Technology Security

When using the electronic version of this handout, there are hyperlinks throughout—including the table of contents—that will allow you to jump right to a specific section or definition or definition.

Table of Contents

Updated: 29 April 2025

Sessions

Don't Be Fooled
Staying Safe
Protecting Your Data
Devices & Social Media

Rules to Live By

Lock Your Phone!
Password Protect Your Computer!
If you are not paying for something then YOU are the product!

Smart Phones

Smart phones have become an essential tool for a majority of Americans (and others around the world). They allow us to go out and about instead of sitting home waiting for a call, and even better, can answer pressing questions such as "Who was the star of the *Wild Wild West* and when did he die?" or "What is that flower I see in the woods each spring?"

There are currently two main flavors of smart phone on the market: Apple devices, and Android devices. Other operating systems (like Windows phone) exist but have a much smaller market share.

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.

Phone Cables

A new cell phone can cost as much as $1000 dollars. A $2 charging cable + a power surge unregulated power can turn your expensive phone into a slab of electronics.

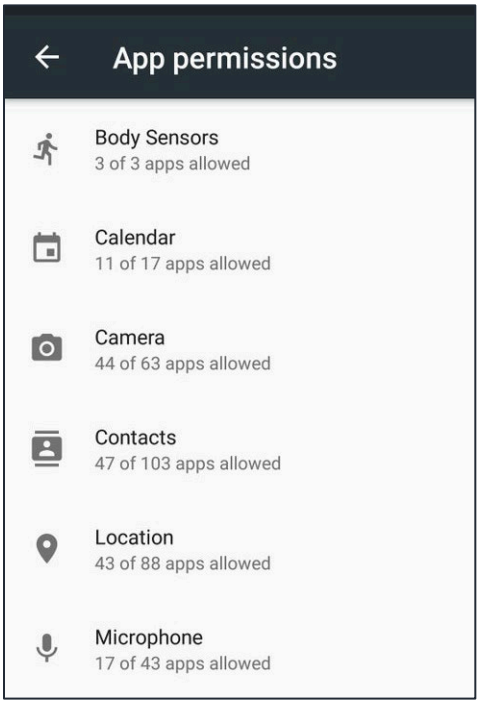
More distressingly, chips are now so small that charging cables can have built-in programs to install spyware on your device without your notice. Buy quality cables and keep one with you.

Phone Apps

Similarly, if you paid $750 for your phone, a $1.99 app is 0.3% of the cost of your phone. Downloading a "free" app with malicious code or permissions because you don't want to spend a couple dollars for an app 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 or a version with ads. Try out an app and once you decide if like it purchase the full version. Purchasing apps protects you *and* supports entrepreneurs.

It is extremely important to pay attention to what permissions your apps have. Does a coupon app need to access your camera AND location AND email AND contacts? What about a solitaire game? If an app wants permissions to access all areas of your phone, be cautious and look for alternatives before installing.



You should regularly go through the apps on your phone and uninstall the ones you don't use.

You have the option with most phones to back up some or all of your data to the cloud. Whether and how you choose to do this depends 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 about doing so. (See page 26)

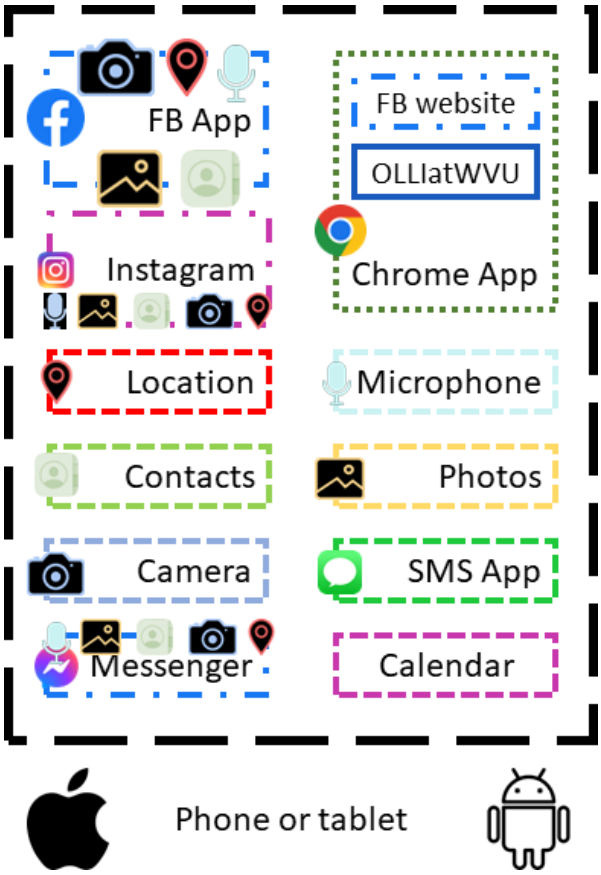
Closing and Removing Apps

If you are no longer using an app you should uninstall it—you can always reinstall it later if you need it.

On an android device, you have the ability to force stop an app. This keeps it from running in the background—and collecting data in the background.

Phone Privacy Settings

Check the settings on your device to see what access apps have. Some apps allow you to remove specific permissions (ie location), but that is opt *out*, and the app will claim it might break forever if you do so. If an app doesn't work after removing permissions, just add them back.



Data Collection

Your cell phone collects a ton of data about you—more than you probably imagine. And the companies that provide those apps use that data for a variety of reasons—primarily to better sell you things.

The data collected by cell phone apps includes (but is not limited to!):

- Usage Data
- Purchases
- Location
- Contact Info
- User Content
- Search History
- Browsing History
- Financial Information
- Health & Fitness
- Biometric Data

This data is used for everything from picking your image out of someone else's pictures (biometric data) to knowing where you spend your time (location data) to who you are related to (contacts). Once companies have that information, you are entirely dependent upon them to use it ethically, which—as we saw with Cambridge Analytica--doesn't always happen.

Even well-meaning uses can have negative consequences. In 2018 the running app Strava created a heat map of user data which was then used to learn the location secret military bases—because there were people exercising in places that were supposedly empty.

A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap

In January 2021, a lack of security on the Parler website and app allowed outsiders to scrape 70 terabytes (TB) of data. "The scrape includes user profile data, user information, and which users had administration rights for specific groups within the social network."

This was not a hack, simply a security failure.

The data retrieved included pictures and videos, none of which had location data removed. In a *couple of hours*, hackers were then able to create a map of where videos had been recorded and link everything together. This allowed *anyone in the world* to look at a map and find and view videos recorded at that precise location.

If this is what hackers can do in a couple of *hours*, I want you to seriously consider what these companies like Facebook can do with all the data they have been collecting about you for *years*, and if you trust these companies to use that information in a way that does not harm you.

Threats

Individual threats

Individual threats are those 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 can protect you from other types of threats. A password manager helps you keep robust and unique passwords for your logins.

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.

Malware: A piece of software specifically designed to disrupt, damage, or gain unauthorized access to a computer system, often to steal information or resources

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

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. You can't do anything about it. Yet even with external threats you can take steps to protect yourself: have a unique password for every site and use multiple email address.

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*** important to understand the technical details of the security threats, but it is good to have a broad understanding, to help you understand your possible risk in a situation.

A good deal of protecting against individual threats means being sensible and vigilant. As easy as technology makes some things in our lives, we 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 be kept somewhere a person with bad intent could easily find them.

The best password is the one in your password manager you never type. (See page 8). However, device passwords/passcodes *do* have to be typed, so you want a password that is easy to remember, easy to type, but hard for a stranger to guess.

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

T-Rex Eats Shuttle!

OR

TR3x_3ats_Shuttle!

OR

TR3x3atsShuttle!

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 be obvious to a stranger. 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).

Admiral Akbar
Barney Miller

Then you can combine those into a phrase:

Barney Miller & Admiral Akbar fight crime!

You'll want to practice typing a password before you settle on it. The harder a password 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.

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 a date such as when you bought your first house.

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) 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.

