Computer Terminology 101 Written by Leslie Eddy Snipes

Edited & Leader Guide by Gay Jarvinen

Presented at Oregon Association for Family & Community Education 2015 Annual Conference by Gay Jarvinen.

This is a very basic guide but it is still time sensitive, please go over the contents before presenting and make sure that the information is still relevant. Check the sources to see if there are updates or additions.

I would suggest that you pause between each subject for questions and answers. If you do not know the answers I would advise the members to go home and look it up on Google.com, unless you have a real computer guru amongst your members, in which case I would advise enlisting their assistance.

For an interactive section you could print out a list of acronyms and their meanings, giving an acronym or a meaning to each member and let them try to match them up. Acronyms available at www.netlingo.com/acronyms

COMPUTER TERMINOLOGY 101 – Written by Leslie Eddy Snipes

These are the topics that we will be covering in this program and we will just be skimming the surface of this subject but, hopefully, you will leave with a little bit more knowledge that will be of use to you.

Glossary/Terminology

1. Cloud – page 2
2. Operating system
3. Server
4. Database
5. CPU vs. Memory

Security

1. Hardware
2. Software
    a. Firewall
    b. Anti-Virus
    c. Anti-Spam
    d. MalWare/AdWare
    e. Passwords

Email

1. ISP (Internet Service Provider) vs. stand-alone
2. Good ones vs. Bad ones
3. Portability

WiFi/Internet – private/public

1. Home/Private
2. Public/Open
3. Downloading

Maintenance

1. File cleanup
2. Disk fragmentation

GLOSSARY

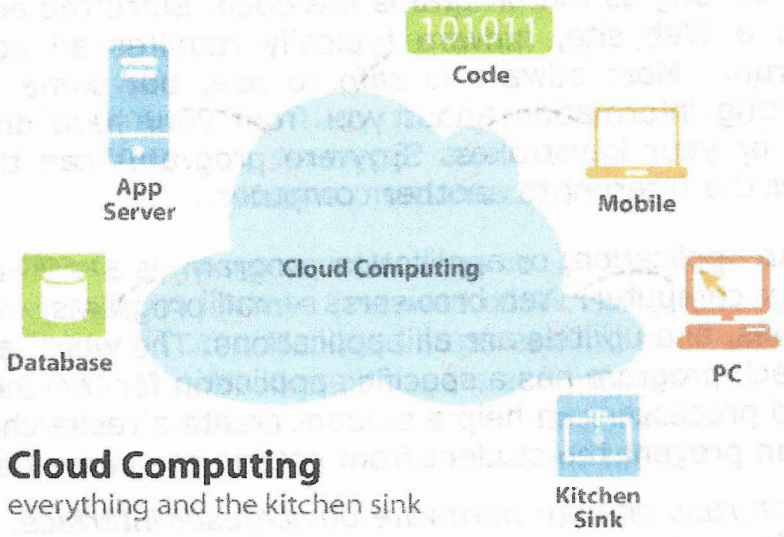
Adware. Adware is free software that is supported by advertisements. Common adware programs are toolbars that sit on your desktop or work in conjunction with your Web browser. They include features like advanced searching of the Web or your hard drive and better organization of your bookmarks and shortcuts. Adware can also be more advanced programs such as games or utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Since the ads often allow you to click to a Web site, adware typically requires an active Internet connection to run. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the Web sites you visit, or your keystrokes. Spyware programs can then send the information over the Internet to another computer.

Application. An application, or application program, is a software program that runs on your computer. Web browsers, e-mail programs, word processors, games, and utilities are all applications. The word "application" is used because each program has a specific application for the user. For example, a word processor can help a student create a research paper, while a video game can prevent the student from getting the paper done.

A local application runs on your hardware device/user interface. An example of this is TurboTax or Microsoft Word. A remote application is one that runs on a server, over a network or the internet, and is accessed by your hardware device/user interface. It typically requires very little software to run on your computer. The USPS.com website used to buy postage is an example of this.

