoid identity theft or fraud.

Safe online dating - If you're looking for romance online, make sure you're doing it safely.

Safeguarding identity - Do not share account information with friends, family or other people. Ensure you always have effective and updated antivirus/antispyware software running. If possible, arrange for paperless bills and statements. File sensitive documents securely, and shred those you no longer need – preferably with a cross-cut shredder. Never divulge private information data in response to an email, text, letter or phone call unless you are certain that the request is from a bona fide source. Always beware of people looking over your shoulder when you are entering private information on a computer, smartphone, tablet or ATM.

Safe property rental - Sound advice on staying safe - whether you're a landlord or a tenant.

Transferring money - Take a few precautions when asked to transfer money.