22/08/2022

GLOSSARY OF CYBER TERMINOLOGY

Term	Definition
419 scams	A type of advance fee fraud, where you are asked to help transfer money out of another country. It originated in West Africa, and 419 is the section of the Nigerian legal code that covers the crime.
802.11	The standard for wireless networks.
Access control	Controlling who has access to a computer or online service and the information it stores.
App	Short for application, this is a software program that is designed to perform a specific function.
Asset	Something of value to a person, business or organisation.
Action Fraud	The UK national reporting centre for fraud and cybercrime.
ActiveX controls	They can enhance your browsing experience by allowing animation or help with tasks, such as installing security updates at Microsoft Update. If you do not trust the website and publisher, click ‘Don’t run’ when prompted.
Administrator	A user with sufficient access rights to allow them to manage the access rights of other users and carry out other high-level computer management tasks.
Advance fee fraud	Any fraud that tricks victims into paying money up front on the false hope of receiving something significant later.
Adware	A form of spyware that displays unwanted advertisements on a computer.
Android	An operating system used by a number of smartphone and tablet manufacturers. The world’s most prolific operating system for smartphones.
Anti-spyware software	Software specifically designed for the detection and prevention of spyware. Often bundled in an internet security package.
Anti-virus software	Software specifically designed for the detection and prevention of known viruses. Often bundled in an internet security package.
Attachment	Files, such as programs or documents, that are attached to an email.
Authentication	The process to verify that someone is who they claim to be when they try to access a computer or online service.
Back door	A loophole in a computer's security systems that allows a hacker to gain access. Often deliberately built in by developers for illicit purposes.
Backing up	To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.
Bandwidth	The speed at which a network can transmit data – typically used to describe speed of internet connections.
Biometric	Using body measurements, such as fingerprints and irises, as a means of authentication.

Term	**Definition**
BIOS password	The BIOS software is built into the PC and is the first software run by a PC when powered up. This software can be password protected, which stops the PC from starting up.
Bit	The basic binary unit of data, representing 0 or 1.
Bluetooth	A type of short-range wireless connection between devices, such as mobile phones, headsets and computers.
Boot	To start up or reset a computer, mobile phone or tablet.
Botnet	A collection of otherwise unrelated PCs, which have been infected by a virus and are under the central control of criminals or hackers. Abbreviation for Robot Network.
Bring your own device (BYOD)	The authorised use of personally owned mobile devices, such as smartphones or tablets, in the workplace.
Broadband	High-speed data transmission system where the communications circuit is shared between multiple users.
Browser	A program that lets users read and navigate pages on the internet, such as Microsoft's Internet Explorer, Mozilla's Firefox, Google's Chrome or Apple's Safari.
Buffer	A region of memory in which data is temporarily held before it is transferred between two locations or devices.
Bug	An error or flaw in a computer program.
Business continuity management	Preparing for, and maintaining, continued business operations following disruption or crisis.
Byte	A unit or measure of computer memory, usually consisting of eight binary digits (bits) processed together; usually enough to store a single letter or digit.
Certification	Declaration that specified requirements have been met.
Certification body	An independent organisation that provides certification services.
Chargeback	A payment card transaction where the supplier initially receives payment, but the transaction is later rejected by the cardholder or the card issuing company. The supplier's account is then debited with the disputed amount.
Chat room	An online discussion group where you can chat (by typing) with other users in real time.
Cloud computing	Delivery of storage or computing services from remote servers online (ie via the internet).
Common text	A structure and series of requirements defined by the International Organisation for Standardisation, that are being incorporated in all management system International Standards, as they are revised.
Computer Misuse Act 1990	UK legislation that outlines cybercrime offences.
Cookie	A small file which asks permission to be placed on your computer's hard drive. Cookies allow web applications to personalise your experience by gathering and remembering information about your preferences.

