DICTIONARY OF
Computer Science

1st Edition

by Mochi Cruise in Jul 2023

CHAPTER 1: Internet Terms Section I

3G

3G is a collection of third generation cellular data technologies. The first generation (1G) was introduced in 1982, while the second generation of cellular data technologies (2G) became standardized in the early 1990s. 3G technologies were introduced as early as 2001, but did not gain widespread use until 2007.

In order to be labeled "3G," a cellular data transfer standard must meet a set of specifications defined by the International Telecommunications Union, known as IMT-2000. For example, all 3G standards must provide a peak data transfer rate of at least 2 Mbps. Most 3G standards, however, provide much faster transfer rates of up to 14.4 Mbps.

While many cell phone companies market phones with "3G technology," there is no single 3G standard. Rather, different companies use their own technologies to achieve similar data transfer rates. For example, AT&T uses a 3G technology based on GSM, while Verizon uses a technology based on CDMA. Additionally, cell phone networks outside the United States use different IMT-2000 compliant standards to achieve 3G data transfer speeds.

3G precedes 4G, the fourth generation of cellular data technologies.

--Updated June 7, 2012

403 Error

A 403 error is an HTTP error code that indicates access to a specific URL is forbidden. Websites often display 403 errors with a generic message such as, "You don't have permission to access this resource."

There are several reasons a web server may produce a 403 forbidden error. Some of the most common include:

- A missing index page
- An empty directory
- Invalid folder permissions
- Invalid file permissions
- Invalid file ownership

When you access a website directory on an Apache web server (a URL ending with a forward slash "/"), the standard behavior is to display the contents of the index page (index.php, index.asp, etc). If no index page is available, the fallback option is to list the contents of the directory. However, for security purposes, many web servers are configured to disallow directory listings. Therefore, if you access an empty directory or a folder without an index page, you may receive a 403 error because the directory listing is forbidden.

Invalid file and folder permissions can also produce 403 errors. Generally, files and folders on web servers must have the following permissions enabled:

- **Files**
  Owner: read, write
  Group: read
  Everyone: read
- **Folders**
  Owner: read, write, execute
  Group: read, execute
  Everyone: read, execute

If a specific file or the parent folder has incorrect permissions, the web server may be unable to access it, producing a 403 forbidden error. Similarly, if a file's "owner" does not match the corresponding website user account, it may generate a 403 error. Ownership discrepancies can occur when files are transferred between accounts on a web server or when a file is uploaded by another user.

In some cases, access to a specific URL is intentionally forbidden for security reasons. In other cases, a forbidden error may be caused by an accidental website misconfiguration. If you unexpectedly receive a 403 error in your web browser, you can contact the webmaster of the corresponding website and provide the URL that produced the error.

--Updated June 19, 2021

404 Error

A 404 error is a common website error message that indicates a webpage cannot be found. It may be produced when a user clicks an outdated (or "broken") link or when a URL is typed incorrectly in a Web browser's address field. Some websites display custom 404 error pages, which may look similar to other pages on the site. Other websites simply display the Web server's default error message text, which typically begins with "**Not Found**." Regardless of the appearance, a 404 error means the server is up and running, but the webpage or path to the webpage is not valid.

So why call it a "404 error" instead of simply a "Missing Webpage Error?" The reason is that 404 is an error code produced by the Web server when it cannot find a webpage. This error code is recognized by search engines, which helps prevent search engine crawlers from indexing bad URLs. 404 errors can also be read by Web scripts and website monitoring tools, which can help webmasters locate and fix broken links.

Other common Web server codes are 200, which means a webpage has been found, and 301, which indicates a file has moved to a new location. Like 404 errors, these status messages are not seen directly by users, but they are used by search engines and website monitoring software.

--Updated October 22, 2010

4G

4G is a collection of fourth generation cellular data technologies. It succeeds 3G and is also called "IMT-Advanced," or "International Mobile Telecommunications Advanced." 4G was made available as early as 2005 in South Korea under the name WiMAX and was rolled out in several European countries over the next few years. It became available in the United States in 2009, with Sprint being the first carrier to offer a 4G cellular network.

All 4G standards must conform to a set of specifications created by the International Telecommunications Union. For example, all 4G technologies are required to provide peak data transfer rates of at least 100 Mbps. While actual download and upload speeds may vary based on signal strength and wireless interference, 4G data transfer rates can actually surpass those of cable modem and DSL connections.

Like 3G, there is no single 4G standard. Instead, different cellular providers use different technologies that conform to the 4G requirements. For example, WiMAX is a popular 4G technology used in Asia and Eastern Europe, while LTE (Long Term Evolution) is more popular in Scandinavia and the United States.

--Updated June 7, 2012

5G

5G is the fifth generation of cellular data technology. It succeeds 4G and related technologies, including LTE. The first 5G cellular networks were constructed in 2018, while 5G devices became widespread in 2019 and 2020.

5G vs 4G

Benefits of 5G include faster speeds, low latency, and greater capacity. The theoretical maximum data transfer rate of 5G is 20 Gbps (2.5 gigabytes per second). That is 20x faster than LTE-Advanced, which has a peak download speed of 1,000 Mbps. 5G latency (the time to establish a connection) is estimated to be 10 to 20 milliseconds, compared to 4G's average latency of 40 ms. The maximum traffic capacity of 5G is roughly 100x greater than a typical 4G network.

4G smartphones and other devices are not compatible with 5G transmitters. Therefore, most 4G towers will be operational for several years after the rollout of 5G networks.

5G Multiband

Compared to previous cellular technologies, 5G uses a wider range of frequency bands. Instead of broadcasting all signals at a low frequency, 5G supports multiple frequencies that can be optimized for different areas. For example, low frequencies travel further but do not provide high data transfer rates. These are ideal for rural areas with a long distance between cellular towers. High frequencies have limited range and are highly impacted by physical barriers, but they support faster speeds. These are ideal for densely populated areas with large numbers of cell towers.

5G frequency bands are separated into three categories:

- **Low-band** - broadcasts at low frequencies between 600 and 1,000 MHz, providing download speeds in the range of 30 to 250 Mbps. Both the frequency and range are similar to a 4G signal.
- **Mid-band** - broadcasts between 1 and 6 GHz and provides speeds of 100 to 900 Mbps. The range of each cell tower is several miles radius. Mid-band is expected to be the most widely deployed.
- **High-band** - broadcasts at ultra-high frequencies between 25 and 40 GHz. The short "millimeter waves" provide data transfer speeds above one gigabit per second. High-band 5G has a limited range of about one mile. It is ideal for city centers, sports stadiums, and other public gathering areas.

NOTE: While the maximum data transfer rates of 5G are much higher than 4G, actual speeds depend on the quality of the signal. The speed of high-band 5G signal, for instance, may drop by 50% if you step behind a building or walk a block away from the closest cell tower. With mid and high-band 5G, it is especially important to have a strong signal.

--Updated May 18, 2020

ActiveX

ActiveX is a technology introduced by Microsoft in 1996 as part of the OLE framework. It includes a collection of prewritten software components that developers can implement within an application or webpage. This provides a simple way for programmers to add extra functionality to their software or website without needing to write code from scratch.

Software add-ons created with ActiveX are called ActiveX controls. These controls can be implemented in all types of programs, but they are most commonly distributed as small Web applications. For example, a basic ActiveX control might display a clock on a webpage. Advanced ActiveX controls can be used for creating stock tickers, interactive presentations, or even Web-based games.

ActiveX controls are similar to Java applets, but run through the ActiveX framework rather than the Java Runtime Environment (JRE). This means you must have ActiveX installed on your computer in order to view ActiveX controls in your Web browser. Additionally, when loading a custom ActiveX control within a webpage, you may be prompted to install it. If this happens, you should only accept the download if it is from a trusted source.

While ActiveX provides a convenient way for Web developers to add interactive content to their websites, the technology is not supported by all browsers. In fact, ActiveX is only officially supported by Internet Explorer for Windows. Therefore, ActiveX controls are rarely used in today's websites. Instead, most interactive content is published using Flash, JavaScript, or embedded media.

--Updated April 1, 2011

Address Bar

An address bar is a text field near the top of a Web browser window that displays the URL of the current webpage. The URL, or web address, reflects the address of the current page and automatically changes whenever you visit a new webpage. Therefore, you can always check the location of the webpage you are currently viewing with the browser's address bar.

While the URL in the address bar updates automatically when you visit a new page, you can also manually enter a web address. Therefore, if you know the URL of a website or specific page you want to visit, you can type the URL in the address bar and press Enter to open the location in your browser.

NOTE: The URL typically begins with "http://", but most browsers will automatically add the HTTP prefix to the beginning of the address if you don't type it in.

The appearance of the address bar varies slightly between browsers, but most browsers display a small 16x16 pixel icon directly to the left of the URL. This icon is called a "favicon" and provides a visual identifier for the current website. Some browsers also display an RSS feed button on the right side of the address bar when you visit a website that offers RSS feeds. In the Safari web browser, the address bar also doubles as a progress bar when pages are loading and includes a refresh button on the right side. Firefox includes a favorites icon on the right side of the address bar that lets you add or edit a bookmark for the current page.

The address bar is sometimes also called an "address field." However, it should not be confused with a browser toolbar, such as the Google or Yahoo! Toolbar. These toolbars typically appear underneath the address bar and may include a search field and several icons.

--Updated November 18, 2010

Adware

Adware is free software that is supported by advertisements. Instead of generating revenue through sales, an adware developer sells online ads that appear while the app runs. The developer may also sell an upgraded ad-free version of their software to users who want to use the app without ads.

Smartphone and tablet applications frequently use an adware model. Apps may include a small banner ad while you use them to provide some revenue for the developer. Some apps, particularly mobile games, may require that you watch a short video ad between uses or game levels. An in-app purchase is often available to remove ads for a one-time purchase or recurring subscription.

Most adware is safe to use, but some may inject ads into other parts of the operating system's user interface, serving as a form of malware. These ads may appear as popups or as extra ads injected into webpages. Ads introduced by malware may be difficult to remove, appearing even after the adware that introduced them is uninstalled. You may need to use antivirus and antimalware software to completely remove malicious ads.

--Updated March 6, 2023

Affiliate

An Internet affiliate is a company, organization, or individual that markets another company's products through their website. In exchange for marketing their products, companies pay affiliates a commission for each sale they generate.

Affiliate programs exist for many different industries, such as travel, clothing, technology, and online services. This allows web publishers to promote specific products or services related to the content of their websites. For example, the webmaster of a fashion website may publish affiliate banners for a clothing store. The owner of a software review website may include affiliate links to different software programs.

Affiliate marketing is a type of PPS advertising, since affiliates are only paid for sales they produce (unlike PPC advertising). Therefore, merchants must offer affiliates high enough commissions to make it worthwhile for the publishers to run their ads. Affiliate commissions vary widely between industries and also depend on average sale amounts. Low-margin products, such as consumer electronics, may offer commissions as low as 2%, while high-margin products, such as computer software, may offer commissions as high as 75%. Most affiliate commissions fall in the range of 5 to 20%.

Affiliate programs provide free marketing for merchants and an extra source of revenue for web publishers. While it is a win-win partnership, setting up an affiliate system to track sales and generate payments is a complex process. Therefore, many companies run their affiliate programs through a third party e-commerce platform, such as Commission Junction or DirectTrack.

--Updated May 30, 2014

Ajax

Ajax is a combination of Web development technologies used for creating dynamic websites. While the term "Ajax" is not written in all caps like most tech acronyms, the letters stand for "Asynchronous JavaScript And XML." Therefore, websites that use Ajax combine JavaScript and XML to display dynamic content.

The "asynchronous" part of Ajax refers to the way requests are made to the Web server. When a script sends a request to the Web server, it may receive data, which can then be displayed on the Web page. Since these events happen at slightly different times, they are considered to be asynchronous. Most Ajax implementations use the XMLHttpRequest API, which includes a list of server requests that can be called within JavaScript code. The data is usually sent back to the browser in an XML format, since it is easy to parse. However, it is possible for the server to send data as unformatted plain text as well.

What makes Ajax so powerful is that scripts can run on the client side, rather than on the server. This means a JavaScript function can make a request to a server after a webpage has already finished loading. The data received from the server can then be displayed on the page without reloading the other content. If a server-side scripting language like PHP or ASP was used, the entire page would need to be reloaded in order for the new content to be displayed.

While you may not realize it, you have probably seen Ajax at work on several different websites. For example, search engines that provide a list of search suggestions as you type are most likely using Ajax to display the suggestions. Image searches that produce more thumbnails as you scroll through the results typically use Ajax to retrieve the continual list of images. When you click "Older Posts" at the bottom of a Facebook page, Ajax is used to display additional postings.

Ajax has helped make the Web more dynamic by enabling webpages to retrieve and load new content without needing to reload the rest of the page. By using Ajax, Web developers can create interactive websites that use resources efficiently and provide visitors with a responsive interface.

--Updated April 13, 2011

Apache

Apache is the most popular Web server software. It enables a computer to host one or more websites that can be accessed over the Internet using a Web browser. The first version of Apache was released in 1995 by the Apache Group. In 1999, the Apache Group became the Apache Software Foundation, a non-profit organization that currently maintains the development of the Apache Web server software.

Apache's popularity in the Web hosting market is largely because it is open source and free to use. Therefore, Web hosting companies can offer Apache-based Web hosting solutions at minimal costs. Other server software, such as Windows Server, requires a commercial license. Apache also supports multiple platforms, including Linux, Windows, and Macintosh operating systems. Since many Linux distributions are also open-source, the Linux/Apache combination has become the most popular Web hosting configuration.

Apache can host static websites, as well as dynamic websites that use server-side scripting languages, such as PHP, Python, or Perl. Support for these and other languages is implemented through modules, or installation packages that are added to the standard Apache installation. Apache also supports other modules, which offer advanced security options, file management tools, and other features. Most Apache installations include a URL rewriting module called "mod_rewrite," which has become a common way for webmasters to create custom URLs.

While the Apache Web server software is commonly referred to as just "Apache," it is technically called "Apache HTTP Server," since the software serves webpages over the HTTP protocol. When Apache is running, its process name is "httpd," which is short for "HTTP daemon."

--Updated January 7, 2011

Applet

An applet is a small application designed to run within another application. While the term "applet" is sometimes used to describe small programs included with a computer's operating system, it usually refers to Java applets, or small applications written in the Java programming language.

Unlike ordinary applications, Java applets cannot be run directly by the operating system. Instead, they must run within the Java Runtime Environment (JRE), or within another program that includes a Java plug-in. If there is no JRE installed, Java applets will not run. Fortunately, Java is freely available for Windows, Mac, and Linux systems, which means you can easily download and install the appropriate JRE for your system. Since Java applets run within the JRE and are not executed by the operating system, they are crossplatform, meaning a single applet can run on Windows, Mac, and Linux systems.

While applets can serve as basic desktop applications, they have limited access to system resources and therefore are not ideal for complex programs. However, their small size and crossplatform nature make them suitable for Web-based applications. Examples of applets designed to run in web browsers include calculators, drawing programs, animations, and video games. Web-based applets can run in any browser on any operating system and long as the Java plug-in is installed.

During the early years of the Web, Java applets provided a way for webmasters to add interactive features that were not possible with basic HTML. However, in recent years, applets have been slowly replaced by newer technologies such as jQuery and HTML 5. Some browsers, like Google Chrome, no longer support the tag, and others, like Apple Safari, do not even enable Java by default. Since web developers cannot fully rely on Java support from web browsers, applets are no longer a common way to provide interactive content on the Web.

--Updated January 20, 2012

Application Server

An application server is a server specifically designed to run applications. The "server" includes both the hardware and software that provide an environment for programs to run.

Application servers are used for many purposes. Several examples are listed below:

- running web applications
- hosting a hypervisor that manages virtual machines
- distributing and monitoring software updates
- processing data sent from another server

Since the purpose of an application server is to run software programs, the most important hardware specifications are CPU and RAM. On the software side, the operating system is most important, since it determines what software the server can run.

Why Use an Application Server?

A web server is designed – and often optimized – to serve webpages. Therefore, it may not have the resources to run demanding web applications. An application server provides the processing power and memory to run these applications in real-time. It also provides the environment to run specific applications. For example, a cloud service may need to process data on a Windows machine. A Linux-based server may provide the web interface for the cloud service, but it cannot run Windows applications. Therefore, it may send input data to a Windows-based application server. The application server can process the data, then return the result to the web server, which can output the result in a web browser.

--Updated November 22, 2019

Archie

Archie is a program that allows you to search for files available on one or more FTP servers. It was commonly used in the early 1990s, but has been replaced by standard web-based search engines and peer-to-peer (P2P) file sharing services.

In the early days of the Internet, large files were often available only through FTP servers. In order to download a specific file, users would have to navigate to the appropriate directory and then find the correct file before downloading it. This made it difficult for people to locate files unless they knew exactly where they were stored on the server. Archie made it possible for users to actually search FTP servers rather than browsing through all the directories.

While Archie is rarely used today, some websites still offer an Archie search feature. You can often identify an Archie search engine by a URL that begins with "archie" rather than "www." Most Archie search engines allow you to search for filenames based on either substrings or exact matches. You can also specify if a search should be case sensitive or not. Additionally, you can use boolean operators such as AND and OR to search for multiple filenames at once.

