Technology Security

Table of Contents

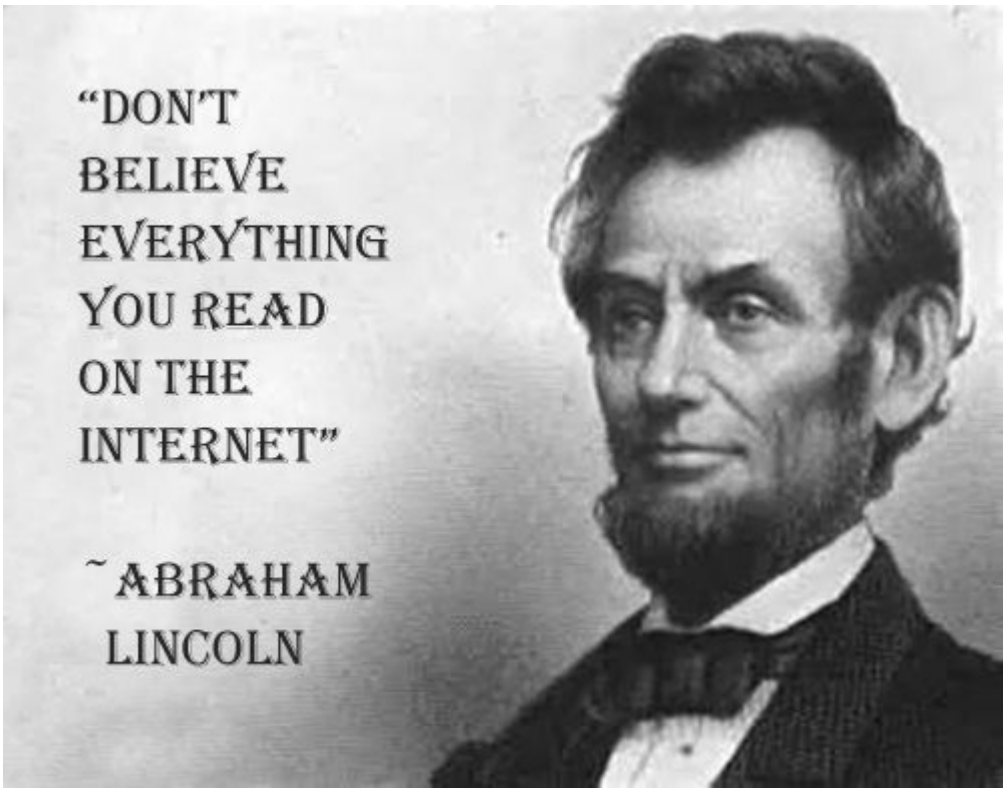
Updated: 30 April 2019

Rules to Live By

Lock Your Phone!

Password Protect Your Computer!

If you are not paying for something then YOU are the product!



Phones

Phone Cases and Screen Protectors

Are you clumsy? Do you give your phone to small children? Then you should purchase a quality phone case and screen protector. That extra plastic and/or glass might well save you from having to replace the screen—or the phone.

Phone Cables

This is not a security issue per se, but a piece of logic sometimes people miss. A new cell phone can cost as much as $1000 dollars. A $2 charging cable plus a surge of unregulated power can turn your phone into a shiny brick. Buy quality cables when they are on sale, put them in all your bags, and leave them in your car and around your house.

Phone Apps

Along the same lines, if you paid $750 for your phone, a $1.99 app is 0.3% of the cost of your phone. Downloading a free app that might contain malicious code that could wipe out your phone is... illogical.

Phone apps are the most important area to remember that if you are not paying for it then YOU are the PRODUCT.

Most apps have a trial version you can use to see if you like the program before your buy it, or a version with ads. Try out an app and once you like it—purchase the full version. Purchasing apps protects you and supports creative entrepreneurs.

It is important to pay attention to what access different apps have. Does a coupon app really need to access your camera AND location AND email AND contacts? Perhaps it does, but that doesn't mean you have to run that app all the time—you can force shut down an app after you use it and reopen it when you need it. (See page 4 for information on how to force close Android apps.)

It's a good idea to regularly go through the apps on your phone and uninstall the ones you don't use. It's common to get an app to do one thing, then forget about it; a year later that app is still sitting there taking up space and possibly even spying on you.

You have the option with most phones to back up some of all of your data to the cloud. Whether you choose to do this, and what data you select to sync, should be dependent upon several factors:

How much data do you have?
What kind of data do you have?
How much do you trust the service you want to use?

The cloud is an excellent way to both transfer files between devices and back up some of your data, but you need to make an informed choice. (See page 23 for more on cloud services.)

Closing Phone Apps

Closing Apps on an iOS Device

1. Double tap on the home button to bring up a screen that displays the open apps.
   OR
   Swipe up twice from the bottom of the screen.
2. Drag an app up towards the top of the screen to close it.

Closing Apps on an Android Device

1. Tap the Recent Applications Menu button, usually at the lower left of the screen. A list of open apps appears
2. To close an individual app, click the **x** beside the app or swipe right on the app.
3. To close all open apps, if available, tap **Close All**.

To be clear, stopping an app frequently leaves parts of that app still running in the background. To end all processes of that app, you need to force the app to stop.

Force Stopping Apps on an Android Device

1. Open your device settings. (Typically available from the list off all applications or by pulling down from the top of the screen to open the system tray, and tapping the gear icon.)
2. From the list of available settings, choose **Apps** or **Applications**. (Depending upon your phone.)
3. Scroll through the list to find the specific app you want to close and/or keep from running in the background.
4. Towards the top of the screen, tap the **Force Stop** button.
5. The device asks if you are sure you want to do this, tap **Force Stop**.

Uninstalling Apps on Android Devices

1. Open your device settings. (Typically available from the list off all applications or by pulling down from the top of the screen to open the system tray, and tapping the gear icon.)
2. From the list of available settings, choose **Apps** or **Applications**. (Depending upon your phone.)
3. Scroll through the list to find the specific app you want to close and/or keep from running in the background.
4. Towards the top of the screen, tap the **Uninstall** button.
5. In the verification window, click **OK** to uninstall the app.

Uninstalling Apps on an Apple Device

1. Long press on the app you want to install. After a few moments all apps will start shaking, and an **x** will appear at the top left corner of every app that can be uninstalled.
2. Tap the **x**.
3. In the dialog box that appears, tap **Delete**.

Privacy Settings

It is important to check the privacy settings on your devices to see what apps have access to what parts of your operating system.

Be cautious when removing permissions from an app, since removal may cause an app to stop working entirely!

Checking Privacy Settings in iOS

1. Open **Settings**.
2. Tap on **Privacy**.
3. Tap on a built-in app to display a list of apps that have access to whatever you selected (ie Photos or Microphone).

Checking Privacy Settings in Android

1. Open your device settings. (Typically available from the list of all applications or by pulling down from the top of the screen to open the system tray, and tapping the gear icon.)
2. From the list of available settings, choose **Apps** or **Applications**. (Depending upon your phone.)
3. Scroll through the list and select an app.
4. Scroll down to Permissions to see what parts of the phone the app is allowed to access.

Types of Security Threats

Individual threats are problems aimed specifically at you, where someone is trying to gain access to your information directly, by fooling or attacking your accounts or devices. An anti-virus program can protect you from threats such as viruses, Trojans, and often spyware. A more robust security suite (often available from the same company that makes anti-virus software) can protect you from snooping and spoofing. A password manager can help you keep robust and unique passwords for all your logins.

External threats are problems that happen on someone else's technology. If someone hacks Jim's Spider Hut, any information you have given Jim's Spider Hut has potentially been stolen: Email address, physical address, phone number.

Yet even with external threats you can take steps to protect yourself: use a unique password for every site and use more than one email address for your various accounts.

Individual threats

Spam: Unsolicited electronic messages (especially advertising).
Viruses: A piece of malicious software that inserts itself into another software program that it uses to replicate itself. Ransomware is a software virus.
Key logging: A device or program that secretly records of the all the keystrokes made on a device so it can be retrieved at a later time by another person.
Browser Hijacking: Where a malicious piece of software modifies a web browser's settings without that user's permission.
Snooping: Unauthorized viewing of or access to data.
Spoofing: Where a malicious actor sends a fake item pretending to be a valid item.

External threats

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.
DNS Hijacking: Where a malefactor redirects visitors from a valid website to an unintended destination.
Denial of Service Attack: 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.

Let me be clear: it's not imperative to understand the technical details of the various security threats, but it is good to have a broad understanding, so that if a threat of some sort is discovered, you'll understand your possible risk.

A good deal of protecting against individual threats means being sensible and vigilant. As easy as technology makes some things in our lives, we do have to work to keep ourselves safe.

Passwords & Passcodes

A password (or pass phrase) is a sequence of letters, numbers, and/or characters used to protect your account or device from access by another entity.

Password Rules

Every website you log into should have a unique password. And those passwords should never been kept somewhere a person would bad intent could easily find them.