Term	Definition
Copycat website	A website posing as a trusted site (e.g. government websites), often mirroring the look and feel of the original official site but charging a substantial premium.
Cracking	Finding a password or PIN by trying many combinations of characters.
Critical update	A software update that fixes a major security flaw.
Cyberbullying	The use of technology to harass, threaten, embarrass or target another person.
Cybercrime	Any crime that involves a computer, the internet or related technology. The computer could be the object of the crime or used as a tool to commit the offence.
Cyber-enabled crime	Normal crime that can exist outside of a computer environment, however the use of a computer has significantly increased its reach and effectiveness.
Cyberstalking	The use of the internet or other electronic communication to stalk or harass an individual, group or organisation.
Data server	A computer or program that provides other computers with access to shared files over a network.
Dark Web	A portion of the internet that cannot be accessed by normal search engines and requires special software or authorisation to access. Notorious for hosting websites with criminal content such as drug marketplaces and child sexual exploitation material.
Decryption	The process of converting encrypted data back into its original form.
Declaration of conformity	Confirmation issued by the supplier of a product that specified requirements have been met.
Deep Web	A portion of the surface web that is not indexed by normal search engines and are usually inaccessible due to them being hidden behind login forms, e.g. webmail, mobile banking and social media profiles.
Denial of service attack (DOS)	Deliberate overloading of a service by criminals to make it unavailable to legitimate users. A DoS attack is usually done by a single individual.
Distributed denial of service attack (DDoS)	Deliberate overloading of a service by criminals to make it unavailable to legitimate users. This is typically done by arranging millions of simultaneous ‘ping’ requests to a server, normally from a botnet.
Digital file delivery	Company portal which facilitates the sharing of files over the internet.
Desktop firewall	Software designed to prevent unauthorised access to a computer over the internet.
Digital footprint	The data trace of a user’s activities, actions, communications or transactions created, when using the internet, which can be used to track the user's activities and devices.

Term	**Definition**
Digital signature	Data that is used to identify and authenticate the sender and integrity of the message data. Can be bundled with a message or transmitted separately.
Discoverable	The status of a Bluetooth device that has been set up to broadcast its existence to other Bluetooth devices.
DMZ	Segment of a network where servers accessed by less trusted users are isolated. The name is derived from the term “demilitarised zone”.
Domain name	A website address, alternatively known as a URL.
Domain Name Server (DNS)	A server that converts recognisable domain names (e.g. microsoft.com) into their unique IP address (e.g. 207.46.245.222).
Download	To obtain content from the internet, as an email attachment, or from a remote computer, to your own hard drive.
Doxing	The act of acquiring someone’s private information like full name and contact details and publishing them online to cause the victim distress.
Dumpster diving	A method of social engineering in which criminals raid rubbish bins to gather personal information that has not been disposed of correctly.
Easter egg	An unexpected ‘feature’ built into a computer program by the author. Can be added for fun or malicious intent.
Eavesdropping	Listening in to voice or data traffic without the knowledge or consent of the sender or recipient.
Elevation of privilege	When a user (particularly a malicious user) gains more access rights than they normally have.
Email attachment	Files, such as documents or photographs, that are attached to an email.
Email filter	Software that scans incoming email for spam or viruses, or outgoing email for viruses and filters it accordingly.
Encryption	The transformation of data to hide its information content.
Escrow	A trusted third-party service that holds money, software or other assets, pending completion of a transaction.
Ethernet	Communications architecture for wired local area networks based upon IEEE 802.3 standards.
Executable file (.exe file)	Used by programs to install and run on computers.
File sharing	Making files available over the internet to other users.
Fingerprint recognition	A biometric form of authentication using fingerprints. Used increasingly on PCs as an alternative to passwords.
Firewall	Hardware or software designed to prevent unauthorised access to a computer, or network, from another computer, or network.
Freeloading	Where unauthorised users gain access to your wireless network connection.
File Transfer Protocol (FTP)	A method of transmitting data files over the internet, normally between businesses.