--Updated February 8, 2012

ASP

ASP has two different meanings in the IT world: 1) Application Service Provider, and 2) Active Server Page.

Application Service Provider

An Application Service Provider is a company or organization that provides software applications to customers over the Internet. These Internet-based applications are also known as "software as a service" (SaaS) and are often made available on a subscription basis. This means ASP clients often pay a monthly fee to use the software, rather than purchasing a traditional software license. Some SaaS applications can be accessed via a web browser, while others operate over a proprietary secure port.

Active Server Page

An Active Server Page, commonly called an "ASP page," is a webpage that may contain scripts as well as standard HTML. The scripts are processed by an ASP interpreter on the web server each time the page is accessed by a visitor. Since the content of an ASP page can be generated on-the-fly, ASP pages are commonly used for creating dynamic websites.

ASP is similar to other scripting platforms, like PHP and JSP, but supports multiple programming languages. While the default ASP language is VBScript, ASP pages can include other programming languages as well, such as C# and JavaScript. However, alternative languages must be defined before the script code using the following declaration:

```
<%@ Page Language="C#"%>
```

ASP pages are part of the ASP.NET web application framework developed by Microsoft. Therefore, ASP pages are most often found on Windows-based web servers that run Microsoft Internet Information Services, or IIS. You can tell if you are accessing an ASP page in your browser if the URL has an ".asp" or ".aspx" suffix.

File extensions: .ASP, .ASPX

--Updated March 15, 2012

ASP.NET

ASP.NET is a set of Web development tools offered by Microsoft. Programs like Visual Studio .NET and Visual Web Developer allow Web developers to create dynamic websites using a visual interface. Of course, programmers can write their own code and scripts and incorporate it into ASP.NET websites as well. Though it often seen as a successor to Microsoft's ASP programming technology, ASP.NET also supports Visual Basic.NET, JScript .NET and open-source languages like Python and Perl.

ASP.NET is built on the .NET framework, which provides an application program interface (API) for software programmers. The .NET development tools can be used to create applications for both the Windows operating system and the Web. Programs like Visual Studio .NET provide a visual interface for developers to create their applications, which makes .NET a reasonable choice for designing Web-based interfaces as well.

In order for an ASP.NET website to function correctly, it must be published to a Web server that supports ASP.NET applications. Microsoft's Internet Information Services (IIS) Web server is by far the most common platform for ASP.NET websites. While there are some open-source options available for Linux-based systems, these alternatives often provide less than full support for ASP.NET applications.

--Updated in 2006

ATM

Stands for "Asynchronous Transfer Mode." Most people know of ATMs as automated teller machines -- those friendly boxes that allow you to withdraw cash from your bank or credit account while charging you a ridiculous surcharge for the service. In the computer world, however, ATM has a different meaning. Asynchronous Transfer Mode is a networking technology that transfers data in packets or cells of a fixed size.

ATM uses 53-byte cells (5 bytes for the address header and 48 bytes for the data). These extremely small cells can be processed through an ATM switch (not an automated teller machine) fast enough to maintain data transfer speeds of over 600 mbps. The technology was designed for the high-speed transmission of all forms of media from basic graphics to full-motion video. Because the cells are so small, ATM equipment can transmit large amounts of data over a single connection while ensuring that no single transmission takes up all the bandwidth. It also allows Internet Service Providers (ISPs) to assign limited bandwidth to each customer. While this may seem like a downside for the customer, it actually improves the efficiency of the ISP's Internet connection, causing the overall speed of the connection to be faster for everybody.

--Updated in 2006

Attachment

An attachment, or email attachment, is a file sent with an email message. It may be an image, video, text document, or any other type of file.

Most email clients and webmail systems allow you to send and receive attachments. To send an attachment along with your email, you can use the "Attach" command, then browse to the file you want to attach. In some email interfaces, you can simply drag a file into the message window to attach it. When you receive an attachment, most email programs allow you to view the attachment in place or save it to your local storage device.

While modern email programs make it easy to send and receive attachments, the original email system (SMTP) was actually not designed to handle binary files. Therefore, attachments must be encoded as text in order to be transferred with an email message. The most common encoding type is MIME (Multi-Purpose Internet Mail Extensions). While MIME encoding makes it possible to send messages with emails, it typically increases the file size of the attachment about 30%. That's why when you attach a file to an email message, the file size of the attachment appears larger than the original file.

You can attach multiple files to a single email message. However, the maximum size of the combined attachments is limited by the sending and receiving mail servers. In other words, the size of the attachment(s) after being encoded cannot be larger than the limit of either the outgoing or incoming mail server. In the early days of email, attachments were limited to one megabyte (1 MB). Today, many mail servers allow attachments larger than 20 MB. However, to protect against viruses and malware, many mail servers will not accept executable file types, such as .EXE or .PIF files. If you need to send an executable file to someone, you can compress the file as a .ZIP archive before attaching it to the email message.

NOTE: Even a large amount of text takes up a small amount of space compared to most binary files. Therefore, attaching a document to an email may increase the size substantially. For example, a typical email may only require one kilobyte (1 KB) of disk space. Attaching a single 1 MB file will make the message 1,000 times larger. Therefore, it is best to share large files using another method like FTP or DropBox. Additionally, if you have almost reached your email quota on your mail server, you can free up a lot of space by deleting old attachments.

--Updated April 24, 2015

AUP

Stands for "Acceptable Use Policy." An AUP is list of rules you must follow in order to use a website or Internet service. It is similar to a software license agreement (SLA), but is used specifically for Internet services.

Most well-known, high traffic websites include an AUP, which may also be called Terms of Service (TOS) or Terms of Use (TOU). You can often find a link to the to the website's AUP in the footer of the home page. Many web services, such as cloud applications require you to agree to an AUP in order to use the online service. ISPs often provide an AUP with each account, which states specific guidelines you must follow.

The specifics of an AUP vary depending on the service offered. Even website AUPs may differ greatly based on the purpose of the website and the website's content. However, most AUPs include a list of general dos and don'ts while using the service, such as the following:

1. Do not violate any federal or state laws.
2. Do not violate the rights of others.
3. Do not distribute viruses or other malware.
4. Do not try to gain access to an unauthorized area or account.
5. Respect others' copyrights and intellectual property.
6. Familiarize yourself with the usage guidelines and report violations.

An AUP serves as an agreement between the user and the company offering the online service. Some rules are basic netiquette, while others may have legal ramifications. If you fail to comply with a policy in a AUP, the company has the right to suspend or terminate your account or take legal action if necessary. Therefore, it is wise to familiarize yourself with the AUPs of the Internet services you use.

--Updated January 16, 2014

Autoresponder

An autoresponder is a script that automatically replies to emails sent to a specific email address. It may be used for away messages, email confirmations, or for several other purposes.

Autoresponders can be configured on a mail server or using an email client. When configured on a mail server, the server automatically sends response emails while the autoresponder is active. Server-based autoresponders are often configured using a webmail interface. For example, Gmail provides a "vacation reply" for this purpose. They can also be created by a server administrator for one or more email addresses. cPanel, a popular web hosting platform for Linux, allows admins to manage autoresponders by logging into the control panel for a specific account and selecting Email → Autoresponders.

To set up an autoresponder using a mail client, you typically create a "rule." For example, you can add a rule that automatically replies to messages sent to a specific email address. This type of rule works well once it has been configured, but the mail client must be open in order for the autoresponder to work. If you set up a vacation reply in your mail program on your home computer, then turn off your computer before you leave, the autoresponder will not work.

When setting up an auto-reply on a server, you may be able to enter a date range for when it is active. If the autoresponder does not turn off automatically, it is a good idea to set a reminder for yourself to turn it off when you return.

NOTE: Email "bounce" messages are sent automatically, but are not considered autoresponders since they are not configured by users.

--Updated August 7, 2017

Avatar

Generally speaking, an avatar is the embodiment of a person or idea. However, in the computer world, an avatar specifically refers to a character that represents an online user. Avatars are commonly used in multiplayer gaming, online communities, and web forums.

Online multiplayer role-playing games (MMORPGs) such as World of Warcraft and EverQuest allow users to create custom characters. These characters serve as the players' avatars. For example, a World of Warcraft player may choose a Paladin with blue armor as his avatar. As the player progresses in the game, his character may gain items and experience, which allows the avatar to evolve over time.

Avatars are also used in online communities, such as Second Life and The Sims Online. These avatars can be custom-designed to create a truly unique appearance for each player. Once a user has created an avatar, he or she becomes part of an online community filled with other users' avatars. Players can interact with other avatars and talk to them using text or voice chat. It's no surprise that "Second Life" refers to a virtual life that players live through their avatars.

Finally, avatars are common in web forums. Online discussion boards typically require users to register and provide information about themselves. Many give users the option to select an image file that represents the user's persona. This image, combined with a made-up username, serves as a person's avatar. For example, a user may select a picture of a Pac-Man and choose the name "pac32" for his avatar. This avatar typically appears next to each posting the user contributes in an online forum.

Regardless of the application, avatars allow people to represent themselves online in whatever way they want. They may be considered alter-egos, since users can customize characters that are completely different than their actual personas. Of course, what's the point of having a "second life" if it's the same as reality?

--Updated April 27, 2009

Azure

Azure is a cloud computing platform built and operated by Microsoft. It allows companies to run applications and host content in the cloud. While Microsoft designed Azure to support enterprise computing requirements, the service is also available to small businesses and individuals.

The Azure infrastructure consists of multiple data centers distributed around the world. The global network of computers provides low latency and high reliability regardless of where users access the service. Azure includes multiple types of servers, including Windows Server, Linux, and SAP HANA machines.

Below are a few examples of the 200+ Azure solutions:

1. SaaS - running web applications and Internet-based services
2. CDN - delivering websites and streaming content from edge nodes around the world
3. E-commerce - providing customized shopping cart experiences localized for each visitor
4. Database storage - enabling high-speed data storage and access
5. Software testing - providing access to virtual machines that run different operating systems

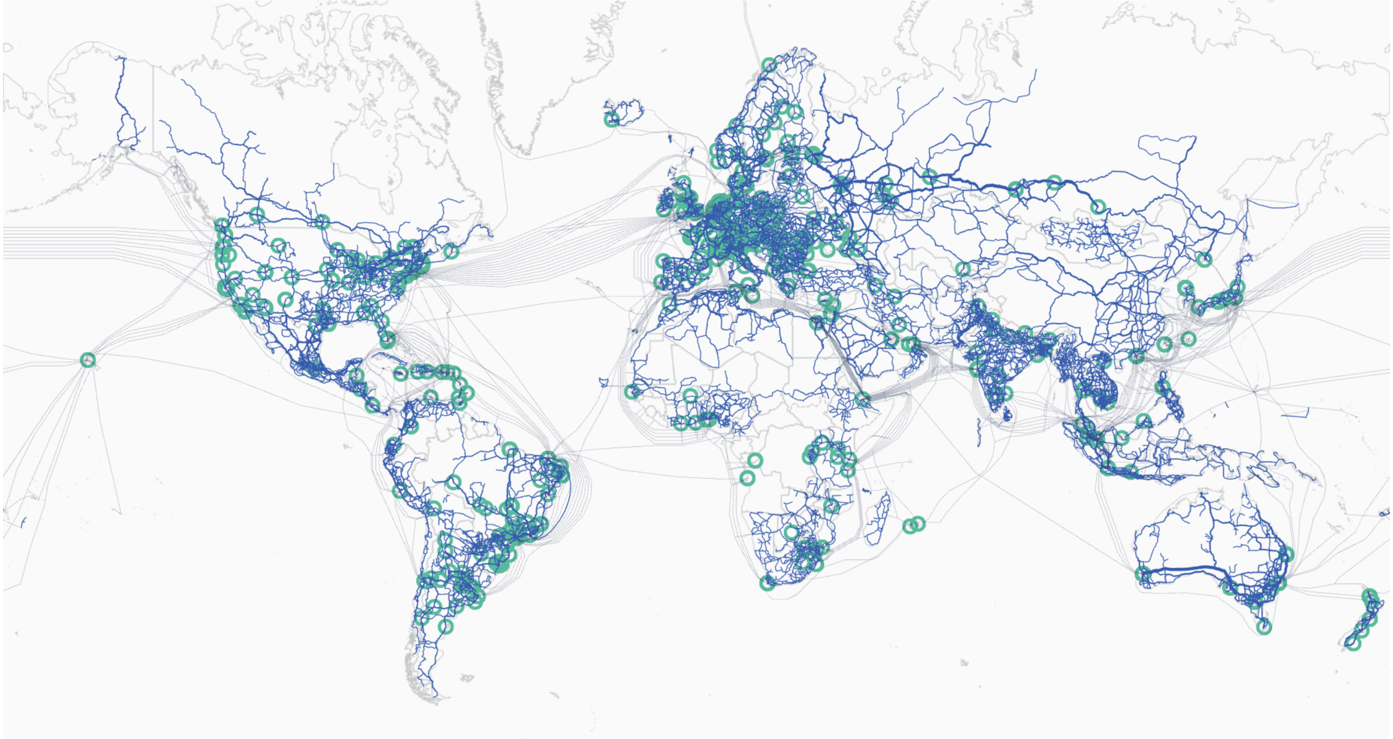
Because of the benefits of a globally-distributed computing network, many businesses have moved locally-hosted data to a cloud service like Azure. While migrating data and applications to Azure may require several steps, starting the process is simple. Developers can sign up for an Azure account, create a new cloud computing "instance," and start using the service immediately.

--Updated March 24, 2022

Backbone

A backbone network is a robust, high-speed network that links multiple local networks into a single wide-area network. Similar to how a person's backbone carries signals to and from smaller groups of nerves in their nervous system, a backbone network forms the central communications infrastructure that transmits data between networks. The largest backbone network connects ISPs around the world to create the Internet.

Computers on a network do not connect to a network backbone directly. Instead, each local network connects to its backbone through an edge router, which directs data packets to their destination using the most efficient route possible. A backbone typically uses faster transmission lines than an individual network — often a trunk of multiple fiber-optic cables. A connection to the backbone often maximizes its speed using link aggregation, which connects a device to several separate lines and sends data across them in parallel. For example, an edge router may link to five 10-gigabit fiber optic lines in aggregate to provide a single 50-gigabit connection.This is a map of global fiber backbone networks and Internet exchange points:



The backbone network that forms the Internet consists of trunks of high-speed fiber optic cables owned by several global telecommunications companies, categorized as Tier 1 ISPs. All Tier 1 ISPs work together through peering agreements that allow the free flow of traffic between their networks via hundreds of high-speed linkages, called Internet exchange points, located around the world. Tier 1 ISPs provide Internet backbone connections to medium-sized (Tier 2) ISPs, who in turn provide service to large enterprises, data centers, and regional (Tier 3) ISPs.

--Updated July 13, 2023

Backlink

A backlink is an incoming link from an external website to specific webpage. For example, if you publish a webpage and 20 other websites link to it, your webpage has 20 backlinks. Links to the page from within your own website are not included in the backlink total.

Web developers benefit from backlinks (or "inlinks") in two different ways — direct traffic and search result placement. As more links to a specific webpage are published on external sites, there is greater potential for traffic to be generated from other websites. This is called direct traffic. By increasing direct traffic, a website can gradually grow its presence on the Web and generate a steady stream of visitors from other websites.

While direct traffic is helpful, most websites generate the majority of their traffic through search engines. Since search engines use backlinks as an important part of the their algorithms for search result placement, external links are important for good search ranking. Therefore, generating backlinks has become common practice for search engine optimization, or SEO. The more backlinks a webpage has, the better the chance that the page will rank highly in search results for relevant keywords. If a website has many pages that have backlinks, the overall number of incoming links may help increase the ranking of all pages within the website. While most backlinks point to a website's home page, incoming links to other pages within the website are beneficial as well.

--Updated December 17, 2010

Banner Ad

Whether you like it or not, much of the Web is run by advertising. Just like television or radio, websites can offer free content by generating revenue from advertising. While you may get tired of Web ads from time to time, most people would agree that seeing a few advertisements here and there is better than paying a usage fee for each website.

Perhaps the most prolific form of Web advertising is the banner ad. It is a long, rectangular image that can be placed just about anywhere on a Web page. Most banner ads are 468 pixels wide by 60 pixels high (468x60). They may contain text, images, or sometimes those annoying animations that make it hard to focus on the page's content. Regardless of the type of banner ad, when a user clicks the advertisement, he or she is redirected to the advertiser's website.

--Updated in 2006

Bcc

Stands for "Blind Carbon Copy." Bcc is an email field that allows you to "blind" copy one or more recipients. It is similar to the Cc field, but email addresses listed in the Bcc field are hidden from all recipients.

When you Bcc someone, that person receives a single copy of the email. He or she will not receive any replies to the message. Therefore, blind carbon copying is a useful way to share an email with one or more users who don't need to follow the email thread.

It is good netiquette to use the Bcc field when sending an email to a large group of people. Hiding the recipient list protects users' privacy and prevents the email addresses from being shared unintentionally. However, if recipients should know who else received the message, it is best to use the Cc field.

To vs. Cc vs. Bcc

Generally, you should use the To field for the primary recipient(s) — the people to whom the message is addressed. Secondary recipients who should follow the email thread belong in the Cc field. If you want to send a copy of the email to others for reference, the Bcc field makes sense.