GLOSSARY

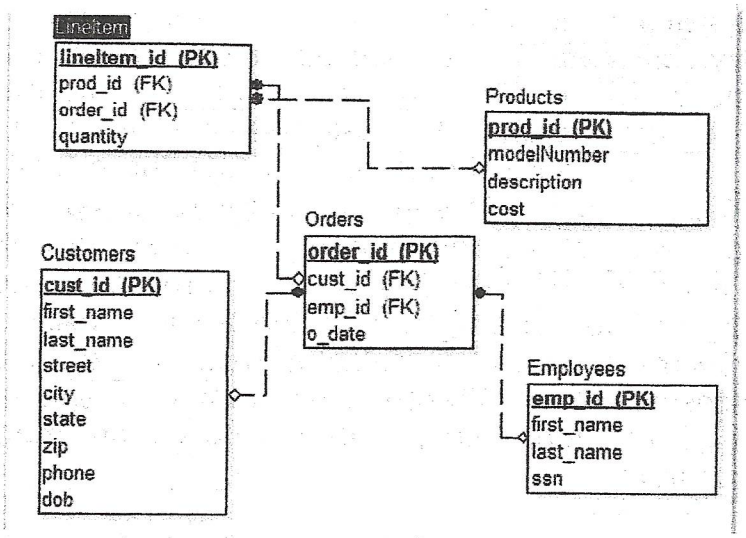
Cloud. The term "cloud" comes from early network diagrams, in which the image of a cloud was used to indicate a large network. The cloud eventually became associated with the entire Internet, and the two terms are now used synonymously. *i.e., the collective group of computers or servers that are connected via the Internet.*



CPU. Stands for "Central Processing Unit." The CPU is the primary component of a computer that processes instructions. It runs the operating system and applications, constantly receiving input from the user or active software programs. It processes the data and produces output, which may be stored by an application or displayed on the screen. The CPU contains at least one processor, which is the actual chip inside the CPU that performs calculations. For many years, most CPUs only had one processor, but now it is common for a single CPU to have at least two processors or "processing cores." A CPU with two processing cores is called a dual-core CPU and models with four cores are called quad-core CPUs. *The speed of the computer or device is determined by the CPU.*

GLOSSARY

Database. A database is a data structure that stores organized information. Most databases contain multiple tables, which may each include several different fields. For example, a company database may include tables for products, employees, and financial records. Each of these tables would have different fields that are relevant to the information stored in the table. *See illustration for* ***Cloud.***

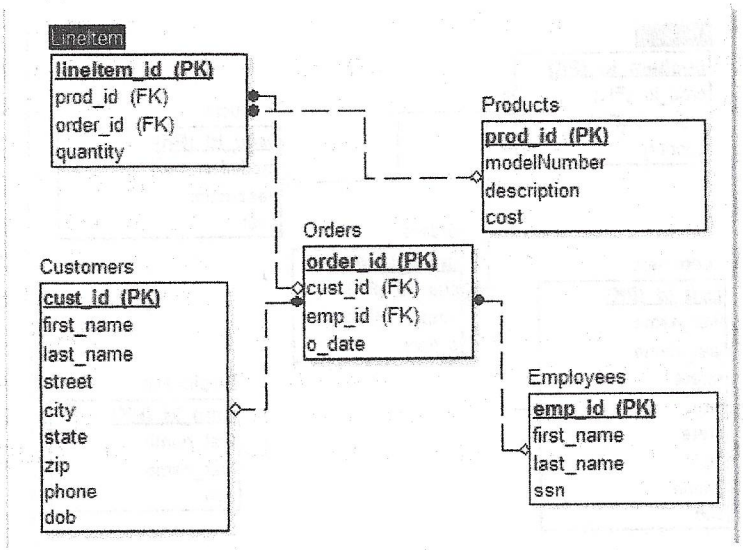


Firewall. A physical firewall is a wall made of brick, steel, or other inflammable material that prevents the spread of a fire in a building. In computing, a firewall serves a similar purpose. It acts as a barrier between a trusted system or network and outside connections, such as the Internet. However, 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. *An example of a hardware firewall is a modem or router.*