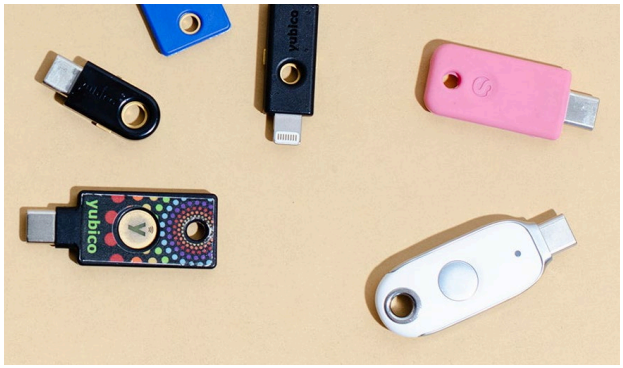
The most common form of 2FA is via text message but there are other kinds as well. The process with a cell phone works like this:

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 cell phone with a 6 to 9 digit number
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.

A second type of 2FA is a separate program that prompts you (usually on a smart phone) to verify you are trying to access a system. WVU uses DuoMobile for this—you log into a WVU website and it sends a command to your smart phone you must acknowledge before you can access the site.

A third type is a device (like a USB key) that must be inserted into the computer for a program to open. I use a device called a Yubi key to protect my password database.



This type of device is more complicated to set up, but extremely secure. If you choose this method you will need to make sure you purchase MULTIPLE keys, all configured the same, so you do not lose access to your files if you lose your (only) key.

Two-factor authentication exists to make it harder for someone to maliciously access your accounts and devices. Even if someone has stolen your username and password, they still can't access your data without the 2FA step.

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:

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 log into should have a unique password.

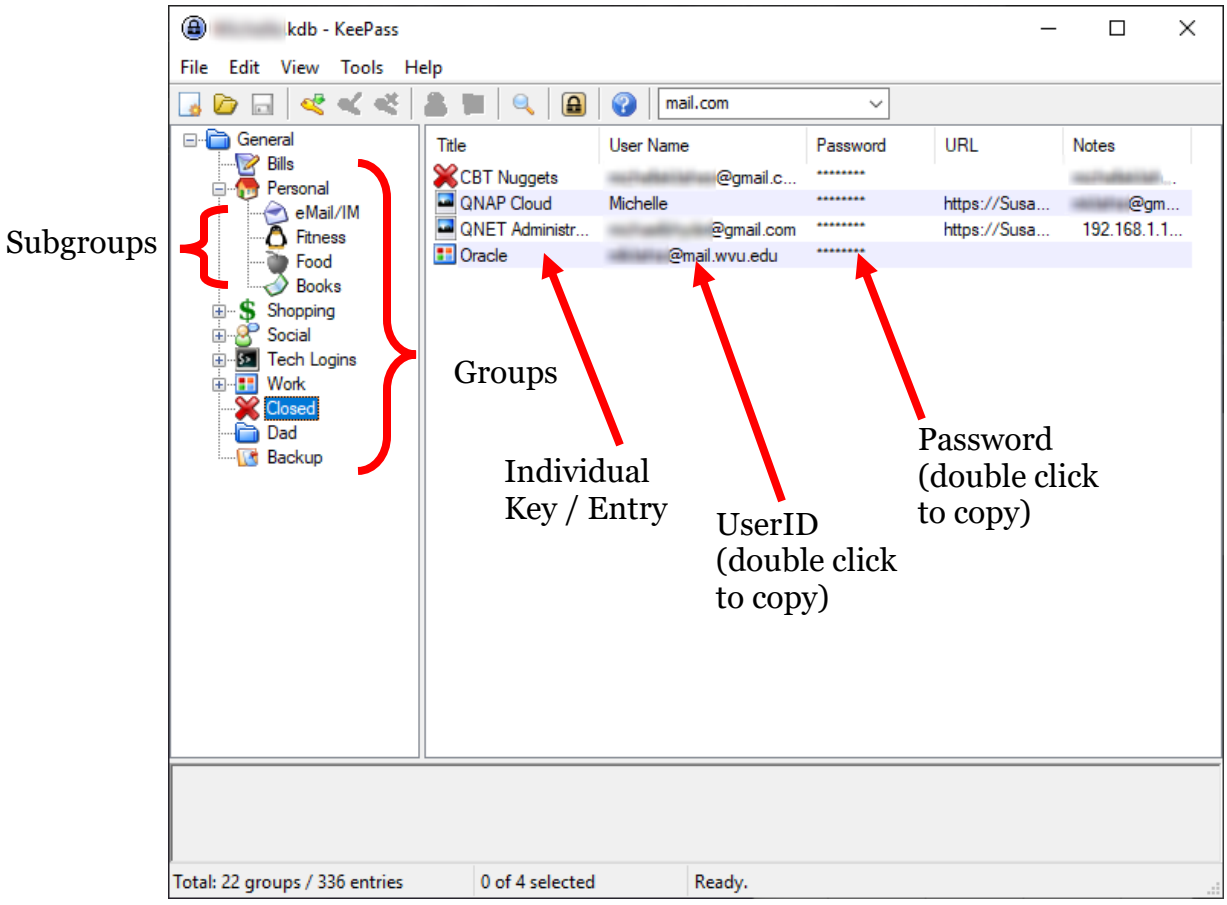
Every. Single. Site.

A password manager is an encrypted, secure program that stores user names, passwords, and other information for websites, apps, and programs. 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 29 for a list of password managers.)



Above 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 usernames 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**, and **Notes**.

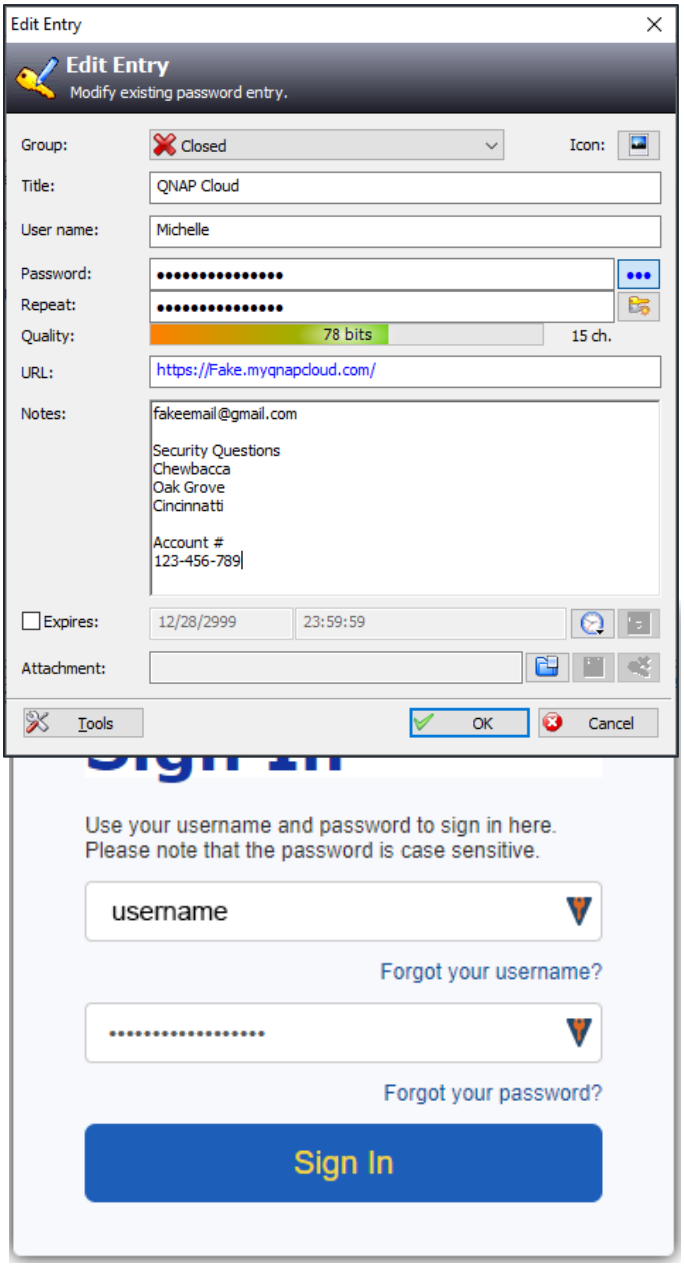
You can store whatever information you want in a notes section, such as:

- Security questions and answers
- Email address
- Account numbers
- Previous passwords

Most password manages can auto-generate a gibberish, complicated, password for you, like O|cU~VHfonA"U8FU3gWq. If you never type a password, that is fine to use, however, if you ***will*** have to type in a password, create something that isn't hideously awful to type in. (See page 8)

Once you have set up your password manager, and installed your browser Add-In (see page 15) for that password manager, when you visit a site, you will see prompts for automatically inserting your password. You can also copy and paste your user name and password from the manager.