Term	**Definition**
Full backup	A backup where all the chosen files are backed up, regardless of whether they have changed since the last backup.
Gateway firewall	A firewall that operates at the point where a private local area network connects to the public internet.
Gap analysis	The comparison of actual performance against expected or required performance.
Gigabyte	1000 megabytes.
Going live	The broadcasting of live videos over the internet. Also known as 'live streaming'.
Hacker	Someone who violates computer security for malicious reasons, kudos or personal gain.
Hard disk	The permanent storage medium within a computer used to store programs and data.
Hoax email	An email that makes a false claim with criminal intentions, for example a virus warning. These emails may in fact carry a real virus and are designed to make the virus spread rapidly.
Honey pot	A security feature built into a network, designed to lure hackers into meaningless locations to avoid harm to genuine, crucial data.
Hotspot	A publicly accessible wireless internet connection.
Hypertext Markup Language (HTML)	The computer code that is used to form the basis of building web pages.
Hyper Text Transfer Protocol (HTTP)	The underlying protocol used by the internet, which defines how messages are formatted and transmitted and what actions web servers and browsers should take in response to various commands.
Hyper Text Transfer Protocol Secure (HTTPS)	Secure version of HTTP. Communications between the browser and website are encrypted by Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL).
iCloud	Apple's secure cloud storage and backup product.
Identification	The process of recognising a particular user of a computer or online service.
Identity theft	The crime of impersonating someone, by using their private information, for financial gain.
IEEE 802.11	A set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.
Internet Engineering Task Force (IETF)	The body that defines the standards underlying the internet.
International Mobile Equipment Identification (IMEI)	A unique serial number built into mobile phones and tablets. To determine a device's IMEI number, dial *#06# on the device.

Term	**Definition**
Incremental backup	A backup where only files that have been changed or added since the last backup are stored, making it faster than a full backup.
Information Commissioner’s Office (ICO)	The independent public body set up to uphold information rights in the public interest, responsible for upholding the Data Protection Act 1998 the Freedom of Information Act 2000 and General Data Protection Regulation (GDPR) 2018.
Information security	The discipline of protecting computers and data from misuse.
Infrastructure-as-a-service (IaaS)	Cloud computing service that offers essential computer, storage and networking resources on demand, as a pay-as-you-go service.
Inspection certificate	A declaration issued by an interested party that specified requirements have been met.
Instant messaging	Chat conversations between two or more people, via typing on computers or portable devices.
Internet service provider (ISP)	Company that provides access to the internet and related services.
Intrusion detection system (IDS)	Program or device used to detect that an attacker is, or has attempted, unauthorised access to computer resources.
Intrusion prevention system (IPS)	Intrusion detection system that also blocks unauthorised access when detected.
iOS	Apple’s operating system used on its iPhone and iPad devices.
IP address	Internet Protocol address - a unique address that is used to identify a computer or mobile device on the internet.
IP security (IPSec)	Provides security for transmission of sensitive information over unprotected networks such as the internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices.
Java	One of today’s most popular and widely used programming languages. Originally developed by Sun Microsystems (now Oracle).
Javascript	A programming language derived from Java that is used to make web pages more interactive.
‘Just in time’ manufacturing	Manufacturing to meet an immediate requirement, not in surplus or in advance of need.
Keyboard / keystroke logger	A virus or physical device that logs keystrokes to secretly capture private information, such as passwords or credit card details.
Kilobyte	1000 bytes.
Leased circuit Communications	Link between two locations used exclusively by one organisation. In modern communications, dedicated bandwidth on a shared link reserved for that user.
Linux	An open-source, freely available operating system.
Live streaming	The broadcasting of live videos over the internet. Also known as 'going live'.