The best password is the one stored in your password manager that you never type. (See page 7 for more on password managers). However, device passwords/passcodes do have to be typed, so that's what we're going to focus on here. You want a password that is easy to remember, easy to type, but hard for someone else to guess.

My personal method is to take two objects sitting in front of my computer and combine them into a password:

T-Rex Eats Shuttle!
or
TR3x_3ats_$huttle!
or
TR3x3ats$huttle!

Every time you sit down at your desk you'll see your password reminder, but if the items are scattered among other objects, it won't at all obvious even to someone sitting down in your chair. More importantly, those objects are not phrases that would come up in casual conversation, so a brute force attack would have an extra difficult time.

Another method is to use the names characters from your favorite books, TV shows, or movies (Bonus points for using obscure science fiction characters with weird spellings).

Hester Prynne
Admiral Akbar
Barney Miller

If you can combine those into a phrase, even better:

Barney Miller & Admiral Akbar fight crime!

You'll also want to practice typing a password before you settle on it. The harder it is to type, the more frustrated you'll be. And typing a password on a keyboard and typing a password on a cell phone are two very different things—if you have to type a password on your portable device, make sure it doesn't contain a character that is annoying to type. (See page 24 for a list of password strength checkers.)

If you need a number password, pick a date that you know, but NOT a birthdate associated with your immediate family, such as your best friend's birthday (including year) or dates like you bought your first house.

If you need a pin, type out a word or the name of someone:

JANE = 5263
SLED = 7533
TREX = 8793

Two-Factor Authentication

Two-factor authentication is a system that provides extra security to your account by forcing you to prove you are who you say you are when you attempt to access an account.

The most common form of two-factor authentication is to via text message. The process works like this:

1. You log into a website to do some shopping.
2. The website asks you to prove who you are.
3. You receive a text message on your phone with a code
4. You type that code into the website and continue shopping.

You can also verify via email, or even have a system call you on a land line with the passcode.

The point of two factor authentication is to make it harder for someone to illegally make purchases or check your email or other nefarious tasks. If someone has stolen your username and password, they still can't access your account until they enter a code sent to your email address or cell phone.

You can typically tell a website "This is a personal computer I use all the time" which keeps you from having to verify all the time, but there are some caveats to this.

If it is a portable device, **DO NOT DO THIS**.
If it is NOT password protected, **DO NOT DO THIS**.
If it is a device that is used by visitors (like small children), **DO NOT DO THIS**.

The point of two-factor authentication is to protect you. If you circumvent these protections, you are making yourself less secure.

Password Managers

Every site you should log into should have a unique password.

Every. Single. Site.

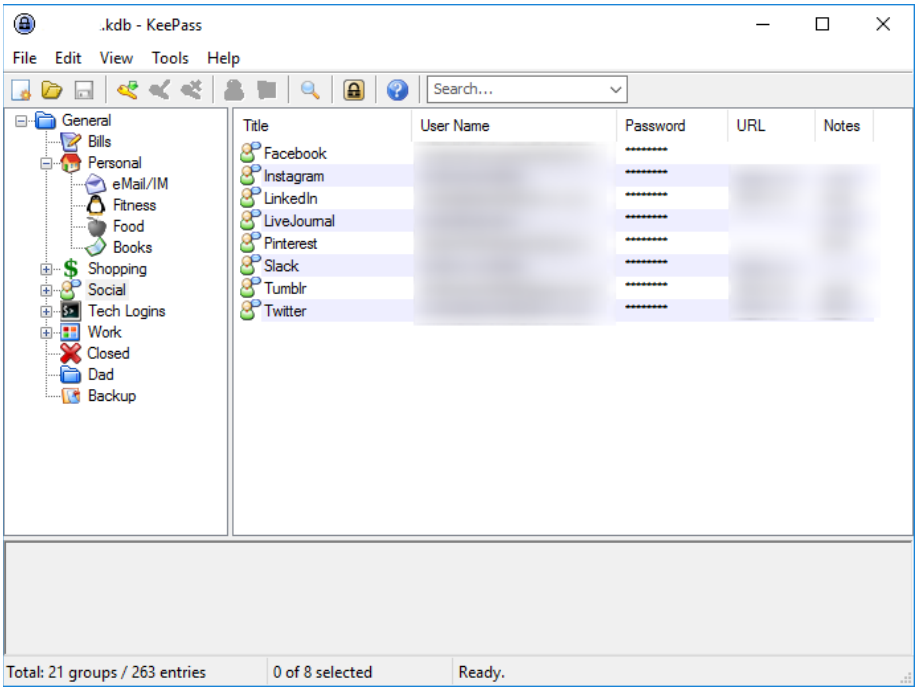
A password manager is an encrypted, secure program that stores user names and passwords for websites, apps, and anything else you want to add. Most password managers have browser add-ins that will do all the heavy lifting for you, making a unique login for every site painless.

Once you have set up your password manager, you should immediately share your login credentials with someone else—a spouse, a sibling, a daughter—that way if something bad happens (you forget your password or you are incapacitated) someone else has all the keys to your digital life.

How does a password manager work?

You store all your usernames and passwords and other information in an encrypted "safe". When you need to log into a website (or program) you copy and paste the username and password from the safe into the website. Most managers also have the ability to auto-fill much of this information for you if you integrate a password manager app into your web browser. (See page 24 for a list of password managers.)

To the right is an example of a password safe (KeePass). You create a variety of groups / folders to organize your login credentials, then populate these folders with individual keys—the user names and passwords and other data for each site or program.

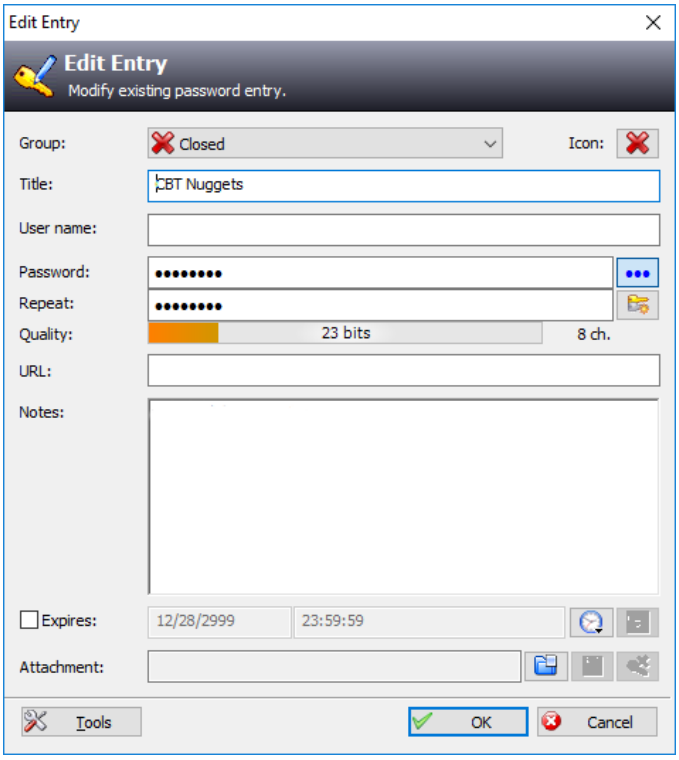


In this program (KeePass), each key, or password entry contains fields for Title, User name, Password, URL, Notes as well as the ability to set a key to expire.

You can store whatever information you want in a notes section, such as:

Security questions and answers
Email address
Account numbers
Previous passwords

Most password manages can auto-generate a jibberish, complicated, password for you, like O|cU~VHfonA"U8FU3gWq. If you never type a password, it's fine to use gibberish, however, if you ***will*** have to type in a password, create something that isn't hideously awful to type in. (See page 7 for hints on creating good passwords.)



Email

Email, short for electronic mail, is a way of sending messages to anyone in the world with access to a device that can read those messages—even eReaders can send and receive email with an internet connection.

All email address contain three bits of information: the user name, the at @ sign, and the domain. (See page 13 for more on domains.) These are put together in the following manner: **username@domain.com**. If you have this information, you can send an electronic message to anyone, anywhere in the world.

Email works by moving data from your device to the recipient's device through a series of mail servers. Mail servers are dedicated computers that shift messages from one place to another.

Your Device <-> Your Email Server <-> Your Friend's Email Server <-> Your Friend's Device

When you receive a message, you generally have three options for responding to that message.

Reply	Respond to the sender
Reply All	Respond to the sender and everyone in to the To or CC fields
Forward	Send the message to a different person entirely

If you do not want to incur the wrath of your friends and family, be cautious when using Reply All.

Email messages are composed of two different parts you can see: the header information and the body. The header information can be thought of as the envelope on a piece of mail—it contains directions for getting the message where it needs to go, information about the sender, and a subject line (to help the recipient and sender keep multiple messages straight). The body of the message contains what the sender wants to tell the recipient.

