

CYBER TERMINOLOGY

Bitcoin	A digital currency/payment system which bypasses the need to use banks.
Bot	Short for web robot. A bot is an application that runs automated tasks/scripts over the internet. Normally the tasks are simple and repetitive and can be performed at great speed. They can be used to aid the sending of spam email and malware.
Botnet	Robot network. A number of internet devices running bots.
Dark Web	The part of the internet that is only accessible by special software allowing users and operators of websites to remain anonymous. Known for being used by criminals.
DoS Attack	Denial of access. Legitimate users of a computer or website are denied access due to hackers who overload the service to render them unavailable. No data is stolen.
Encryption	Conversion of information/data into a secret code to prevent unauthorised access.
Firewall	Protects a network or device from unauthorised access. The firewall monitors and controls incoming and outgoing traffic against specified security rules.
Malware	Malicious software such as viruses, Trojans and ransomware.
Patches	Software that updates a computer program to update it, fix bugs or fix security vulnerabilities to improve performance.
Phishing	Using email in attempt to trick people into divulging confidential or sensitive information (credit card details, account details, user names and passwords) for malicious purposes. The email is disguised as being from a trustworthy source (colleague or bank) and will often direct the victim to a website which will ask them to share their sensitive information.
Ransomware	Malicious software that blocks or restricts access to a computer system, device or files until a release fee or ransom is paid.
RAT	Remote access Trojan. (see Trojan) Allows cyber criminals backdoor access to a computer device.
Smishing	Social engineering targeting mobile devices (phones) using text (SMS) messages to obtain sensitive/confidential information or to facilitate the download of malware. (see phishing and social engineering)

CYBER TERMINOLOGY

Social Engineering	Tricking people to break normal security procedures and reveal sensitive or confidential information. For instance login information for online bank accounts.
Spam	Junk mail delivered electronically (junk email). Can be used to spread viruses or can just be unsolicited advertising.
Spear Phishing	A phishing attack directed at specific individuals / companies. (see phishing)
Trojan	Malicious computer program which misleads as to its true intent. Appearing harmless such as a form for completion or email attachment but can allow someone else to control your computer or collect sensitive information.
Virus	Malicious computer coding that can corrupt or destroy data or negatively affect the working of computer equipment/systems. Equipment is contaminated unknowingly with viruses spread by methods such as email attachments or downloads from the internet. The coding runs automatically in the background on opening of the infected file.
Vishing	Social engineering using the phone to induce people to divulge sensitive/confidential information. For example bank details. (see phishing and social engineering)