BRIEFCASE

Laptop Security

If you provide your staff with laptops (or other portable computers, such as tablets) what security measures should you ensure are in place? Your first port of call should be to seek professional IT advice to ensure appropriate security measures are in place. Remember, often the data stored on a laptop is more important than the laptop itself!

Basics

- Don't store any sensitive information, such as PII (personally identifiable information) on the laptop's hard drive.
- Instead store sensitive information (and all data, if possible) on a remote server or cloud solution with adequate security.
- Where this cannot be achieved, for example due to a lack of Wi-Fi access, ensure laptop users are trained to keep data on local machines for as short a time as possible and to upload it to your server/cloud as soon as possible.

Always use a password for login

- All devices must only be accessible via a strong password or more secure protection, such as biometrics (fingerprints or eye scanners, which are common on some portable devices).
- Always use complex passwords with a combination of letters, capitals, numbers and punctuation.
- If possible, put in place IT/system policies to ensure passwords are strong enough.
- Change passwords regularly.
- Do not store passwords centrally if this can be avoided.

Logging off and shutting down

- Turn laptops off at the end of the working day.
- Adjust settings so that laptops (and all your pcs) log out if they are unused for (eg) ten minutes.

Make your laptops stand out!

- Brand laptops with permanent company graphics, making them less valuable/attractive to thieves.

Antivirus software:

- Use a credible antivirus with regular updates.

Firewall

- Use a suitable firewall with regular updates.

Update all your software

- Keep software up to date, especially the browser and anti-virus and firewall software.
- Keep your operating system up to date.

Backup

- Regularly back up your server and/or cloud solution.
- Include laptops in your back up protocol.

Travelling

- Never leave a laptop in a car except when locked in the boot.
- When travelling with luggage, keep devices in your main suitcase, not in an extra laptop bag.

Physical security lock

- Most laptops have a connection port allowing a cable to be securely attached. Attach the other end to a desk or other heavy object.

Other ideas…

- Consider encrypting the storage in your device.
- Consider installing software that enables you to remotely disable, encrypt or wipe laptops or devices remotely.
- Consider installing tracking software to allow you to locate a missing laptop when connected to the internet.

You may consider covering your webcam when not in use to avoid information being gathered by the camera if your laptop is compromised.