Term	Definition
Local area network (LAN)	Communications network linking multiple computers within a defined location, such as an office building.
Log file	A file that lists actions that have occurred in a computer or network device over a period of time.
MAC address	A media access control address of a device is a unique identifier assigned to a network interface controller (NIC) for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi.
Macro	A type of programme used to eliminate the need to repeat the steps of common tasks over and over, such as adding or removing rows and columns or protecting or unprotecting worksheets.
Macro virus malware	Malicious software that uses the macro capabilities of common applications such as spreadsheets and word processors to infect data.
Malware	Software intended to infiltrate and damage or disable computers. Shortened form of malicious software.
Management system	A set of processes used by an organisation to meet policies and objectives for that organisation.
Megabyte	1000 kilobytes.
Memory stick	A removable memory device, normally connected to a computer via USB.
Meme	An activity, concept, catchphrase, or piece of media that spreads, often as mimicry or for humorous purposes, from person to person via the internet. It may take the form of an image (typically an image macro), hyperlink, video, website, or hashtag and is also described as viral content.
Modding	Editing a video game’s original files to enable the gamer to perform tasks that were unintended by the original developers. These can come in the form of cheats or other additional content.
Money laundering	The process of concealing the source of money obtained illegally, by carrying out financial transactions or operating fake businesses in order to camouflage the illegal source.
Money mule	Someone who is recruited by a fraudster to transfer money illegally gained in one country to another country, usually where the fraudster lives. The term comes from an analogy with drug mules.
MP3	The technology used to store sound files, typically for music or podcasts. Played on MP3 player device.
Network	A number of computers that are connected to one another, together with the connecting infrastructure.
Network firewall	Device that controls traffic to and from a network.
Network interface card (NIC)	A circuit board, or card, that is installed in a computer so that it can be connected to a network. A network interface

Term	Definition
	card provides the computer with a dedicated, full-time connection to a network.
Non-repudiation	The ability to prove that a specific individual has carried out an activity on a computer or online, so that it cannot later be denied.
Online backup	A backup method in which data is transmitted over the internet for storage, often referred to as ‘cloud’ backup.
Online fraud	Fraud that is committed on the internet.
Online grooming	Where children, young people and vulnerable adults are exploited online for sexual or other purposes.
Online radicalisation	Where someone is exploited online and encouraged to adopt a terrorist, or extremist, ideology.
Open source	A term generally used to describe computer software that has been developed in a collaborative way, often by volunteers on a non-commercial basis.
Operating system	The software that interacts with your computer’s hardware and allows it to perform functions.
Outsourcing	Obtaining services by using someone else’s resources.
Owned	Slang word used when a computer has been taken over by hackers, usually through a root exploit.
Padlock	A symbol in a web browser that indicates that an encrypted (SSL) connection is being used to communicate with a site that has a valid certificate. Normally accompanied by ‘https’ at the beginning of the address line
Pairing	When two Bluetooth-enabled devices are linked, in order to communicate with each other.
Passing off	Making false representation that goods or services are those of another business.
Password	A secret series of characters used to authenticate a person’s identity.
Patch	A software update, often related to improving security.
Portable Document Format (PDF)	A method of saving a document so that it can be opened and viewed on devices using different operating systems.
Peer-to-peer	A network comprising of two or more PCs that connect and share resources with one another directly, without the use of a separate server computer.
Penetration testing	Legally hacking into a computer system or website, with the approval of the owner, to reveal vulnerabilities and find opportunities for improving its security.
Personal firewall	Software running on a PC that controls network traffic to and from that computer.
Personal information	Personal data relating to an identifiable living individual.
Pharming	An exploit in which criminals disrupt the normal functioning of DNS software which translates internet domain names into addresses. The user enters a correct address but is redirected to a fake website.
Phishing	Method used by criminals to try to obtain financial or other confidential information (including usernames and

