Your A-Z Guide to IT Jargon Terminology

More IT jargon terminology words are being created and used in everyday language. For all the non-computer users out there, this can be a nightmare!

When dealing with computers, the IT jargon can be so complex that it feels like you are trying to communicate in two languages.

Therefore, we have started to compile an IT jargon buster of technical terms to help anyone understand the most complex of terms.

A

Antivirus: Software designed to detect and destroy computer viruses.

AI (Artificial Intelligence): Intelligence demonstrated by machines, primarily devices that perceives their environment and takes actions. Examples of Artificial Intelligence (AI) in 2024 are ChatGPT and Gemini

Algorithm: A set of rules to be followed in calculations, especially by a computer.

API (Application Programming Interface): A set of rules that allow the creation of applications which access the data of an operating system, applications or service.

Application: A piece of software developed to be installed on mobile devices.

Adware: Software that automatically displays or downloads advertising material when a user is online.

B

BIOS (Basic Input / Output System): A set of computer rules in the firmware that controls the input and output operations.

Byte: A unit of data that contains eight binary bits. Or a series of eight zeros and ones.

Backdoor: The access of a computer system with encrypted data that bypasses the system's security system.

Bandwidth: The amount of data transferred or passed from one destination to another.

C

Cache: These are temporary files downloaded for web content. Your computer reloads these files when you revisit a webpage.

ChatGPT: ChatGPT is a large language model created by OpenAI that can generate human-like text based on input prompts.

Cloud: The cloud is where data is stored and controlled from remote servers via an internet connection. An example of the Cloud is Google Drive or OneDrive solutions for storing your small businesses' data.

Corrupted: A data file no longer usable, usually from virus infection.

Cryptocurrency: A digital currency in which encryption skills are used to generate currency units to verify the transfer of funds regularly.

Cyberattacks: A group of hackers who aim to damage or destroy a computer network or system.

Cyber Essentials: A government-backed scheme designed to make the UK a safer place for online

Cyber Insurance: Cyber insurance is insurance that covers businesses from cyber-related issues.

Cybersecurity: A term created to describe all the security put in place to protect computers from cyberattacks.

D

Dark Web: A part of the World Wide Web that is only reachable via special software and applications. The dark web allows users to operate whilst remaining untraceable.

Data Breach: A security incident where sensitive and personal information is copied, transmitted, viewed or stolen.

DDoS (Distributed Denial of Service): The intention of harming and stopping a computer network by flooding it with data sent from many individual computers.

Decryption: Encoding encrypted text and translating it into text the user understands.

Disaster Recovery: An IT service that provides a full backup of information, data and service so that a business can quickly resume.

Digital Transformation: Digital transformation refers to updating a business to the modern workplace. The likes of the VoIP telephony system and the use of the cloud and tools such as Microsoft SharePoint, to help increase productivity, collaboration and security.

DNS (Domain Name System): The internet's system for converting alphabetic names into numeric IP addresses, e.g. Submitting a URL and taking the user to the IP address associated with that name.

Downtime: A total outage of power, communication or business.

E

Encryption: The process of changing information or data into a code, mainly to prevent unauthorised access.

EXE: A file extension for an executable format. Used to unload software to be installed on a computer.

F

Firewall: A network security system that controls any incoming or outcoming network traffic.

File sharing: A technique to distribute access to digital media, documents or e-books.

FTP (File Transfer Protocol): A client protocol for transferring files with a host computer. Usually authenticated with usernames and passwords.

G

Gigabyte: A unit of data that contains data equal to one thousand million bytes.

GIF (Graphic Interchange Format): A file format that supports animated and static images.

GUI (Graphical User Interface): A user interface with graphical elements, like windows, icons and buttons.

H

Hacker: A person who uses a computer to gain unauthorised access to data.

HTML (Hypertext Markup Language): A universally known system for text tagging files. Meaning you can achieve font, colours, graphics and hyperlinks to be used on World Wide Web pages.

Hotspot (WiFi): A physical location where people may obtain Internet access using WiFi technology. This can be done via a router connected to a WLAN.

I

Infrastructure: The IT infrastructure refers to everything; the network, the servers etc.

IT (Information Technology): Anything related to computing technology.

IMEI (International Mobile Equipment Identity): A 15 or 17 digital code uniquely identifying mobile phone devices.

IP Address: A unique address that identifies a device on the internet or a local network.

ISP (Internet Service provider): A company that provides customers with Internet access.

IOS: An operating system used for mobile devices manufactured by Apple.

J

Java: A programming language that produces software for a host of platforms.

JavaScript: An object-orientated computer programming language used to create interactive effects on web browsers mainly.

JPEG (Joint Photographic Experts Group): An image file format used for storing and compressing digital images, commonly used for photographs and graphics on the web. A JPEG file is commonly used to replace PNGs to increase website loading speed.

K

Key Logger: Software records/logs the keys struck on a keyboard.

Kilobyte: A unit containing data equal to a thousand and twenty-four bytes.

L

LAN (Local Area Network): A computer network that spans a relatively small area, usually based in a single room or building.

Linux: An open-source operating system modelled on UNIX.

M

Malware: Software which specifically disrupts or damages a computer or gains access to a user's system.

Managed Service Provider (MSP): Managed services to provide proactive support to keep businesses up and running.

Megabyte: A unit of data that contains data equal to one million, forty-eight thousand, five hundred and seventy-six bytes.

Motherboard: A printed circuit board containing the principal components of a computer or other device.

N

NAT (Network Address Translation): A method used to map private IP addresses to public IP addresses for communication over the internet.

NCSC (National Cyber Security Centre): Helping to make the UK the safest place to live and work online.