Email Headers

Headers are lines of text that identify routing information for an email message, including the sender, recipient, date and subject. The To, From, and Date headers are all mandatory and must be displayed. Header information is important because it can generally tell you if a message is valid or not.

Common Header Information

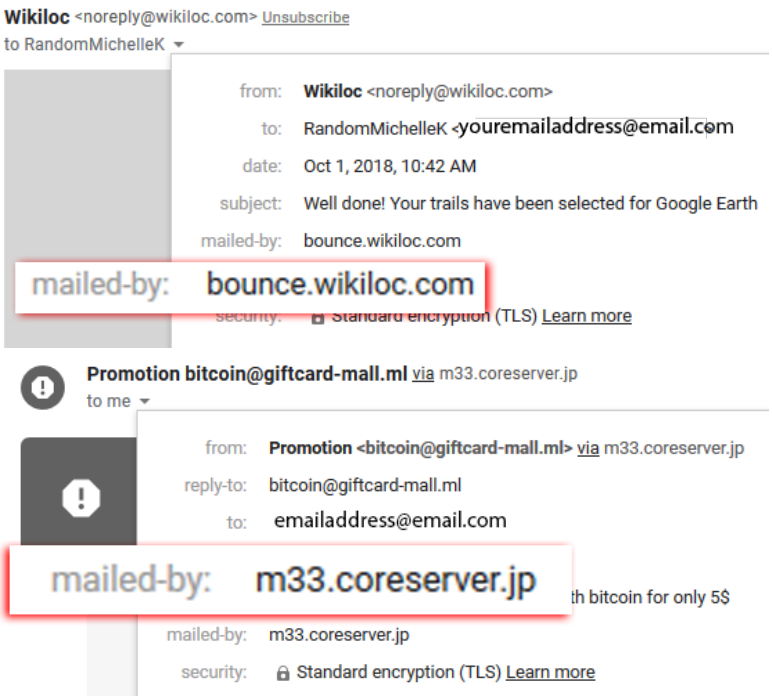
From	Who sent the message
To	Who is the message being sent to
CC	Who is an additional recipient of this message
BCC	Who is secretly being sent this message
Subject	What is this message about
Date and Time	When was this message sent

Email programs hide the complicated bits of the header information from plain sight. Looking at this information can sometimes help you determine if the message you received is genuine or not.

Here are a few common examples of how to view extra header information:

Viewing Header Information in Gmail

1. At the top of the message, click the small triangle at the end of **to (YourName)**.
2. In the pop-up window look at the information to see if there are discrepancies.



Viewing Full Headers in Gmail

1. At the top of the message, on the right side, click the three dots.
2. From the drop down menu select **Show original**.

Viewing Header Information in Yahoo Mail

1. Hold your cursor over the sender.
2. A pop-up menu displays more information.

Viewing Full Headers in Yahoo Mail

1. At the top of the message, on the right side, click the three dots.
2. From the drop down menu select **View raw message**.

Viewing Full Headers in Outlook Online

1. At the top of the message, on the right side, click the down-pointing arrow beside Reply.
2. From the drop down menu select **View message source**.

Viewing Full Headers in Apple Mail

You can't.

Using Multiple Email Accounts

This may not be intuitive, but it is a good idea to have multiple email accounts.

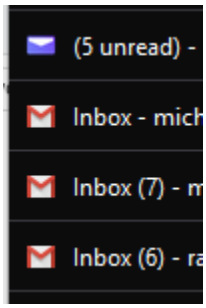
You should have different email accounts for different purposes, such as an account for friends and family, an account for online shopping, and an account for bills and banking. This adds an additional layer of security to your logins, since phishing emails sent to your shopping account are more obvious.

I recommend having at least four separate email accounts: Personal, Shopping, Banking & Bills, Junk.

Multiple email addresses are easy to set up with free online services, and you can generally create as many accounts as you want. Remember, however, when using a free email account, they technically own your email. Do not send private information such as medical records or SSN through email. For a list of free email services see page 25.

There are several different ways to handle multiple email accounts.

One is to keep those accounts open on your web browser all the time. Most services will display an unread message number in the title, letting you know when a new message comes in. (All browsers have an option to “Restore previous session” when opening the browser.)

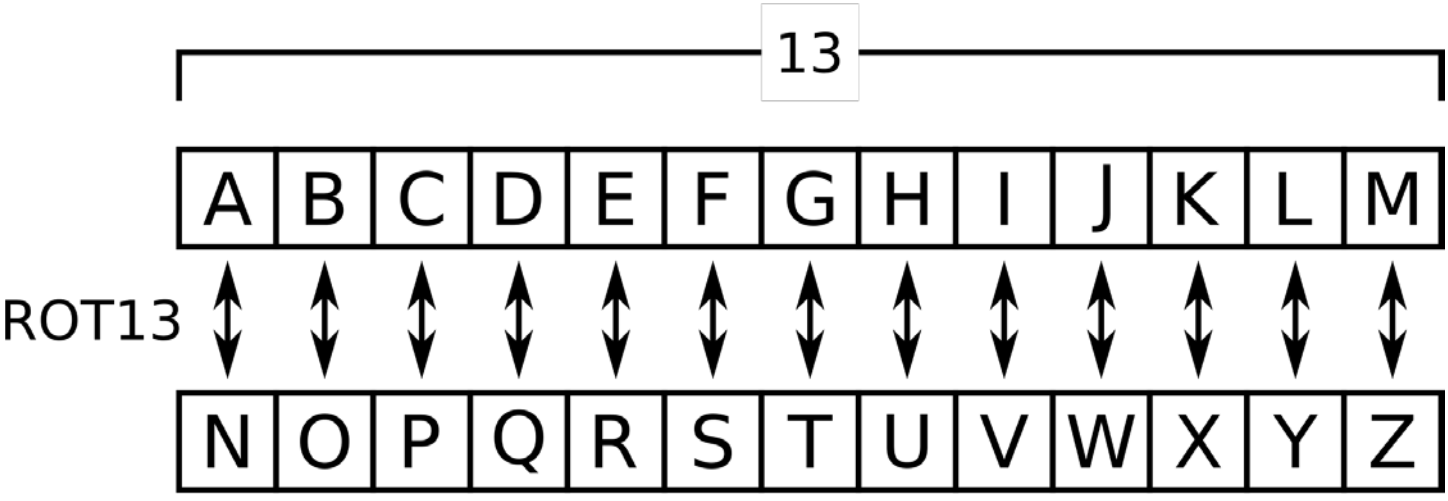


A second option is to install an email program on your computer (a smart phone will have a mail program installed by default). This has the advantage of allowing you to download messages to the hard drive of your computer to keep them for posterity.

Once you have a system set up, check that system every day the same way you would check a single email account.

Encryption

Encryption is the encoding of data so that if it is intercepted it cannot be read by a third party. The simplest form of encryption is ROT-13 (rotate 13 places).



PASSWORD = CNFFJBEQ

Information sent across the internet—especially if across a wireless network—can be intercepted by a third party. If no encryption has been applied, you are essentially shouting out your message for anyone who might be listening to hear. Encryption makes that message unintelligible for someone else to understand, unless they are willing to a LOT of work into figuring out what you said.

The important thing for an end user to know about encryption is if it is being implemented, and how strong the encryption is. Encryption is not something you need to understand, but is something you need to verify before sending data across the internet. (See also https on page 13.)

Web Browsers

A web browser is a program that takes computer code (generally from the internet) and changes it into text and images that you can view and understand. Most computers come with a web browser installed, either Microsoft Edge or Safari. You are not, however, restricted to those default options, and in fact I encourage you to download one or more alternate web browsers.





Why should you use alternate browsers? 1) Because a site that doesn't work in one browser will often work perfectly well in a different browser and 2) because it is far more difficult for websites to track you across browsers and if a site stops working, an easy check is to use another browser. (See page 25 for a list of web browsers)

Cache and Saved Data

Cache is the files your computer has stored behind the scenes to make browsing faster and easier. If something is not working as expected on a website it is often due to your website cache. The first (and easiest) solution is to visit the site using a different browser. The second option is to clear your cache and cookies. This is also important to do after you have changed a website password. (See page 25 for instructions on how to clear browser cache.)

Cookies

Cookies, when they pertain to a website, do not have anything to do with delicious baked goods. Web cookies are tiny pieces of data websites save to your computer while you are browsing. Cookies are how you can place items in an online shopping cart or to have a website remember your user name.

Cookies in and of themselves are good and useful pieces of code. However, they can also be used for evil, tracking you across multiple websites. If you've ever noticed that Facebook has an ad for an item you were recently shopping online for, cookies are the culprit. "Third-party tracking cookies" are the types of cookies that can collect data across multiple websites over time.

Facebook gathers much of its data using cookies and tracks what you do across multiple sites—even if you are not a Facebook user. If you see a Facebook "Like" or "Share" button, there is a Facebook tracking cookie on that page.

