Technology Glossary

Anti-Virus: A program that protects you from malicious software. Most anti-virus programs have options for purchasing additional security measures such as firewalls, email scanning, etc.

Apple ID: This is the username and password that you create with Apple to link a specific device to your Apple account. If you have an iPad and an iPhone, you would use the same Apple ID with both of those devices.

App: Short for Application.

Application: An application is a piece of software that lets your device do something, like play music or give directions. An application is the same thing is a program.

Autocorrect: Auto correct is when your phone automatically changes what you were typing to what it thought you wanted to type.

Autoplay: When you visit a website and music or video starts playing without asking.

Browser: Short for Web Browser.

Browser Hijack: Where a malicious piece of software modifies a web browser's settings without your permission.

Brute Force Attack: Where a hacker tries many passwords for passphrases in an attempt to break into your account. The longer your password (or passphrase) the harder it is for someone to use this kind of attack to break into your account.

Cache: Temporary storage space that allows your computer to quickly bring up information, such as previously viewed web pages.

Cellular Data: The connection your cell phone makes to a cell tower that allows you to do things like surf the internet, download emails, and send SMS messages.

Cloud: Storage that is physically somewhere other than where you are. Cloud storage is generally accessible from multiple devices, because those files are stored on a hard drive that belongs to a company that hosts the cloud service. Cloud storage is like a self-storage unit for your electronic files, except you can access your stuff from anywhere.

Cookie: A piece of data that a website saves on your computer. Cookies were designed to save user information such as preferences or logins, but can sometimes be read by third parties. Cookies are also used to collect browsing data long-term.

CPU: Central Processing Unit. The bit of a computer or electronic device that processes information.

Database: An organized collection of information. An address book is a very basic database. Complicated databases link information between multiple tables allowing for analysis of the contained information.

Data Breaches: The release of secure or private information. A data breach can be accidental or malicious, where an individual hacks into a system to steal information.

Denial of Service Attack (DOS): A cyber-attack where the malefactor seeks to make a network resource (such as a website) unavailable by flooding the target with requests or visits.

DNS Hijacking: Where a malefactor redirects visitors from a valid website to a different destination—often one that exists to steal data.

Domain: The sometimes arbitrary grouping that designates what a website does or where it is based. The most common domains are .com .net .edu and .org. The domain is what you should check first when you want to verify the authenticity of a website.

Domain Name: The string of text that identifies a place on the Web. A basic domain name is a word or abbreviation followed by a period followed by the domain extension: wvu.edu

Email: Email is an electronic letter sent from one email address to another email address. Email addresses always have an **@** (at sign) in them. Sending an email on your phone requires the use of cellular data. Each email address is unique, and email addresses are often used as unique identifiers or login credentials by databases.

Encryption: The encoding of data so that only authorized persons or devices can read/view the information. The stronger the encryption, the more unlikely it is that a malfeasant could decode the intercepted data through a brute force attack.

Firewall: A firewall is a security system that monitors incoming and outgoing network traffic to prevent unauthorized access to a system.

GPS: Global Positioning System is a piece of hardware that allows a device to contact a satellite to determine the location of the device in latitude and longitude. On most devices, software makes these data points usable to the end user by placing them on a map.

Hardware: The electronic components of a device; the bits you can touch. A cell phone, a keyboard, and a CPU are all hardware.

HDR: High Dynamic Range. A photographic process where a camera takes multiple pictures at different exposures and combines them into a single image—this allows all areas of your image to be well-exposed, but can also look unreal if used too much.

Hotspot: A type of Wireless Access Point. A device that allows you access the internet from a public place. Hotspots are generally open and unsecured and you should assume any data you submit is visible to people with ill-intent.

http: Hypertext Transfer Protocol is how data is moved between a website and an end user.

https: Hypertext Transfer Protocol (Secure) is an encrypted form of http. This protects against interference or snooping by third parties.

iCloud: Apple's cloud service.

iPad: Apple's tablet computer, running iOS.

iPhone: Apple's cellular phone, running iOS, that was built upon the iPod.

iPod: Apple's music player. The iPod is general similar to an iPhone, only without cellular service.

iTunes: Apple's music service.

Internet: A system of inter-connected computer networks.

Keylogger: Keystroke logger (also keyboard capture). A piece of hardware or a software program that can record every key struck on the keyboard.

Location Services: Information from GPS, wireless access points, cell towers, and Bluetooth devices that helps your phone know where you are.

MMS: Multimedia Messaging Service is a kind of text messaging that allows you to send text messages that contain pictures or audio, as well as messages longer than 160 characters or to multiple people.