NOTE: Bcc'd recipients can still see the email addresses listed in the To and Cc fields.

--Updated February 4, 2021

BGP

Stands for "Border Gateway Protocol." BGP is a protocol used for routing data transmissions over the Internet. It helps determine the most efficient path, whether sending data down the street or across the globe.

BGP manages the flow of data similar to how the post office handles the delivery of physical mail. For example, when a user in Los Angeles accesses a website in New York, BGP first routes the data from the New York-based server to the Internet backbone. The data travels through large fiber optic cables across state lines, then through smaller networks until it arrives at the user's ISP in Los Angeles. The ISP then routes the data locally to the user's device.

Each router along the data transmission route is called a "hop." You can view the hops between your location and a server using a traceroute command, such as the ones below:

Unix - traceroute techterms.com
DOS - tracert techterms.com

Fundamental to the Border Gateway Protocol are routing tables, which are plain text files that list available routers by IP address. BGP routers use these tables to determine the best path for each data transmission. Routing tables are frequently updated since the fastest route can change based on network traffic and outages. High-traffic routers may request updates once a minute or even every few seconds.

Benefits of BGP

1. A standard means of communication between routers
2. Efficient routing of data over the Internet
3. Adaptability for network congestion
4. Redundancy when network outages occur
5. Scalability to add or remove routers
6. Autonomous operation

NOTE: While BGP enables efficient routing of data across long distances, CDNs provide an even greater benefit by hosting data at "edge nodes" around the world.

--Updated March 18, 2022

Big Data

The phrase "big data" is often used in enterprise settings to describe large amounts of data. It does not refer to a specific amount of data, but rather describes a dataset that cannot be stored or processed using traditional database software.

Examples of big data include the Google search index, the database of Facebook user profiles, and Amazon.com's product list. These collections of data (or "datasets") are so large that the data cannot be stored in a typical database, or even a single computer. Instead, the data must be stored and processed using a highly scalable database management system. Big data is often distributed across multiple storage devices, sometimes in several different locations.

Many traditional database management systems have limits to how much data they can store. For example, an Access 2010 database can only contain two gigabytes of data, which makes it infeasible to store several petabytes or exabytes of data. Even if a DBMS can store large amounts of data, it may operate inefficiently if too many tables or records are created, which can lead to slow performance. Big data solutions solve these problems by providing highly responsive and scalable storage systems.

There are several different types of big data software solutions, including data storage platforms and data analytics programs. Some of the most common big data software products include Apache Hadoop, IBM's Big Data Platform, Oracle NoSQL Database, Microsoft HDInsight, and EMC Pivotal One.

--Updated August 27, 2013

Bing

Bing is a search engine developed by Microsoft. It provides a standard web search, as well as specialized searches for images, videos, shopping, news, maps, and other categories.

Bing originated from MSN Search, which later became Windows Live Search (or simply "Live Search"). Microsoft renamed the search engine to "Bing" in June of 2009. The name change also reflected Microsoft's new direction with the search engine, which the company branded as a "decision engine." Bing is designed to help users make important decisions faster. This focus is summarized in the search engine's slogan, "Bing and decide."

Bing differentiates itself from other search engines like Google and Yahoo in several different ways. For instance, Bing's home page includes a background image or video that is updated every day. You can click on different areas of the background to learn more about the daily topic. Bing also uses Microsoft's proprietary search algorithm to provide relevant search results. These results may include "instant answers," which provide helpful information at the top of the search results page for specific types of queries. The search results may also include images, videos, shopping information, or news stories that are relevant to the keywords you entered.

You can choose to sign into Bing using your Windows Live ID or your Facebook login. When you are logged into Facebook, Bing displays which of your friends "Like" specific webpages in the search results. If you want even more Facebook integration, you can download the "Bing Bar," which provides News Feed updates directly from the toolbar in Internet Explorer. The Bing Bar also provides one-click access to weather, maps, videos, stock quotes, and other information.

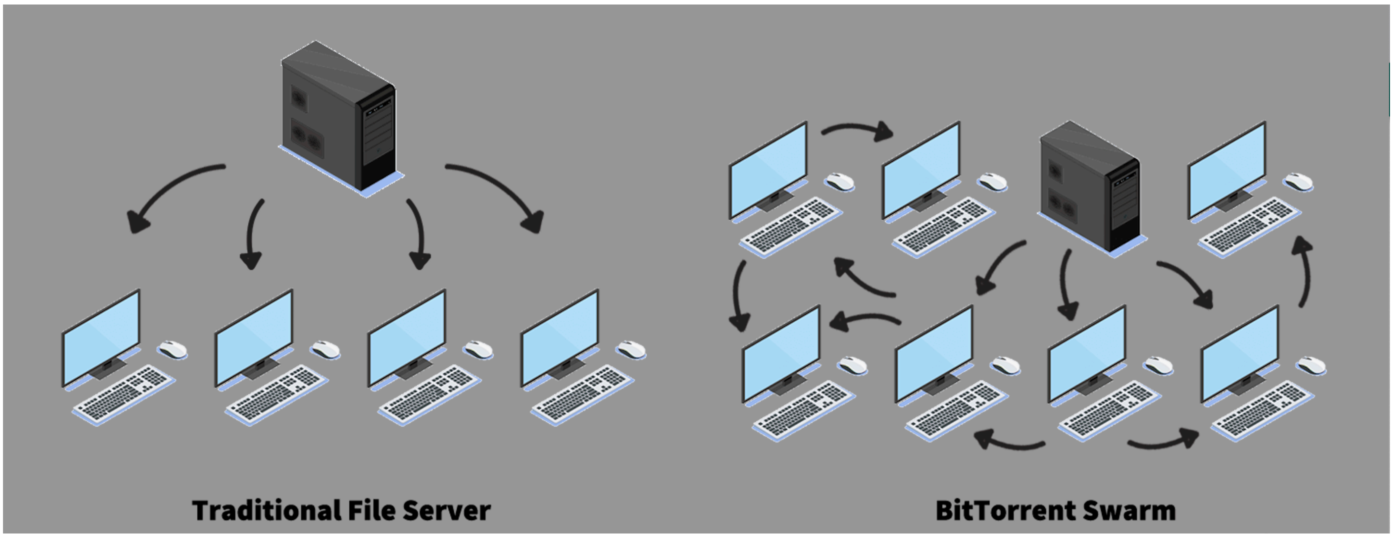
Try Bing for yourself.

--Updated February 20, 2012

BitTorrent

BitTorrent is an open-source peer-to-peer (P2P) file-sharing protocol. It decentralizes the distribution of files by making each client that downloads a file also act as a server other clients can download from. It even allows the original file host to drop offline without affecting the availability of that file as long as at least one other computer has a full copy of it.

BitTorrent helps distribute files without the use of a dedicated file server. Instead, people can create and download torrent files containing information and metadata about shared files. A torrent file also includes an address for a tracker — a server that coordinates file transfers by tracking the IP addresses for every computer downloading and sharing that torrent. Once connected to the torrent's swarm, the client can begin downloading from seeds and sharing with peers.BitTorrent allows fast file downloads amongst a swarm of computers while reducing the load on a single server



Traditional file servers transfer files to clients progressively, starting at the beginning of a file and sending its contents in order. BitTorrent instead splits files into small, uniformly-sized pieces and transfers them out of sequential order, prioritizing the rarest pieces that the fewest peers have. Once the client finishes downloading each piece, it begins uploading it to other peers and moves on to another one. This way, a client can add redundancy to the network and reduce the overall demand on the seeds.

The BitTorrent protocol has several benefits over traditional file servers, making it ideal for specific uses. Many free and open-source software communities use BitTorrent to distribute their software for free to reduce server costs. It also helps quickly distribute large files that see immediate high demand without overloading a single file server. For example, Blizzard used a custom BitTorrent client to release game updates for World of Warcraft, allowing gamers to get the update quickly without the risk of a file server crash. However, the most popular use of BitTorrent is the distribution of pirated movies, TV shows, music, and software.

--Updated June 26, 2023

Blog

Short for "Web Log," this term refers to a list of journal entries posted on a Web page. Anybody who knows how to create and publish a Web page can publish their own blog. Some Web hosts have made it even easier by creating an interface where users can simply type a text entry and hit "publish" to publish their blog.

Because of the simplicity of creating a blog, many people (often young kids and adults) have found a new presence on the Web. Instead of writing confidential entries in a book that no one is supposed to see, people now can share their personal feelings and experiences with thousands of people around the world. Blogs are typically updated daily, monthly, or anywhere in between. "Blog" may also be used as a verb, as in "Wow, Matt sure blogged a lot last week."

--Updated in 2006

Bookmark

A bookmark is a saved shortcut that directs your browser to a specific webpage. It stores the title, URL, and favicon of the corresponding page. Saving bookmarks allows you to easily access your favorite locations on the Web.

All major web browsers allow you to create bookmarks, though each browser provides a slightly different way of managing them. For example, Chrome and Firefox display your bookmarks in an open window, while Safari displays them in a list in the sidebar of the browser window. Internet Explorer uses the name "Favorites" to refer to bookmarks, and like Safari, it displays all your favorites in a list within the browser window sidebar.

To create a bookmark, simply visit the page you want to bookmark and select Add Bookmark or Bookmark this Page from the Bookmarks menu. In Internet Explorer, you can click the star icon to open the Favorites sidebar and click Add to Favorites to add the current page to your bookmarks. The website title will show up in your bookmarks list along with the website's favicon if available. As your collection of bookmarks grows, you can create folders to organize your bookmarks into different categories.

It is helpful to bookmark frequently visited websites and useful references since you don't have to remember the URLs. Additionally, you can just click the bookmarks instead of typing in the full web addresses. Some browsers even display your bookmarked pages in the autocomplete drop down menu as you type in the address bar. This allows you to visit bookmarked pages without even opening the bookmarks window or sidebar in your browser.

NOTE: A bookmark only stores the location of a webpage, not store the contents of the webpage itself. Therefore, when you open a previously saved bookmark, the contents of the page may have changed since the last time you viewed it.

--Updated February 11, 2014

Bot

A bot (short for "robot") is an automated program that runs over the Internet. Some bots run automatically, while others only execute commands when they receive specific input. There are many different types of bots, but some common examples include web crawlers, chat room bots, and malicious bots.

Web crawlers are used by search engines to scan websites on a regular basis. These bots "crawl" websites by following the links on each page. The crawler saves the contents of each page in the search index. By using complex algorithms, search engines can display the most relevant pages discovered by web crawlers for specific search queries.

Chat bots were one of the first types of automated programs to be called "bots" and became popular in the 1990s, with the rise of online chatrooms. These bots are scripts that look for certain text patterns submitted by chat room participants and respond with automated actions. For example, a chat bot might warn a user if his or her language is inappropriate. If the user does not heed the warning, the bot might kick the user from the channel and may even block the user from returning. A more advanced type of chat bot, called a "chatterbot" can respond to messages in plain English, appearing to be an actual person. Both types of chat bots are used for chatroom moderation, which eliminates the need for an individual to monitor individual chatrooms.

While most bots are used for productive purposes, some are considered malware, since they perform undesirable functions. For example, spambots capture email addresses from website contact forms, address books, and email programs, then add them to a spam mailing list. Site scrapers download entire websites, enabling unauthorized duplication of a website's contents. DoS bots send automated requests to websites, making them unresponsive. Botnets, which consist of many bots working together, may be used to gain unauthorized access to computer systems and infect computers with viruses.

--Updated February 14, 2014

Botnet

A botnet is a group of computers that are controlled from a single source and run related software programs and scripts. While botnets can be used for distributed computing purposes, such as a scientific processing, the term usually refers to multiple computers that have been infected with malicious software.

In order to create a malicious botnet, a hacker must first compromise several computers. This might be done by exploiting a security hole through a Web browser, IRC chat program, or a computer's operating system. For example, if a user has turned off the default firewall settings, his or her computer may be susceptible to such a botnet attack. Once the hacker has gained access to several computers, he can run automated programs or "bots" on all the systems at the same time.

A hacker may create a botnet for several different purposes, such as spreading viruses, sending e-mail spam, or crashing Web servers using a denial of service attack. Botnets can range from only a few computers to several thousand machines. While large botnets can cause the most damage, they are also easiest to locate and break apart. The unusual amount of bandwidth used by large botnets may trigger an alert at one or more ISPs, which might lead to the discovery and dismantling of the botnet.

In most situations, users do not know that their computers have become part of a botnet. This is because hackers typically hide their intrusion by masking the activity within regular processes, similar to a rootkit attack. Therefore, it is a good idea to install antivirus or anti-malware software that regularly checks for such intrusions on your computer. It is also wise to make sure your system firewall is turned on, which is usually the default setting.

--Updated June 9, 2010

Bounce

The term "bounce" has several different IT related meanings, yet none of them include bouncy balls. The most common definition of bounce used in the computer world refers to e-mail messages.

1、**Returning E-mail**

When you send an e-mail message to another person, the mail server processes the message and delivers it to the appropriate user's mailbox. For example, if you send a message to "Kobe@mail.com," the mail.com server looks for a user named "mrman" to deliver the message to. If the user does not exist, the mail server may bounce the message back to the sender, saying "Sorry, that user does not exist." These messages often come from "Mail Delivery Subsystem" and have a subject line that reads "Returned mail: see transcript for details."

If you receive a bounced message, you may want to check the e-mail address you sent the message to and make sure it was typed correctly. If the address is correct, it may help to read the body of the bounced message for more details. The transcript may say something like "User quota over limit," which means the recipient has reached his or her e-mail quota and must delete some messages and/or attachments in order to receive new mail. If this is the case, you may want to call the person or use an alternative e-mail address to let the person know he or she has some Inbox maintenance to do.

2、Restarting a Computer

The term "bounce" can also describe the process of rebooting or restarting a computer. For example, a workstation may need to be bounced after installing new software. Similarly, a Web server may be bounced if websites hosted on the server are not responding correctly.

3、Exporting Audio

"Bounce" can also describe the process of exporting several tracks in an audio mix to one mono track or two stereo tracks. This helps consolidate audio tracks after they have been mixed. Bouncing audio tracks limits the need for processing power since the computer only has to process one track instead of all the tracks individually. Digital Performer is the primary audio software program that uses bouncing to export audio.

4、Hiding a Network Connection

Finally, "bouncing" can also be used in networking to describe a method of hiding the source of a user's network connection. This type of bouncing is often abbreviated "BNC." Someone who bounces his network connection is called a "bouncer," though this is not the same person who checks your ID at the bar.

--Updated October 18, 2007

Broadband

Broadband refers to high-speed data transmission over a single cable, carrying a large amount of data across multiple signals simultaneously. It commonly refers to a high-bandwidth, always-on Internet connection. The most common types of broadband connections are DSL, cable, fiber, and mobile wireless.

Different countries have different standards for what is considered broadband. It generally applies to any Internet connection that is both faster than dial-up or ISDN and is always connected. The speed at which an Internet connection is deemed broadband changes over time as technology improves. For example, the US FCC once considered a connection that offered 4 Mbps download / 1 Mbps upload to be broadband before later updating their standards to 25 Mbps down / 3 Mbps up.

Types of Broadband Internet

Several different types of broadband Internet connection are commonly available. Some require dedicated lines and only operate in tight geographic areas, while others are more widely available. Speeds, prices, and the quality of service can vary greatly based on the type of connection.

- **Digital Subscriber Line**, or DSL, is a type of broadband connection that operates over telephone lines. A DSL line's speed depends on several factors — the quality of the line, the number of other customers in an area, and the distance between the customer and the ISP. Typical speeds range from 1-5 Mbps on the low end up to 100 Mbps.
- **Cable** Internet operates over coaxial cables originally designed for cable television service. Like DSL, a high number of customers in an area can result in a slower speed for everyone, so many cable ISPs implement monthly data caps to limit usage. Speeds range from 30-100 Mbps on the low end to more than 1 Gbps.
- **Fiber** Internet service runs over dedicated fiber optic cables. Fiber networks are not as affected by local network traffic as DSL and cable, so most fiber connections are uncapped and offer symmetrical download and upload speeds. Fiber's availability requires the local ISP to run new lines, so it is more geographically limited than options that use the existing phone and cable lines. Fiber Internet speeds range from 100 Mbps on the low end up to 2 Gbps.
- **Wireless** Internet can run over normal cellular networks or a fixed wireless connection. Customers of 4G and 5G mobile carriers can use dedicated hotspots or their own mobile phones to connect their homes to the Internet. Fixed wireless uses lower frequencies that travel from the ISP's radio tower to a dedicated outdoor radio receiver. Connection quality depends on the type of service, the signal strength, and whether there is a clear line of sight to the tower. Speeds range from 5-10 Mbps up to 1 to 2 Gbps.
- **Satellite** Internet is delivered from satellites in orbit to a dish or receiver mounted outside of a home. Since a signal has to travel to orbit and back, satellite Internet has higher latency than other types of broadband. It is generally more expensive than wired connections but can operate nearly anywhere. Satellite signals also require a line of sight to the sky and can suffer from interference caused by trees and weather conditions. Speeds range from around 10 Mbps up to 500 Mpbs.

--Updated October 31, 2022

Brute Force Attack

A brute force attack is an attempt to gain access to a system using successive login attempts. It can be performed manually or by using an automated script. In either case, a brute force attack tries different username and password combinations with the hope of discovering a valid login.