Web Forms and Passwords

All browsers will offer to save your form information and passwords. This is convenient but **NOT SECURE**. You should not allow a web browser to auto-fill your password. If you would like your login credentials to be auto-filled, get an add-on for your password manager. (See page 7 for password managers.)

Common Domains

Most people are aware of the more common domains—major businesses use .com—but it's good to know other common domains so you can verify authenticity.

.com	commercial
.org	organization
.net	network
.us	United States
.co	Colombia
.int	international
.mil	military
.edu	education
.gov	government

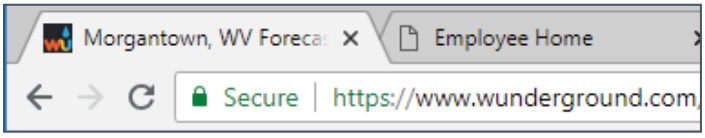
.ca	Canada
.cn	mainland China
.fr	France
.ch	Switzerland
.au	Australia
.in	India
.de	Germany
.jp	Japan
.nl	Netherlands
.uk	United Kingdom
.mx	Mexico
.no	Norway
.ru	Russia
.br	Brazil
.se	Sweden
.es	Spain

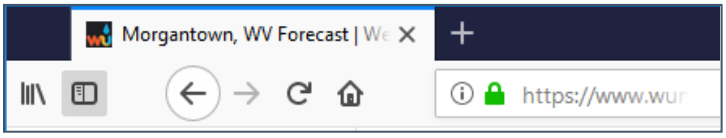
.biz
.info
.jobs
.mobi
.name
.ly
.tel
.kitchen
.email
.tech
.estate
.xyz
.codes
.bargains
.bid
.expert

https

At the start of every URL you will find the letters http or https. http, or HyperText Transfer Protocol, is the method for transferring data between you and a website. **https** (HyperText Transfer Protocol (Secure)) is an encrypted version of this. This means that someone cannot easily capture information shared between you and a website.

HTTPS uses security certificates to verify that a website is who they say they are. If you receive a certificate error, this means either 1) the website is not who they say they are or 2) the website has allowed their security certificates to elapse. Web browsers display https in two ways: a lock icon beside the location bar, and/or by seeing **https** (instead of http) at the start of the URL.





If you are only viewing a website, it doesn't matter much if the site does not have https. But if you do anything involving money or personal information DO NOT proceed unless you can use **htpps**.

Browser Add-Ons

Add-ons allow you to make your web browser behave the way YOU want to it, rather than the way the designers think it should. More importantly, there are add-ons that protect your privacy and security.

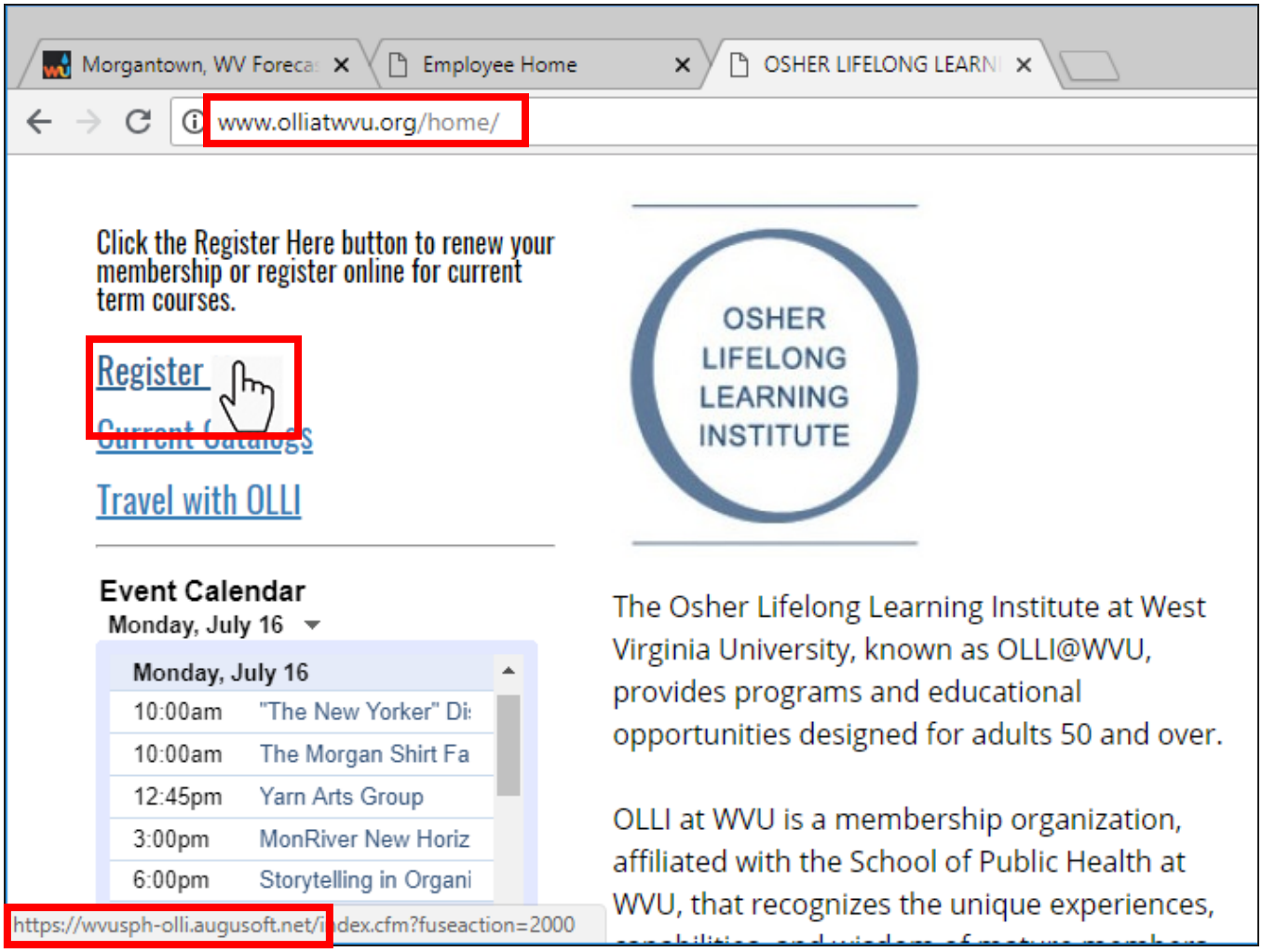
Privacy Add-Ons

These add-ons work to keep third party cookies from sticking their tentacles into everything you do on the internet, to warn you of malicious websites, and to prompt you to be aware of security. (See page 26 for a list of privacy add-ons.)

Hover Text

Phishing emails are messages that pretend to be from a real company, and prompt you to go to a website or reply to a message and give them your username and password. When you hold your cursor over a hyperlink, you can see the URL to which that link is going. This is the best way to avoid a phishing attack.

NO reputable company should EVER ask for your username and/or password over email. If a company does this, it is not one with whom you should be doing business. If you receive an email you think might be fraudulent, do NOT click on any links in that email, but instead go to the site from your bookmarks or open your search engine and look for that company yourself.



A link that redirects somewhere else is not necessarily fraudulent—many websites do not have the capability to process payments and so must send you to a third party website—but if a link is trying to redirect you to an odd domain, it's a distinct possibility the website is fraudulent.

Consider the websites store.ru and store.com ".ru" is a Russian domain while ".com" is generally an American domain.

Search Engines

There are multiple search engines available for your research needs. Google is the most common, but there are many others, all of which use different methods for curating information. Sometimes using a different search engine can give you different results. (A list of reliable search engines is on page 25.)

Reliability

The internet is a wonderful place where you can discover all sorts of amazing things. It is also a place where anyone can say absolutely anything, and it is up to you to ferret out the truth of the matter.

"On the Internet, nobody knows you're a dog."

If there is contention or debate, the easiest way to check is to search for source data. Was the information from a reputable source? Do the majority of sources support what is being said? It is a good idea to familiarize yourself with the kinds of sources that are generally recognized as reputable: a peer-reviewed journal is going to be a reputable source. The National Enquirer is not. The wire services are good starting points for current events and news.

One way to think about reliability is to consider the source. Would you trust a study about the health benefits of that was funded by Anheuser Busch? It's possible this study is valid, but you should look very carefully at their study design and data analysis before accepting their conclusions.

You can also do your own verifications on subjects about which you are familiar, and research from primary sources can help you become familiar with new subjects. If you are unsure how to begin your research, librarians are generally delighted to get you pointed in the correct direction.

You should also ask friends who are experts what resources they trust on their subject or whether an article is based in fact. This can help you get a feel for the reliability of what articles and information are coming to you from other sources.

(See page 24 for the media bias chart.)