Hardware/Software. Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners. The internal hardware parts of a computer are often referred to as components, while external hardware devices are usually called peripherals. Together, they all fall under the category of computer hardware. Software, on the other hand, consists of the programs and applications that run on computers. Because software runs on computer hardware, software programs often have system requirements that list the minimum hardware required for the software to run. *Examples of hardware devices include laptops, desktop or personal computers, notebook computers, tablets or iPads, and cell phones. Inside these devices are the internal hardware components.*

GLOSSARY

Database. A database is a data structure that stores organized information. Most databases contain multiple tables, which may each include several different fields. For example, a company database may include tables for products, employees, and financial records. Each of these tables would have different fields that are relevant to the information stored in the table. *See illustration for **Cloud**.*



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. *An example of a hardware firewall is a modem or router.*

Hardware/Software. Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners. The internal hardware parts of a computer are often referred to as components, while external hardware devices are usually called peripherals. Together, they all fall under the category of computer hardware. Software, on the other hand, consists of the programs and applications that run on computers. Because software runs on computer hardware, software programs often have system requirements that list the minimum hardware required for the software to run. *Examples of hardware devices include laptops, desktop or personal computers, notebook computers, tablets or iPads, and cell phones. Inside these devices are the internal hardware components.*

GLOSSARY

Router. This is a hardware device that routes data (hence the name) from a local area network (LAN) to another network connection. A router acts like a coin sorting machine, allowing only authorized machines to connect to other computer systems. Most routers also keep log files about the local network activity.

Server. A server is a computer that provides data to other computers. Many types of servers exist, including web servers, mail servers, and file servers. *Also app servers (see illustration for **Cloud**), print servers, etc.*

Spam. Originating from the name of Hormel's canned meat, "spam" now also refers to junk e-mail or irrelevant postings to a newsgroup or bulletin board. The unsolicited e-mail messages you receive about refinancing your home, reversing aging, and losing those extra pounds are all considered to be spam.

Trojan horse. Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer. For example, a Trojan horse might appear to be a computer game, but once you double-click it, the program starts writing over certain parts of your hard drive, corrupting your data.

USB. Stands for "Universal Serial Bus." USB is the most common type of computer port used in today's computers. It can be used to connect keyboards, mice, game controllers, printers, scanners, digital cameras, and removable media drives, just to name a few.

User Interface aka "UI". A user interface, also called a "UI" or simply an "interface," is the means in which a person controls a software application or hardware device. A good user interface provides a "user-friendly" experience, allowing the user to interact with the software or hardware in a natural and intuitive way. *An example of a software UI is a web browser. Examples of hardware UI's are a keyboard, mouse, or touchscreen.*

Virus. Like a biological virus, a computer virus is something you don't want to get. Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious little programs can create files, move files, erase files, consume your computer's memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.

GLOSSARY

Web Browser aka Internet Browser aka Browser. A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

Worm. Just like regular worms tunnel through dirt and soil, computer worms tunnel through your computer's memory and hard drive. A computer worm is a type of virus that replicates itself, but does not alter any files on your machine. However, worms can still cause havoc by multiplying so many times that they take up all your computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash. If the worm affects your hard disk space, your computer will take a long time to access files and you will not be able to save or create new files until the worm has been eradicated. Worms are hard to detect because they are typically invisible files. They often go unnoticed until your computer begins to slow down or starts having other problems. Unlike viruses and Trojan horses, worms can replicate themselves and travel between systems without any action from the user.

Italicized comments were added by Leslie Eddy Snipes.

Source: http://techterms.com/

Source for Cloud Illustration: www.forbes.com

Source for Database Illustration: www.masorawamm.me

Computer Security

There are several facets to security. Most are software-related, but there are a few hardware-related protections too.

Hardware security is primarily provided thru use of a modem or router which set up a physical firewall to prevent intrusion from outside the network. However, if the default network name and password are in place on these pieces of hardware, they can be easily hacked. That's why it is important when setting up your home network that you change the network name and add a password for accessing your network. This combination is different than the administrative username and password that is used to administer the modem or router.

Software security is provided in several layers.