Term	Definition
	passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organisation (often a bank). The email usually contains a link to a fake website that looks authentic.
PHY	Abbreviation of the physical layer of the OSI model and refers to the circuitry required to implement physical layer functions. Connects a link layer device (often called MAC as an abbreviation for medium access control) to a physical medium such as an optical fibre or copper cable.
PIN	Personal Identification Number.
Ping	A simple program that communicates with another computer over a network to see if it is responsive.
Piracy	Illegal duplication or use of material covered by intellectual property laws, such as copyright.
Platform-as-a-service (PaaS)	The provision of remote infrastructure allowing the development and deployment of new software applications over the internet, without the complexity of building and maintaining the infrastructure.
Pop-up	A small window which appears over a web page, usually to display an advertisement.
Port	A physical or virtual connection in a computer that enables applications to communicate with pre-determined external devices.
Portable device	A small, easily transportable computing device such as a smartphone, laptop or tablet computer.
Premium rate	A telephone number, typically prefixed by 09, which is very expensive when dialled. Often connected with scams.
Privileges	Access rights to computers or data, normally varying between users according to what they are and are not entitled to see.
Profile	A list of personal details revealed by users of social networking, gaming, dating and other websites. Profiles may normally be configured to be public or private.
Proxy server	Server that acts as an intermediary between users and other servers, validating user requests.
QR Code	A code designed to be scanned by smartphone camera, which contains a link to a website belonging to the code’s originator. Like a barcode, not readable by the human eye.
Ransomware	A form of malicious software (malware), in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.
Removable media	Storage devices that can be removed from a computer, such as CDs/DVDs, USB sticks and portable hard drives.
Remote Access Trojan	A trojan that downloads remote access applications that allow the attacker to connect remotely to the victim’s PC and control it. Remote access applications are legitimate

Term	Definition
	products that in this case are used maliciously so they will likely not be detected by antivirus.
Restore	The recovery of data following computer failure or loss.
Risk	Something that could cause an organisation not to meet one of its objectives.
Risk assessment	The process of identifying, analysing and evaluating risk.
Root kit	A set of tools used by hackers to get control of a computer it would otherwise not be allowed to. Often used as part of a multi-stage attack to regain access to systems.
Router	Device that receives and directs traffic within, or between, networks.
Scam	A dishonest or illegal attempt to obtain money, or something else of value.
Script kiddies	Hackers who have little to no technical ability and rely on scripts or programmes developed by other hackers.
Screen scraper	A virus or physical device that logs information sent to a visual display to capture private or personal information.
Security control	Something that modifies or reduces one or more security risks.
Security exploit	A piece of software, or sequence of commands, that takes advantage of a software bug, glitch or vulnerability to cause problems, often with criminal intent.
Sexting	The sending of sexually explicit digital images, videos, text messages, or emails, usually by mobile phone.
Security information and event management (SIEM)	Process in which network information is aggregated, sorted and correlated to detect suspicious activities.
Security perimeter	A well-defined boundary within which security controls are enforced.
Server	Computer that provides data or services to other computers over a client-server network.
Sharenting	The overuse of social media by parents to share sensitive content based on their children.
Shoulder Surfing	The act of observing someone else’s computer activity, without their knowledge, to acquire confidential information, such as login details.
Skimming	The act of counterfeiting a bank card by using a device to capture the card and account information embedded on the card’s magnetic strip.
Smart card	A form of user security authentication that relies on a credit card-sized card or USB adapter with an embedded chip.
Smartphone	A mobile phone built on a mobile computing platform that offers more advanced computing ability and connectivity than a standard mobile phone.
Social engineering	Use of deceit, either online or offline, to gain access to secure systems or personal information, for example impersonating a technical support agent.