You should also have the ability to save new credentials to your password managers from your web browser, as you create them.



Email

Email is a way of sending electronic messages to anyone in the world with access to a computer, smart phone, or tablet with an internet connection—even eReaders.

All email address contain three bits of information: the user name, the at @ sign, and the domain. (See page 13) These are put together in the following manner: **username@domain.com**.

Email works by moving data from your device to the recipient's device through a series of mail servers (dedicated computers that shift data 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

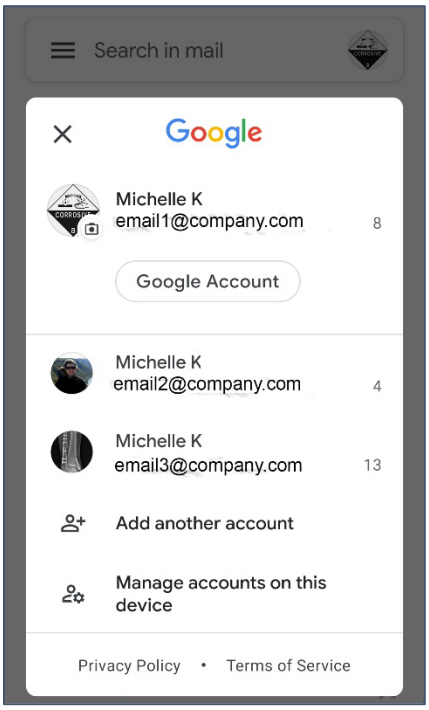
Headers are lines of text that identify routing information for an email message, including the sender, recipient, date and subject. The To, From, and Date headers are all mandatory and must be displayed. Header information is important because it can generally tell you if a message is valid or not.

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. Why do you care? Because looking at this information can sometimes help determine if the message is genuine.

Multiple Email Accounts

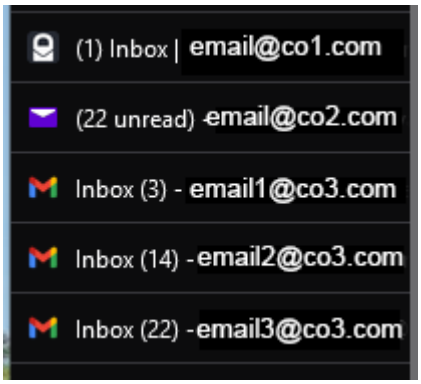


This may not be intuitive, but it is a good idea to have multiple email accounts.

You want different 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, making phishing attempts more obvious.

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

Multiple email addresses are easy to set up with free services, and you can generally create as many accounts as you want. (See page 29)



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 so you never have to open each tab individually.)

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 save them for posterity.

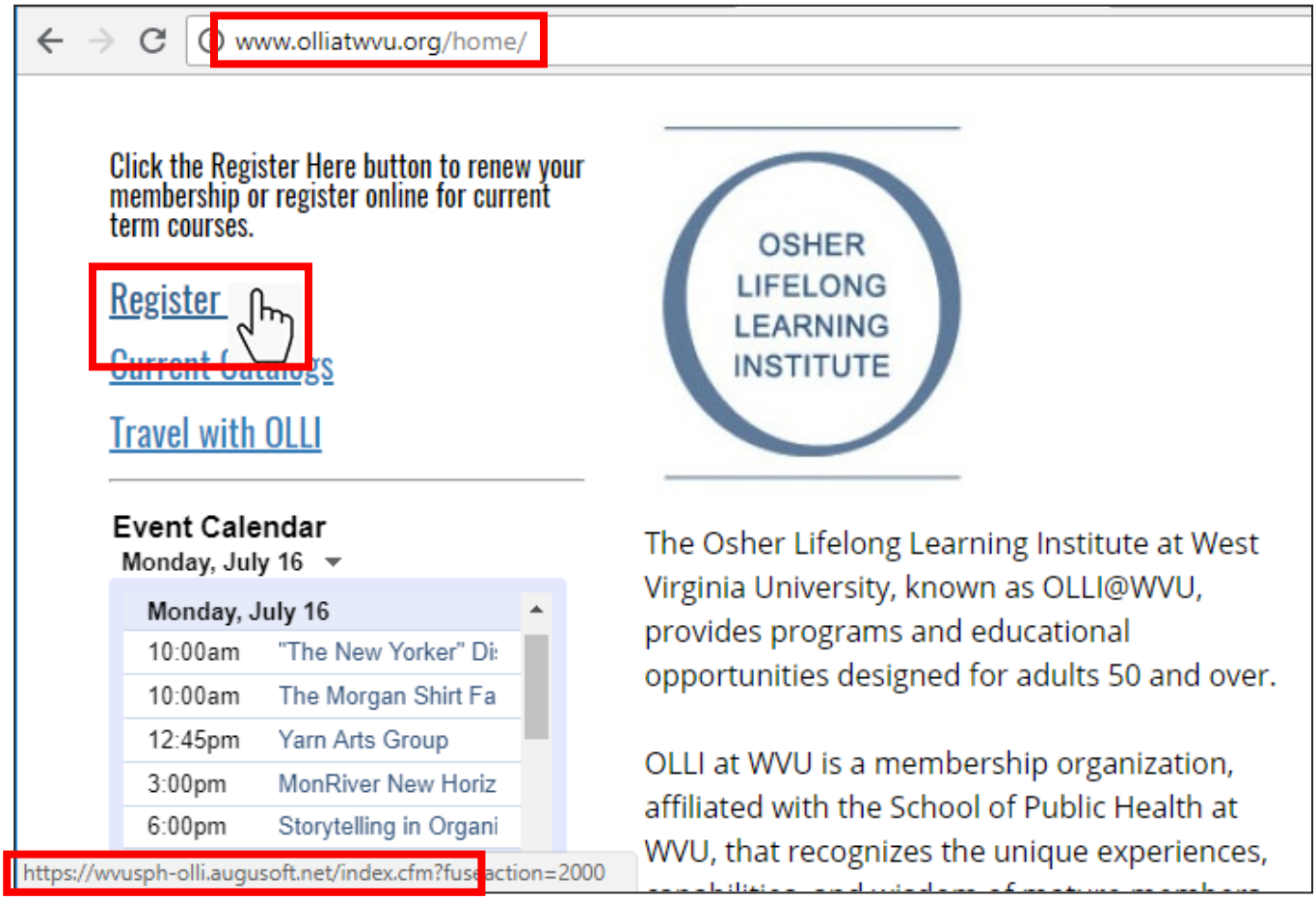
Once you have a system set up, check that system every day the same way you would check a single email account.

Do not send private information such as medical records or your SSN through email.

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.