1. Software firewall. Microsoft Windows provides a firewall which can be accessed thru the Control Panel->Systems and Security menu option. If you are running an anti-virus with firewall, it is not necessary to run the Windows firewall too.
2. Anti-Virus. There are numerous anti-virus software packages available, some of them are either freeware or have freeware versions. Norton and McAfee were originally developed for corporate computer systems and are "resource hogs" (memory and CPU) on the personal computer. They also charge too much for their software and their customer service is poor. There are several free software packages or you can upgrade to a paid version, which use less system resource (memory) and are more inclusive. Some of the most familiar are AVG, Avast and Webroot. Check http://www.pcmag.com/article2/0,2817,2372364,00.asp. for their latest recommendations. Do not forget your cell phone if you use it for on-line shopping and banking, they need a good anti-virus protection too.
3. Anti-Spam for email. Most of the ISP and stand-alone email providers have a spam filter, but it doesn't eliminate all the spam. Many times they don't get the information on new spam attacks until after the anti-virus companies. The good anti-virus packages have a spam scanner for email. However, I heard that because Gmail does such a good job, Avast was erroneously targeting a lot of good email as spam and is not catching anything that Gmail already had, in that situation you might want to turned it off. This is something to experiment with.
4. Malware/Adware. It is best to run a special software suite to catch these buggers. A good recommendation is MalwareBytes anti-

10.

malware, a free software from https://www.malwarebytes.org/, http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html, or http://filehippo.com/download_malwarebytes_anti_malware.

5. Passwords. The recommended length for a password is now 18-24 mixed characters. This sounds daunting, however it's very easy to create and more importantly REMEMBER this length password by choosing a phrase that you know or use a lot and adding a significant set of numbers like a birthdate to it. Apparently, it would take years to crack a password of this length so it becomes basically impossible. Example: IloveFCEscholarships2015 is a 24-digit password and should be easy for you to remember ;)! It also has upper and lower case letters and numbers. It could be harder to crack by making it: IloveFCE5cholar5h1p52015, replacing the "i" with a "1" and the "s" with a "5". However, the first version is long enough and easy to remember. When using a lengthy password, you shouldn't have to worry about creating different passwords for everything.

Email Options. There are many Internet Service Providers (ISP's), which provide email as a service to the internet they provide you. Examples in our area are centurylink.net and charter.net. As long as you receive your internet service from the ISP, you have an email account with them, whether you use it or not. You can read your email at home using either a web browser or MS Outlook or other personal computer software. When you are travelling, you have to use the web browser to read the email or a special application on your cell phone called Email. Once you give up the internet service, or change companies, your email account is closed and you have to start with the new company. There are other email providers such as Yahoo or Google (mail.yahoo.com, mail.google.com) who provide a stand-alone email product which is not ISP dependent. That means that if you use their email service and you change ISP, you can still use the same email account and have what is called "portability" in the computer stratosphere. If you want to change email accounts, there is usually a forwarding service available to route your incoming email from the old account to the new account for a set period of time, kind of like the USPS does when you move to a new home and submit a change of address card to them. Based on my experience, I strongly discourage my friends and family from using AOL or MSN email accounts as I know too, too many people who have been hacked having those type accounts.

WiFi/Internet – Private and Public

Private networks are the safest and typically what you would have in your home, locked down to the selected users with a password. In our area, most people have DSL, satellite, a mobile hotspot, or air card. Each of these providers provide some sort of modem which is used to route the internet communications coming into and going out of the home. In the case of DSL, data is delivered over the incoming phone line from a remote router for the local area. The data is delivered to that router via fiber optic cable which is underground. In the case of satellite, a satellite dish is connected to the home's modem and transmits data to a ground station or hub, aka gateway. Some satellite internet providers are two-way and some only one-way (download) where the upload is via phone connection. Both DSL and satellite are pretty much stationary in the home, you can't take it with you. On the other hand either a mobile hotspot or an air card is very portable. You can take it with you. It's about the size of a cell phone or even smaller in the case of an air card which is equivalent in size to the larger size thumb drive. Air cards are wireless adapters that are used to connect to the internet through the use of cellular data. They are most commonly connected to laptops or other devices with USB ports, creating a strong and secure connection. Once connected, the air card allows the user access to the internet from data signals sent from cell towers, using the same technology that cellphones use for online functionality. Mobile hotspots are small wireless devices that pulse WiFi signals that you can connect internet-ready devices to. Since the mobile hotspot is wireless and there's nothing to physically attach, the process for connecting your device to the hotspot is the same as the internet connection at Fred Meyer. The mobile hotspot requires a data plan, and comes with the ability to simultaneously connect multiple devices to a cellular network.

