CYBER BASICS #02

THE "WHAT, WHY AND HOW" TO SECURING YOUR COMPUTERS, DEVICES AND YOURSELF

ANTI VIRUS SOFTWARE

What?

Computers and electronic devices are all vulnerable to malicious software (malware). Malware can come in many different forms - some can lock your files, steal financial information or provide a cyber criminal with complete access to your system.

Why?

Anti-virus software greatly reduces the chance of a computer being infected by known malware. In most cases, anti-virus software will also remove infections found on the system. It protects your computer and your information making it an extremely important tool. Ensuring that your anti-virus definitions are kept up to date will protect your computer from the latest threats.

How?

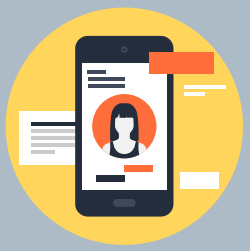
Many computers and devices have inbuilt anti-virus already installed but, if not, there are a wide range of anti-virus software packages available. Many of them also offer additional security and privacy capabilities, such as a firewall and VPN . Don't delay in installing anti-virus software because without it you have much higher risk of being infected. There are plenty of free options available, so do some research of reputable brands and secure your computers and devices as soon as possible. Check your anti-virus settings regularly to ensure that it is turned on and performing automatic scans. Also consider performing a manual full scan once a month as some files can be downloaded and stored before the anti-virus software recognises them.

PRIVACY SETTINGS

What?

Consider what you post online on social media, forums and other services which place your personal information and opinions in the public domain.

Why?



Your online presence can provide criminals with a profile of your life. They can potentially find out where you live, your current location,your job title and other information about you that can help them to commit a variety of criminal acts such as burglary, spear-phishing/whaling3 or financial fraud.

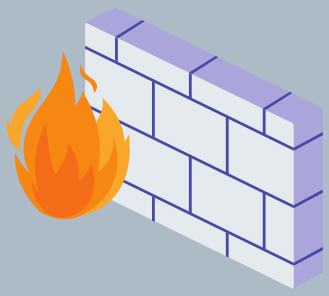
How?

Occasionally do a search of yourself using a search engine (e.g. Google, Bing) - if you can see it, so can everyone else. Also consider the social networks and forums you use - visit their privacy settings pages to lock down any information you wouldn't want people other than your friends and family to see.

ADDITIONAL INFORMATION

& RESOURCES

DEFINITIONS



Firewall

A virtual boundary surrounding a network or device that is used to protect it from unwanted access. It can be hardware-based (physical device) or software (computer application).
Most Operating Systems have a firewall already built-in – it's an important element of maintaining a secure computer so ensure it is turned on.

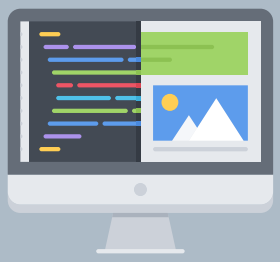
Virtual Private Network (VPN)

A virtual boundary surrounding a network or device that is used to protect it from unwanted access. It can be hardware-based (physical device) or software (computer application). Most Operating Systems have a firewall already built-in – it's an important element of maintaining a secure computer so ensure it is turned on.

Phishing, Spear-phishing & Whaling

Phishing, spear-phishing & Whaling – Phishing is an email or electronic communications scam that aims to steal sensitive information, install malicious software (malware) or compel the target to make a payment by masquerading as a legitimate, trustworthy person or organisation. Spear-phishing is a type of phishing scam targeted towards a specific individual, organization or business, whereas whaling is a type of spear-phishing attack that targets high-profile employees, such as the CEO or CFO.

USEFUL WEBSITES



Office of Cyber Security & Information Assurance
www.gov.im/ocsia

UK National Cyber Security Centre (NCSC)
www.ncsc.gov.uk