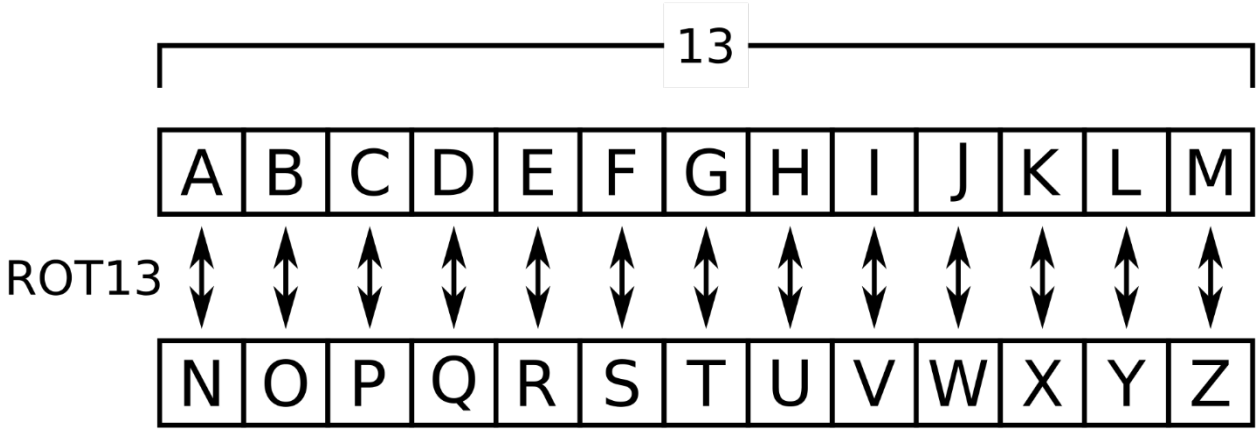
NO reputable company should EVER ask for your username and/or password over email. If a company does this, it is not one with whom you should be doing business. If you receive an email you think might be fraudulent, do NOT click on any links in that email, but instead go to the site from your bookmarks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

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 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 put a LOT of work into figuring out what you said.

The important thing to know about encryption is *if it is being implemented*. (See page 14)

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

Note that different countries have different domains. What this means is that if you are in the US, you should be suspicious if the site you end up on has am unexpected domain, such as .ru (Russia) or .ml (Malaysia).

Web Browsers

A web browser is a program that takes computer code (generally from the internet) and changes it into formatted text and images 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 I encourage you to download one or more alternate web browsers. See page 30 for a list of web browsers.




Why should you use alternate browsers?

1. A site that doesn't work in one browser will sometimes work perfectly well in a different browser
2. It is far more difficult for websites to track you across browsers
3. If a site stops working an easy check is to visit the page in another browser.

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, which is also important to do after you have changed a website password. (See page 30)

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 username.

Unfortunately, cookies can be used by "third parties" to track what you are doing, and Facebook does a lot of this. If you see a Facebook "Like and Share" button on a web page, then Facebook is collecting information about what you are doing on that page.

Facebook collects this information whether you have a Facebook account or not.

Facebook collates and uses this information **whether you have a Facebook account or not**.

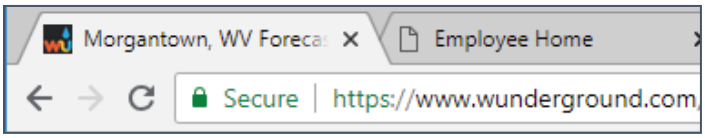
Web Forms and Passwords

All browsers will offer to save your form information and passwords. This is convenient but **NOT SECURE**. If you would like your login credentials to be auto-filled, get an add-on for your password manager. (See page 8)

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 or HyperText Transfer Protocol (Secure) is an encrypted version of http. 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 lapse. 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.

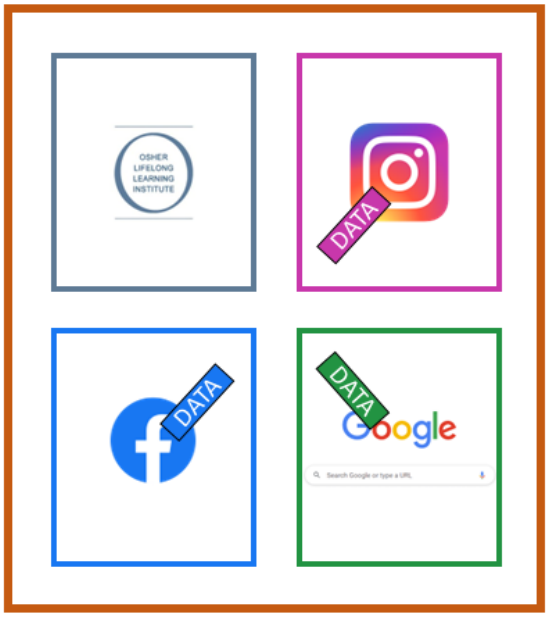


If you are only viewing a website, it doesn't matter if the site does not have https. But if you do anything involving money or personal information DO NOT proceed unless you can use **htpps**.

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.

Firefox Web Browser



Firefox Web Browser
With Privacy Add-On

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 30)

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. Using a different search engine usually gives you different results. (See page 30)

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.

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 beer 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.

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

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 28)

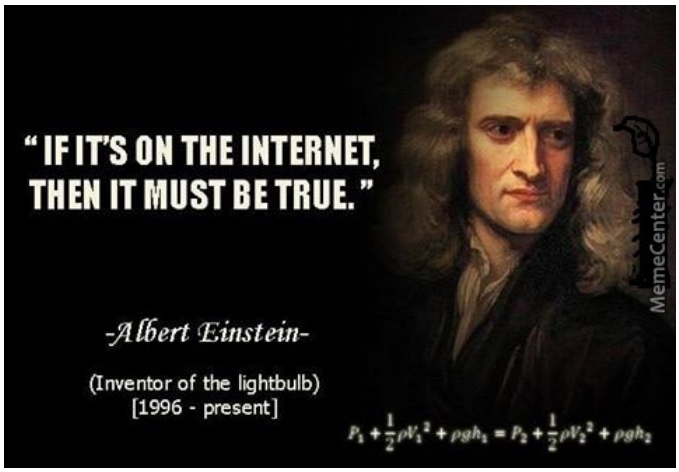
Fact Checking

- Accepting a fake friend request will give hackers access to ALL your online information!
- People have died after sniffing poisonous perfume samples!
- People have died drinking a mixture of Coca-Cola and Mentos!
- 86.7% of statistics are made up on the spot!

There is a LOT of false information circulating out there. Don't make it worse by sharing dubious but intriguing articles without checking their veracity.

In general, if a post invokes a strong emotional reaction from you (especially rage) it is more likely to be false or misleading.

There are several unbiased fact checking websites. I recommend them as an antidote to almost everything you see on Facebook. (See page 28)



Correlation vs Causation

Correlation means there is a relationship between two or more variables. Ice cream sales are directly correlated with shark attacks.

Causation means one of those variables directly causes the other. Heat waves cause an increase in the use of air conditioning. Ice cream sales to NOT cause an increase in shark attacks. The two are related, because both occur when the weather is hotter, but one does not cause the other.

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 viewing results from a valid tech websites, such as CNet or Wired. (See page 30.)

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, IMDB, Ring, Whole Foods, Zappos
~~**Facebook**~~ **Meta**: Facebook, Instagram, Messenger, Oculus VR, WhatsApp
~~**Google**~~ **AlphaBet**: Google, BlogSpot, YouTube
Microsoft: Bing, LinkedIn, Minecraft, Nokia, Skype

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

Terms of Service

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

> *ARBITRATION NOTICE: You agree that disputes between you and us will be resolved by binding, individual arbitration and you waive your right to participate in a class action lawsuit or class-wide arbitration. We explain some exceptions and how you can opt out of arbitration below.*

The Terms of Service for an app or program (or anything) outline what rights you have and what responsibilities the service provider has. These are generally written to give the service provider minimum responsibilities and the user minimum rights. Can the service provider share your data (pictures, phone number, vital statistics) with other companies? If you are harmed or your device is broken, who is responsible?

> *However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.*

Amazon Lumberyard

In general, these terms will be in the favor of the company.

- **We do not claim ownership of your content, but you grant us a license to use it.** Nothing is changing about your rights in your content. We do not claim ownership of your content that you post on or through the Service and you are free to share your content with anyone else, wherever you want. However, we need certain legal permissions from you (known as a "license") to provide the Service. When you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Service, you hereby grant to us a non-exclusive, royalty-free, transferable, sub-licensable, worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This license will end when your

Instagram

User Tracking

You've probably noticed that when you shop for something, ads in Facebook immediately appear for that item. This is neither coincidence nor black magic, but is due primarily to two things (there are others, but these are the important ones): unique identifiers and web cookies.