Public or open networks are what you find in department stores like Fred Meyer or Home Depot for the convenience of their customers to access their websites and do comparison shopping. They are also in places like Starbucks in the form of WiFi hotspots, and airports. These open networks are not very secure and you should be careful sharing your personal information over them. However, they are great for checking on movie times as you're shopping, or the latest news headlines.

Downloading over networks is quite easy with the newest operating systems. For the home computer, the browser typically has an option to download. If you are on an open network, you should be careful and make sure your malware, firewall, and anti-virus software is running to prevent a virus from piggy-backing on the download. This includes your cell phone. See the topic on **Security**.

Laptop/Desktop Maintenance . Periodically, the computer may slow down or not respond as quickly as we would like. Typically this is due to network "latency" (a network engineer's fancy term for the time it takes data to travel between your computer and the server). However, before first blaming the network for being slow, a computer user should make sure their computer "house" is in order – excess files removed, memory not over-taxed, files not fragmented, viruses or malware not on the system, etc. There are free tools available on the internet to help with these tasks. The following is a list of software recommended by power-users and highly rated by cnet.com, one of the go-to websites for "techies".

File cleanup: CCleaner, a freeware system optimization, privacy and cleaning tool. It removes unused files from your system allowing Windows to run faster and freeing up valuable hard disk space. It also cleans traces of your online activities such as your Internet history. Additionally it contains a fully featured registry cleaner. Available for download at http://download.cnet.com/CCleaner/, http://filehippo.com/download_ccleaner/, or https://www.piriform.com/**ccleaner**.

Defragmentation: Defraggler, defragments hard drives or individual folders and files and monitors the health and performance of your disc drives. Available for download at http://download.cnet.com/Defraggler/3000-2248_4-10752905.html, http://filehippo.com/download_defraggler, or https://www.piriform.com/defraggler.

Acronyms have always been an integral part of computer culture, and they have since spawned a new language on the Internet. Commonly thought of as a series of letters that make up a 'word' there is a distinction between acronyms and shorthand.

Online enthusiasts are learning that shorthand are in fact called acronyms, but this is incorrect. The difference between acronyms and shorthand is that with acronyms, *you pronounce the letters as a new word* (for example, 'FUBAR' is pronounced 'foo-bar' and 'RADAR' is pronounced 'ray-dar'). In contrast, shorthand pronunciations are like an initialism (a set of initials) in which you *say the letters one-by-one* (for example, 'ESP' is an initialism for 'extra sensory perception' whereas 'esp. is an abbreviation for especially). The online practice is to refer to shorthand, initialisms, or abbreviations as acronyms.
The majority of the expressions you see above are not acronyms, but rather shorthand used while text messaging or IMing. There are several terms to describe different kinds of jargon including anacronym, backronym, weather acronyms, city acronyms, leetspeak and textonyms.

BTW: If you ever see someone TYPING AN ENTIRE SENTENCE IN ALL CAPITAL LETTERS that means SHOUTING! It is not proper netiquette to TYPE IN ALL CAPS (even in email), in fact, it's annoying. People with limited eyesight may use all caps to see the words better, but otherwise, TURN THE CAPS LOCK OFF, *unless you're using an acronym or shorthand.*
- See more at: http://www.netlingo.com/acronyms.php

Some of these can be really obvious such as 2 which can mean to, too or two, and OMG or LOL that most of us know by now. Others can be more complicated, like 9 which means "parent is watching" and 99 which says "parent is no longer watching" or BHIMBGO which means "Blood Hell I Must Be Getting Old" or EMRTW which is "Evil Monkeys Rule The World". Just one more, *$ which is "Starbucks".

In case you are still wondering RADAR stands the Radio Detecting And Ranging.