Create

Jargon Buster

Contents

A

Access control
Controlling who has access to what information.

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.

AIM
AOL's instant messaging system.

Android
An operating system used by a number of smartphone and tablet manufacturers. The world's most prolific operating system for smartphones.

Antispyware software
Software specifically designed for the detection and prevention of spyware. Often bundled in an internet security package.

Antivirus software
Software specifically designed for the detection and prevention of known viruses. Often bundled in an internet security package.

ATM
Automated Teller Machine: a cash machine, often referred to as a 'hole the wall'.

Attachment
Files, such as programs or documents, that are attached to an email.

Authentication
The process for verifying that someone or something is who or what it claims to be. In private and public computer networks (including the internet), authentication is generally done with passwords.

B

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.

Backup
Copying data to ensure its availability in the case of computer 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.

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 like mobile phones, headsets and computers.

Boot
To start up or reset a computer, mobile phone or tablet.

Boot password
A password that is needed before a computer starts up or any operating system can be loaded.

Botnet
A collection of otherwise unrelated PCs which have been infected by a virus and which are under the central control of criminals or hackers. Abbreviation for Robot Network.

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.

Buffer overflow
When more information is added to a buffer than it was designed to hold. An attacker may exploit this vulnerability to take over a system.

Bug
An error or flaw in a computer program.

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.

C

Certificate
An encrypted file containing user or server identification information, which is used to verify a website owner's identity and to help establish a security-enhanced link.

Chargeback
The process of reversing a transaction and return of payment to a customer – typically when goods have not been received or are faulty.

Chat room
An online discussion group where you can chat (by typing) with other users in real time.

Client
An application or system that accesses a service made available by a server – generally refers to a personal computer on a network.

Cloud
See cloud computing.

Cloud computing
The delivery of storage and computing capacity to end users via the internet. Commonly used for backing up data and hosting applications.

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.

Cracking
Finding a password, password or PIN by trying many combinations of characters.

Critical update
A software update that fixes a security flaw.

D

General Data Protection Regulation (GDPR)
The Data Protection Act 2018 sets out the legal basis for handling, processing and protecting personal data in the UK.

Decryption
The process of converting encrypted data back into its original form.

Denial of service attack
Deliberate overloading of a service by criminals to make it unavailable to legitimate users. For example, by arranging millions of simultaneous visits to a website – normally from a Bot Net.

Desktop firewall
Software designed to prevent unauthorised access to a computer over the internet.

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.

Domain name
A website address, alternatively known as a URL.

Domain Name Server (DNS)
A server that converts recognisable domain names (eg microsoft.com) into their unique IP address (eg 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.

Dumpster diving
A method of social engineering in which criminals raid rubbish bins to gather personal information.

E

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.

Encrypted
See encryption.

Encryption
The process of converting data into cipher text (a type of code) to prevent it from being understood by an unauthorised party.

Escrow
A trusted third party service that holds money, software or other assets pending completion of a transaction.

.exe file
Executable file: used by programs to install and run on computers.

F

File sharing
Making files available over the internet to other users, typically music or video files.

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 over the internet.

Freeloading
Where unauthorised users gain access to your wireless network connection.

FTP
File Transfer Protocol, a method of transmitting data files over the internet, normally between businesses.

Full backup
A backup where all the chosen files are backed up, regardless of whether they have changed since the last backup.

G

Gateway firewall
A firewall that operates at the point where a private local area network connects to the public internet.

Gigabyte
1000 megabytes.

Grooming
The process by which someone develops a relationship with someone else with illegal or immoral intent. Often used to describe how paedophiles develop relationships with unsuspecting children.

H

Hacker
A hacker is a person who violates computer security for malicious reasons or for personal gain.

Hard disk
A fixed magnetic disk drive used to store data on computers.

Hard drive
See hard disk

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.

HTML
Hypertext Mark up Language: the computer code that is used to form the basis of building web pages.

I

iCloud
Apple’s secure cloud storage and backup product.

Identity theft
The crime of impersonating someone – by using their private information – for financial gain.

IETF
Internet Engineering Task Force is the body that defines the standards underlying the internet.

IMEI
International Mobile Equipment Identification: a unique serial number built into mobile phones and tablets. To determine a device’s IMEI number, dial *#06# on the device.

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
The UK Information Commissioner’s Office (ICO) is the independent public body set up to uphold information rights in the public interest, responsible for upholding the Data Protection Act 1998 and the Freedom of Information Act 2000.

Information security
The discipline of protecting computers and data from misuse.

Instant messaging
Chat conversations between two or more people via typing on computers or portable devices. Systems include BlackBerry Messenger, Facebook Chat, MSN Messenger, AOL Instant Messenger, Yahoo!

iOS
Apple’s operating system used on its iPhone and iPad devices.

ISP
Internet Service Provider: a company that provides access to the internet.