Unique Identifiers

If you want to understand how to make your online presence more secure and more private, you need to understand the basics of how companies collect and collate your data in the first place.

When you log into Facebook, your login credentials require your email address. This email address is your unique identifier.

How does this work? Because your email address unique to you, every time it appears in an advertiser database, it is directly linked to your Facebook account. If you use the same email address for everything, all your data *could* become aggregated into a single file.

Just how important are these unique identifiers to Facebooks business model? When Apple rolled out its iOS with App Tracking Transparency in 2021, Facebook estimated that change would cause it to lose around $10 billion dollars.

Facebook

Facebook is the elephant in the room when it comes to privacy and security—it's used around the world and has a terrible reputation for privacy and security. But because it's so widely used, it's also the best way to keep in contact with friends and family who are scattered across 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.
- 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 your 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 on Facebook.

- Do you want Facebook to have your cell phone number?
- Do you want your birthdate to be available to everyone on Facebook?
- Do you want Facebook to auto-tag you on photos?

All of the above options do have positive uses (ie, if you are named John Smith, having your birthday visible on Facebook might help people find you) but they also may have negative consequences (letting people see when you aren't home).

Other Social Media Platforms

These rules also apply to other social media websites: use add-ons to secure your browsing history, create unique 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.

Information Security and Social Media

With any social media platform, your information security should always be a top consideration. Remember, your email address is a unique identifier, so all sites for which you use the same email address have the *ability* collaborate and tie together your data.

Cookies and other browsing data can sometimes be shared between sites, and such data can reveal far more information than you might expect. For example, Target can predict whether a woman is pregnant based upon her purchase of unscented lotion, vitamins, and cotton balls. You are giving away far more information than you think when you browse the web, and when that data can be tied to a social media account, the company has *even more* data.

Ways to protect your privacy

- Use multiple email addresses
- Check your settings on your social media accounts
- Limit use of social media apps on your phone (use a web browser if possible)

Dynamic Pricing

Dynamic pricing is the practice of varying the price of a product or service to reflect changing market conditions, primarily, charging a higher price when demand is highest.

Ride Share services are a prime example of this. Getting home on New Year's Eve after the ball drops is going to incredibly expensive, because so many people are out and trying to get home, while the same trip on a weeknight when there are no events happening can be significantly cheaper.

But as retail stores and restaurants switch to digital menus, they can increase and decrease prices on the fly, so you'll never know precisely what an item may cost you at any point in time.

Dynamic pricing is not the same as price gouging, although the two are similar. Price gouging, which is illegal in many places, often happens in response to an emergency or unexpected shortage, where the prices of goods such as bottled water, are raised to the point that many consumers cannot afford the items.

WV law states that during a state of emergency or preparedness, prices for vital services and goods cannot be increased more than 10%. This means you can't be charged 200% more for drinking water during a flood, but you can be charged 50% or more if you want a ride home during a thunderstorm.

Personalized Pricing

Personalized pricing is related to, but not the same as dynamic pricing. Personalized pricing is the practice of setting the cost of items upon individual consumer data rather than setting a fixed price for all consumers.

In practice this can mean you and your neighbor pay different prices for items, based upon the information any particular company has on you. It also means that physical stores can't compete with online retailers who can use GPS data to determine when a user is in a store and then drop their online prices of items to beat that physical retailer.

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:

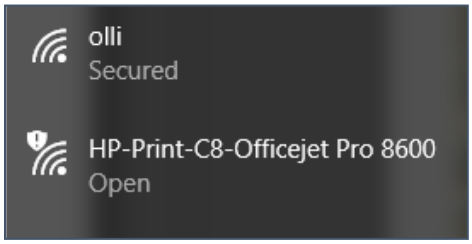
- Purchase your own wireless router
- Create a complex Wi-Fi password
- Change the administrator password
- Turn on wireless network encryption
- Create a separate "guest" wireless network for your smart devices
- Use firewall / security software
- Keep your router's firmware up-to-date

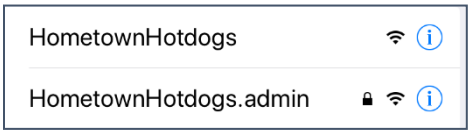
Public Wi-Fi

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-Fi 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.

Smart Devices & Internet of Things (IoT)

The Internet of Things, or IoT, is the network of collection of internet embedded devices that have some to surround us. These devices can be coffee makers, thermostats, dog collars, blood pressure cuffs—anything that that collects information and sends it to your smart phone or computer. These sensors allow us to do everything from turning on the porch light when we're coming home after dark, to reminding you to change your furnace filter and much more.

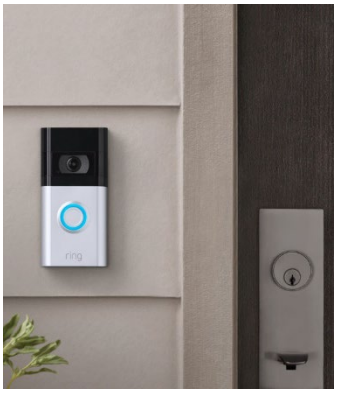
On the plus side, these devices can provide us with extra security, from remotely checking cameras in our homes to letting us turn off forgotten appliances to easily tracking our health stats and sharing that information with our doctor.

The down side is we must trust the companies that create these devices both to keep us safe from hackers and to protect our privacy.

Smart devices are another modern technology with amazing potential but which can be problematic in implementation. Smart devices give you the ability to place lights on a schedule, check items remotely, and see who is at your door. 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 home locks are tied into an insecure system, the consequences could be far graver.

Consider the individual devices and not only what they do, but how they do it. Security cameras can make you feel safer, but is that footage being uploaded to the internet? Is the company maintaining that footage reliable and security conscious?

Additionally, cameras in private spaces frequently record into public spaces, and those recordings can be shared by the owner. Think about that the next time you do an innocuous but potentially embarrassing activity when you think no one is watching. There are certainly multiple recordings of me tripping over my own feet as I walk down an empty sidewalk.



Just as with websites, all your devices should have unique user IDs and passwords. And your devices should be connected through a secondary guest wireless network—one separate from your main network you use for your computer.

Data privacy laws won't do much to protect you from malicious actors, and some leading smart device manufacturers face Congressional scrutiny and lawsuits over their data-collection and security practices.

Does the company behind the smart home device you're considering have a worrisome privacy policy that hints at exorbitant data collection practices? What data does the company collect and who does it share that data with? Does the manufacturer have a history of data breaches, or an otherwise poor record when it comes to keeping private data private?