Term	**Definition**
Social media	Computer-based technology that facilitates the sharing of ideas and information and the building of virtual networks and communities.
Social networking	The use of internet-based social media programs to make connections with friends, family, classmates, customers and clients for social purposes, business purposes or both, through sites such as Facebook, Twitter, LinkedIn, Instagram and Snapchat.
Software-as-a-service (SaaS)	The delivery of software applications remotely by a provider over the internet, rather than bought and installed on individual computers.
Spam	Unsolicited commercial email. Also known as junk email.
Spoofing	When an unauthorised person makes a message (typically an email) appear to come from a genuine sender by using either the genuine, or a very similar, address.
Spyware	Malware that passes information about a computer user's activities to an external party.
Service Set Identifier (SSID)	The wireless network name which enables users and WiFi-enabled devices to identify one wireless network from another.
Secure Socket Layer (SSL)	An encryption system that secures internet communications.
Supply chain	A set of organisations with linked resources and processes involved in the production of a product.
Surface Web	Standard internet that can be accessed by anyone, through the use of a search engine. Sometimes referred to as the clear web.
Sync to link two devices	Typically, synchronising a computer and smartphone or tablet, to ensure they hold the same data such as contacts, emails and music files.
Tablet	An ultra-portable, touch screen computer that shares much of the functionality and operating system of smartphones, but generally has greater computing power.
Transmission Control Protocol (TCP)/ Internet protocol (IP)	The protocols, or conventions, that computers use to communicate over the internet. IP is the part that obtains the address data is sent. TCP is responsible for data delivery once the IP address has been found.
Terabyte	1000 gigabytes.
Threat	Something that could cause harm to a system or organisation.
Threat actor	A person who performs a cyber-attack or causes an accident.
Transport Layer Security (TLS)	A protocol that is primarily to provide privacy and data integrity between two or more communicating computer applications
Token	A physical object, such as a smart card, used to authenticate users.

Term	Definition
The Onion Router (TOR)	A special search engine that hides your IP address from a website, through the use of proxies, allowing you to browse the internet anonymously. TOR can also allow you to connect to the Dark Web, if you know the specific website you are looking for.
Traffic	The transmission of information over a network, or the internet.
Trojan	Software posing as an authentic application, which actually conceals an item of malware.
Trolling	The act of posting inflammatory, inappropriate, or off-topic messages in an online community, such as a forum, chat room, or blog, with the primary intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion.
Tweet	A message or image posted on Twitter
Two-factor authentication	Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.
Universal Serial Bus (USB)	A means of physically connecting computers and peripherals, such as external storage, keyboards and MP3 players.
Usenet	An internet-based public bulletin board system that allows users to post messages to different newsgroups.
User account	The record of a user kept by a computer to control their access to files and programs.
Username	The short name, usually meaningful in some way, associated with a particular computer user.
Virtual private network (VPN)	Link(s) between computers, or local area networks across different locations, using a wide area network that cannot access, or be accessed, by other users of the wide area network.
Virus	Malware that is loaded onto a computer and then run without the user’s knowledge or knowledge of its full effects. Requires that the programme be run to take effect.
Virus signature	A virus’s 'fingerprint', which contains the characteristics of a virus or type of virus. Internet security software uses a database of signatures to detect viruses.
Vishing	The practice of attempting to obtain personal or financial information via a telephone call, in order to commit fraud or identity theft.
Voice over Internet Protocol (VoIP)	- a technology for transmitting phone-like voice conversations over the internet.
Virtual Private Network (VPN)	A method of creating a secure connection between two points over the internet. Normally used only for business-to-business communications.
Vulnerability	A flaw or weakness that can be used to attack a system or organisation.

Term	Definition
Webmail	An email system that uses a web browser to read and send emails, rather than a standalone email program, such as Microsoft Outlook or Apple Mail.
Wired Equivalent Privacy (WEP)	A type of data encryption to prevent eavesdropping and access to a wireless network by malicious users. Defined by the 802.11 standard.
Wide Area Network (WAN)	Communication network linking computers, or local area networks, across different locations.
Wi-Fi	Wireless local area network based upon IEEE 802.11 standards.
Wireless hotspot	A publicly accessible wireless internet connection.
Wireless network	A local area network which uses radio signals instead of a wire to transmit data.
Worm	Malware that replicates itself so it can spread to infiltrate other computers. Only requires to be run once before it can self-replicate.
Wi-Fi Protected Access (WPA)	A type of data encryption to prevent eavesdropping and access to a wireless network by malicious users. Defined by the 802.11 standard. Provides stronger security than WEP.
Wi-Fi Protected Access 2 (WPA2)	A type of data encryption to prevent eavesdropping and access to a wireless network by malicious users. Defined by the 802.11 standard. Provides stronger security than WPA or WEP