IP address
Internet Protocol address: a unique address that is used to identify a computer or mobile device on the internet.

IPSec
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.

IT security
See 'information security'

J

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.

K

Key logger
See keystroke logger.

Keystroke logger
A virus or physical device that logs keystrokes in order to capture private information, passwords or credit card information.

Kilobyte
1000 bytes.

L

Laundering
See money laundering.

Linux
An open-source, freely-available operating system.

LAN
Local Area Network: a local computer for communication between computers. Can be wired or wireless.

Log file
A file that lists actions that have occurred.

M

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
A virus which uses the macro capabilities of common applications such as spreadsheets and word processors to implement virus-like behaviour.

Malware
Software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Short for 'malicious software'.

Megabyte
1000 kilobytes.

Memory stick
A removable memory device, normally connected to a computer via USB.

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.

MP3 player
A device that plays MP3 music files.

MSN Messenger
See 'instant messaging'

N

Network
A number of computers that are connected to one another, together with the connecting infrastructure.

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.

O

Online backup
A backup method in which data is transmitted over the internet for storage, often referred to as ‘cloud’ backup.

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 enables your computer or mobile device to operate.

Owned
When a computer has been taken over by hackers.

P

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.

Patch
A software update, often related to improving security.

PDF
Portable Document Format: 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 typically used to share music and video files and applications between individuals over the internet.

Penetration testing
Legally hacking into a computer system or website with the approval of the owner, to reveal vulnerabilities and finding opportunities for improving its security.

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
An attempt at identity theft in which criminals lead users to a counterfeit website in the hope that they will disclose private information such as user names or passwords.

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.

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.

Premium rate
A telephone number, typically prefixed by 09, which is very expensive when dialled. Often connected with scams.

Privileged user access
See privileges.

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
A server that manages internet traffic to and from a local area network and can provide other functions, such as internet access control.

Q

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.

R

Recordable DVD
A DVD that is capable of storing data when used in a DVD recorder.

Removable media
Storage devices that can be removed from a computer, such as CDs/DVDs, USB sticks and portable hard drives.

Root kit
A set of tools used by hackers to get control of a computer.

Router
A device that routes network or internet traffic. Typically found in home/small office environments within a WiFi device (wireless hub).

S

Script kiddies
Hackers who carry out their illicit activity for notoriety rather than criminal intent.

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.

Server
A computer that serves files or services to other computers over a network or the internet.

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 authentication that relies on a credit card-sized card with an embedded chip.

Smartphone
A mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a standard mobile phone.

Social engineering
Use of deceit offline to gain access to secure systems or personal information, for example impersonating a technical support agent.

Spam
Unsolicited commercial e-mail. Also known as junk e-mail.

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 secretly monitors a user's activity or scans for private information.

SSID
The wireless network name which enables users and WiFi-enabled devices to identify one wireless network from another. Acronym for *service set identifier*.

SSL
Secure Socket Layer, an encryption system that secures internet communications.

Sync
To link two devices – typically a computer and smartphone or tablet – to ensure they hold the same data such as contacts, emails and music files. Short for synchronise.

T

Tablet
An ultra-portable, touchscreen computer which shares much of the functionality and also the operating system of smartphones, but generally with more computing power.

TCP/IP
Transmission Control Protocol / Internet Protocol. The protocols, or conventions, that computers use to communicate over the internet.

Terabyte
1000 gigabytes.

Token
A physical object, such as a smart card, used to authenticate users.

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. Term comes from Trojan Horse in Greek mythology.

Two factor authentication
A method of obtaining additional evidence of identity to simply using passwords – such as a bank card.

U

USB
Universal Serial Bus: 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
Gives individuals access to files and programs on a computer. Access is often controlled by login.

Username
A code name that, with a password, unlocks a user account.

V

Virtual Private Network
See VPN.

Virus
A file written with the sole intention of doing harm, or for criminal activity.

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.

VoIP
Voice over IP: a technology for transmitting phone-like voice conversations over the internet.

VPN
Virtual Private Network: a method of creating a secure connection between two points over the internet. Normally used only for business-to-business communications.

Vulnerability
Any product flaw, administrative process or act, or physical exposure that makes a computer susceptible to attack by a malicious user.

W

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.

WEP
Wired Equivalent Privacy: a type of data encryption to prevent eavesdropping and access to a wireless network by malicious users. Defined by the 802.11 standard.

WiFi
See 'wireless network'.

Wireless hotspot
A publicly accessible wireless internet connection.

Wireless hub
See router.

Wireless hub/router
See router.

Wireless network
A local area network which uses radio signals instead of a wire to transmit data.

Worm
A type of virus which can spread itself across networks needing no human intervention to do so.

WPA
WiFi Protected Access: 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.

WPA2
WiFi Protected Access 2: 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.