-- https://www.cnet.com/home/security/beef-up-your-smart-home-security-in-5-easy-steps/

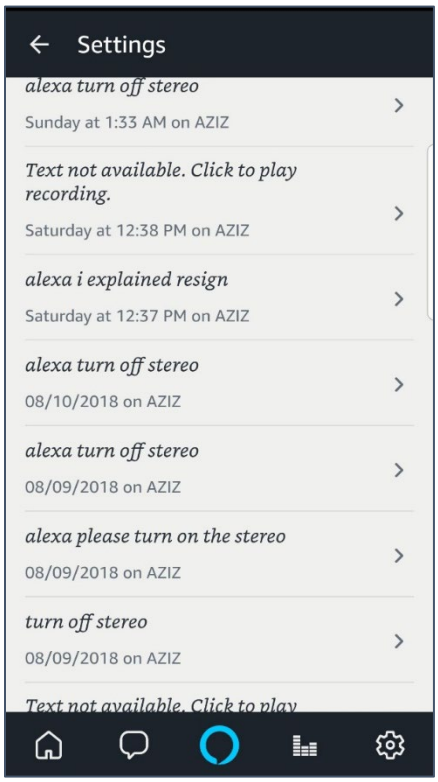
Virtual Personal Assistants

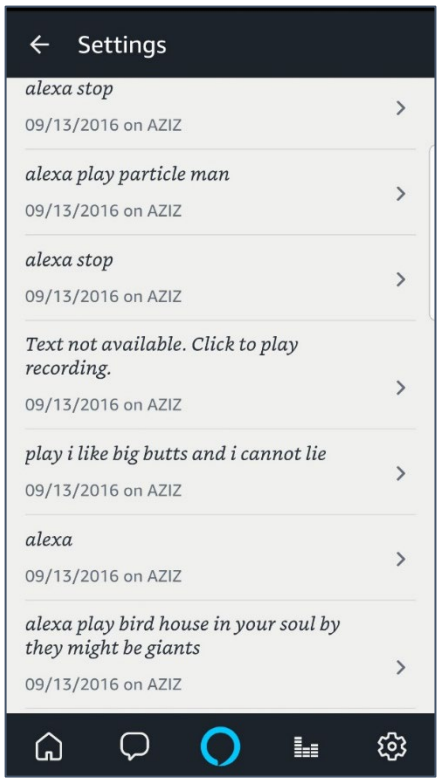
Virtual personal assistants are the programs on your phone like Apple's Siri, or on devices like the Amazon Echo (Alexa) that that can be controlled by voice commands—anything from adding items to a shopping list to setting a timer or alarm to learning the definition of inconceivable (I do not think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





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 our bank site regularly to check for unapproved purchases.
- Bookmark websites you freqiently 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.
- 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.

Payment Apps

Payment apps are becoming common, as a way to avoid cash. These digital wallets can be linked to your bank or credit cards to allow you to send and receive money.

An excellent example of when you might use one, is when going out to lunch with friends. Instead of trying to get separate checks, or handing the server multiple credit cards with notes as to which meal goes on which card, you can have one person pay the whole thing, and then everyone else sends them money via a cash app.

Some landlords only take payment through apps, since it means they no longer have to deal with checks, and these apps don't have the overhead of credit cards.

Some frequently used payment apps:

- Venmo (bank transfers)
- Zelle (bank transfers)
- Cash App (Square)
- PayPal
- Apple Pay (Apple)
- Google Pay (Google)

All of these apps are reputable and can be linked to either your bank account or credit card. In fact, Zelle is used by several major banks as their preferred transfer app.

You obviously want to be careful when using one of these apps, and to pay attention to any associated costs for fees. For example, most apps charge you a percentage fee to use your linked credit card, or to send money to strangers, but not to family or using your bank account. So check carefully before deciding if you want to use one of these apps.

GPS and Location Services

GPS (Global Positioning Systems) 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 at places they frequently visit.
- Post vacation pictures *after* I'm home.

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, and those files are accessible at any time from any computer you log into. (See page 30)

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. (See page 29)

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.

Resources

Internet Domains

Internet Top Level Domains

Media Bias Chart

Media Bias Chart

Password Strength Checkers

How Secure Is My Password (Security.org)
How Secure Is My Password (LastPass)

Privacy Spy

Privacy Spy

Opt Out

Simple Opt Out

Terms of Service

Terms of Service; Didn't Read
Clickwrapped

Fact Checking Websites

PolitiFact
FactCheck
TruthOrFiction
Lead Stories
FullFact.org
Snopes
Media Bias/Fact Check

Home Network Security Tips

Cybersecurity Best Practices (CISA.gov)

What Is Encryption?

How Does HTTPS Work?
What is encryption? (IBM)
What is Encryption and How Does it Work? (University of Miami)

2FA Security Keys

The Best Security Key for Multi-Factor Authentication
The Best Hardware Security Keys for 2024

Apps to Monitor Phone Usage

Screen Time (iOS)
Digital Wellbeing (Android)
Quality Time (Android)
Forest

Cloud Storage Services

Service	Free?	Website	Price
Sync.com	5GB	https://www.sync.com	200GB ~$5/month
SugarSync	0	https://www.sugarsync.com	250 GB ~ $9.99/month
pCloud	4 GB	https://www.pcloud.com	500GB ~ $49.99/year
OneDrive	5 GB	https://onedrive.live.com	100GB ~ $19.99/year
MEGA	25 GB	https://mega.nz	2TB ~ $105.50/year
iDrive	10 GB	https://www.idrive.com	100 GB/~$2.95/year
iCloud	5 GB*	https://www.icloud.com	50GB ~ $0.99/month
Google Drive	15 GB	https://www.google.com/drive	100GB ~ $19.99/year
Dropbox	2 GB	https://www.dropbox.com	2TB ~ $12/month
Box	10 GB	https://box.com	100GB ~ $5/month
Amazon Drive	5GB*	https://www.amazon.com/clouddrive	100GB ~ $19.99/year

Anti-Virus and Security Suites

Avast	Free AV option	https://www.avast.com
AVG	Free AV option	https://www.avg.com
BitDefender	Free AV option	https://www.bitdefender.com
Malwarebytes	Free AV option	https://www.malwarebytes.com
ESET NOD32	No free option	https://www.eset.com/us
F-Secure	No free option	https://www.f-secure.com
McAffee	No free option	https://www.mcafee.com
Norton	No free option	https://us.norton.com/antivirus
Sophos	No free option	https://www.sophos.com
Trend	No free option	https://www.trendmicro.com
Webroot	No free option	https://www.webroot.com

Search Engines

Ask	https://www.ask.com	Bing	https://www.bing.com
Duck Duck Go	https://duckduckgo.com	Google	https://www.google.com
Google Scholar	https://scholar.google.ca	Lycos	https://www.lycos.com
MetaCrawler	https://www.metacrawler.com	Yahoo	https://www.yahoo.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
Tutanota	https://tutanota.com
Yahoo	https://login.yahoo.com/account/create

Password Managers

Product	Benefits	Site
1Password	Family pricing; multi-platform	https://1password.com
Bitwarden	Multi-platform; open source; family plan; free plan	https://bitwarden.com
Dashlane	2FA, multi-platform; free plan	https://www.dashlane.com
Enpass	Self-hosted	https://www.enpass.io
KeePass	Self-hosted but more complicated to use	https://keepass.info
Keeper	Multi-platform, sharing	https://www.keepersecurity.com
LastPass *	2FA, multi-platform	https://www.lastpass.com
NordPass	2FA	https://nordpass.com
Roboform	Form auto-fill w/ multiple identities; multi-platform	https://www.roboform.com

* Has had recent security breaches and is no longer a top recommendation

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

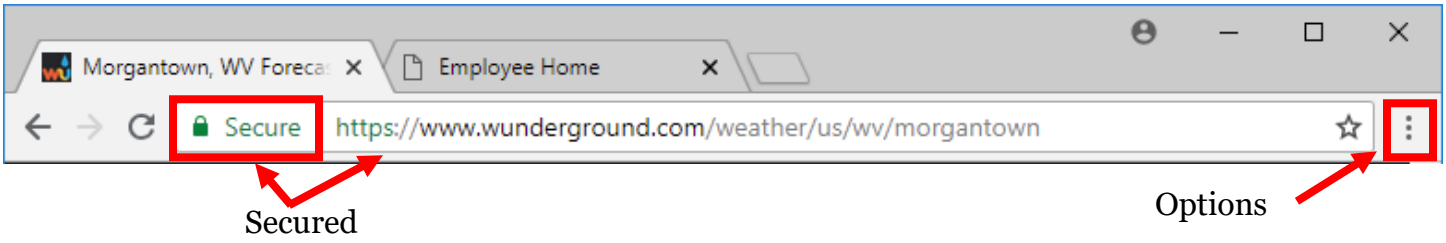
Web Browsers

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

Web Browser Add-Ons

Disconnect	Firefox, Chrome, Safari, Opera	https://disconnect.me/disconnect
Privacy Badger	Firefox, Chrome, Edge, Opera	https://privacybadger.org
Privacy Spy	Firefox, Chrome	https://privacyspy.org/
Terms of Service Didn't Read	Firefox, Chrome, Opera, Safari, Edge	https://tosdr.org/

Browser Settings: Chrome



Browser Settings

1. Click **Options** (Customize and control), and from the drop-down menu, select **Settings**.
2. The left pane contains a variety of browser settings..

