# I.T. Dictionary

Geek speak refers to any talking in words that are considered technical jargon, especially words or acronyms related to computers, handhelds, or other technological devices. The term is thought to have become popular due to its use by the press in 1998 while covering a Microsoft antitrust case.

## Geek Speak in Plain English

**AdWare:** software that displays advertising and/or pop-ups on your computer. Adware can be legitimate software, but is often installed maliciously without the consent of the end-user. This software can slow down your computer and internet browsing experience.

**ASP:** ***A****pplication* ***S****ervice* ***P****rovider*, a third-party company that manages and distributes software-based services and solutions to their customers over a wide-area network, usually the Internet.

**BDR:** ***B****ackup and* ***D****isaster* ***R****ecovery Server*, a hardware appliance physically housed at the client's office. This "server" takes "snapshot" backups of the office servers as often as every 15 minutes and sends a copy of these backups offsite every day. These backups are image-based and can be used to perform a bare-metal restore to get your network up and running fast.

**Blackberry Enterprise Server (BES):** a software and service that connects to messaging and collaboration software (Microsoft Exchange, Lotus Domino, Novell GroupWise) on enterprise networks and redirects emails and synchronizes contacts and calendaring information between servers, workstations and BlackBerry mobile devices. Newer Blackberry devices aren't relying as heavily on Blackberry Enterprise Servers and are now offering "active sync" to communicate directly with Microsoft Exchange.

**Browser Hijacker:** malicious software that changes your default homepage and search engine without your permission.

**BYOD:** ***B****ring* ***Y****our* ***O****wn* ***D****evice*, the concept of using non-company-owned assets to access a company-owned resource. An example of this would be end-users accessing a corporate network via personal tablets or smart phones. Security is a major concern where BYOD is allowed (see MDM).

**Business Continuity:** The process of keeping your business systems and functions running continuously or with minimum downtime or interruption to critical processes.

**Cloud Computing:** internet based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, as with the electricity grid.

**Content Filtering:** software that prevents users from accessing objectionable content via your network. Although this usually refers to Web content, some programs also screen inbound and outbound e-mails for offensive information. This software is not designed for virus, worm, or hacker prevention.

**Cookie:** a file placed on your computer to allow websites to remember something. Originally designed to be helpful, cookies can save and share information such as your purchasing habits, your location, and even your identity. Cookies aren't actually capable of damaging your computer, but they can compromise your identity.

**CPU:** ***C****entral* ***P****rocessing* ***U****nit*, the brains of a computer (see processor below).

**DHCP:** ***D****ynamic* ***H****ost* ***C****onfiguration* ***P****rotocol*, a method for dynamically assigning IP addresses to devices on request, rather than explicitly programming an IP address into each device. If you have a server on your network, configuring that server as a DHCP server will make it much easier to add or reconfigure individual workstations on the network.

**Default Gateway:** in a TCP/IP network, this is the gateway that computers on that network use to send data to, and receive it from, computers and networks outside of the local network. Typically, this is the router or firewall that connects the local network to the public Internet, although it might also be a router that connects to another remote server or computer within the same company.

**Disaster Recovery:** The process of recovering business data, functions and systems after a disaster to the RPO (recovery point objective). This is NOT the same as a data backup or business continuity.

**Disaster Response Team:** A designated group of people who will be responsible for the execution and management of the Disaster Recovery Plan.

**DMZ:** ***D****emilitarized* ***Z****one*, a separate area of your network that is isolated from both the Internet and your protected internal network. A DMZ is usually created by your firewall to provide a location for devices such as Web servers that you want to be accessible from the public Internet.

**DNS:** ***D****omain* ***N****ame* ***S****ystem (or* ***S****erver)*, an Internet service that translates domain names into IP addresses. Even though most domain names are alphabetic, hardware devices (like your PC) can only send data to a specific IP address. When you type www.microsoft.com into your Web browser, or send an e-mail message to someone@business.com, your Web browser and e-mail server have to be able to look up the IP address that corresponds to the microsoft.com Web server, or to the mail server that receives e-mail for business.com. DNS is the mechanism for doing this lookup.

**DSL:** ***D****igital* ***S****ubscriber* ***L****ine*, a high-speed Internet service delivered over a telephone line. Compared to newer services, DSL is usually considered to be a slower technology.

**Failover:** In computing, **failover** is switching to a redundant or standby computer server, system, hardware component or network facility upon the failure or abnormal termination of the previously active application, server, system, hardware component, or network facility.

**Firewall:** a device or software program designed to protect your network from unauthorized access over the Internet. It prevents traffic from coming into your network unless that traffic was requested by an internal source. It may also provide Network Address Translation (NAT) and Virtual Private Network (VPN) functionality.

**Fractional T-1:** one or more channels of a T-1 service. A complete T-1 carrier contains 24 channels, each of which provides 64 Kbps. Most phone companies also sell fractional T-1 lines, which provide less bandwidth but are less expensive. See T-1.

**Google AdWords:** Google's online advertising program. Through this program, a company pays Google to advertise their products or services when users search Google for specific keywords.

**Hard Drive:** Disks which store, read, and write data. Hard disk drives do not lose data when power is turned off (see RAM).