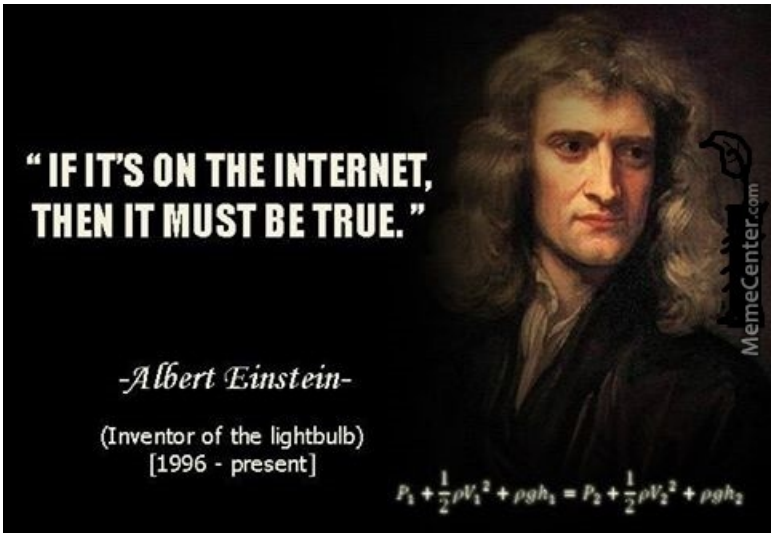
Snopes

86.7% of statistics are made up on the spot.

Snopes is the best known site for debunking lies on the internet. Just because something is being shared widely on Facebook or through email, that does not make it true.

Before you forward the latest awful thing you see, check Snopes or a valid news source.

https://www.snopes.com/



Trusted Tech Websites

Often what you want to search for is tech related—what is the best cell phone or laptop computer—but there are countless websites with reviews of all tech things under the sun, many of which are bogus or set up to push a specific item or site. You can increase the reliability of your results by making you're viewing results from a valid tech websites, such as CNet or Wired. (A list of trusted tech websites is on page 26.)

Social Media

There is a lot of ground to cover with social media—truly, one needs an entire semester-long class to talk about everything—but there are some general rules to follow to make things safer.

Facebook

Facebook is the elephant in the room when it comes to privacy and security—it's the most used website, and its privacy and security issues are all over the news. But because it's the most used site, it's also the best way to keep in contact with friends and family who are scattered across the country and the world.

You can use Facebook safely, but it takes a bit of work, which is of course what the company is counting on. Here's a list of things you can do to make Facebook safer and more private.

- Do NOT use the Facebook app on your phone. Use a web browser on your phone instead.
- Do NOT use the Facebook Messenger app on your phone.
- Install a browser on your computer / device that you ONLY use for Facebook.
- Go through all your Facebook privacy settings.
- Do NOT use Facebook to log into other websites; create credentials for every site.
- Regularly remove third-party apps that have permissions to our account.
- Use privacy and security add-ons to restrict access to your browsing history.
- Create an email address you only use for Facebook.

Something else to consider is what personal information you share with Facebook and share publicly on Facebook.

- Do you want Facebook to have your cell phone number? (This is another data point that can be used as a unique identifier.)
- Do you want your birthdate to be available to everyone on Facebook? (With your first and last name, a birth date can be used as a unique identifier to allow companies to aggregate data.)
- Do you want Facebook to auto-tag you on photos?
- Do you want Facebook to auto-tag you on locations?

All of the above options do have positive uses (ie, if you are named John Smith, having your birthday visible on Facebook might let people find you) but they also may have negative consequences (letting people see you are out of town, FREX). There is nothing wrong with using these convenient services on Facebook.

Other Social Media Platforms

Most of the rules above apply to other social media websites—use add-ons to secure your browsing history, create logins for websites instead of using Facebook or Google for your credentials etc. But you also need to make yourself aware of who owns what in the world of technology, and tech companies might be sharing with the subsidiaries and vice versa.

Besides Facebook, some other popular social media platforms are: Instagram, Twitter, Tumblr, and LinkedIn.

The Big Four

The Big Four Tech Companies are as follows: Amazon, Apple, Facebook, and Google. These are the companies that, with their subsidiaries, dominate the market.

Amazon: Abe Books, Audible, Goodreads, Whole Foods, Zappos
Facebook: Instagram, Oculus VR, WhatsApp
Google: BlogSpot, YouTube
Microsoft: Bing, LinkedIn, Skype

Assume that even if they are not currently doing so, all subsidiaries of a company will share information. This means that unique identifiers like email address can be used to aggregate data across the companies.

You also need to do what no one ever does, and that is PAY ATTENTION TO THE TERMS OF SERVICE.

Luckily, for those who don't have an hour every week to read all the terms of service and the changes that come out every week, you can check out the site TS;DR (Terms of Service, Didn't Read), which points out the positives and negatives of various terms of service. (See page 24)

Wi-Fi

Wi-Fi is the abbreviation for a wireless internet connection. Don't look for the "F" in that, because you won't find it; it's simply a play on the term Hi-Fi.

Wi-Fi is what allows us to not trip over multiple cords when using our laptops on the sofa, to check our email on our phones when we're somewhere without cell service, and to get on the internet away from home and work. It is incredibly convenient but also the easiest way for someone unscrupulous to steal data.

Wi-Fi Security

Wi-Fi security is akin to the locks on your house. If you would not leave all the doors and windows to your house unlocked then you should not leave your home wireless network unprotected.

In your home, unless you live in the middle of nowhere a mile from the nearest neighbor, your wireless network should be password protected and encrypted. If your home is in a high-density residential area, there are additional steps you can take to protect your network, but at a bare minimum, you need a strong password and encryption.

There are multiple things you can do to make your home wireless network more secure, however, it is beyond the scope of this document to explain how to configure various routers. There are online videos and instructions to walk you through the process for your model, but if you feel uncomfortable attempting these things on your own, you should hire a professional to help you.

Steps to secure your home wireless network:

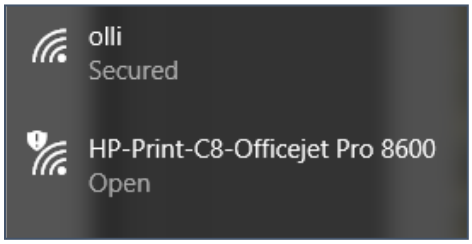
Purchase your own wireless router, rather than using one supplied by your ISP
Create a complex Wi-Fi password
Change the administrator password
Turn on wireless network encryption
Use firewall / security software
Keep your router's firmware up-to-date

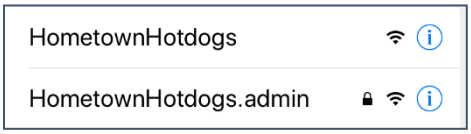
Public Wi-Fi

The best way to protect your data over public Wi-Fi is to not use public Wi-Fi.

Unfortunately, you sometimes have no choice, in which case you need to be *very* careful about *everything* you do while connected to public Wi-Fi, because everything you do can be viewed by an interloper. If you wouldn't yell it in a coffee shop, don't type it over public Wi-Fi. This means you must check the security of the Wi-Fit network you are using before you start checking your email or browsing websites.

You can tell at a glance whether a Wi-Fi network is secured: the operating system will display either a lock icon or the word “Secured” beside the available networks.





It is also important to disable sharing over public networks. Allowing public sharing means unknown devices can snoop around on your device without your knowledge.

Disabling Sharing over Public Networks

Windows: Press the Windows key, type in **Control Panel** and click the link. From the Control Panel, select **Network and Internet**, then select **Network and Sharing Center**, then in the left pane select **Change advanced sharing settings**. Scroll down to **Guest or Public** and turn off “Network discovery” and “File and printer sharing”. Click **Save**.

Mac: Click the **Apple menu**, click **System Preferences**, click **Sharing**, and uncheck the "File Sharing" box.