While brute force attacks are simplistic by nature, their implementation is often complex. Since most servers will block a user or IP address after multiple failed logins, a hacker may use multiple systems to perform a single brute force attack. Some attacks may use hundreds or even thousands of devices, similar to a distributed denial of service DDoS attack.

While the odds of guessing a correct login via a brute force attack are low, it is still one of the most common ways online accounts are compromised. Using enough attempts, it is theoretically possible to discover any login. However, short and common passwords are the most vulnerable.

How to Protect Against Brute Force Attacks

The two primary ways to protect your online accounts from brute force attacks are to 1) choose strong passwords and 2) use two-factor authentication.

1. **Choose strong passwords**

   A fundamental step in securing any online account is to choose a strong password. This means choosing a password that:

   is long – at least eight characters, preferably 12 or more.

   - **contains special characters –** including numbers and symbols, as well as lowercase and uppercase characters.
   - **is not personally identifiable –** using a special date or the name of someone close to you makes it easy for someone to manually hack your account.

   It is especially important to choose a strong password for your email account since your username (half of your login) is your

   public email address. Additionally, if someone gains access to your email, he or she can easily discover your other passwords.

2. **Use Two-Factor Identification**

Some services allow you to enable two-factor authentication, which requires authentication from two devices. For example, you may be asked to enter a username and password on your computer, followed by a code sent via text to the phone number listed in your account. With two-factor authentication, even if a hacker knows your username and password, he or she will not be able to successfully log in to your account.

--Updated June 17, 2019

Captcha

A captcha is program used to verify that a human, rather than a computer, is entering data. Captchas are commonly seen at the end of online forms and ask the user to enter text from a distorted image. The text in the image may be wavy, have lines through it, or may be highly irregular, making it nearly impossible for an automated program to recognize it. (Of course, some captchas are so distorted that they can be difficult for humans to recognize as well.) Fortunately, most captchas allow the user to regenerate the image if the text is too difficult to read. Some even include an auditory pronunciation feature.

By requiring a captcha response, webmasters can prevent automated programs, or "bots," from filling out forms online. This prevents spam from being sent through website forms and ensures that wikis, such as Wikipedia, are only edited by humans. Captchas are also used by websites such as Ticketmaster.com to make sure users don't bog down the server with repeated requests. While captchas may be a minor inconvenience to the user, they can save webmasters a lot of hassle by fending off automated programs.

The name "captcha" comes from the word "capture," since it captures human responses. It may also be written "CAPTCHA," which is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."

--Updated May 8, 2009

Cc

Stands for "Carbon Copy." The term comes from carbon copying, in which a piece of carbon paper copies writing from one paper to another (often used when filling out forms). However, the term is now commonly used in reference to e-mail. When you send an e-mail message, you typically type the recipient's address in the "To:" field. If you want to send the message to one or more other recipients, you can use the "Cc:" field to add additional addresses. This will send the e-mail to the address in the "To:" field and to each address listed in the "Cc:" field as well.

The "Cc:" option is often used in business communications when a message is intended for one person, but is relevant to other people as well. For example, a retail employee may e-mail another employee saying he can work for her on a certain day. He might include his manager's and assistant manager's e-mail addresses in the "Cc:" field to let them know he is taking the work shift. Similarly, a team member working on a product design may e-mail his boss with the latest design revisions and may "Cc:" the other members of his team to let them know the e-mail has been sent.

"CCing" (yes, it can also be used as a verb) is a quick way to let other people in on your e-mail communications. It is efficient because you don't have to send separate messages to each individual address. However, remember that When you Cc an e-mail, all the recipients can see the other addresses the message was sent to. If you want to hide the additional addresses, use Blind Carbon Copy (Bcc) instead.

--Updated November 24, 2006

CDN

Stands for "Content Delivery Network." A CDN is a group of servers distributed in different locations. Small CDNs may be located within a single country, while large CDNs are spread across data centers around the world.

CDNs are used to provide content to users in different locations as quickly as possible. For example, a user in San Francisco may receive website content from a server in Los Angeles, while a user in England may receive the same content from a server in London. This is accomplished using data replication, which stores the same data on multiple servers. Whenever you access a website hosted on a CDN, the network will intelligently provide you with the content using the server closest to the your geographical location.

By providing Internet-based content over a CDN, large businesses can avoid bottlenecks associated with serving data from a single location. It also helps limit the impact of security breaches, such as denial of service attacks. If hardware fails on one server, the CDN can quickly reroute traffic to the next best server, limiting or even eliminating downtime.

While CDNs are often used to host websites, they are commonly used to provide other types of downloadable data as well. Examples include software programs, images, videos, and streaming media. Cloud computing services are often provided over content delivery networks as well. Since CDNs automatically choose the best server for each user, there is no need to manually choose the most efficient location, like some FTP download services require.

NOTE: While CDNs are often accessed via standard URLs, many CDNs include the letters "cdn" in their web address.

--Updated September 13, 2013

Certificate

An SSL certificate, or digital certificate, is a file installed on a secure web server that identifies a website. A digital certificate establishes the identity and authenticity of the company that runs a website so that visitors can trust that the website is secure and reliable. In order to verify that these sites are legitimate (that the owners are who they say they are), the companies and their websites are verified by a third-party certificate authority, such as IdenTrust or DigiCert.

Once the certificate authority establishes the legitimacy of an organization and that they run the associated website, it will issue an SSL certificate. The cost for a certificate varies, depending on the level of support provided — some certificates are issued for free, but many cost around $60-$100 per year (or more). This digital certificate is installed on the web server and will be viewable when a user visits the website. Sites with a valid certificate load using HTTPS, and display a padlock icon next to the URL in the address bar. To view the certificate, click the padlock icon.

Because digital certificates verify a company's current status, they do not last forever. Most SSL certificates expire after a year, with free certificates expiring after three months. If the certificate is not renewed in time, a site's visitors will see a warning in their web browser before the page loads, informing them that "This website's certificate has expired." While this does not necessarily mean the site is fraudulent, it does show that the site's administrators allowed their certificate to expire before renewing it.

NOTE: Even though they are called SSL certificates by certificate authorities and website administrators, they now use the TLS security protocol. TLS replaced SSL in 1998, and SSL was eventually deprecated in 2015.

--Updated March 8, 2023

CIFS

Stands for "Common Internet File System." CIFS is a standard file system designed for sharing files over the Internet. It is part of the SMB protocol, which allows multiple types of computers to share data and peripherals over a network. CIFS enables users to access files remotely from multiple platforms, including Windows, Mac, Linux, and others.

Each operating system has its own file system, which defines how files and folders are organized. For example, most Windows computers use NTFS, while Macs user HFS. Proprietary file systems are fine when accessing files locally (from the computer itself), but it can cause compatibility issues when users try to access files from a remote system. If the remote device does not recognize the file system of the computer, it won't be able read the files. CIFS solves this problem by serving as a universal file system that is supported by multiple platforms.

The Common Internet File System provides a standard set of commands that computers can use to access a remote system and read and write files remotely. It supports both anonymous file transfers and authenticated access, which can be used to prevent unauthorized access to certain folders and files. CIFS also includes file locking, which prevents multiple users from editing the same file at the same time.

--Updated December 19, 2012

Client

Businesses have clients and servers have clients. In both instances, there exists a one-to-many relationship. Just like a business may have several clients, a server can communicate with multiple clients. In computer networking, this is called the client-server model.

A client is any device that communicates with a server. It may be a desktop computer, laptop, smartphone, or any other network-compatible device. In a home network, "smart" devices, such as Wi-Fi-enabled thermostats, lights, and appliances, are considered clients. In an office network, systems that access files from network-attached storage are clients of the file server. Most networks allow client-to-client communication, though the data flows through a central point, such as a router or switch.

On a larger scale, whenever you access a website, your device is the client, and the web server hosting the website is the server. From a software perspective, your web browser is the client software and the program that responds to requests on the web server (Apache, IIS, etc.), is the server software. Similarly, when you check your email, you connect to a mail server. Your device is a client of the mail server, and your email program or webmail interface is the client software.

--Updated February 6, 2021

Cloud

The term "cloud" comes from early network diagrams, in which the image of a cloud was used to indicate a large network, such as a WAN. The cloud eventually became associated with the entire Internet, and the two terms are now used synonymously. The cloud may also be used to describe specific online services, which are collectively labeled "cloud computing."

Examples of popular cloud-based services include web applications, SaaS, online backup, and other types of online storage. Traditional Internet services like web hosting, email, and online gaming may also be considered part of the cloud since they are hosted on Internet servers, rather than users' local computers. Even social networking websites such as Facebook and LinkedIn are technically cloud-based services, since they store your information online.

While "the cloud" is simply a buzzword for most consumers, it plays an important role for businesses. By moving software services to the cloud, companies can share data more efficiently and centralize their network security. Additionally, cloud-based virtualization can help businesses reduce the number of computer systems and software licenses they need to buy. The end result and a more efficient and less costly way of running a business.

--Updated May 30, 2012

Cloud Computing

Cloud computing refers to applications and services offered over the Internet. These services are offered from data centers all over the world, which collectively are referred to as the "cloud." This metaphor represents the intangible, yet universal nature of the Internet.

The idea of the "cloud" simplifies the many network connections and computer systems involved in online services. In fact, many network diagrams use the image of a cloud to represent the Internet. This symbolizes the Internet's broad reach, while simplifying its complexity. Any user with an Internet connection can access the cloud and the services it provides. Since these services are often connected, users can share information between multiple systems and with other users.

Examples of cloud computing include online backup services, social networking services, and personal data services such as Apple's MobileMe. Cloud computing also includes online applications, such as those offered through Microsoft Online Services. Hardware services, such as redundant servers, mirrored websites, and Internet-based clusters are also examples of cloud computing.

--Updated April 23, 2009

Cloud Waste

Cloud waste is unnecessary spending on cloud services. It refers to unused or underused services during one or more billing cycles, which results in "wasted" spending.

Many types of cloud waste exist. Some examples include:

1. Unused apps in Adobe Creative Cloud
2. Unused Microsoft 365 subscriptions
3. Underutilized server bandwidth
4. Unnecessary cloud security features
5. Underused cloud computing services
6. Underused monthly mailing list email sends

Cloud waste affects everyone from home users to enterprise businesses. For example, a student who purchases an annual Creative Cloud subscription but only uses it for six months may waste several hundred dollars a year. A company that purchases 10,000 Microsoft 365 licenses or "seats" but only uses 8,000 may waste thousands of dollars a month in unused subscription fees.

In recent years, many companies have switched from desktop software to SaaS solutions to reduce costs. However, CTOs and other managers must monitor SaaS usage since unnecessary subscriptions can go overlooked for months or even years.

Cloud computing platforms like Azure, AWS, and Google Cloud provide usage-based billing, which helps reduce cloud waste. Similar to an electrical meter, these services track each client's specific usage, such as compute time, API calls, bandwidth used, etc. Still, many cloud platforms have base monthly service fees and charge for add-ons that may go underutilized over time.

Cloud-based services provide an efficient and cost-effective way for companies to manage IT solutions. However, it is essential for individuals and organizations to regularly review their cloud subscriptions to make sure they are not wasting money on unnecessary services.

--Updated June 23, 2022

CMS

Stands for "Content Management System." A CMS is a software tool that allows you to create, edit, and publish content. While early CMS software was used to manage documents and local computer files, most CMS systems are now designed exclusively to manage content on the Web.

The goal of a CMS is to provide an intuitive user interface for building and modifying webpage content. Each CMS also provides a web publishing tool that allows one or more users to publish updates live on the Web. The editing component is called the content management application (CMA), while the publishing tool is called the content delivery application (CDA). These two components are integrated together in a CMS to streamline the web development process.

Content management systems are available as installable applications and web-based user interfaces. While CMS software programs, such as Adobe Contribute, were popular for a few years, they have largely been replaced by web-based CMSes. Most people prefer a web interface, since it simplifies the website updating process. Additionally, most web-based CMSes are updated automatically, ensuring all users have the latest tools to manage their content.

Several web-based CMS tools are available. The following are some of the most popular ones:

1. **WordPress** - free web software designed for creating template-based websites or blogs
2. **Blogger** - Google's blogging tool designed specifically for maintaining a blog
3. **Joomla** - a flexible web publishing tool that supports custom databases and extensions
4. **Drupal** - an open source platform often used for developing community-based sites
5. **Weebly** - a web-based platform for building simple personal and business websites
6. **Wix** - a collection of web publishing tools for creating a highly customizable website

Some CMS tools are free to use, while others require a monthly fee. Many CMSes provide free basic components, but charge for high-quality templates, web hosting, custom domain names, or other features. Before deciding on a CMS, it is a good idea to review multiple options so you can choose the one that best fits your website goals.

--Updated March 28, 2013

Cookie

A cookie is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application.

While cookies serve many functions, their most common purpose is to store login information for a specific site. Some sites will save both your username and password in a cookie, while others will only save your username. Whenever you check a box that says, "**Remember me on this computer**," the website will generate a login cookie once you successfully log in. Each time you revisit the website, you may only need to enter your password or you might not need to log in at all.

Cookies are also used to store user preferences for a specific site. For example, a search engine may store your search settings in a cookie. A news website may use a cookie to save a custom text size you select for viewing news articles. Financial websites sometimes use cookies to store recently viewed stock quotes. If a website needs to store a lot of personal information, it may use a cookie to remember who you are, but will load the information from the web server. This method, called "server side" storage, is often used when you create an account on a website.

Browser cookies come in two different flavors: "session" and "persistent." Session cookies are temporary and are deleted when the browser is closed. These types of cookies are often used by e-commerce sites to store items placed in your shopping cart, and can serve many other purposes as well. Persistent cookies are designed to store data for an extended period of time. Each persistent cookie is created with an expiration date, which may be anywhere from a few days to several years in the future. Once the expiration date is reached, the cookie is automatically deleted. Persistent cookies are what allow websites to "remember you" for two weeks, one month, or any other amount of time.

Most web browsers save all cookies in a single file. This file is located in a different directory for each browser and is not meant to be opened manually. Fortunately, most browsers allow you to view your cookies in the browser preferences, typically within the "Privacy" or "Security" tab. Some browsers allow you to delete specific cookies or even prevent cookies from being created. While disallowing cookies in your browser may provide a higher level of privacy, it is not recommended since many websites require cookies to function properly.

NOTE: Since cookies are stored in a different location for each web browser, if you switch browsers, new cookies will need to be created.

--Updated July 9, 2011

CORS

Stands for "Cross-Origin Resource Sharing." CORS allows scripts on webpages to request resources from other domains. Most web browsers block these types of requests by default for security purposes.

A webpage can request resources from another domain — as long as the requests come from the HTML. For example, the section may reference resources, such as CSS files, fonts, and JS files other domains. Examples include Google Analytics scripts, jQuery libraries, and fonts hosted on another server. Similarly, the can request images from a CDN or other domain. Cross-origin resource requests in the HTML do not require CORS permissions.

When a script or iframe element makes a cross-origin request, CORS is required. For example, an AJAX method – which runs after the page is loaded – cannot request a resource from another domain. CORS overrides this default browser setting and allows the request to go through.

CORS is implemented using "access control" HTTP headers. A server admin can add or modify the response headers, which are sent to a client's browser when a webpage is accessed. These settings, which can be applied to Apache and IIS servers, may be site-specific or server-wide. Below are common request and response headers:

CORS Request Headers:

- Origin

- Access-Control-Request-Method
- Access-Control-Request-Headers

CORS Response Headers:

- Access-Control-Allow-Origin
- Access-Control-Allow-Methods
- Access-Control-Expose-Headers

CORS Example

If a script on techterms.com requests a resource from sharpened.com using a GET action, it may send the following request headers:

```
Origin: https://techterms.com
Access-Control-Request-Method: GET
```

To allow the request, sharpened.com may respond with the following headers:

```
Access-Control-Allow-Origin: https://techterms.com
Access-Control-Allow-Methods: GET
```

Access-Control-Allow-Origin can be set to specific domains or a wildcard using an asterisk (*). The wildcard setting allows cross-resource requests from all domains, which may be a security risk. Access-Control-Allow-Methods can be set to PUT, POST, DELETE, and others, including a wildcard (*) setting that allows all methods.

--Updated November 3, 2020

CPA

Stands for "Cost Per Action," and is used in online advertising. CPA defines how much revenue a publisher receives when a user clicks an advertisement on his website and then completes a certain action. For example, a publisher may place a banner or text link from an advertiser on his website. When a user clicks the link, she is directed to the advertiser's website. She might then be asked to fill out a form or take a survey. If she completes the form or survey, the action has been completed, and the advertiser pays the publisher a certain amount based on the CPA.

CPA and CPL (cost per lead) are often used interchangeably, though CPA is more generic.

--Updated in 2006

CPC

Stands for "**Cost Per Click**."

CPC is a term used in online marketing that refers to how much an advertiser pays a website or ad network each time someone clicks one of their ads. It applies to ads displayed on search engine results pages, websites, social media, or anywhere else online. CPC is also known as PPC (Pay Per Click).