NOS (Network Operating System): A computer operating system designed primarily to support a personal computer.

NTFS (New Technology File System): A file system that Windows uses for storing and retrieving files on a hard disk.

O

Offline: A state in which a device or system is not connected to the internet or a network

Open Source: Software distributed with its source code can be freely used, modified & shared

Operating System: This software supports a computer's basic functions.

P

Patching: is a term used to describe a hotfix to implement new features, bug fixes or improve security.

Phishing: A practice of sending fraudulent emails pretending to be from reputable companies to induce individuals to reveal personal information.

PDF (Portable Document Format): A file format for capturing and sending electronic information so that it can be viewed in exactly the intended format.

Peer-to-Peer: Networks where each computer can act as a server for the other, allowing file sharing without a central server.

PNG (Portable Network Graphics): It is a lossless file format for web graphics and transparent images.

POP (Post Office Protocol): A type of computer networking that extracts and retrieves email from a remote mail server.

Protocol: The official procedure of rules for transmitting data between electronic devices, such as computers.

Proxy Server: A server between a client application, like a web browser, and a real server.

Q

QR Code: A two-dimensional barcode scanned by a smartphone or mobile device to access information or content.

QoS (Quality of Service): A term used to describe the ability of a network or system to provide predictable and reliable performance under varying conditions.

Quantum Computing: A computing paradigm that uses quantum-mechanical phenomena, such as superposition and entanglement, to perform calculations much faster than classical computers.

Query: A request for data from a database or search engine.

Queue: A data structure used to store and manage a collection of elements, with the first element added is the first one removed (FIFO).

R

Ransomware: A type of malicious software designed to block access to a computer system or network until money has been paid.

RAM (Random Access Memory): A type of computer memory that can be accessed randomly. This means any byte of memory can be accessed without touching the preceding bytes.

Router: A networking device that transfers data packets between computer networks.

ROM (Read Only Memory): A storage medium that permanently stores data, meaning it can only be read and not written.

Romance Scam: Individuals posing as romantic partners on various online platforms aim to deceive their targets and obtain their financial assets.

S

Secure IT: Our cybersecurity training and awareness platform. Short courses to help prevent the likelihood of being a victim of phishing or data breaches, from as little as £2 per user per month.

Server: A computer or computer program that manages access to network resources.

Software: A set of instructions or programs instructing a computer to do specific tasks. Software is the universal term to describe computer programs.

Software Services: When off-the-shelf solutions don’t quite fit your needs. This can bridge the gap between what a Company has and what is needs.

Spyware: Software installed on a computer device with the computer users knowing about it.

SEO (Search Engine Optimization): Increasing the quantity and quality of traffic to a website.

Spam: Internet messages that are irrelevant and unsolicited, typically to many users. Usually for advertising, phishing or spreading viruses.

T

TCP/IP: Transmission Control Protocol/Internet Protocol, the basic communication protocol used for the internet and most computer networks.

Terminal: A device used to communicate with a computer system remotely or locally, typically using a command-line interface.

Troubleshoot: The process of analysing and solving a serious problem.

Trojan Horse: A computer program designed to appear harmless but is malicious and loaded with a computer virus.

Two-factor Authentication (2FA): Two-factor authentication is a security measure that requires users to provide two different forms of identification to access an account or service.

U

UX (User Experience): The concept of encompassing all aspects of the end user's interaction with a website, program or application.

UNIX: A multi-user operating system designed for flexibility, UNIX was one of the first operating systems to be written in C language.

UAC (User Account Control): A feature that is in place to stop unauthorized changes to your computer by telling the user that an action could potentially affect the safety of your computer.

USB (Universal Serial Bus): A common interface that enables communication between devices and a host controller, such as a computer.

V

Virtual Memory: Computer memory appears to exist as main storage, although it is supported as secondary storage.

Virus: A piece of code capable of destroying itself and having a detrimental effect, usually corrupting the system or destroying computer data.

VoIP Telephony: VOIP stands for Voice over Internet Protocol, and this is the future of telephony. VoIP is a cost-effective way to bring flexibility, scalability and enterprise-grade features to a business telephone system.

VPN (Virtual Private Network): A network constructed using public wires connects remote users or regional offices to a company's network.

W

Worm: A standalone malware computer program that replicates itself to spread to other computers.

WAN (Wide Area Network): A network that exists over a large-scale area. The purpose is to connect smaller networks, such as LAN and metro area networks.

WEP (Wired Equivalent Privacy): A security protocol that is designed to provide a wireless local area network (WLAN) with a level of security and privacy.

Wi-Fi: A wireless networking technology that allows computers and other devices to communicate over a wireless signal.

WLAN (Wireless Local Area Network): A wireless distribution method for two or more devices that use high-frequency radio waves to include an access point to the internet.

X

XML (Extensible Mark-up Language): A metalanguage which allows users to define their customized mark-up languages to display documents on the internet.

XaaS (Anything as a Service): A term used to describe cloud computing services that provide various IT resources, such as infrastructure, software, or platforms, on a subscription basis.

Y

Y2K: A term used to describe the Year 2000 problem, a computer bug that was expected to cause widespread issues due to the way dates were programmed.

YAML: A human-readable data serialization format used for configuration files.

Yarn: A package manager used for Node.js applications, similar to npm.

Yellow screen of death: An error message displayed on a computer or mobile device indicating a serious problem.

Z

Zero-day: A security vulnerability or exploit unknown to the software vendor has not yet been patched or fixed.

Zip file: A computer file with compressed contents for storage or transmission.

Zombie: A compromised computer or device remotely controlled by an attacker to perform malicious activities without the owner’s knowledge or consent.