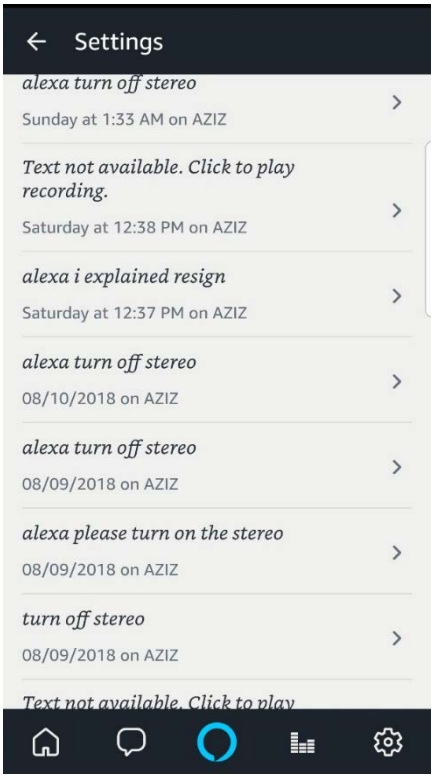
Virtual Personal Assistants

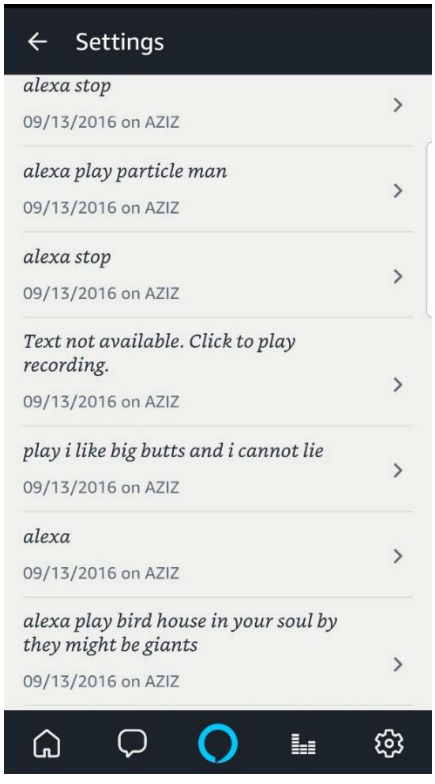
Virtual personal assistants are the programs on your phone like Apple’s Siri, or on devices like the Amazon Echo (Alexa) that that can be controlled by voice commands—anything from adding items to a shopping list to setting a timer or alarm to learning the definition of inconceivable (I do not think it means what you think it means).

These personal assistants are incredibly useful, but they also have potential for abuse.

With some devices, such as Amazon’s Alexa, you can view the entire history of what that device is hearing / listening to, to determine if the device is picking up things you don’t expect or want it to.

Other devices do NOT allow you to view your history. I personally find this problematic, since you are unable to determine if the device is recording unexpected information.





Smart Devices

Smart devices are another modern technology that has amazing applications but could be problematic in implementation. Smart devices give you the ability to place lights on a schedule and check items remotely, but if these devices themselves are not secured, or are connected through an insecure system, you are opening your home to virtual intruders. This isn't a big deal if all you have is a smart light bulb, but if your electronic home locks are tied into an insecure system, the consequences could be far graver.

As with all types of technology, smart devices are not inherently good or bad, however, without proper security they have a risk of negative consequences.

Shopping

If you live in a remote area without access to a variety of local stores, or are limited in your ability to leave your home, online shopping is the best thing ever—all the things you need comes right to your door! And for the most part—especially with large retailers—online shopping is safe and secure.

However, that doesn't mean you shouldn't take precautions.

- Make purchases from known retailers.
- If you're unsure about a retailer, use PayPal to make your purchase.
- Make purchases ONLY with a credit card, NOT a debit card.
- Have a credit card dedicated to online purchases.
- Log into bank site regularly and check for unapproved purchases.
- Bookmark websites you commonly visit.
- Turn off shopping apps on your phone when you're not actively using them.
- Avoid sending credit card information across Wi-Fi.
- NEVER send credit card information over public or unencrypted Wi-Fi.
- Pay attention to logos and website design.
- Carefully check URLs before clicking on links from emails.
- Create an email address that you use *only* for shopping.

PayPal

Most reputable online retailers accept PayPal as a method of payment. If you link your PayPal account to a credit card, this gives you an additional level of protection when making online purchases because the retailer never sees your credit card information—they only receive a transfer of money from PayPal.

Your credit card <-> PayPal <-> Small online business

You do NOT have to link PayPal to your bank account to make purchases, only to accept money.

There are other online payment services available, but PayPal dominates the market and is accepted by most retailers. Some common alternatives are: Square, Amazon Payments, Apple Pay, and Google Wallet.

GPS and Location Services

GPS and location services can be a tremendous benefit: you can use them to find a lost or stolen phone, to track a teenage driver, or to find local restaurants.

On the other hand, GPS and location services can let people know where your house is, where your kids spend their time, and when you're away from home. They can also give companies a LOT of information about your habits.

On a cell phone, your location can be determined from any or all of four services: wireless access points, cellular towers, Bluetooth devices, and GPS. Even if you turn off GPS, your device can determine your location based upon any or all of the other three.

If a website or app requests your location, it's a good idea to consider WHY they need your location before granting them access. A mapping app needs your location to get you from point A to point B. Does a health app really need to know your location?

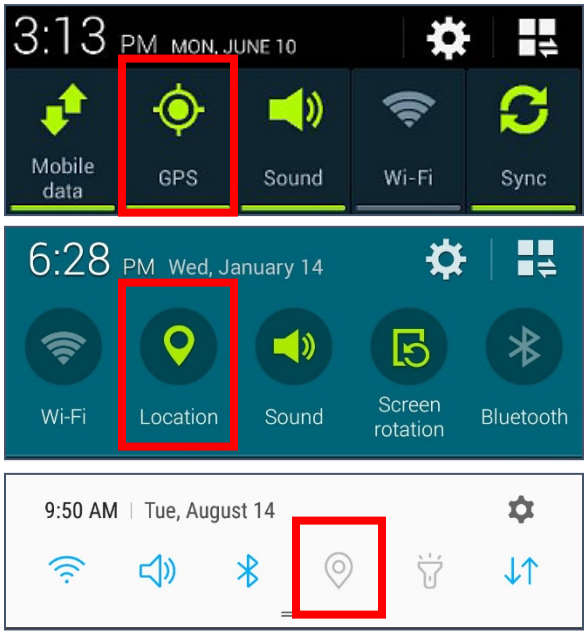
You should also be cautious of attaching location data to your pictures. If you are taking pictures of children, you don't want strangers to know where those children live. If you are on vacation, you don't want people to know you are currently across the country and your home is sitting empty.

My personal rules for location services are:

- Turn off the GPS when I'm not using it (this is contraindicated it you often lose your phone and use "Find My Phone" to locate it).
- Do not attach locations to pictures taken in my home or the homes of friends.
- Do not attach locations to pictures taken of kids.
- Post vacation pictures *after* I'm home.

Toggling GPS on an Android Device

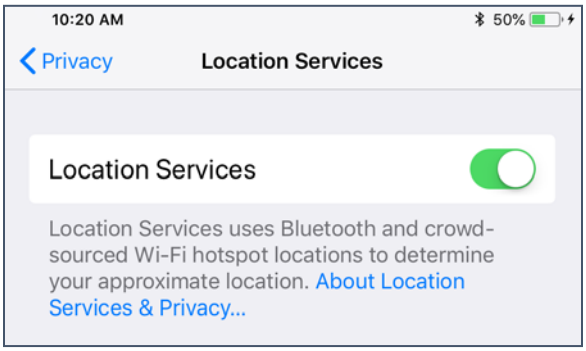
1. Drag down from the top of the screen to view the system tray.
2. Tap the GPS icon to toggle GPS on or off.



GPS services on the iPhone are slightly more difficult to manage. You cannot toggle off just the GPS, but instead must toggle off "Location services" which includes locations from cellular data, wireless, and Bluetooth.

Toggling Location Services on an iOS Device

1. Open **Settings**.
2. Tap on **Privacy**.
3. Select **Location Services**.
4. Tap the toggle to turn location services on or off.



Privacy Settings

Websites, social media sites, email providers, and other online services and content providers have privacy settings that you should go through. Especially if you did not read through the TOS (terms of service) before signing up with the site.

It's important to recognize that with online services, the terms of service can change at any time, and you are not always notified as to those changes.

For all those reasons (and more) it's important to go through the privacy settings of the services you use most frequently.

Accessing Privacy Settings

Google Privacy Settings (Gmail)

Click on your picture (or initials if you do not have a picture associated with your google account).
From the menu select **Privacy**.
Go through the various settings.

Apple Privacy Settings (General)

Log into https://appleid.apple.com
Scroll down to Data & Privacy.
Go through the various settings.

Microsoft Privacy Settings (Outlook)

Log into Office 365: https://outlook.live.com/owa
In the right corner of the web page, click on your name. From the drop down menu, select View Account.
Select Privacy.
Go through the various settings.

Cloud Storage

Cloud storage—when you put files on a server they are available from any device with an internet connection—is incredibly convenient.

What people sometimes forget is that your data is now living on someone else's hardware, which makes you completely dependent upon that company to protect your files. Using cloud storage means you need to balance ease of access with security.

NEVER leave sensitive data in cloud storage. This means tax returns, bank statements, or any other documents that contain information you would not want someone else to steal.

Please note that cloud storage is quite different from a back-up. Services such as Carbonite back up your data in case of loss, but do not necessarily make that data readily accessible—your files are typically encrypted and stored elsewhere. With cloud storage, ONLY the files you have designated as accessible on the cloud are saved if your computer dies, but are accessible at any time from any computer you log into. (or a list of cloud storage sites see page 26.)

Anti-Virus

A virus is a piece of malicious software that attempts to insert itself into your system for evil purposes. Viruses can be written to do anything from completely crash your computer to secretly take over your computer to turn it into a zombie that attacks other computers.