When advertisers want to run an ad online, ad networks have them bid against other advertisers by setting a maximum CPC. The maximum CPC is part of a formula that looks at the keywords and demographics targeted, the advertiser's industry, how relevant the ad is, and when the ad runs. After the formula selects which ad to run, the ad network charges the advertiser just enough to win the bid, often less than the maximum CPC.

The goal of CPC bidding, when compared to CPM (Cost Per Mille) bidding, is the focus on click-through rate, or CTR. Advertisers that use CPC bidding want people to click their ad to visit their website, often to sell a product or service. Advertisers using CPM bidding may instead just want their ads seen as widely as possible to build brand awareness without caring whether people click the ads.

--Updated October 9, 2022

CPL

Stands for "**Cost Per Lead**."

CPL is a term used in online marketing that refers to how much an advertiser pays a website or ad network each time they acquire a lead through an advertising campaign. This advertising model is also called "online lead generation." Once the ad campaign gathers leads, further marketing efforts attempt to convert those leads into customers.

Advertisers running a campaign using a CPL pricing model tend to have a different focus than those using a CPC (Cost per Click) or CPM (Cost per Mille) model. Instead of paying for people to click or view an ad, a CPL model pays for leads — someone who has chosen to sign up to receive more information or express interest. First, an online ad sends a potential lead to the ad campaign's landing page. From there, they explicitly choose to share their information and express interest by the method set by the ad campaign — they may sign up for an email newsletter, a rewards program, a free trial, or otherwise share their personal information and express interest.

These advertising campaigns tend to cost more, but the advertiser ends up with a more-valuable pool of leads. Leads who choose to sign up are more likely to become paying customers and even repeat customers.

--Updated November 4, 2022

CPM

Stands for "Cost Per 1,000 Impressions," and is used in online advertising. CPM defines the cost an advertiser pays for 1,000 impressions of an advertisement, such as a banner ad or other promotion. An impression is counted each time an advertisement is shown.

While some advertisers pay publishers an amount based strictly on impressions, most advertisers pay for individual clicks or leads generated from their advertisements. Therefore, in Web advertising, it may be more effective to measure pay per click (PPC) or pay per lead (PPL) rates. Either way, the advertiser's goal is to generate as many leads as possible by keeping the rates as low as possible.

Web publishers also use the CPM to measure the revenue per 1,000 impressions. While technically this should be "revenue per 1,000 impressions," or RPM, the terms CPM and RPM are often used interchangeably from the publisher's perspective.

--Updated October 16, 2007

CRM

Stands for "Customer Relationship Management." This is a business term that started somewhere in the deep abyss of the IT (Information Technology) world. CRM refers to solutions and strategies for managing businesses' relationships with customers. (I suppose that's why they call it customer relationship management). With the advent of Web retailing, companies have found it hard to develop relationships with customers since the e-commerce interface is so impersonal. After all, don't you miss the firm handshake and sparkling smile of the salesperson who just sold you the most expensive computer system in the store? Well, whether or not you miss the personal experience of the retail store, the goal of CRM is to give you that feeling when you buy products over the Internet. When it comes to CRM, customer service is the number one priority. Yes, all companies seem to make that claim, but when online businesses create CRM models, it really is the case.

--Updated in 2006

Cross-Browser

When a software program is developed for multiple computer platforms, it is called a crossplatform program. Similarly, when a website is developed for multiple browsers, it is called a cross-browser website.

The job of a Web developer would be much easier if all browsers were the same. While most browsers are similar in both design and function, they often have several small differences in the way they recognize and display websites. For example, Apple's Safari uses a different HTML rendering engines than Internet Explorer. This means the browsers may display the same Web page with slightly different page and text formatting. Since not all browsers support the same HTML tags, some formatting may not be recognized at all in an incompatible Web browser. Furthermore, browsers interpret JavaScript code differently, which means a script may work fine in one browser, but not in another.

Because of the differences in the way Web browsers interpret HTML and JavaScript, Web developers must test and adapt their sites to work with multiple browsers. For example, if a certain page looks fine in Firefox, but does not show up correctly in Internet Explorer, the developer may change the formatting so that it works with Internet Explorer. Of course, the page may then appear differently in Firefox. The easiest fix for browser incompatibility problems is to use a more basic coding technique that works in both browsers. However, if this solution is not possible, the developer may need to add code that detects the type of browser, then outputs custom HTML or JavaScript for that browser.

Making a cross-browser site is usually pretty simple for basic websites. However, complex sites with a lot of HTML formatting and JavaScript may require significant extra coding in order to be compatible with multiple browsers. Some developers may even generate completely different pages for each browser. While CSS formatting has helped standardize the appearance of Web pages across multiple browsers, there are still several inconsistencies between Web browsers. Therefore, cross-browser design continues to be a necessary aspect of Web development.

--Updated January 2, 2009

CSS

Stands for "**Cascading Style Sheet**."

CSS is a style sheet language used for formatting content in HTML webpages. CSS style sheets can define the appearance and formatting of text, tables, and other elements separately from the content itself. Styles may be found within a webpage's HTML file or in a separate document referenced by multiple webpages.

CSS helps web developers create a uniform look across an entire website. Instead of formatting the appearance of each table and block of text in a webpage's HTML code, a style is defined once in a CSS style sheet. Common HTML formatting tags, like <h2>, <strong>, and <em> can have custom formatting defined in a CSS file; custom styles can also be created and applied to text, images, and tables. Once a style is defined, it can be used by any page that links to the CSS file.

By separating a webpage's content from its formatting, CSS makes it easy to update styles across several pages at once. For example, if you want to increase the body text size from 10pt to 12pt across dozens of separate HTML pages, you only need to change the style once in the CSS file. The text size changes for every instance of that style on any webpage using that style sheet.

Some web browsers include a reader mode that automatically changes text formatting from the webpage's default to a special built-in stylesheet optimized for easy reading.

NOTE: The word "cascade" refers to the priority scheme used by CSS when multiple style rules overlap. User-defined CSS overrules styles applied directly to an HTML tag, which overrule any styles defined within the HTML document's header, which overrule any styles defined in an external CSS file.

--Updated March 7, 2023

CTR

Stands for "**Click-Through Rate**."

CTR is a term used in online marketing that measures the percentage of times an ad gets clicked out of the times it appears. It is one measurement of the success of an advertisement in an online marketing campaign using a Pay Per Click (PPC) model.

Online marketers track the CTR for a campaign as a whole, as well as for each individual ad and keyword. This allows advertisers to see which ads are most effective, then tailor their ads for the most effective messaging.

Search engines that show advertisements often take an ad's CTR into account when determining its relevancy and overall quality score. An ad with a high quality score will appear more often and cost less on a Cost Per Click (CPC) basis, which incentivizes advertisers to continually improve the CTR of their ads.

The number that is considered "good" for a CTR depends on the context of the ad. Most display and banner ads have a CTR of under 1%, social media ads are typically between 1-2%, and a good search keyword CTR is around 3-5%.

CTR is also a metric tracked in email marketing, measuring the percentage of readers that click a link in an email. Other measurements for email marketing include the open rate (what percentage of people who received an email opened it) and the bounce rate (what percentage of emails sent were not delivered).

--Updated November 10, 2022

Cyberbullying

There are bullies and then there are cyberbullies. While bullying typically happens at school or work, cyberbullying takes place over cyberspace. This includes both Internet and cell phone communication. Like physical bullying, cyberbullying is aimed at younger people, such as children and teenagers. It may involve harassing, threatening, embarrassing, or humiliating young people online.

Cyberbullying can take many forms. The following are just a few examples:

- Making fun of another user in an Internet chat room.
- Harassing a user over an instant messaging session.
- Posting derogatory messages on a user's Facebook or MySpace page.
- Circulating false rumors about someone on social networking websites.
- Publishing lewd comments about another person on a personal blog.
- Posting unflattering pictures of another user on the Web.
- Spamming another user with unwanted e-mail messages.
- Sending threatening or provocative e-mails.
- Repeatedly calling another person's cell phone.
- Sending unsolicited text messages to another user.

Cyberbullying may seem humorous to some people, but it is a serious matter. Kids who are bullied online often feel hurt and rejected by their peers. This can lead to low self esteem and depression. Therefore, cyberbullying should not be tolerated and should be reported to authorities.

NOTE: Technically, cyberbullying takes place between two young people. When adults are involved, it may be called cyber-harassment or cyberstalking.

--Updated September 15, 2009

Cyberspace

Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers. For example, an object in cyberspace refers to a block of data floating around a computer system or network. With the advent of the Internet, cyberspace now extends to the global network of computers. So, after sending an e-mail to your friend, you could say you sent the message to her through cyberspace. However, use this term sparingly, as it is a popular newbie term and is well overused.

The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984. Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data" (New York: Berkley Publishing Group, 1989), pp. 128.

--Updated in 2006

Cybersquatter

In the early days of the United States, pioneers traveled west and claimed federal land as their own. These people were called "squatters," since they claimed rights to the land simply by occupying it. In the mid-1800s, during the California gold rush, squatters became especially prominent and settled land throughout the west coast.

In the early 1990s, a new gold rush began, but this time the rush was for domain names, rather than gold. Many early Internet users saw the potential value of prominent domain names and began to register as many domains as they could. Over the course of a few years, nearly all common "dot coms" were registered. Many of these domain names were registered for investment purposes, rather than being used for legitimate websites. This practice soon became known as "cybersquatting."

Cybersquatters may own anywhere from a single domain to a few thousand domain names. These "domainers," as they are also called, typically register domain names that contain popular words and phrases. High profile domain names may generate traffic through manual "type-ins" or may simply be attractive to potential buyers. Some domainers, called "typosquatters," register domain names that are similar to well-known websites, but contain typos. The goal of these domains is to generate traffic through mistyped URLs. Generally, cybersquatters profit from their domain names by one of two ways: 1) generating advertising clicks on parked pages (single-page websites), or 2) selling the domains at a significant premium to those interested in buying them.

While some cybersquatters have made huge profits by selling high-interest domain names, others have been forced to give up domains to the rightful owners. The Anticybersquatting Consumer Protection Act (ACPA) was passed in 1999, which gives owners of trademarked or registered names legal rights to a related domain name. In general terms, the law states that users cannot register a domain name that is the same or similar to the name of a known entity. This prevents cybersquatters from extorting money from businesses or individuals by obtaining a specific domain name.

If a dispute over a domain name arises, the two parties may bring the case through a legal proceeding. However, since this is a time-consuming process, ICANN has developed the Uniform Domain Name Dispute Resolution Policy (UDRP), which givens trademark owners a simple means to retrieve domain names from cybersquatters. While cybersquatters still exist and remain prominent today, the rightful owners of certain names now have an easier (and much less expensive) way of getting the domain names they deserve.

--Updated December 23, 2010

Datagram

Datagram is a combination of the words data and telegram. Therefore, it is a message containing data that is sent from location to another. A datagram is similar to a packet, but does not require confirmation that it has been received. This makes datagrams ideal for streaming services, where the constant flow of data is more important than 100% accuracy.

Datagrams are also called "IP datagrams" since they are used by the Internet protocol (IP). This protocol defines how information is sent between systems over the Internet. For example, each device connected to the Internet must have an IP address, which serves as a unique identifier. Whenever data is transmitted via the Internet protocol, it is broken up into packets or datagrams, which each contain a header plus the actual data transmitted.

A datagram header defines the source and destination of the data as well as other information, such as the total length (or size) of the datagram, time to live (TTL), and the specific protocol used to transfer the data. Generally, datagrams are sent via the UDP protocol, which is used for media streaming and other services that do not require confirmation that the data has been received. Packets, on the other hand, are typically sent via TCP, which guarantees all the data sent has been received.

--Updated September 22, 2016

Del.icio.us

Del.icio.us, pronounced simply "delicious," is a community bookmarking website in which users can save Web pages they find and share them with other users. Because users' bookmarks are made public and viewable by other users, other people often bookmark Web pages that they find within other users' bookmarks. Del.icio.us keeps track of how many people bookmark each site and posts the most popular websites on its home page.

Common Web pages bookmarked by Del.icio.us users include news stories, online learning resources, and tech support pages. Since other users add useful pages to their bookmarks, the best Web pages eventually rise to the top of the popularity chain. The result is a collection of Web pages that are helpful and worthwhile visiting.

Users can either browse or search the database of bookmarks on Del.icio.us. When a user saves a bookmark, he or she can add a description and tags (keywords) that are pertinent to the Web page. This help the page show up for relevant searches. The results of Del.icio.us searches are often of higher quality than a regular search engine since the sites have all been chosen by users. Apparently, other Web surfers agree, since the website became so popular that Yahoo! bought the Del.icio.us at the end of 2005.

The domain name "del.icio.us" is a creative modification of the standard domain syntax, where "del" is the domain prefix and "icio.us" is the domain name, with "us" being the domain suffix.

--Updated in 2006

Denial of Service

A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system.

Denial of service (DoS) attacks may be initiated from a single machine, but they typically use many computers to carry out an attack. Since most servers have firewalls and other security software installed, it is easy to lock out individual systems. Therefore, distributed denial of service (DDoS) attacks are often used to coordinate multiple systems in a simultaneous attack.

A distributed denial of service attack tells all coordinated systems to send a stream of requests to a specific server at the same time. These requests may be a simple ping or a more complex series of packets. If the server cannot respond to the large number of simultaneous requests, incoming requests will eventually become queued. This backlog of requests may result in a slow response time or a no response at all. When the server is unable to respond to legitimate requests, the denial of service attack has succeeded.

DoS attacks are a common method hackers use to attack websites. Since flooding a server with requests does not require any authentication, even a highly secured server is vulnerable. However, a single system is typically not capable of carrying out a successful DoS attack. Therefore, a hacker may create a botnet to control multiple computers at once. A botnet can be used to carry out a DDoS attack, which is far more effective than an attack from a single computer.

Denial of service attacks can be problematic, especially when they cause large websites to be unavailable during high-traffic times. Fortunately, security software has been developed to detect DoS attacks and limit their effectiveness. While many well-known websites, like Google, Twitter, and WordPress, have all been targets of denial of service attacks in the past, they have been able to update their security systems and prevent further service interruptions.

--Updated August 11, 2011

DHCP

Stands for "Dynamic Host Configuration Protocol." DHCP is a protocol that automatically assigns a unique IP address to each device that connects to a network. With DHCP, there is no need to manually assign IP addresses to new devices. Therefore, no user configuration is necessary to connect to a DHCP-based network. Because of its ease of use and widespread support, DHCP is the default protocol used by most routers and networking equipment.

When you connect to a network, your device is considered a client and the router is the server. In order to successfully connect to a network via DHCP, the following steps must take place.

1. When a client detects it has connected to a DHCP server, it sends a DHCPDISCOVER request.
2. The router either receives the request or redirects it to the appropriate DHCP server.
3. If the server accepts the new device, it will send a DHCPOFFER message back to the client, which contains the client device's MAC address and the IP address being offered.
4. The client returns a DHCPREQUEST message to the server, confirming it will use the IP address.

5. Finally, the server responds with a DHCPACK acknowledgement message that confirms the client has been given access (or a "lease") for a certain amount of time.

DHCP works in the background when you connect to a network, so you will rarely see any of the above steps happen. The time it takes to connect via DHCP depends on the type of router and the size of the network, but it usually takes around three to ten seconds. DHCP works the same way for both wired and wireless connections, which means desktop computers, tablets, and smartphones can all connect to a DHCP-based network at the same time.

--Updated August 19, 2014

Dial-up

Dial-up refers to an Internet connection that is established using a modem. The modem connects the computer to standard phone lines, which serve as the data transfer medium. When a user initiates a dial-up connection, the modem dials a phone number of an Internet Service Provider (ISP) that is designated to receive dial-up calls. The ISP then establishes the connection, which usually takes about ten seconds and is accompanied by several beeping an buzzing sounds.

After the dial-up connection has been established, it is active until the user disconnects from the ISP. Typically, this is done by selecting the "Disconnect" option using the ISP's software or a modem utility program. However, if a dial-up connection is interrupted by an incoming phone call or someone picking up a phone in the house, the service may also be disconnected.

In the early years of the Internet, especially in the 1990s, a dial-up connection was the standard way to connect to the Internet. Companies like AOL, Prodigy, and Earthlink offered dial-up service across the U.S., while several smaller companies offered local dial-up Internet connections. However, due to slow speeds (a maximum of 56 Kbps), and the hassle of constantly disconnecting and reconnecting to the ISP, dial-up service was eventually replaced by DSL and cable modem connections. Both DSL and cable lines, known as "broadband" connections, offer speeds that are over 100 times faster than dial-up and provide an "always on" connection. While we don't get to listen to the fun buzzing and beeping noises of older modems anymore, it certainly is nice to download data in a fraction of the time.

--Updated April 7, 2009

Digital Footprint

A digital footprint is a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services.

A "passive digital footprint" is a data trail you unintentionally leave online. For example, when you visit a website, the web server may log your IP address, which identifies your Internet service provider and your approximate location. While your IP address may change and does not include any personal information, it is still considered part of your digital footprint. A more personal aspect of your passive digital footprint is your search history, which is saved by some search engines while you are logged in.

An "active digital footprint" includes data that you intentionally submit online. Sending an email contributes to your active digital footprint, since you expect the data be seen and/or saved by another person. The more email you send, the more your digital footprint grows. Since most people save their email online, the messages you send can easily remain online for several years or more.

