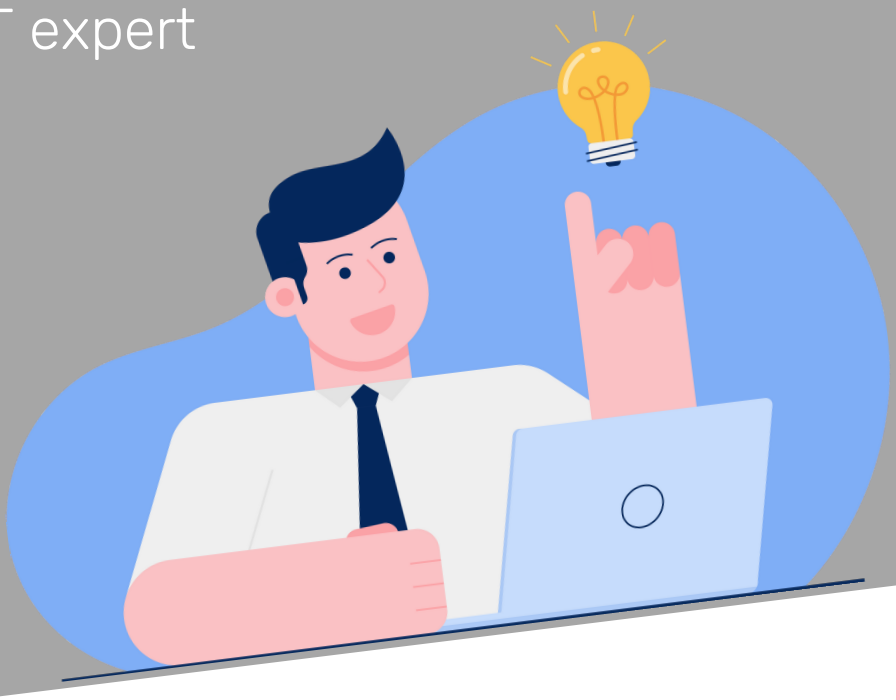
Learn to talk tech with our IT Jargon Buster

Our A-Z of some of the terms you might hear when talking with an IT expert



Turn Key Solutions

Securing Your Technology. Empowering your Business

www.turnkeysol.com 225-751-4444

A few words of a foreign language can get you a long way in a strange land.

We know that IT jargon is an alien language to a lot of people, and we do our best to keep the tech talk to a minimum when we're working with our clients.

In any case, you probably have enough of your own office jargon to start worrying about ours.

But in a tech-led world, a lot of IT terms are cropping up more and more in everyday conversation. And if you do have a problem you need help with – or just a question you'd like to ask us about your business IT – it'll save a lot of time if you have a few words of lingo in your locker.

Our new guide is a great place to start. It won't tell you everything, but if you need an easy A-Z of some of the most common terms you'll hear when you're talking with an IT expert, then you've come to the right place.

Let's start at the beginning...

A

Adware
Software that automatically downloads adverts when you're online, such as banner ads and pop-ups

---

Access Point
A device that allows wireless-equipped computers & other devices to communicate with a wired network

---

AI (Artificial Intelligence)
Systems and devices that simulate human behaviors and decisions. This can include creating systems, language processing, speech recognition, writing text and machine vision

---

Antivirus
Software that identifies and removes viruses from your device. Also known as anti-malware

---

API (Application Programming Interface)
Software that allows two or more applications or programs to communicate with each other and share information

---

Authentication
The process of identifying yourself & the verification that you're who you say you are. Computers, where restricted information is stored, may require you to enter your username & password to gain access.

B

Backdoor
A vulnerability in a security system that allows unwanted access to files and data

Bandwidth
The maximum amount of data you can send and receive in a given amount of time, over an internet connection. Imagine a big pipe compared with a small pipe

---

Botnet
A network of private computers infected with malware and controlled as a group to spread the virus further

---

BYOD: Bring Your Own Device
A business & technology policy that allows employees to bring in personal mobile devices and use these devices to access company data, e-mail, etc

C

Cache
A temporary file that stores information on your device to speed things up. For instance a web cache might remember the last thing you were doing so it can reload a page where you left off

---

(The) Cloud
Data storage and computing power that lives on remote servers, which are accessed via the internet

---

Corrupted
An unstable data file

Cybersecurity
Any and all security measures put in place to protect your devices, systems and network from cyber attack

Content Filtering
Software that blocks access to inappropriate websites and content, including explicit material, gambling & shopping sites. It's not intended for virus, worm or hacker prevention.

D

Darkweb
A hidden part of the internet, accessed using special software. It's rife with criminal activity. This is where stolen data, such as credit card details, is often sold.

Data breach
A security incident where private data is viewed or stolen by unauthorized persons

---

DDoS (Distributed Denial of Service)
A type of cyber attack that harms or stops a network by flooding it with data from numerous other devices

---

DNS: Domain Name Server
An internet service that translates domain names to IP addresses for hardware devices to communicate. It enables web browsers & email servers to look up IP addresses for domain names.

Downtime
The period of time a network or systems are offline (or 'down'), preventing the normal running of a business

E

Encryption
The process of encoding data to make it unreadable without the right access information - usually a password, passkey or authentication app.

Endpoint Protection
Also referred to as endpoint security, it's an approach to detecting malicious activity while protecting secure networks, including servers, computers & devices from an attack.