Many new computers come with anti-virus pre-installed. This means the only thing you need to do is check and make sure your anti-virus software is running and up to date. If you choose to select your own anti-virus program, you can get additional bells and whistles to help further protect you, such as a firewall, browser security, junk mail filters, and more.

Anti-virus programs are the exception to the rule about always paying for something—there are several very good anti-virus programs that provide basic anti-virus protection for free. But you should consider paying for a more comprehensive security suite if you regularly spend time online or have a wireless network. (For a list of anti-virus suites see page 24.)

Resources

Internet Domains
https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

Media Bias Chart
https://www.adfontesmedia.com/

Most Common Passwords of 2017
http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

Password Strength Checkers
https://lastpass.com/howsecure.php
http://www.passwordmeter.com/
https://howsecureismypassword.net/

Terms of Service; Didn't Read
https://tosdr.org/

US-CERT Home Network Security Tips
https://www.us-cert.gov/ncas/tips

What Is Encryption?
https://www.techworld.com/security/future-of-technology-in-warfare-3652885/

xkcd
https://xkcd.com

How to Clean Up Facebook App Permissions
1. Open Settings: Along the top of the page, click the **Gear** icon and from the menu select **Settings**.
2. In the left pane, click on **Apps and Websites**.
3. Click the box beside the app from which you want to remove permissions.
4. Click **Remove**.

Anti-Virus and Security Suites

Product	Price	Site
BitDefender	Free	https://www.bitdefender.com/solutions/free.html
Avast	Free / Paid	https://www.avast.com/en-us/index#pc
AVG	Free / Paid	https://www.avg.com/en-us/free-antivirus-download
Trend	$29.95 / 1 year	https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html
Symantec / Norton	$29.99 / 1 year	https://us.norton.com/antivirus
Webroot	$29.99 / 1 year	https://www.webroot.com/us/en/home
F-Secure		https://www.f-secure.com/en/web/home_global/anti-virus
Kaspersky	$29.99 / 1 year	https://usa.kaspersky.com/antivirus
McAffee	$54.99 / 1 year	https://www.mcafee.com/consumer/en-us/store/m0/index.html
Sophos	Free to WVU Employees	https://www.sophos.com/en-us.aspx

Cloud Storage Services

Product	Price	Free Space	Site
Box	$10/mo for 100GB	10 GB	https://box.com
Dropbox	$10/mo for 1TB	10 GB	https://www.dropbox.com
Google Drive	$2/mo for 100GB	15 GB	https://www.google.com/drive
iCloud	$0.99/mo for 50GB	5 GB	https://www.icloud.com
One Drive	$2/mo for 50GB	5 GB	https://onedrive.live.com
SugarSync	$89.88/year 250 GB	0	https://www.sugarsync.com/
Sync.com	$96/year 2TB	5GB	https://www.sync.com

Email Providers, Free

Gmail	https://mail.google.com/
iCloud Mail	https://www.apple.com/icloud/
Mail.com / GMX	https://www.mail.com/
Outlook	https://outlook.live.com/owa/
Proton Mail	https://protonmail.com/
Yahoo	https://login.yahoo.com/account/create

Password Managers

Product	Price	Benefits	Site
1Password	$35.88/year $58.88/year	Family pricing; sharing with authorized users; emergency kit; multi-platform	https://1password.com/
Dashlane	$40/year premium	2-factor authentication; sharing; hacking notifications; multi-platform	https://www.dashlane.com
KeePass	Free (Open source)	Can be saved anywhere but more complicated to use	https://keepass.info/
LastPass	$24/year	2 factor authentication; hacking notifications; multi-platform; browser plugins	https://www.lastpass.com
Roboform	$20/year $40/year	Form auto-fill w/ multiple identities; multi-platform	https://www.roboform.com/

Search Engines

Ask	https://www.ask.com/	Qwant	https://www.qwant.com/
Duck Duck Go	https://duckduckgo.com/	WolframAlpha	https://www.wolframalpha.com/
Google	https://www.google.com/	Yahoo	https://www.yahoo.com/
Google Scholar	https://scholar.google.ca/		

Tech Websites

Ars Technica	https://arstechnica.com/
CNet	https://www.cnet.com/
Gizmodo	https://gizmodo.com/
Lifehacker	https://lifehacker.com/
Techcrunch	https://techcrunch.com/
TechRadar	https://www.techradar.com/
Wired	https://www.wired.com/

Web Browsers

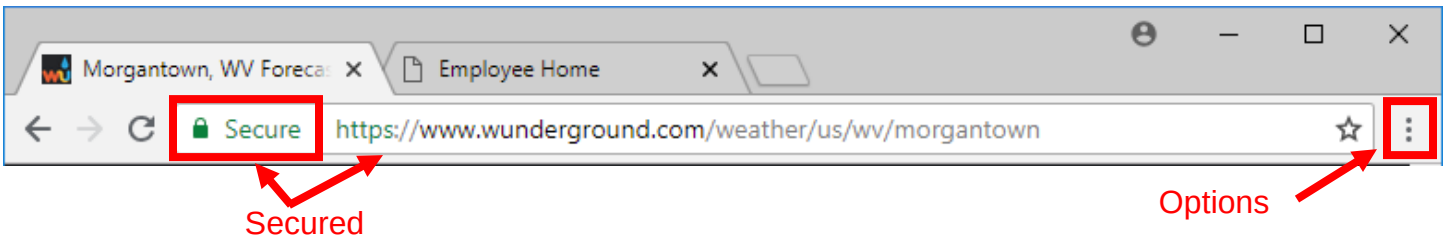
Product	Site
Chrome	https://www.google.com/chrome/
Firefox	https://www.mozilla.org/en-US/firefox/new/
Opera	https://www.opera.com/

Web Browser Add-Ons

Product	Availability	Site
AdBlock Plus	Firefox, Chrome, Safari	https://adblockplus.org/
Disconnect	Firefox, Chrome, Safari, IE	https://disconnect.me/disconnect
Do Not Track Me	Firefox, Chrome, Opera, Safari, IE	https://abine.com/index.html
Ghostery	Firefox, Chrome, Safari, IE	https://www.ghostery.com/
HTTPS Everywhere	Firefox, Chrome, Opera	https://www.ghostery.com/

Browser Settings

Chrome



To Access Your Browser Settings

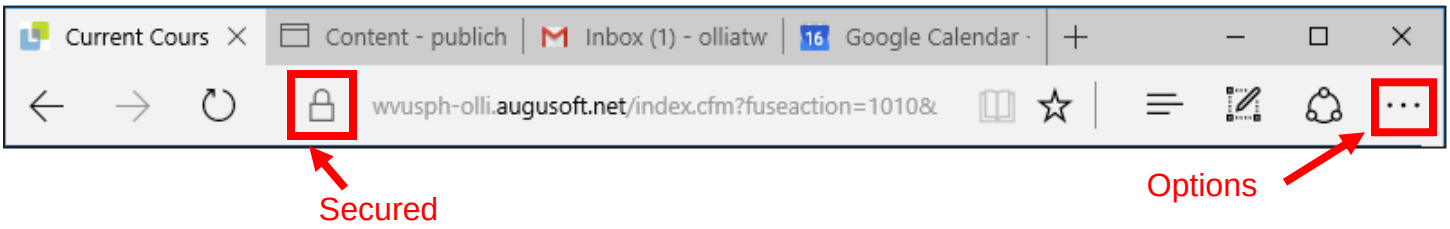
1. Click the **Options** (Customize and Control) button in the right corner of the window.
2. From the menu, select **Settings**.
3. To access additional settings, scroll down to the bottom of the window and click **Advanced**.

To View Add-Ons
1. Open **Options** and from the menu select **More Tools**.
2. From the pop-out menu, select **Extensions**.
3. In the top Left corner, click on the **three parallel lines** beside Extensions.
4. From the drop down menu, click on **Open Chrome Web Store**.

To Clear Cache
1. Open **Options** and from the menu, select **Settings**.
2. Scroll down to the bottom of the window and click **Advanced**.
3. At the bottom of the Privacy & Security section, click **Clear browsing data** and in the pop-up window, set the Time Range as desired, select the items to be deleted, and click **Clear data**.

To Clear Saved Passwords
1. Open **Options** and from the menu, select **Settings**.
2. Scroll down to the bottom of the window and click **Advanced**.
3. Scroll down to the **Passwords and forms** section and click on the **Manage passwords** link.
4. Toggle **Offer to save passwords** and clear any saved passwords.