OS: An Operating System is the base upon which software and apps are added. An Apple device generally uses iOS (iPhones) or macOS (laptop computers). PCs typically used the Windows OS, but there are other operating systems, such as Linux that can be installed. Non-Apple cell phones frequently use some form of the Android OS. How your device looks and works is dependent upon the operating system installed.

Passcode: This is the secret code to get into a specific device. If you have an iPhone and an iPad, they can have different passcodes. You can sometimes use a fingerprint instead of a passcode to get into a device.

Password Manager: A program that stores electronic passwords.

PayPal: A method of online money transfer and payments.

Phishing: A fraudulent attempt to gain personal or sensitive information, by sending an email or creating a website that pretends to be from a real company or person, but is not.

Predictive Text: An input technology that guesses what you want to type both from what you are currently typing and, if you have allowed the software to learn, from what you have typed in the past. Predictive text makes typing faster and easier if you have good software on the back end.

Program: A program is a piece of software that lets your device do something like send a text message or video chat. A program is the same thing as an application.

Public Network: An electronic connection where the traffic between devices is visible to anyone.

Ripping: Extracting digital content from a container, such as a CD or DVD. Ripping a CD means that the music is copied without loss from the CD to your computer.

Router: A networking device that forwards data between networks.

Search Engine: A software system designed to find information on the web. The results from a search engine can be webpages, files, or images. Generally, behind the scenes a program runs an algorithm that crawls through the web cataloging everything it sees. This catalog is then organized by a different program where pages are associated with various terms.

Server: A device (or program) that allows you to access something not on the device you are physically touching. A mail server stores your email and drops it to your device upon request. A web server allows you to connect to the internet.

Siri: Apple's personal assistant.

SMS: Short Messaging Service. A brief message that is sent from one phone number to another phone number. SMS does not use cellular data.

Snooping: Unauthorized listening in to data transmission.

Software: The programs that run on your computer or phone. Can also be called an application.

Spam: Unsolicited electronic messages (especially advertising).

Spoofing: When a person or program pretends to be someone else, by falsifying data, to gain access to your account or data.

Spyware: A piece of malicious software that secretly installs itself to gather information about the user or device.

Sync: Short for synchronize, when a file is synced, changes to that file are saved are pushed from one device to all other devices with access to that file, via a remote server.

TXT: Text message.

Text Message: A brief message that is sent from one phone number to another phone number via a protocol called SMS. Text messages are generally limited to 160 characters, and messages with more characters than that will be broken down into multiple messages when sent. Text messages are asynchronous: a message sent to someone whose phone is off is delivered when their phone is turned back on. Text messages generally do not require cellular data but do require a cellular connection.

Trojans: A type of malicious computer virus that presents itself as a useful item, such as a document.

Two-Factor Authentication: This is a way to make both your device and your account more secure. When you log into your Apple ID on a new iPad (or iPhone) for the first time OR you log into iCloud from a computer you have never used before, Apple wants you to verify that YOU are the person attempting to access your account.

URL: Uniform Resource Locator is the address of a space on the web. Every website has a unique address, and that address can often tell you something about the web page you are visiting.

Viruses: A piece of malicious software that inserts itself into another software program that it uses to replicate itself. Ransomware is a software virus.

Web: Also called the World Wide Web, this is an information space on the Internet that is accessible from devices such as computers, cell phones, and tablets, using a URL as the address.

Web Browser: A software program that allows you to access sites on the Internet, or web.

Wi-Fi: Short for wireless (the "fi" is an arbitrary syllable added on)

Wireless: A technology that allows computers to connect to a network and/or the internet without using a physical connection. Wireless is available in an area when a wireless access point (also called a hotspot) has been created and made accessible to devices. Public wireless is less secure and caution should be used (ie, don't make purchases or send private emails over a wireless network). Private wireless networks (such as in your home) should be secured with a password.

Wireless Access Point: A device that allows your device to access the internet. If a wireless access point (or router) does not have a password, it is unsecure, and you should assume that anyone can see what you are doing on your device.

Wireless Router: A piece of hardware that allows devices to connect to the internet without being plugged into the wall. Your wireless at home should be password protected, so that strangers cannot access all devices in your home using that wireless network.

Please Support OLLI@WVU!

Osher Lifelong Learning Institute
Mountaineer Mall Unit C-17
PO Box 9123
Morgantown, WV 26506-9123
Office: (304) 293-1793
Email Address: olli@hsc.wvu.edu
http://www.olliatwvu.org