

Portable Device Security

IT So many of us now have portable internet devices such as mobile smart phones and tablets. But because we use them so often there is the risk of them being lost or stolen. Consider how much personal information is kept on these devices. It is vital that they have the right level of security.

Turn on Password Protection – Ensure you enable any inbuilt protection offered by the device such as a password / PIN screen lock or the use of your fingerprint or face scan for ID. Combine this with a strong and difficult to guess password or passphrase and you will boost your security. Many of these devices also have an option where all the information on the device is automatically removed if the wrong password is entered too many times. Consider using this option if possible.

Keep it up to date – It is important that that software updates for both the Operating Systems and any Applications are enabled for automatic update. Check to see if **Anti-Virus** software is installed (**and turned on**) and if not consider adding it.

Don't use public Wi-Fi unless it is encrypted (secure) – whilst a simple and attractive option, most public Wi-Fi networks offer much lower security than your own personal network. Criminals can even monitor who is using public Wi-Fi to find targets, or impersonate the public Wi-Fi network itself.

If available, the use of a VPN (Virtual Private Network) will enable you to connect securely to a network.

Only use **Trusted App Stores**, untrusted ones may include apps containing **Malware**.