Edge



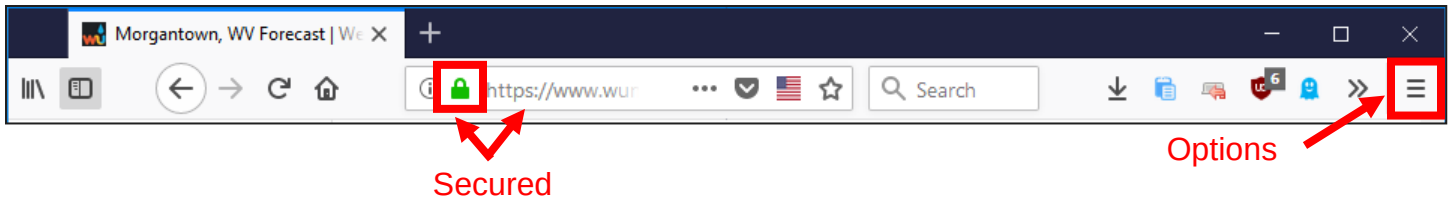
To Access Your Browser Settings
1. Click the **Options** (More) button in the right corner of the window.
2. From the drop down menu select **Settings**.
3. To access more options, scroll down and click the **View advanced settings**.

To View Add-Ons
1. Open **Options** and from the drop down menu select **Extensions**.
2. Click the link for **Get extensions from the store**.

To Clear Cache
1. Open **Options** and from the drop down menu select **Settings**.
2. Click the **Choose what to clear** button.
3. Check the desired options and click the **Clear** button.

To Clear Saved Passwords
1. Open **Options** and from the drop down menu select **Settings**.
2. Scroll down to the bottom of the menu and click the **View advanced settings**.
3. Scroll down to the Privacy and services section and toggle off **Offer to save passwords**. Click on **Manage my saved passwords** to delete existing saved passwords.

Firefox



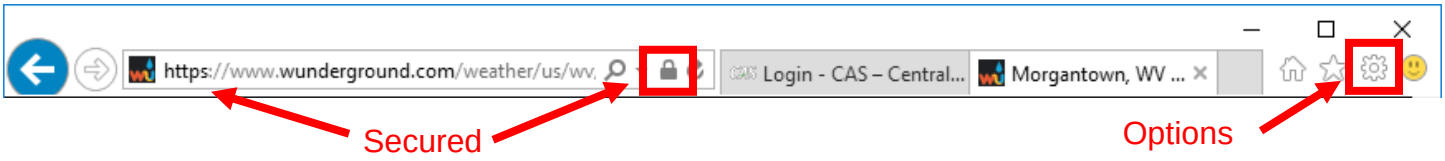
To Access Your Browser Settings
1. Click the **Options** (Open menu) button in the right corner.
2. From the drop down menu select **Options**.
3. Along the left side select **Privacy & Security**.

To View Add-Ons
1. Click the **Options** (Open menu) button in the right corner.
2. From the drop down menu select **Add-Ons**.
3. In the text box in the top right corner, enter a search term for an add-on (such as privacy).

To Clear Cache
1. Click the **Options** (Open menu) button in the right corner.
2. From the drop down menu select **Options**.
3. Along the left side select **Privacy & Security**.
4. In the Cookies and Site Data section, click the **Clear Data** button.
5. Check both options and click **Clear**.

To Clear Saved Passwords
1. Click the **Options** (Open menu) button in the right corner.
2. From the drop down menu select **Options**.
3. Along the left side select **Privacy & Security**.
4. In the Forms & Passwords section, uncheck Ask to save logins and passwords for websites.
5. Click the Saved Logins button to delete existing saved data.

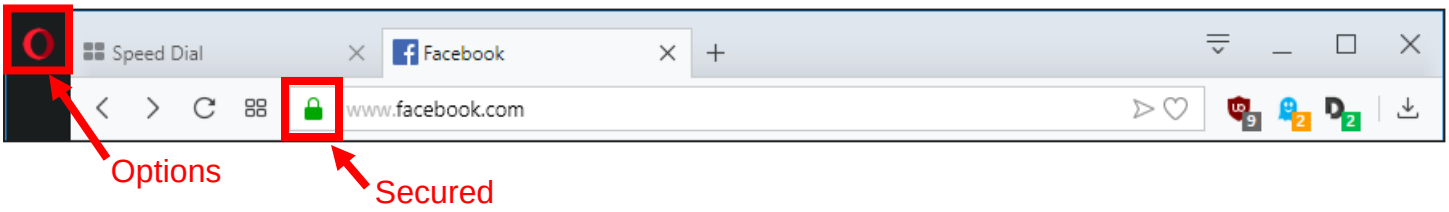
Internet Explorer



To Access Your Browser Settings
1. Click the **Options** button in the right corner.
2. From the menu select **Internet Options**.
3. Along the top select the **Security** tab or the **Privacy** tab.

To Clear Your Cache and Delete Saved Passwords
1. Click the **Options** button in the right corner.
2. From the menu select **Internet Options**.
3. In the Browsing history section, click **Delete**.
4. Select the options to remove and click the **Delete** button.

Opera Settings



To Access Your Browser Settings
1. In the top left corner, click the red **O**.
2. From the drop down menu select **Options**.
3. In the left pane select **Privacy & Security**.

To View Add-Ons
1. In the top left corner, click the red **O**.
2. From the drop down menu select **Extensions** then from the pop-out menu select **Extensions**.

To Clear Cache
1. In the top left corner, click the red **O**.
2. From the drop down menu select **History**, then select **Clear browsing data**.
3. Select the desired time frame and the desired items to erase, then click the **Clear browsing data** button.

Index

Technology Glossary

Add-on: An accessory piece of software designed to increase the capability of the software to which it is appended.

Android: Googles mobile operating system, built on open source software.

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.

App: Short for Application.

Apple: Technology company that designs and develops hardware and software.

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.

BCC: Blind carbon copy. Secretly send a copy of the message to someone else. The primary recipient cannot see that this person received the message.

Bluetooth: A wireless technology that allows data to be shared over short distances using short-wave UHF radio signal.

Browser: Short for Web Browser.

Browser Add-on: See Browser Extension.

Browser Extension: A small software module that is used to customize a 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.

CC: Carbon copy. Send a copy of the message to someone else. The primary recipient can see this person received the message.

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.

Codec: A device or program that encodes/decodes a data stream, such as an audio file, for storage.

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.

Email Header: The portion of an email message that contains the routing information. The header can be used to help determine if a message is fraudulent.

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.

Facebook: An online media and networking company.

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

Force Stop: A way to completely stop an app that is running in the background. An app that has been closed may still have bits active and collecting data.

Google: A technology company that specializes in serves and products related to the internet.

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.

Hover text: When you hold your cursor over a hyperlink, the document should display the URL for that link. This allows you to verify links.

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.

Install: A process that writes the code used to run the program (application) onto the hard drive of your device. Installing a piece of software embeds it into the device and allows it to work.

Internet: A system of inter-connected computer networks.

iOS: Apple's mobile operating system.

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 with pictures or audio, as well as messages longer than 160 characters or to multiple people.

Network: A group of computers connected for the purpose of sharing resources. A network can be as small as two computers or as vast as the Internet.

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: The secret code to access a restricted resources. Passwords are usually required to use a minimum of eight characters, and contain special characters, such as numbers or upper case letters.

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.

Privacy: The information that is shared between your device and the external resources to which it is connected, as well as how that information is used, and with whom that information is shared.

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.

Reply: A response to an electronic message.

Reply All: A response to an electronic message that is returned to ALL recipients of the original message.

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.

ROT-13: One of the most basic forms of encryption; a substitution encryption where characters are rotated 13 places.

Router: A networking device that forwards data between devices.

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.

Security: Protecting electronic systems from theft or damage. This can be protection from physical theft, but often refers to electronic damage, where systems can be disrupted or data stolen.

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.

Smart Device: An electronic device that connects to other devices or the internet through a wireless protocol such as Bluetooth or Wi-Fi.

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.

Snopes: One of the first internet fact-checking resources, Snopes started as a site to debunk urban legends, but expanded into general fact-checking. (https://www.snopes.com/)

Social Media: Interactive computer technologies and websites that allow for the sharing of information. Facebook is the most famous social media site, and allows friends to connect automatically, but LinkedIn is another type of social networking site, that focuses on career and job networking.

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.

Terms of Service: The rules you agree to abide by when you sign up use an online service.

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.

TLDR: Too Long, Didn't Read

TOS: Terms of Service

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.

TXT: Text message.

Uninstall: The removal or a software program or application from the operating system of a device. Although uninstall removes the visible aspects of a program, there are often bits and pieces of the program left behind.

Upload: To move files from your computer to a cloud service or network.

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.

Username: Also called Account name, login IS, user ID. The credentials you use to access an electronic resources, such as your computer or a website. Every account on a website or device must be unique to that service, so as to keep account information separate.

USB: Short for Universal Serial Bus, this is the industry standard for cables that connect devices and their peripherals through a wire. This connection can be used for both communication and power. There are several types of USB connections: USB, USB-mini, USB-micro, and the newest standard: USB-C.

Virtual Personal Assistant: A software program that preforms tasks or services based upon verbal commands. Some of the most well-known services are Siri and Alexa.

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
Phone Numbers:

Office: (304) 293-1793
Email Address: olli@hsc.wvu.edu

http://www.olliatwvu.org