**Hosted Applications (i.e. Hosted Sharepoint or Hosted Exchange):** a service whereby a provider makes a software (e.g. email) and space available on a server so its clients can host their data on that server.

**IP Address:** an identifier for a computer or device on a TCP/IP network. The format for an IP address is a 32-bit numeric address separated by periods (IPv4)(example: 207.46.20.60). Within an isolated network, you can assign an IP address at random, as long as each IP address on that network is unique. However, if you are connecting a network or computer to the Internet, you must have a registered IP address to avoid duplicates.

**Lync:** formerly known as Microsoft Office Communicator, Lync is Microsoft's secure instant messaging client. Lync is available as part of Microsoft's Cloud offering (Office 365) and includes instant messaging and video chat.

**Malware:** a generic term used to describe various malicious software such as viruses, Trojans, spyware, and worms.

**Maximum Tolerable Outage (MTO):** Also called Maximum Tolerable Outage (MTO) is the maximum amount of time critical business functions and data may be unavailable due to a major interruption before your business is severely impacted. The MAO encompasses all activities from the point of the disaster happening to the point of recovery.

**MDM:** ***M****obile* ***D****evice* ***M****anagement*, the series of processes and programs used to control portable devices (e.g. laptops, smart phones, tablets, etc.) which access company-owned resources. MDM usually consists of policies which govern end-users and at least one application installed on the portable device which can be used to locate or erase a lost device.

**Office 365:** Microsoft's cloud service that provides a combination of hosted email (Exchange), online document collaboration (Sharepoint), and secure instant messaging and video (Lync).

**POP3:** ***P****ost* ***O****ffice* ***P****rotocol 3*, a method of communication between an e-mail server and an e-mail client. In most cases, when the client software connects to a POP3 server, the e-mail messages are downloaded to the client and are no longer available on the server.

**Processor:** short for microprocessor or CPU. A chip (usually silicon) that is the "heart" of a computer. It controls the logic of digital devices (micromave oven, alarm clocks, and computers).

**Protocol:** an agreed format for transmitting data between two devices.

**RAM (Random Access Memory):** Computer memory which is accessed "randomly". This means that one byte can be accessed without accessing the bytes around it. This memory is typically used to store "working" files that you or your computer are using and is typically erased when the computer is turned off or restarted.

**Recovery Time Objective (RTO):** The recovery time goal for business functions, systems and data after a disaster is declared. For instance, if the RTO is set to 4 hours, then offsite, mirrored backups must be continuously maintained; a daily offsite data backup or tape backup is not sufficient to deliver a 4-hour RTO. Also, different functions, systems and data residing in the same location may have different RTOs. Payroll may have an RTO of 24 hours where documents on your server may have a 7-day RTO.

**Recovery Point Objective (RPO):** The acceptable point of recovery where IT systems, data and processes will be restored to after a disaster. For example, if your server failed, all data was corrupt and you were doing daily backups in the evening, then the expected RPO would be returning to where the server was the day before, when the last backup was done.

**SEO:** ***S****earch* ***E****ngine* ***O****ptimization*, the ongoing process or configuring a website or webpage to increase traffic directed by internet search portals.

**Sharepoint:** a document collaboration program from Microsoft that may be installed and used "on premise" or hosted in the cloud as part of Microsoft's Office 365 Suite. Sharepoint allows for secure communication among a team or workgroup.

**Spam:** unsolicited email that comes to your inbox (i.e. junk mail). Spam is often used to distribute various types of malware.

**Spyware:** malicious software that allows a third-party to gather confidential information from your computer without your permission.

**T-1:** a dedicated digital transmission line that sends and receives data at a rate of 1.544 Mbps. T-1 lines can be used to carry voice traffic, data traffic, or a combination of both. In years past, T-1 lines were considered very fast. However, with the increase in hosted services and online data, T-1 lines are often too slow for most offices.

**TCP/IP:** ***T****ransmission* ***C****ontrol* ***P****rotocol/* ***I****nternet* ***P****rotocol*, the basic language that governs traffic on the global Internet, as well as on most private networks.

**Trojan:** a program that appears to be legitimate but is actually a harmful program. For example, many of today's free game downloads on the internet are actually Trojans which can damage or destroy the data on your computer.

**URL:** ***U****niform* ***R****esource* ***L****ocator*, the global address of documents, Websites, and other resources on the Web.

**Virus:** a malicious program that spreads by replicating itself. Viruses can spread from computer-to-computer or network-to-network. Viruses can give control of your computer to a hacker or even damage/destroy data.

**VoIP:** ***V****oice-****O****ver-****I****nternet-****P****rotocol*, a category of hardware and software that allows you to use the Internet to make phone calls and send faxes. This technology is becoming very popular with businesses and home users alike because it can greatly reduce telephone costs.

**VPN:** ***V****irtual* ***P****rivate* ***N****etwork*, a network constructed by using public wires (the Internet) to connect nodes (usually computers and servers). A VPN uses encryption and other security mechanisms to ensure that only authorized users can access the network and the data it holds. This allows businesses to connect to other servers and computers located in remote offices, from home, or while traveling, in a secure manner.