Publishing a blog and posting social media updates are another popular ways to expand your digital footprint. Every tweet you post on Twitter, every status update you publish on Facebook, and every photo you share on Instagram contributes to your digital footprint. The more you spend time on social networking websites, the larger your digital footprint will be. Even "liking" a page or a Facebook post adds to your digital footprint, since the data is saved on Facebook's servers.

Everyone who uses the Internet has a digital footprint, so it is not something to be worried about. However, it is wise to consider what trail of data you are leaving behind. For example, understanding your digital footprint may prevent you from sending a scathing email, since the message might remain online forever. It may also lead you to be more discerning in what you publish on social media websites. While you can often delete content from social media sites, once digital data has been shared online, there is no guarantee you will ever be able to remove it from the Internet.

--Updated May 26, 2014

Direct Digital Marketing

Direct digital marketing, also known as "DDM," is a type of marketing that is done exclusively through digital means. It may be used to supplement or even replace traditional physical marketing strategies. The primary channels of direct digital marketing include e-mail and the Web.

While most of us still receive an abundance of physical marketing materials in our mailboxes each week, many of these mailings have been replaced by e-mail. By using e-mail marketing, companies can drastically reduce their mailing costs, since the cost of sending e-mail messages is essentially free. Compare this to mailing physical brochures that may cost $0.50 per recipient. If a company sends out one million mailings, using e-mail could save the company $500,000 in mailing costs.

While e-mail marketing is great asset for many businesses, it can also be abused. Since it doesn't cost anything to send e-mail messages, it is possible to distribute unsolicited messages to large lists of recipients at little to no cost. This kind of unwanted electronic junk mail has become widely known as "spam." Fortunately, junk mail filters have helped reduce the impact of these messages for most users. Many companies and organizations also offer an "unsubscribe" option in their mailings, which allow users to remove themselves from the mailing lists.

The Web is another popular medium for direct digital marketing. Many companies now advertise on websites through banner ads, text links, and other types of advertisements. By using Web marketing, companies can drive visitors directly to their website with a single click. This provides a tangible benefit over print and television advertising, which may fully not capture a viewer's interest. Additionally, companies can target their ads on pages with relevant content using contextual ad placement services, such as Google AdSense. This allows businesses to attract people who are the most likely to be interested in the products or services they offer.

In the past few years, DDM has revolutionized the marketing industry. By using digital communications, businesses can advertise in several new ways that were not possible before. While e-mail and the Web remain the most popular mediums for DDM, digital marketing continues to expand into other areas as well. Mobile phones and video games are already being used for DDM and you can expect many other mediums to follow.

--Updated October 29, 2009

DKIM

Stands for "DomainKeys Identified Mail." DKIM is an email authentication technology that verifies a message was sent from a legitimate user of an email address. It is designed to prevent email forgery or spoofing.

DKIM works by attaching a digital signature to the header of an email message. The header is generated by the outgoing mail server and is unique to the domain hosted on the server. The receiving mail server can check the header against a public key stored in the sending server's DNS record to confirm the authenticity of the message.

Many popular email services like Gmail, Yahoo! Mail, and Outlook use DKIM by default. Other email accounts, such as those set up on web servers may require DKIM to be manually activated. For example, cPanel – a popular Linux web server application – allows an administrator to activate DKIM in the Email → Authentication section of the cPanel interface. Once DKIM is enabled, it is activated for all users automatically.

While DKIM provides a simple way to verify a message has been sent from the corresponding domain, it is not a foolproof solution. For example, the receiving mail server must also support DKIM or the header information will be ignored. Additionally, messages with a valid signature can be forwarded or resent from another email address. It is also important to note that DKIM is designed to authenticate messages, not prevent spam. While a valid DKIM header may mean a message is less likely to be spam, it has no relation to the content of the message.

History

The DomainKeys Identified Mail specification was created in 2005 when Yahoo! and Cisco merged their respective DomainKeys and Identified Internet Mail into a single solution. It was published by the Internet Engineering Task Force (IETF) the same year and has been in use ever since.

NOTE: DKIM is commonly used along with SPF (Server Policy Framework), though the two verification methods are completely separate.

--Updated January 6, 2017

DNS

Stands for "**Domain Name System**."

Domain names serve as memorizable names for websites and other services on the Internet. However, computers access Internet devices by their IP addresses. DNS translates domain names into IP addresses, allowing you to access an Internet location by its domain name.

Thanks to DNS, you can visit a website by typing in the domain name rather than the IP address. For example, to visit the Tech Terms Computer Dictionary, you can simply type "techterms.com" in the address bar of your web browser rather than the IP address (67.43.14.98). It also simplifies email addresses, since DNS translates the domain name (following the "@" symbol) to the appropriate IP address.

To understand how DNS works, you can think of it like the contacts app on your smartphone. When you call a friend, you simply select his or her name from a list. The phone does not actually call the person by name, it calls the person's phone number. DNS works the same way by associating a unique IP address with each domain name.

Unlike your address book, the DNS translation table is not stored in a single location. Instead, the data is stored on millions of servers around the world. When a domain name is registered, it must be assigned at least two nameservers (which can be edited through the domain name registrar at any time). The nameserver addresses point to a server that has a directory of domain names and their associated IP addresses. When a computer accesses a website over the Internet, it locates the corresponding nameserver and gets the correct IP address for the website.

Since DNS translation creates additional overhead when connecting to websites, ISPs cache DNS records and host the data locally. Once the IP address of a domain name is cached, an ISP can automatically direct subsequent requests to the appropriate IP address. This works great until an IP address changes, in which case the request may be sent to the wrong server or the server will not respond at all. Therefore, DNS caches are updated regularly, usually somewhere between a few hours and a few days.

--Updated August 30, 2014

DNS Record

A DNS record is a plain text entry in a zone file that contains important information about a domain, and is an important part of the Domain Name System. A domain's zone file contains multiple DNS records that help translate human-readable domain names into machine-readable IP addresses, including a domain's name server and mail server information. A DNS record can also include domain aliases for forwarding domains and subdomains.

Each DNS record in a zone file contains a single piece of information, which work together to provide a full set of instructions for accessing that domain and its resources. There are multiple types of DNS record that each provide different information. Some of the most common types of DNS record are listed below.

- **NS records** list the domain's name servers.
- **A records** list the domain's IPv4 address.
- **AAAA records** list the domain's IPv6 address.
- **SOA (Start of Authority) records** include authoritative information for a domain, including its primary name server and timers that instruct how often to refresh its DNS information.
- **MX records** list mail servers that handle email sent to the domain.
- **CNAME records** create aliases (or canonical names) that forward requests to another domain or subdomain.

DNS records in a zone file typically follow the same pattern, starting with the domain or hostname, followed by a record type, and then listing details for that record type. Several examples are listed below.

```
example.com  IN  NS  ns1.example.com

example.com  IN  A  192.168.0.1

example.com  IN  AAAA  2001:db8:85a3::8a2e:370:7334

example.com  IN  MX  mail.example.com

app.example.com  IN  CNAME  web.example.com
```

--Updated July 12, 2023

DNSSEC

Stands for "Domain Name System Security Extensions." It is an extension of the standard domain name system (DNS), which translates domain names to IP addresses. DNSSEC improves security by validating the authenticity of the DNS data.

The original domain name system was developed in the 1980s with minimal security. For example, when a host requests an IP address from a name server using a standard DNS query, it assumes the name server is valid. However, a name server can pretend to be another server by spoofing (or faking) its IP address. A fake name server could potentially redirect domain names to the wrong websites.

DNSSEC provides extra security by requiring authentication with a digital signature. Each query and response is "signed" using a public/private key pair. The private key is generated by the host and the public key is generated by a DNS zone, or group of trusted servers. These servers create a chain of trust, in which they validate each other's public keys. Each DNSSEC-enabled name server stores its public key in a hashed "DNSKEY" DNS record.

Enabling DNSSEC

While DNSSEC is not required for web servers or mail servers, many web hosts recommend it. To configure DNSSEC, you must use a nameserver that supports it, like PowerDNS or Knot DNS. Then you must enable DNSSEC on your server and configure it within the control panel interface.

If you are using a public nameserver, activating DNSSEC up may be as simple as clicking "Enable DNSSEC." If you are using a custom name server, you may need to manually create one or more delegation signer (DS) records. After you have enabled DNSSEC, it may take several hours to activate since the server must validate the DS records with other servers within the DNS zone.

--Updated June 27, 2020

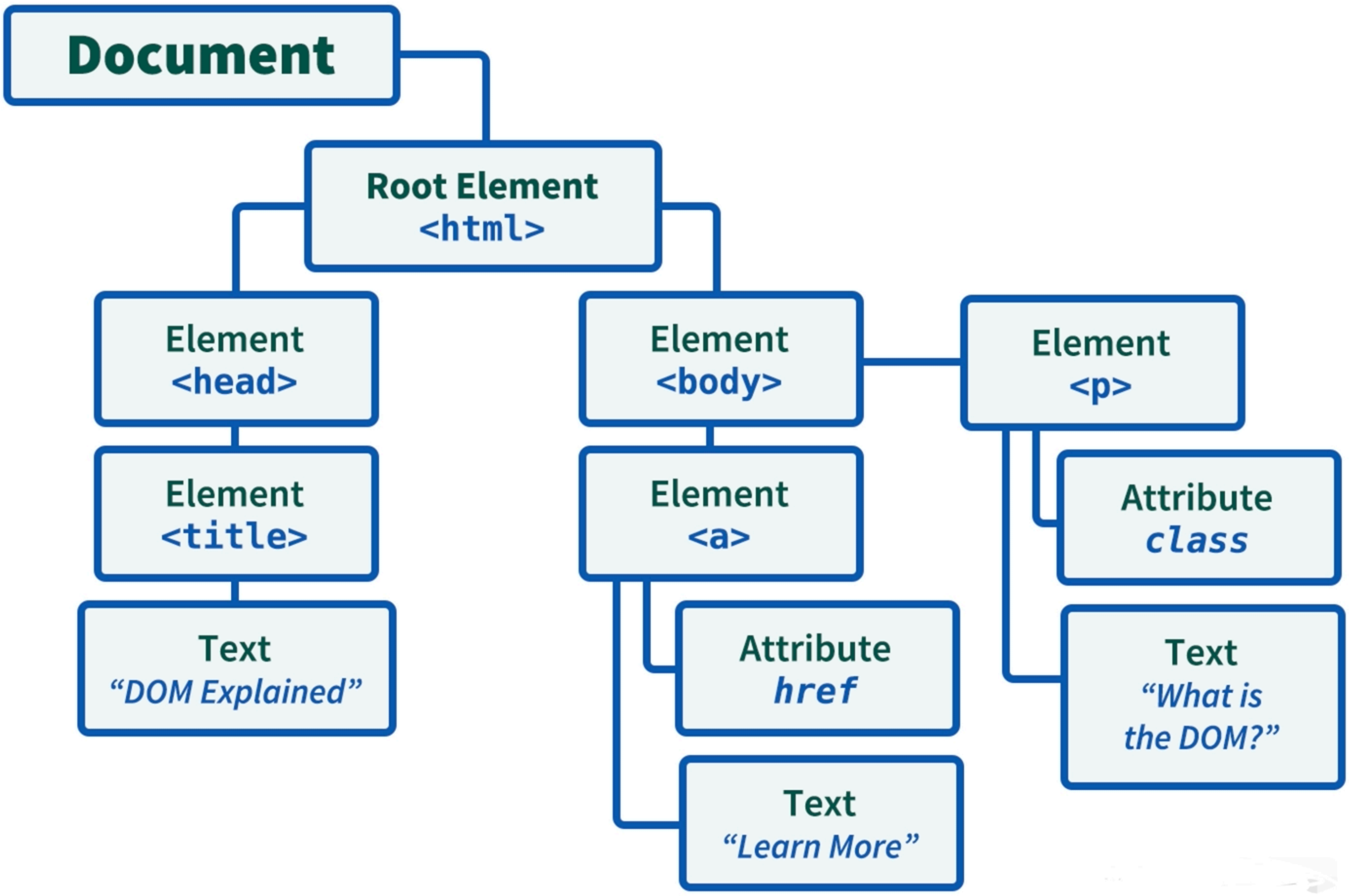
DOM

Stands for "**Document Object Model**."

The DOM is a programming interface for accessing and modifying the content of webpages and XML documents. It defines the logical structure of a document, treating it like a tree where each branching node represents individual elements. Programs and scripts can access the DOM to read and modify the document's structure, content, and style.

The DOM organizes the structure of HTML and XML files in a hierarchy of objects called "nodes." At the root is the Document node, which represents the document as a whole. Next are the Element nodes that represent individual HTML or XML tags. Element nodes are themselves hierarchical in the way that they're nested. For example, the <html> node is closest to the root of the document and contains both the <head> and <body> nodes, and each of those contains child nodes like <div> and <p> elements.

Each element node in the DOM includes several Attribute nodes that modify its properties. For example, an <img> element node could include attribute nodes for src, alt, width, and height that would allow some JavaScript to modify any of those attributes. Finally, Text nodes contain the text within each element, making up the document contents. Text nodes are the leaves of the tree and have no further levels after them.The DOM hierarchy showing several elements and how they relate to each other.



Using JavaScript (or other scripting languages) to access a page's DOM allows you to create dynamic and interactive webpages. For example, event handlers attached to nodes can wait for user interactions like mouse clicks or keyboard input, then modify the page contents in response. JavaScript events can use the DOM to remove existing nodes and add new ones. Scripts can fetch data from a database on a server and use the DOM to insert that data into specific text elements. Scripts can also use the DOM to modify the CSS properties of elements and change the document's appearance and layout.

--Updated June 22, 2023

Domain Name

A domain name is a unique name that identifies a website. For example, the domain name of the Tech Terms Computer Dictionary is "techterms.com." Each website has a domain name that serves as an address, which is used to access the website.

Whenever you visit a website, the domain name appears in the address bar of the web browser. Some domain names are preceded by "www" (which is not part of the domain name), while others omit the "www" prefix. All domain names have a domain suffix, such as .com, .net, or .org. The domain suffix helps identify the type of website the domain name represents. For example, ".com" domain names are typically used by commercial websites, while ".org" websites are often used by non-profit organizations. Some domain names end with a country code, such as ".dk" (Denmark) or ".se" (Sweden), which helps identify the location and audience of the website.

Domain names are relatively cheap to register, though they must be renewed every year or every few years. The good news is that anyone can register a domain name, so you can purchase a unique domain name for your blog or website. The bad news is that nearly all domain names with common words have already been registered. Therefore, if you want to register a custom domain name, you may need to think of a creative variation. Once you decide on a domain name and register it, the name is yours until you stop renewing it. When the renewal period expires, the domain name becomes available for others to purchase.

NOTE: When you access a website, the domain name is actually translated to an IP address, which defines the server where the website located. This translation is performed dynamically by a service called DNS.

--Updated September 14, 2012

Domain Suffix

A domain suffix is the last part of a domain name, consisting of the final "." and two or more letters. A domain suffix is also known as a "top-level domain" or TLD. Popular domain suffixes include ".com," ".net," and ".org," but there are more than a thousand domain suffixes approved by ICANN.

Each domain suffix is intended to define the type of website represented by the domain name. For example, ".com" domains are meant for commercial websites, while non-profit organizations use ".org" domains. Each country also has a unique domain suffix meant for websites within the country. For example, Brazilian websites may use the ".br" domain suffix, Chinese websites may use the ".cn" suffix, and Australian websites may use the ".au" suffix.

A country code suffix does not always mean that a website is hosted in that country or primarily meant for that country's people. Some countries allow outside people and businesses to purchase domains using their country codes, with some TLDs popular in certain industries or communities. For example, Anguilla's ".ai" TLD is commonly used by technology companies specializing in artificial intelligence; ".me" (Montenegro), ".tv" (Tuvalu), and ".fm" (the Federated States of Micronesia) are other examples that see significant use outside of their countries.

As the number of websites on the Internet continuously grows, the initial set of TLDs limits the namespace available for new domains. With most good ".com" domain names already taken in the late 1990s, people began pressuring ICANN to add new generic TLDs for businesses, personal websites, and other groups. They first added a new batch of generic TLDs in 2000 — including ".biz" and ".info." In 2013 ICANN began approving requests for many additional suffixes like ".art," ".dev," ".store," and ".app" that allow a website owner to choose a TLD for nearly any website niche.

--Updated January 6, 2023

Download

Download can be used as either a verb or a noun. As a verb, it refers to the process of receiving data over the Internet. Downloading is the opposite of uploading, or sending data to another system over the Internet. As a noun, download may refer to either a file that is retrieved from the Internet or the process of downloading a file.

Every time you use the Internet, you download data. For example, each time you visit a webpage, your computer or mobile device must download the HTML, CSS, images, and any other relevant data in order to display the page in your web browser. When you click a "Download Now" link, your browser will start downloading a specific file that you can open.

You can also download data using mediums besides the web. For example, you can download files using an FTP program, download email messages with an email client, and download software updates directly through your operating system. You can manually initiate a download (such as clicking a download link), though most downloads happen automatically. For example, your smartphone may download email messages and software updates in the background without you knowing it.