F

Firewall
A security measure that controls what data can come in and out of your network

---

FTP (File Transfer Protocol
Protocol used for transferring files from a server to a computer across a network. This is usually authenticated with usernames and passwords

G

GIF (Graphic Interchange Format)
A type of image file than can be either animated or static

Gigabyte (GB)
Unit of data equal to one thousand million bytes. A typical movie download might be between 1 and 4 GB

H

Hardware
The physical devices in your IT world – computers, printers, phones, tablets

---

Hotspot (Wi-Fi)
A physical location where you can gain internet access via Wi-Fi

HTML (Hypertext Markup Language)
The universal language of the internet, used to structure web pages, tell your web browser how to display them and create links between them

I

Infrastructure
Your entire system – your network, servers, and all your devices

---

IaaS: Infrastructure as a Service
In the most basic cloud service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources.

---

iOS
Operating system manufactured by Apple and used exclusively on its hardware

---

IP (Internet Protocol) address
A unique number that identifies a device connected to the internet

J

Java
A widely used programming language used in millions of applications and devices around the world

---

Javascript
Unrelated to Java, Javascript is a programming language used everywhere on the internet within all web browsers to perform a whole range of functions

K

Keylogger
Software used by cybercriminals to record the keys pressed on a keyboard. This information can be used to access login credentials and other sensitive info

L

LAN (Local Area Network)
A network of connected devices that spans a small area, such as your office or home

M

Malware
Malicious software, a type of virus, designed to infect your system and disrupt, damage, or gain access to your device, server or network. This can lead to the unauthorized access or theft of data and private information

---

Megabyte
Unit of data equal to one million forty-eight thousand, five hundred and seventy bytes

---

Multi-Factor Authentication (2FA/MFA)
Two-factor authentication (2FA) requires presenting two or more pieces of evidence (knowledge, possession, inherence) to access a computer system

N

Next-Gen Endpoint Security
Next-gen endpoint security uses AI and machine learning to analyze user/system behavior, combat threats, and adapt methods quickly & efficiently.

NOS (Network Operating System)
A specialized operating system for a network device, like a router or firewall

---

NTFS (Network Transfer File System)
A file system used by Windows for storing and retrieving files on a hard disk

O

OS (Operating System)
Software that manages a computer's basic functions, and provides common services for computer programs

P

Patch
Piece of software designed to update a program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.

Phishing
Scam emails that pretend to be from a credible source and aim to steal personal information and/or login credentials

---

Protocol
The set of rules that allows different devices to communicate with each other

Proxy Server
A server that sits between a device requesting information, and the server providing that information. For example, it could be a gateway between your laptop and the internet, that stops hackers from reaching your network

R

RAM (Random Access Memory)
A form of temporary computer memory that's usually used to store working data

---

Ransomware
Malware that encrypts sensitive data and demands a ransom for its release (ransoms should never be paid – data is often never properly released, or is only partially returned)

Remote Desktop
A Windows feature that allows you to have access to a Windows session from another computer in a different location.

RMM: Remote Monitoring & Management
Software for managed service providers to remotely monitor and manage IT assets, including accessing devices, reviewing data, deploying patches, etc

---

Router
A device that directs data to the right places in a network

S

SaaS: Software as a Service
A software distribution model where a third-party provider hosts applications & customers access them via the internet. SaaS is one of three main categories of cloud computing, alongside IaaS & PaaS

SAN: Storage Area Network
A dedicated storage network that gives servers access to consolidated, block-level storage; it has its own network of devices inaccessible through the regular network

---

Server
A computer or program that manages access to a network and holds data in one location for multiple users to access

---

SIEM: Security Info & Event Management
A software solution that aggregates & analyzes activity from many different resources across your network. SIEM collects security from network devices, servers & more.

SOC: Security Operations Center
A central unit for organizational and technical security issues. SOC monitors sites using data processing & device monitoring for threats

---

Software
Programs and apps that make devices work

Spyware
Malware that spies on the actions you take on your device. This can be used to steal data or passwords, or listen in to conversations

T

Trojan
A form of malware that looks harmless but conceals a virus

Troubleshoot
To analyze a problem with a view to solving it (something we do a lot of!)

U

UAC (User Account Control)
A feature that only allows authorized users to make changes to a system or device

---

USB
A type of widely used cable that connects or charges devices. This could be a keyboard connecting to a computer, or a flash drive transferring data

V

Virus
A malicious computer program or code that can copy itself and spread throughout a network, corrupting or damaging data and systems

---

VoIP: Voice over Internet Protocol
A means of using the Internet as the transmission medium for phone calls. An advantage is you do not incur any additional surcharges beyond the cost of the Internet access

VPN (Virtual Private Network)
A more secure way of connecting to a company's network remotely, or using the internet over a public Wi-Fi connection

W

WAN (Wide Area Network)
A network of devices that are connected across a wider area than a LAN, and allows you to connect to smaller networks

WLAN (Wireless Local Area Network)
A wireless network that connects two or more devices, creating a LAN

WPA: Wi-FI Protected Access
A standard designed to improve on the security features of WEP

Worm
A type of malware that replicates itself to spread to other devices across a network without human activation

Z

Zero Trust Security
Approach to security where only an approved list of users and systems are granted access to specific areas and files, while everything else is blocked

Zip File
A file that compresses its contents to create a smaller file that's easier to share or store

We hope this has helped.

Yes, we operate in a technical world with some jargon that can be off-putting if it's not something you're used to talking about.

But your business IT is there to make your life easier and more efficient. We take a lot of pride in our ability to work with our clients, helping them to understand their systems without sending their heads into a spin.

So if your current IT support provider can't do that – or you don't have support you can call on for help and advice whenever you need them – we'd love to have a chat to find out how we can help you.

Get in touch anytime to arrange a no-obligation conversation. You're guaranteed it will be jargon-free.

Turn Key Solutions

www.turnkeysol.com / 225-751-4444

BOOK YOUR FREE CONSULT

turnkeysol.com/bookaconsult/