Malware and Ransomware

Malware is malicious software, which - if able to run - can cause harm in many ways, including:

- causing a device to become locked or unusable
- stealing, deleting or encrypting data
- taking control of your devices to attack others
- obtaining credentials which allow access to your systems or services that you use
- 'mining' cryptocurrency
- using services that may cost you money (e.g. premium rate phone calls).

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network.

Usually you're asked to contact the attacker via an anonymous email address or follow instructions on an anonymous web page, to make payment. The payment is invariably demanded in a cryptocurrency such as Bitcoin, in order to unlock your computer, or access your data. However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files.

Malware can get into a computer or device via:

- contaminated email attachments
- infected websites
- corrupted memory sticks, floppy disks, DVDs, CDs, cameras or networks

Ways to protect against malware

- Use antivirus software and keep it up to date.
- Only open email attachments from trusted sources. Check with them if you are unsure about something before opening it.
- Back up your data regularly and keep copies in a safe place.

- Use a firewall.
- Don’t connect any unknown devices to your computer.