While you can download a file, the word "download" may also refer to the file itself. A common way you might see "download" used as a noun is in an online advertisement that says, "Free Download." This phrase implies that clicking the download link will download a file (often a software program or installer) and use it for free. The noun "download" can also be used like the word "transfer" to describe the process of downloading data. For example, a program may display a status update that says, "Download in progress" or "Download complete."

--Updated September 18, 2014

Drive-By Download

A drive-by download is a download that happens automatically when you visit a webpage. The download starts without you initiating it and may take place in the background without any notification.

Drive-by downloads can occur on both legitimate and malicious websites. For example, if a hacker gains access to a trusted website, he can install code on webpages that will initiate automatic downloads on visitors' computers. Malicious websites, such as those used in phishing and pharming activities, may intentionally download malware on users computers.

There are multiple ways a webmaster can implement drive-by downloads in a webpage. One method is to insert JavaScript code that automatically opens a downloadable file once the page has loaded. Another method involves using an iframe that references another URL, which initiates the download. A less common method is to use a browser plug-in or extension that downloads files automatically. In rare cases, online advertisers can even insert code in display ads that initiate downloads on users computers. Most ad networks now prevent this type of behavior.

While drive-by downloads happen automatically, it is rare that the an executable file will run without your permission. This is because most browsers notify you when a file has been downloaded and will not open downloaded files automatically. Therefore, you can prevent damage from drive-by downloads by simply not opening unknown files downloaded by your web browser.

--Updated August 10, 2016

Dynamic Website

Dynamic websites contain Web pages that are generated in real-time. These pages include Web scripting code, such as PHP or ASP. When a dynamic page is accessed, the code within the page is parsed on the Web server and the resulting HTML is sent to the client's Web browser.

Most large websites are dynamic since they are easier to maintain than static websites. This is because static pages each contain unique content, meaning they must be manually opened, edited, and published whenever a change is made. Dynamic pages, on the other hand, access information from a database. Therefore, to alter the content of a dynamic page, the webmaster may only need to update a database record. This is especially helpful for large sites that contain hundreds or thousands of pages. It also makes it possible for multiple users to update the content of a website without editing the layout of the pages.

Dynamic websites that access information from a database are also called database-driven websites.

--Updated June 13, 2009

E-commerce

E-commerce (or electronic commerce) refers to commercial activity conducted over the Internet. An e-commerce transaction occurs whenever someone buys goods or services from a business' website. An e-commerce transaction can take lots of forms, such as a person buying a piece of software that they can download, ordering a pair of shoes to be delivered, or hiring an artist to draw a picture.

E-commerce has several advantages over in-person commerce but also some drawbacks. Buying a digital good — like software, music, or a movie download — can happen instantly, but buying a physical product requires it to be shipped and delivered. An e-commerce retailer can have a large selection of products available to ship, but the customer does not have the opportunity to examine things in person. Advances in augmented reality (AR) are beginning to offer customers the chance to see what a product would look like in their homes.

There are four main types of e-commerce based on who is buying and who is selling.

- **Business to Consumer** (B2C) is the most common form, where a person visits a website to buy something. A person buying a product or service from a business, once or on a subscription basis, is B2C e-commerce.
- **Business to Business** (B2B) is when one business purchases goods or services from another business. A business selling to a government or other organization, while not strictly B2B, is also considered B2B e-commerce.
- **Consumer to Consumer** (C2C) is when one person sells something to another person, facilitated by a website or other Internet service. Auction sites like eBay were the earliest forms of C2C e-commerce, and sites like Etsy now allow individuals offering products and services to find customers easily.
- **Consumer-to-Business** (C2B) e-commerce is where an individual sells a product (or, more often, a service) to a business. One common form of this is freelance contract work, like a photographer licensing an image to a stock photo agency or a developer creating a custom application for a business.

--Updated October 27, 2022

E-mail Bankruptcy

In this day and age, most of us receive several e-mails a day. Depending on your job, you may even receive dozens of daily messages that are not spam. While it is hard enough to keep up with this plethora of e-mails received in a single day, if you fall behind a few days, it can be nearly impossible to catch up. After awhile, you may end up with hundreds of messages in your inbox that have not been replied to.

If your become submerged underneath an endless pile of e-mail in your inbox, the only way out may be to declare e-mail bankruptcy. Similar to a financial bankruptcy, e-mail bankruptcy involves writing off the losses and starting over. The most tactful way of declaring e-mail bankruptcy is to paste all the e-mail addresses from the messages you have not responded to into a single message. Then send a message explaining that you have fallen too far behind on your e-mail and apologize for not responding. The quicker, but less considerate option is to simply delete all the old messages and start over like nothing ever happened.

While it is best to avoid e-mail bankruptcy by keeping up with your e-mail, for some people it may be the only way to get current with their correspondence. If you are in a situation where you feel overwhelmed by the growing number of messages in your inbox, make sure you first reply to the most important messages. Then, as a last resort, declaring e-mail bankruptcy may give you the fresh start you need.

--Updated August 7, 2007

Edge Caching

Edge caching is a mechanism content delivery networks (CDNs) use to cache Internet content in different locations around the world. Examples include website data, cloud storage, and streaming media. By storing copies of files in multiple "edge" locations, a CDN can deliver content to users more quickly than a single server can.

CDNs may have tens or hundreds of global data centers. Each data center contains edge servers that intelligently serve data to nearby users. In most cases, edge servers "pull" data from an origin server when users request content for the first time. Once an edge server pulls an image, video, or another object, it caches the file — typically for a few days or weeks. The CDN then serves subsequent requests from the edge server rather than the origin.

Tiered Caching

A CDN may automatically propagate newly pulled content to all servers or wait for each server to request the data. Automatic propagation reduces trips to the origin server but may result in unnecessary duplication of rarely-accessed files. Waiting for local requests is more efficient but increases trips to the origin server. Modern CDNs use **tiered caching** to balance the two methods. The first time a user accesses a file, the CDN caches it on the local edge server and several "primary data centers." It reduces unnecessary propagation of cached files and limits trips to the origin server.

CDNs provide customizable cache settings, such as how frequently to check for updated files or when to let cached files expire. Most have a "purge" feature, which allows webmasters to remove old content from all edge servers at once. Purging files is useful when updating static assets, such as CSS documents and image files.

Edge Caching Benefits

Edge caching reduces latency, providing faster and more consistent delivery of Internet content to users around the world. For example, a user in Sydney, Australia, may experience a two-second delay when accessing a server in Houston, Texas. If the data is cached in Australia, the delay may be less than one-tenth of a second.

While the primary purpose of edge caching is to improve content delivery speed, it also provides two other significant benefits: bandwidth reduction and redundancy.

Edge caching reduces Internet bandwidth by shortening the distance data needs to travel to each user. Local edge servers reduce Internet congestion and limit traffic bottlenecks. Replicating data across multiple global data centers also provides redundancy. While CDNs typically pull data from an origin server, individual data centers can serve as backups if the origin server fails or becomes inaccessible.

--Updated April 23, 2022

Edge Server

An edge server is a computer located at the "edge" of the Internet, serving users in a specific area. CDNs and edge computing services use edge servers to provide Internet content and computing power as fast as possible.

Edge servers are distributed around the world at locations called points of presence, or PoPs. By placing servers closer to users, latency is reduced, and Internet users can access data more quickly. For example, if someone in Tokyo accesses a website hosted in New York, the ping may be over half a second, causing a delay before the webpage loads. If the content is hosted on an edge server in Tokyo, the ping may be only a few milliseconds, allowing the webpage to load much faster.

CDN Edge Servers

Content delivery networks, or CDNs, use edge servers to cache content, such as websites and streaming media. They retrieve data from an origin server, then replicate it globally across the edge network. When a user in Brasil accesses a website with an origin server in England, the CDN may serve the content from an edge server in Rio de Janeiro.

CDNs often host static assets, such as CSS, JavaScript, and image files. However, they can also cache and serve HTML. Pages with dynamic content must be regularly refreshed or "purged" so users do not receive outdated pages stored in the CDN cache.

Edge Computing Servers

Edge computing networks use edge servers to perform calculations in different locations worldwide. Handing computation tasks closer to the source of each request reduces roundtrip delays and provides faster response times. Examples include online ad targeting, video conferencing, and multiplayer gaming.

While edge servers provide users faster access to Internet content, they also have a secondary benefit — reducing Internet traffic. Since edge servers deliver content and computing power from locations close to each user, they decrease the data travel and total bandwidth required for each request.

--Updated April 9, 2022

EDI

Stands for "**Electronic Data Interchange**."

EDI is a standardized method for transferring data between business networks. An EDI system translates data from a company's internal system into a common language that can be understood by that company's trading partner's systems. Businesses use EDI to transfer documents like purchase orders, invoices, and inventory documents. By sending this data electronically, businesses save the time that would have been spent printing forms, mailing them, and entering data that they've received into their system.

Two businesses can exchange EDI data in several different ways. They can connect their systems directly, using the Internet to securely send data from one system to another. This process can be cumbersome when dealing with a large number of trading partners, so many businesses use a Value Added Network (VAN), which acts as a virtual post office to facilitate data transfers. VANs route EDI data from one business to another using customer IDs, authenticate the messages and transmitting partner, and notify a business when new data is received. They can provide additional benefits to businesses, like full encryption, analytics, and auditing services.

There are several standard EDI formats in use that specify how documents are formatted and transmitted, like EDIFACT (International), X12 (North America), and TRADACOMS (UK). Each standard has a set of forms and data types that all systems using that standard can process. EDI forms are categorized and specialized to certain tasks, like credit/debit adjustments, shipment and billing notices, and return authorizations.

--Updated November 8, 2022

Email

Email, short for "electronic mail," is one of the most widely used features of the Internet, along with the web. It allows you to send and receive messages to and from anyone with an email address, anywhere in the world.

Email uses multiple protocols within the TCP/IP suite. For example, SMTP is used to send messages, while the POP or IMAP protocols are used to retrieve messages from a mail server. When you configure an email account, you must define your email address, password, and the mail servers used to send and receive messages. Fortunately, most webmail services configure your account automatically, so you only need to enter your email address and password. However, if you use an email client like Microsoft Outlook or Apple Mail, you may need to manually configure each account. Besides the email address and password, you may also have to enter the incoming and outgoing mail servers and enter the correct port numbers for each one.

The original email standard only supported plain text messages. Eventually, email evolved to support rich text with custom formatting. Today, email supports HTML, which allows emails to be formatted the same way as websites. HTML email messages can include images, links, and CSS layouts. You can also send files or "email attachments" along with messages. Most mail servers allow you to send multiple attachments with each message, but they limit the total size. In the early days of email, attachments were typically limited to one megabyte, but now many mail servers support email attachments that are 20 megabytes in size or more.

Email Netiquette

When composing an email message, it is important to use good netiquette. For example, you should always include a subject that summarizes the topic of the email. It is also helpful to begin each message with the recipient's name and end the message with your name or "signature." A typical signature includes your name, email address, and/or website URL. A professional signature may include your company name and title as well. Most email programs allow you to save multiple signatures, which you can insert at the bottom of an email.

If you want to send an email to multiple recipients, you can simply add each email address to the "To" field. However, if the email is primarily intended for one person, you should place the additional addresses in the "CC" (carbon copy) field. If you are sending an email to multiple people that don't know each other, it is best to use the "Bcc" (blind carbon copy) field. This hides the email addresses of each recipient, which helps prevent spam.

NOTE: Email was originally written "e-mail," but is now more commonly written as "email" without the dash.

--Updated October 31, 2014

Email Address

An email address is a unique identifier for an email account. It is used to both send and receive email messages over the Internet. Similar to physical mail, an email message requires an address for both the sender and recipient in order to be sent successfully.

Every email address has two main parts: a username and domain name. The username comes first, followed by an at (@) symbol, followed by the domain name. In the example below, "mail" is the username and "techterms.com" is the domain name.

mail@techterms.com

When a message is sent (typically through the SMTP protocol), the sending mail server checks for another mail server on the Internet that corresponds with the domain name of the recipient's address. For example, if someone sends a message to a user at techterms.com, the mail server will first make sure there is a mail server responding at techterms.com. If so, it will check with the mail server to see if the username is valid. If the user exists, the message will be delivered.

Email Address Formatting

While a basic email address consists of only a username and domain name, most email clients and webmail systems include names with email addresses. An email address that contains a name is formatted with the name first, followed by the email address enclosed in angle brackets, as shown below.

Full Name user@domain.com

Email can be sent to recipients with or without a name next to the email address. However, emails sent to addresses that include a name are less likely to be filtered as spam. Therefore, it is a good idea to fill in your full name when setting up an email account. Most mail clients and webmail systems will automatically include your name in your sending email address.

NOTE: When manually typing an email address into the To: field, it is a good idea to use the "Full Name" formatting as shown above and include the person's name before the email address. This will help prevent the message from being incorrectly flagged as spam.

--Updated October 13, 2016

Email Bomb

An email bomb or "mail bomb" is a malicious act in which a large number of email messages are sent to a single email address in a short period of time. The purpose of an email bomb is typically to overflow a user's inbox. In some cases, it will also make the mail server unresponsive.

Email bombing is often done from a single system in which one user sends hundreds or thousands of messages to another user. In order to send the messages quickly, the email bomber may use a script to automate the process. By sending emails with a script, it is possible to send several thousand messages per minute.

If performed successfully, an email bomb will leave the recipient with a pile of email messages in his or her inbox. It may also max out the recipient's email quota, preventing the user from receiving new email messages. The result is a frustrating situation where the user has to manually delete the messages. If the recipient's email client or webmail system does not allow the user to select all the unwanted messages at once, this process can take a long time to complete.

Fortunately, most mail servers are capable of detecting email bombs before a large number of messages are sent. For example, if the server detects that more than ten messages are received from the same email address within one minute, it may block the sender's email address or IP address. This simple action will stop the email bomb by rejecting additional emails from the sender.

--Updated February 8, 2016

Emoticon

The term emoticon comes from "emotion and icon" and refers to facial expressions represented by keyboard characters. For example, the emoticon :-) represents a happy face and :-(represents a sad face. By inserting an emoticon into a message, you can help the recipient better understand the feeling you want to get across.

While most emoticons represent expressions, they have branched out to symbolize many other things, such as people, animals, objects, and actions. Some emoticons are meant to be read left-to-right, while others are displayed vertically. Below are examples of different types of emoticons:

- :-D - very happy
- o.O - confused
- =^.^= - cat
- :o3 - dog
- *<:o) - clown
- C[_] - coffee cup
- T.T - crying

"Kaomoji" emoticons, which originated in Japan, use Japanese symbols and uncommon characters to create unique emoticons. For example, the emoticon ＝(^o^)ノ___ｏ represents a person throwing a bowling ball. The "flipping table" emoticon (╯°□°)╯ ︵ ┻━┻ can be used to say you are really upset.

The popularity of text-based emotions led to the creation of actual icons or "emojis." Emojis (which are sometimes called emoticons) are now part of the standard character set in most mobile and desktop operating systems. This means you can insert actual smiley faces (or other expressions) instead of using a string of characters. For example, you can insert a ❤️ instead of using the text-based <3 emoticon.

NOTE: If you want to have good netiquette, it's best to avoid using emoticons in formal communication. However, it's fine (and rather common) to use emoticons in text messages, informal emails, and on social media websites.

--Updated November 3, 2014

Extranet

If you know the difference between the Internet and an intranet, you have an above average understanding of computer terminology. If you know what an extranet is, you may be in the top echelon.

An extranet actually combines both the Internet and an intranet. It extends an intranet, or internal network, to other users over the Internet. Most extranets can be accessed via a Web interface using a Web browser. Since secure or confidential information is often accessible within an intranet, extranets typically require authentication for users to access them.

Extranets are often used by companies that need to share selective information with other businesses or individuals. For example, a supplier may use an extranet to provide inventory data to certain clients, while not making the information available to the general public. The extranet may also include a secure means of communication for the company and its clients, such as a support ticket system or Web-based forum.

Unlike the Internet, "extranet" is not a proper noun and therefore should not be capitalized.

--Updated August 26, 2008

Facebook

Facebook is a social networking website that was originally designed for college students, but is now open to anyone 13 years of age or older. Facebook users can create and customize their own profiles with photos, videos, and information about themselves. Friends can browse the profiles of other friends and write messages on their pages.

Each Facebook profile has a "wall," where friends can post comments. Since the wall is viewable by all the user's friends, wall postings are basically a public conversation. Therefore, it is usually best not to write personal messages on your friends' walls. Instead, you can send a person a private message, which will show up in his or her private Inbox, similar to an e-mail message.

Facebook allows each user to set privacy settings, which by default are pretty strict. For example, if you have not added a certain person as a friend, that person will not be able to view your profile. However, you can adjust the privacy settings to allow users within your network (such as your college or the area you live) to view part or all of your profile. You can also create a "limited profile," which allows you to hide certain parts of your profile from a list of users that you select. If you don't want certain friends to be able to view your full profile, you can add them to your "limited profile" list.

Another feature of Facebook, which makes it different from MySpace, is the ability to add applications to your profile. Facebook applications are small programs developed specifically for Facebook profiles. Some examples include SuperPoke (which extends Facebook's "poke" function) and FunWall (which builds on the basic "wall" feature). Other applications are informational, such as news feeds and weather forecasts. There are also hundreds of video game applications that allow users to play small video games, such as Jetman or Tetris within their profiles. Since most game applications save high scores, friends can compete against each other or against millions of other Facebook users.

