

Antivirus



Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Cyber security



The protection of devices, services and networks - and the information on them - from theft or damage.

Firewall



Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Ransomware



Malicious software that makes data or systems unusable until the victim makes a payment.

Two-factor authentication (2FA)



The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Botnet



A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Denial of Service (DoS)



When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Internet of Things (IoT)



Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Software as a Service (SaaS)



Describes a business model where consumers access centrally-hosted software applications over the Internet.

Water-holing (watering hole attack)



Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Bring your own device (BYOD)



An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Digital footprint



A 'footprint' of digital information that a user's online activity leaves behind.

Macro



A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Social engineering



Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Whaling



Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Cloud



Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Encryption



A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

Patching



Applying updates to firmware or software to improve security and/or enhance functionality.

Spear-phishing



A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Whitelisting



Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Cyber attack



Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

End user device



Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Phishing



Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Trojan



A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Zero-day



Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.