



Computer Basics: Terms and Definitions

5. Security

Malware	An umbrella term for malicious software such as viruses, worms, Trojans or ransomware. Malware often finds its way onto a computer by downloading or opening unknown file attachments from suspicious emails or unsecure sources.
Virus	A virus is a type of malware that attaches itself to files or programmes and can spread when they are used or shared.
Computer worm	A computer worm can spread autonomously, often via networks, without the user having to actively share an infected file.
Trojan	A Trojan is malware that disguises itself as a useful or harmless programme.
Spyware	Spyware secretly collects information about users, devices or their activities and can transmit this to third parties.
Ransomware	Ransomware can encrypt data or block access to systems and then demand a ransom.
Antivirus programmes	Antivirus programmes detect malware and can block, remove or quarantine it. The virus protection is constantly updated so that new threats can be detected.
Firewall	A firewall monitors network connections and can block unwanted or unauthorised access.
Passwords	Passwords should be as long and unique as possible. Do not use personal details or easily guessable words. Where possible, use multi-factor authentication.