

NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the @NCSC Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit www.ncsc.gov.uk/glossary.

Antivirus



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

Botnet



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

Bring your own device (BYOD)



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

Cloud



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

Cyber attack



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

Cyber security



Denial of Service (DoS)



Encryption

End user device

Digital footprint

behind.

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

Internet of Things (IoT)



Firewall

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

Hardware or software

traffic to prevent

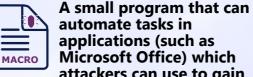
which uses a defined rule

set to constrain network

unauthorised access to

(or from) a network.

Macro



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

Patching



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

Phishing

 $\hat{\mathbf{x}}$ **A A**

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

Ransomware



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

Software as a Service (SaaS)



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

Social engineering



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

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.

Trojan



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





Collective term to describe modern

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

smartphones, laptops

to an organisation's

network.

and tablets that connect

A 'footprint' of digital

online activity leaves

information that a user's

Two-factor authentication (2FA)



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

Water-holing (watering hole attack)



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

Whaling



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

Whitelisting

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

Zero-day



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

For more information go to \Box www.ncsc.gov.uk $\forall @$ ncsc