To Clear Cache

1. In the left pane, select **Privacy and security**.
2. Select **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**.

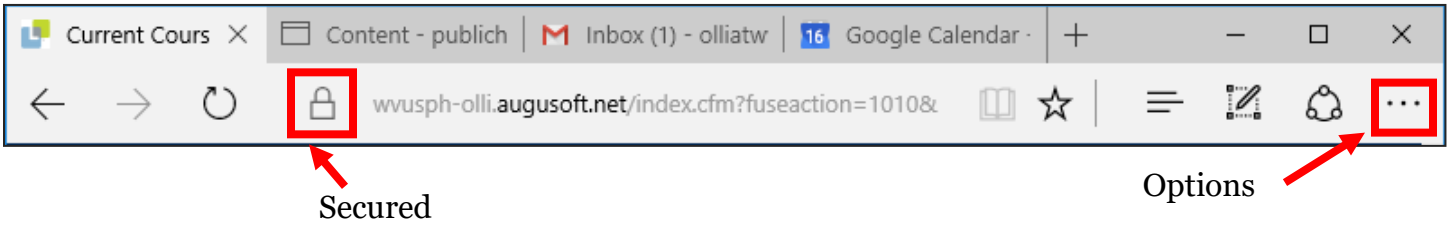
To Clear Saved Passwords

1. In the left pane, select **Autofill**.
2. In the main window select **Password Manager**.
3. Beside Offer to save passwords, switch the toggle to off.

Add-Ons

1. Open **Options** (Customize and control) 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**.

Options pointing to options icon on web browserBrowser Settings: Edge



To Access Your Browser Settings

1. Click the **Options** (Settings and more) button in the right corner of the window.
2. From the drop-down menu select **Settings**.

To Clear Cache

1. In the top left corner, in the Settings Search box, type in **Cache**.
2. Click **Choose what to clear**, then select your desired options and click **Clear now**.

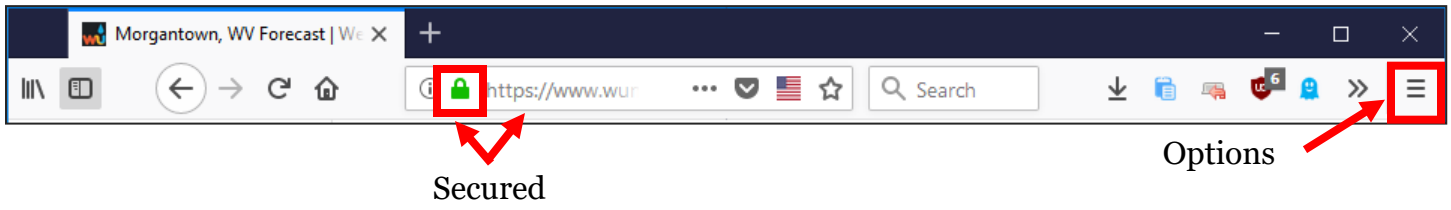
To Clear Saved Passwords

1. In the top left corner, in the Settings Search box, type in **Password**, then select **Passwords**.
2. Toggle off Offer to save passwords.
3. Click on **Manage my saved passwords** to delete existing saved passwords.

To View Add-Ons

1. Open **Options** (Settings and More) and from the drop-down menu select **Extensions**.
2. Click the link for Get extensions from the store.

Browser Settings Firefox



To Access Your Browser Settings

1. Click the **Options** (Open application menu) button in the right corner.
2. From the drop-down menu select **Settings**.

To Clear Cache

1. Along the left side select **Privacy & Security**.
2. In the Cookies and Site Data section, click the **Clear Data** button.
3. Check both options and click **Clear**.

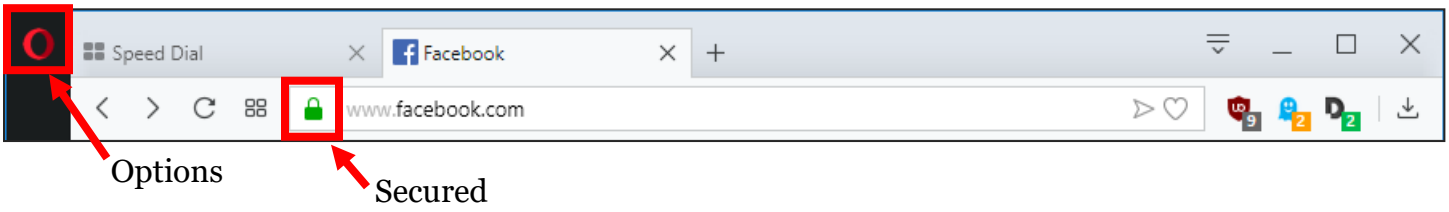
To Clear Saved Passwords

1. Along the left side select **Privacy & Security**.
2. In the Logins & Passwords section, click the Saved Logins button to delete existing saved data.

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).

Browser Settings: Opera



To Access Your Browser Settings

1. In the top left corner, click the red **O** (Customize and control Opera).
2. From the drop-down menu select **Settings**.
3. In the left pane select **Privacy & Security**.

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.

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**.

Closing Apps on an Android Device

1. Tap the Recent Applications Menu button. A list of open apps appears
2. To close an individual app, click the **x** beside the app or swipe up.
3. To close all open apps, tap **Close All**. To end all processes of that app, you need to **force stop** the app.

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.

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.

Uninstalling Apps on an iOS 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

Checking Privacy Settings in iOS

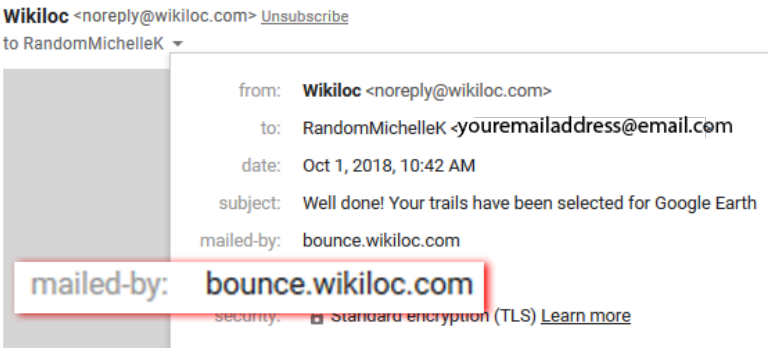
1. Open Settings.
2. Tap on **Privacy**.
3. Tap on an app/function to display a list of apps that have access to what you selected.

Checking Privacy Settings in Android

1. Open Settings.
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.

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

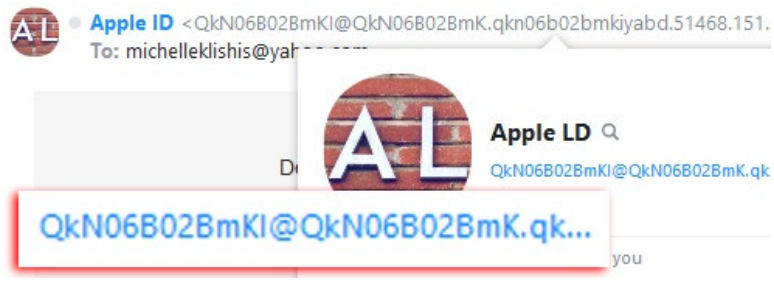
1. At the top of the message, on the right side, click the three dots.
2. From the drop down menu select **Show original**.

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

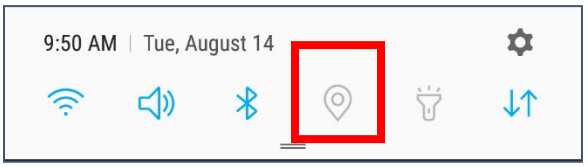
You can't.