Facebook provides an easy way for friends to keep in touch and for individuals to have a presence on the Web without needing to build a website. Since Facebook makes it easy to upload pictures and videos, nearly anyone can publish a multimedia profile. Of course, if you are a Facebook member or decide to sign up one day, remember to use discretion in what you publish or what you post on other user's pages. After all, your information is only as public as you choose to make it!

--Updated January 14, 2008

Favicon

A favicon is a small icon that identifies a website in a web browser. Most browsers display a website's favicon in the left side of the address bar, next to the URL. Some browsers may also display the favicon in the browser tab, next to the page title. Favicons are automatically saved along with bookmarks or "favorites" as well.

Favicons have been around since the early 2000s and are supported by all major web browsers. However, different browsers provide different implementations of the favicon. For example, Firefox, Internet Explorer, and Safari all display favicons in the address bar, but Google Chrome only displays them in the page tabs. Most browsers support favicons saved as .GIF, .PNG, or .JPG files, but Internet Explorer only displays favicons saved in the .ICO format.

The standard way to implement a favicon on a website is to upload a small 16x16 pixel image named favicon.ico to the root directory of the website. When a user loads a page from the website in a web browser, the browser looks for the favicon.ico file, and if it finds one saved in a supported format, it automatically displays the icon next to the URL or the page title. The favicon can also be specified in the HTML of a webpage as follows:

The HTML method typically overrides the favicon saved in the root directory, which can be useful if you want to display a custom favicon for certain pages within a website.

NOTE: The standard size of a favicon is 16x16 pixels, though most browsers will recognize favicons saved as 32x32, 48x48, and 64x64 pixel images as well. Favicons larger than 16x16 pixels are typically scaled down to 16x16 so that they display in the browser correctly. However, browsers that support retina displays will display 32x32 pixel icons in their native resolution.

--Updated September 5, 2013

Fios

Stands for "Fiber Optic Service." Fios is a telecommunications network owned by Verizon that uses fiber optic cables to transfer data. It is considered a "Fiber to the Premises," or FTTP service, since it brings fiber optic data transmission to residential homes as well as businesses. Fios supports data transfer rates of 940 Mbps downstream and 880 Mbps upstream.

Services include Fios Internet, Fios TV, and Fios Digital Voice. Fios Internet is a high-speed broadband connection to the Internet where Verizon serves as the ISP. Fios TV is high-definition television service that provides over 400 channels, similar to cable television. Fios Digital Voice is similar to a traditional telephone service. It provides a phone number and supports both domestic and international calls.

Since Fios uses 100% fiber optic cables, it is one of the fastest Internet services available. It is also known for its high reliability. However, Fios is only available in specific areas of the United States that are connected to Verizon's fiber optic network. To find out if you can get Fios where you live, check Verizon's Fios Availability.

--Updated August 24, 2018

Firewall

A physical firewall is a wall made of brick, steel, or other inflammable material that prevents the spread of a fire in a building. In computing, a firewall serves a similar purpose. It acts as a barrier between a trusted system or network and outside connections, such as the Internet. However, a computer firewall is more of a filter than a wall, allowing trusted data to flow through it.

A firewall can be created using either hardware or software. Many businesses and organizations protect their internal networks using hardware firewalls. A single or double firewall may be used to create a demilitarized zone (DMZ), which prevents untrusted data from ever reaching the LAN. Software firewalls are more common for individual users and can be custom configured via a software interface. Both Windows and OS X include built-in firewalls, but more advanced firewall utilities can be installed with Internet security software.

Firewalls can be configured in several different ways. For example, a basic firewall may allow traffic from all IP addresses except those flagged in a blacklist. A more secure firewall might only allow traffic from systems or IP addresses listed in a whitelist. Most firewalls use a combination of rules to filter traffic, such as blocking known threats while allowing incoming traffic from trusted sources. A firewall can also restrict outgoing traffic to prevent spam or hacking attempts.

Network administrators often custom configure hardware and software firewalls. While custom settings may be important for a company network, software firewalls designed for consumers typically include basic default settings that are sufficient for most users. For example, in OS X, simply setting the firewall to "On" in the "Security & Privacy" System Preference prevents unauthorized applications and services from accepting incoming connections. Some firewalls even "learn" over time and dynamically develop their own filtering rules. This helps them become more adept at blocking unwanted connections without any manual customization.

--Updated December 18, 2014

Flaming

Flaming is the act of posting or sending offensive messages over the Internet. These messages, called "flames," may be posted within online discussion forums or newsgroups, or sent via e-mail or instant messaging programs. The most common area where flaming takes place is online discussion forums, which are also called bulletin boards.

Flaming often leads to the trading of insults between members within a certain forum. This is an unfortunate result, as it often throws the discussion of a legitimate topic well off track. For example, the topic of a discussion forum may be "Choosing a Mac or a PC." Some Mac user may post a message gloating about the benefits of a Mac, which in turn prompts a response from a PC user explaining why Macs suck and why Windows is obviously the better platform. The Mac user may then post a reply saying that Mac users are, in fact, a more intelligent species who are not as naive as PC users. This kindles a more personal attack from the PC user, which incites an all out flame war.

These flame wars, also called "pie fights," are not limited to only two people at a time, but may involve multiple users. This causes a swell of negatively within online discussion groups and results in little, if any, productively. Flaming is unfortunately one of the most common breaches of online netiquette. Instead of being considerate of others' viewpoints, "flamers" force their own agendas on other users.

While some flaming is intentional, some is not. This is because users may misunderstand the intent of a another user's message or forum posting. For example, someone may make a sarcastic comment that is not understood as sarcastic by another user, who may take offense to the message. Using emoticons and clearly explaining one's intent can help avoid online misunderstandings. Because of the adverse effects of flaming, it is best to err on the side of humility and be courteous when posting or sending messages online.

--Updated in 2006

Flash

Macromedia Flash (later Adobe Flash) was a multimedia web browser plug-in that enabled animations, video, and interactive content on websites. Flash was an extremely popular plug-in for more than a decade, but it eventually fell out of favor due to a combination of performance and security problems and the introduction of HTML5 and its multimedia features.

Originally called FutureSplash Animator and released in 1996, Flash first became popular as a vector-based animation tool. It allowed people to easily create animations that could be played back in any web browser with the Flash plug-in installed. Later updates introduced ActionScript (an object-oriented programming language that added new levels of interactivity) and support for high-quality video streaming. By 2010 the Flash plug-in was included by default with most web browsers, and it was common to see interactive games, streaming video, and even entire websites built using Flash.

However, the Flash plug-in had its drawbacks. It was very resource-intensive when content was playing, quickly draining batteries on laptop computers. The plug-in also proved to be a security risk that allowed an attack vector for malware. The lack of support for Flash on Apple's iPhone, and growing browser support for HTML5 video, ultimately caused Adobe to end support for the Flash plug-in in 2020. The animation tool itself was renamed Adobe Animate and now supports HTML5, WebGL, and SVG animation output.

NOTE: "Flash" may also refer to flash memory. Erasing a flash memory cell is often called "flashing" the memory.

--Updated January 10, 2023

Fluid Layout

A fluid layout is a type of webpage design in which layout of the page resizes as the window size is changed. This is accomplished by defining areas of the page using percentages instead of fixed pixel widths.

Most webpage layouts include one, two, or three columns. In the early days of web design, when most users had similar screen sizes, web developers would assign the columns fixed widths. For example, a fixed layout may include a main content area that is 960px wide with three columns that have widths of 180px, 600px, and 180px. While this layout might look great on a 1024x768 screen, it might look small on a 1920x1080 screen and would not fit on a 800x600 screen.

Fluid layouts solve this problem by using percentages to define each area of the layout. For example, instead of creating a content area of 960px, a web developer can create a layout that fills 80% of the screen and the three columns could take up 18%, 64%, and 18% respectively. By using percentages, the content can expand or shrink to fit the window of the user's computer. The CSS used to create a fixed layout vs a fluid layout is shown below.

Fixed Layout	Fluid Layout
.content { width: 960px; } .left, .right { width: 180px; } .middle { width: 600px; }	.content { width: 80%; } .left, .right { width: 18%; } .middle { width: 64%; }

The CSS classes in the examples could each be assigned to a div within a page's HTML where the .left, .right, and .middle classes are enclosed within the .content class. The content class could also be a assigned to a table and the other classes could be assigned to table cells. The fixed width .content class does not require a defined width since it automatically spans the width of the enclosed divs or table cells.

Fluid Layout vs Responsive Design

The terms "fluid layout" and "responsive web design" are sometimes used interchangeably, but they are two different things. A page created using responsive web design includes CSS media queries, which load different styles depending on the width of the window or the type of device used to access the page. Responsive web design requires more CSS (and sometimes JavaScript) than a basic fluid layout, but it also provides more control over layout of the page.

--Updated May 5, 2015

Friend

A friend, in the traditional sense of the word, is a close acquaintance. An online friend, however, is simply a person added to your list of friends on a social networking website.

For example, on Facebook, you can select a user and click "Add as Friend" to send a friend request to that user. When the user receive your friend request, he or she may choose to accept or decline the invitation. If the user accepts your request, he or she will be added to your list of friends. Likewise, you will be added to that user's list of friends as the same time. MySpace includes a similar feature.

Once you become friends with a user, that person will be able to access your profile with the additional viewing rights. This means he or she may be able to view more or your profile and post comments on the "wall" of your profile page. Since non-friends may not be able to view any of your profile, it is common practice to accept most friend requests. Of course, this has led to a rather liberal definition of "friend," since many people have hundreds of online friends who they hardly know.

The word "friend" can also be used as a verb, which means adding a user as a friend. When you delete a friend, you "unfriend" that person.

--Updated November 20, 2009

Friendly URL

A friendly URL is a Web address that is easy to read and includes words that describe the content of the webpage. This type of URL can be "friendly" in two ways. 1) It can help visitors remember the Web address, and 2) it can help describe the page to search engines.

User-Friendly URLs

Friendly URLs that are short and easy to remember are considered "user-friendly URLs." These URLs help visitors remember web addresses, which means they can revisit pages by simply typing in the URL address bar. For example, a company may use the URL "www.[company].com/support/" for the support section of their website. This is much easier to remember than a long convoluted URL, like "www.[company].com/section/support/default.aspx?id=1&lang=en".

Since dynamic sites often load different content based on the variables in the URL (which are usually listed after the question mark), creating user-friendly URLs is not always easy. Therefore, many webmasters now use a strategy called "URL rewriting" to create simpler URLs. This method tells the Web server to load a different URL than the one in the address bar. Therefore, a simple Web address can point to a more complex URL with lots of variables. Since the URL is redirected at the server level, visitors only see the simple Web address.

Search Engine-Friendly URLs

While user-friendly URLs are helpful for visitors, most webmasters are more concerned with creating search engine-friendly URLs. These URLs include important keywords that describe the content of the page. Since most search engines include the Web address as part of the information that describes a page, placing keywords in the URL can help boost the ranking of the page. Therefore, this strategy has become a popular aspect of search engine optimization or SEO.

For example, a blog that includes tips for Windows 7 may have a URL like "blogger.blogger.com/2011/02/windows7.html". A search engine friendly version of this URL may be "blogger.blogger.com/2011/02/helpful-tips-for-using-windows-7.html". While this type of descriptive URL may help with search engine ranking, it is important not to create ridiculously long URLs just to describe the page. After all, search engines still focus primarily on the content of each page when indexing websites.

--Updated February 11, 2011

FTP

Stands for "File Transfer Protocol." FTP is a protocol designed for transferring files over the Internet. Files stored on an FTP server can be accessed using an FTP client, such as a web browser, FTP software program, or a command line interface.

An FTP server can be configured to enable different types of access. For example, an "anonymous FTP" configuration allows anyone to connect to the server. However, anonymous users may only be allowed to view certain directories and may not be able to upload files. If anonymous FTP access is disabled, users are required to log in in order to view and download files.

The standard FTP protocol is not encrypted, meaning it is vulnerable to packet sniffers and other types of snooping attacks. Therefore, the FTPS and SFTP protocols were developed to provide secure FTP connections. FTPS (FTP with SSL security) provides SSL encryption for all FTP communication. SFTP (SSH File Transfer Protocol) is a secure version of FTP that uses SSH to encrypt all data transfers.

To you connect to an FTP server, you first need to enter the server name and port number. The server name often starts with "ftp," such as "ftp.example.com." The standard port number for FTP is 21, while SFTP uses port 22 (SSH). If you connect via FTPS, you might be required to enter a custom port number, but the most common one is 990. In order to access an SFTP or FTPS server, you will also need to enter a username and password.

--Updated January 30, 2015

Google

Google is the world's most popular search engine. It began as a search project in 1996 by Larry Page and Sergey Brin, who were two Ph.D. students at Stanford University. They developed a search engine algorithm that ranked Web pages not just by content and keywords, but by how many other Web pages linked to each page. This strategy produced more useful results than other search engines, and led to a rapid increase in Google's Web search marketshare. The Google ranking algorithm was later named "PageRank" and was patented in September of 2001. In only a short time, Google became the number one search engine in the world.

According to Google's website, the company's mission is to "organize the world's information and make it universally accessible and useful." While the Web search remains Google's primary tool for helping users access information, the company offers several other services as well. Some of these include:

- Froogle - price comparison shopping
- Image Search - search for images on the Web
- Google Groups - online discussion forums
- Google Answers - answers to questions based on a bidding system
- Google Maps - maps and directions
- Google Toolbar - a downloadable search tool
- Blogger - a free blogging service
- Gmail - Web-based e-mail with several gigabytes of storage

- AdWords - Advertising services for advertisers
- AdSense - Advertising services for Web publishers

Google has become such a popular search engine that the term "Google" is now often used as a verb, synonymous with "search." For example, if you are looking for information about someone, you can Google that person using Google's search engine.

To Google your own term or phrase, visit Google's home page.

--Updated in 2006

Google Drive

Google Drive is a service offered by Google that allows you to store and share files online. The service was launched on April 24, 2012 and provides 5 GB of free storage. Additional storage can be purchased for a monthly fee.

The goal of Google Drive is to provide a central place to store your files online so that you can access them from anywhere. Additionally, you can access your Google Drive from multiple devices, since the software is available for Windows, Mac OS X, Android, and iOS platforms. The service also provides a web-based interface that allows you to organize your files and search for documents by filename or content.

Besides online file storage, Google Drive provides tools for sharing files and collaborating on projects with other users over the Web. For example, instead of emailing large attachments, you can send links to the files from your Google Drive to one or more users. You can also use the web-based Google Docs applications to create or edit documents online. When you share a document with other Google Drive users, everyone can view and edit the document at the same time.

Google Drive allows you to view over 30 file types directly in your web browser. These include Google's proprietary formats, as well as other popular file types, such as Adobe Photoshop and Illustrator documents. For more information about Google Drive's proprietary file types, view the Google Drive File Types article at FileInfo.com.

--Updated April 25, 2012

Graymail

Graymail describes email messages that are generally unwanted, but do not fit the definition of spam. Unlike spam, graymail includes messages from mailing lists and newsletters that you have legitimately signed up to receive. Over time, these messages can begin to clutter your inbox and can easily be mistaken for spam.

The term "graymail" was coined by the Microsoft Hotmail team in 2011, when the company introduced new methods of filtering incoming messages. Graymail differs from spam in the following ways:

1. **The email is solicited.** You request to receive graymail by opting in, either directly or indirectly. For example, a direct method is subscribing to a mailing list. An indirect method is providing your email address when you register with an e-commerce website.
2. **The email is legitimate.** Graymail messages are sent by reputable sources who value their relationship with the recipient. The messages usually contain an unsubscribe option, which is honored by the sender.
3. **The email content is targeted to specific users.** Graymail messages generally contain content that is specific to your interests. While the emails may include text that is similar to spam messages, such as special offers and promotions, the offers are directed to you and other specific users.

Based on Microsoft's research, newsletters and special offers make up the majority of messages in the average user's inbox. By identifying these messages as graymail, Hotmail is able to filter them appropriately. This includes moving newsletters to a specific "Newsletters" category and providing a "Schedule Cleanup" tool that moves or deletes outdated email promotions.

--Updated February 13, 2012

Grid Computing

Grid computing (also called "distributed computing") is a collection of computers working together to perform various tasks. It distributes the workload across multiple systems, allowing computers to contribute their individual resources to a common goal.

A computing grid is similar to a cluster, but each system (or node) on a grid has its own resource manager. In a cluster, the resources are centrally managed, typically by a single system. Additionally, clusters are usually located in a single physical space (such as a LAN), whereas grid computing often incorporates systems in several different locations (such as a WAN).

In order for systems in a computing grid to work together, they must be physically connected (over a network or the Internet) and run software that allows them to communicate. The software used in grid computing is called middleware since it translates the information passed from one system to another into a recognizable format. This allows the data computed by one node within the grid to be stored or processed by another system on the grid.

Grid computing has many different scientific applications. For example, it is used to model the changes in molecular structures, analyze brain behavior, and compute complex physics models. It is also used to perform weather and economic simulations. Some companies also use grid computing to process internal data and provide services over the Internet. Cloud computing, for instance, is considered to be a subset of grid computing.

--Updated February 11, 2015