Browser
The computer software or app you use to access the internet. E.g. Internet Explorer, Google Chrome, Safari

Hack
An attempt to gain unauthorised access to a computer or account

Malware
Malware is short for ‘malicious software’

Operating system
The software that manages different programs on a computer

Phishing
An attempt at identity theft in which criminals direct users to a counterfeit website to trick them into disclosing private information

Pop-up
A small window that suddenly appears (or ‘pops up’) on a webpage, usually an advertisement or an alert

Profile
A description that may include your personal details and is used to identify you on a social networking website

Router
A device that connects your computer to a broadband-enabled telephone line and emits your home internet signal

Smartphone
A mobile phone which, can connect to the internet, send emails etc.

Social networking website
An online community where you can connect with friends, family and other people who share your interests, e.g. Facebook, Twitter and Instagram

Spam
A commercial email that you did not request, also known as junk mail

Spyware
An unwanted program that runs on your computer, which can make it slow and unreliable or even make you a target for online criminals

Tablet
A larger handheld device with a touchscreen, which can connect to the internet

Viruses
Programs that spread from one computer to another by email or through malicious websites. They can slow your computer down, display unwanted pop-up messages and even delete files

Wireless network
Also known as wi-fi, this is a way for your computer to connect to the internet without using wires or cables

Produced by H Towle October 2017

U3A
THE UNIVERSITY OF THE THIRD AGE

NEWCASTLE EMLYN

Protecting your computer

With hacks, scams, malware and more, the Internet can feel like a dangerous place these days. And, the recent proliferation of devices, from smartphones and tablets to Internet-connected appliances, has opened us up to even greater risks.

But the good news is that by taking just a small handful of security measures we can greatly reduce our exposure to all these threats.

1. **Keep your computer updated**
   Every computer has an operating system (such as Windows or Mac), which is software that organises and controls all hardware and programs. Your computer can be better protected from viruses if you keep the operating system updated. You should receive notifications when new updates are available, but you can also update your system manually.

2. **Protect your wireless network**
   If you have a wireless router, check that your wireless network is secure so that people living nearby can't access it. It is best to set up your network so that only people with a wireless 'key' (i.e. password) can connect to your network.
   If your network is secured by a password, users will be prompted for a password when they try to access the network for the first time and there should be a padlock symbol next to your wireless network. If this doesn't happen, your network isn't protected and anyone can connect to your network.
   Read the instructions that came with your router to find out how to set up a wireless key and make your network more secure.

3. **Keep your software up to date**
   Not keeping your software up to date can result in serious issues, affecting both your computer and your own personal security.
   The software that may be on your computer includes:
   - ✓ Microsoft Products (either bundled with the Windows operating system or purchased separately)
   - ✓ Commonly Pre-Loaded (when you buy the computer)
   - ✓ Other Applications (which you load yourself from a CD/DVD or via the internet)

   As is the case with the Microsoft Windows operating system, online criminals quickly find vulnerable areas in other software and continue to do so for the lifetime of the version. To counter this, the software manufacturers release regular updates such as security updates or critical updates, which protect against malware and security exploits. Other types of updates correct errors that enhance the software's functionality.
   Downloading the latest software updates does not negate the need to be running the latest versions of antivirus, anti-spyware and firewall software. You will generally receive a notification from the software manufacturer in the form of an alert on your screen, that updates are available. You will normally be given the choice of whether to download and install the update immediately or later. It is recommended to download and install as soon as possible.
   Some software updates require you to restart your computer in order to complete the installation process. Again, it is recommended that you do this as soon as possible. Turn on automatic updates so you don't have to think about it, and make sure that your security software is set to run regular scans.

4. **Always have internet security software loaded switched on and kept updated on your computer**. (e.g. anti-virus, anti-spyware)
   Anti-virus software will look for and remove viruses before they can infect your computer.
   Anti-spyware software prevents unwanted adverts from popping up, tracking your activities or scanning your computer for personal information.
   The best option for beginners is to buy a 'package' from a reputable provider (such as McAfee or Norton), which will include a range of security software. You can download these programs from the internet or visit a retail computer store for guidance.
   Your internet service provider might also offer security software as part of your internet deal. There are also popular free security software programs available to download online, such as AVG, Avast or Microsoft Security Essentials.

5. **Use a Firewall**.
   Even if your network is secure, you should still use a firewall. This is an electronic barrier that blocks unauthorized access to your computers and devices, and is often included with comprehensive security software. Using a firewall ensures that all of the devices connected to your network are secured.

Glossary of terms

Anti-spyware
Helps protect your computer against pop-ups, slow performance and security threats caused by spyware and other unwanted software

Anti-virus
Software that detects and prevents known viruses from attacking your computer

Apps (applications)
A type of computer program that you can download for your computer, tablet or mobile phone

Attachment
Files, such as photos, documents or programs, which are sent along with an email