Cleaning Up Facebook App Permissions

1. Open Settings: Along the top of the page, click your profile pictures icon, and from the menu select **Settings & privacy**.
2. Select Settings,
3. Click on Security and login.
4. In the left pane, click on **Apps and Websites**.
5. Click the box beside the app from which you want to remove permissions.
6. Click **Remove**.

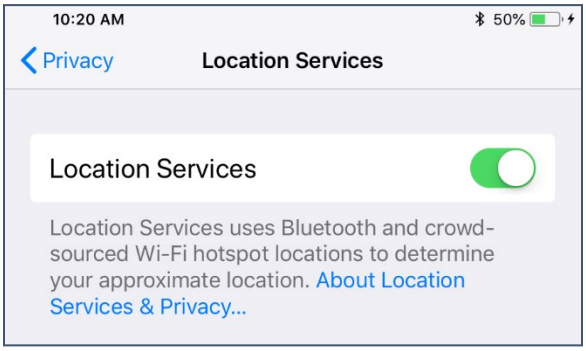
Toggling GPS on an Android Device

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.



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.



Accessing Privacy Settings

Google Privacy Settings (Gmail)

1. Click on your picture (or initials if you do not have a picture associated with your google account).
2. Click Manage your Google Account
3. Select Privacy & Personalization.
4. Go through the various settings.

Apple Privacy Settings (General)

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

Microsoft Privacy Settings (Outlook)

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

Index

Technology Glossary

5G
The fifth generation technology standard for cellular networks. It can support up to 10,000 devices per cell and have download rates up to 10 gigabits per second

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

Address Bar
In a web browser or windows explorer, it is a rectangle, usually towards the top of the window, that shows you the current location or address of your web page or file.

Address Book
See Contacts

Adobe Digital Editions (ADE)
Adobe proprietary format for eBooks.

Alexa
Amazon's virtual assistant.

Algorithm
A set-of rules to be followed in calculations or problem-solving operations. Algorithms are frequently used to manipulate data sets.

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 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 use the same Apple ID with both of those devices.

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.

ARPANET
Advanced Research Projects Agency NETwork. The first true internet, it connected military installations, a handful of universities, and some third-party contractors together.

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.

AVI
Audio Video Interleave. A multimedia format for audio and video files.

AZW / AZW3
Amazon proprietary eBook format.

Backbone
Long-distance networks that carry data between data centers and consumers

Backup
A copy of computer data that is taken and stored somewhere else, to be used in the event of data loss.

Bandwidth
The amount of data that can be transmitted at one time. It is measured in bits per second

BCC
Blind carbon copy. Covertly send a copy of the message to a third party. The primary recipient cannot see the person was added.

Biometric
Unique physical characteristics that are be used for recognition. The most common types of biometric identifiers are fingerprints, voice, face, iris, and palm/finger veins.

Blockchain
Also Block Chain. A list of records (blocks) linked using cryptography. These records are a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchains are generally used on a peer-to-peer network. Data in one block cannot be altered without changing all other blocks.

Bluetooth
A wireless technology that allows data to be shared over short distances using short-wave UHF radio signal. The name comes from Harald "Bluetooth" Gormsson, king of Denmark and Norway, who united the Scandinavians.

Boolean
A system of logical propositions. Common Boolean operators: AND, OR, NOT, “ “, ( ) . Based on the work of George Boole.

Broadband
A fast, reliable, always-on connection to the internet.

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.

Browser
Short for Web Browser.

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

Byte
A unit of digital information that consists of eight bits. A byte is the number of bits used to encode a single character of text.

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

Cambridge Analytica
A British political consulting firm that used misappropriated digital assets, data mining, and other processes to influence political elections around the world.

Causation
Relation that holds between two temporally simultaneous or successive events when the first event (the cause) brings about the other (the effect). **NOT** the same as correlation.

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 a cell phone makes to a cell tower that allows you to do things like surf the internet, download emails, and send MMS 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.

Cloud Service
A service provided by a third party or company that allows you to provide access to files and applications remotely.

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

Contacts / Contact List
A collection of screen names and the various data associated with them, such as email addresses and telephone numbers.

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.

Correlation
A mutual relationship or connection between two or more things. See also Causation.

Cortana
Microsoft's virtual assistant.

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

Cryptocurrency
A digital asset that uses strong cryptography and is designed to work as a form of money. They used decentralized control, or a public financial database to keep track of who owns what.

Cryptography
Greek for "hidden writing", it is the study of secure communication—creating protocols to keep third parties from reading private messages.

Data Breach
The release of secure or private information. A data breach can be accidental or malicious, such as when an individual hacks into a system to steal information.

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

Data Center
Room(s) full of servers that store user data and host online apps and content.

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.

Dial-up
An early way to connect a home computer to the internet. A phone line was used to connect a personal computer to the Internet Service Provider.

Directory
A system that catalogs / organizes computer files.

Displayport
A high-quality audio-visual cable capable of transmitting HD and 4k.

DMCA
Digital Millennium Copyright Act. The 1998 United States copyright law that criminalizes production and dissemination of technology, devices, or services that circumvent measures to control access to copyrighted works (DRM).

DNS
Domain Name System. The phonebook of the Internet.

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

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

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.

Download
To move data and files from the internet or a server to your computer or mobile device.

DRM
Digital Rights Management. A format that protects electronic media from being illegally copied.

DVD
Digital Video Disc / Digital Versatile Disc. A digital optical disc data storage system.

DSL
Digital Subscriber Line. A fixed connection to the internet that runs through copper phone lines.

DSLR
Digital Single-Lens Reflex

DVI
Digital Video Interface. A video display interface that connects your computer to your monitor.

eBook
An electronic file formatted (for the most part) to be read on a small handheld device, or on a computer screen in an eReader program / app.

eInk
A brand of electronic paper (e-paper) display technology from the E Ink Corporation (1997)

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.

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.

Emoji
Small images used to represent emotions, ideas, or expressions. 🙂

Emoticons
Representations of facial expressions using keyboard characters. These are used to portray moods or feelings. For example, a smiling face could be **:)** or ☺

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.

EPUB
Electronic Publication. A digital book format that allows you to read your eBook on any electronic device. EPUB files are reflowable.

eReader
eBook reader that use black and white eInk screens that give a similar reading experience to physical books.

Ethernet
Wired networking technology that allows multiple computers to talk to one another via a protocol (set of rules). Ethernet is used when speed, stability, and security are needed.

EULA
End-User License Agreement. The legal contract between a software vendor and the user of that software. It specifies the rights and restrictions which apply to the use of the software.

External Storage
Devices that store data outside of a computer or other electronic device. They are often removable, such as USB thumb drives.

Facebook
An online media and networking company.

Facial Recognition
Technology capable of identifying or verifying a person from a digital image. Facial recognition can be used to unlock an electronic device.

Fiber Optics
A flexible glass or plastic fiber that can transmit light signals with very little loss of strength

File Extension
Also called a filename extension or file type, is the identifier suffix for a computer file name, and tells you the kind of program needed to open the file. By default, these extensions are hidden, but can still be used in search. If you change a file extension, that file will most often break.

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

Fixed-layout
Content remains locked in a specific place, when the document is enlarged you often have to scroll around to read the entire thing. A pdf is a fixed-layout document

Folder
See Directory.

Follow
Choose to see another user's posts in their content feed.

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.

GB
Gigabyte. A computer memory unit equal to 1000 megabytes. The prefix giga means 10^9.

GIF
Graphics Interchange Format. An image format that is often used in logos and animated pictures.

Google
A technology company that specializes in services 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.

GUI
Graphical User Interface (pronounced gooey). The windows, icons, menus, and pictures that allow you to interact with your computer using your mouse. Windows 10 and Mac OS (Big Sur) are operating system GUIs.

Hard Drive
A data storage devices that stores and retrieves digital data. In your computer, this is where all your programs are installed and files saved.

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

HD
High Definition. Generally a higher resolution and quality than standard definition video.

HDMI
High-Definition Multimedia Interface. Audio/video interface for transmitting uncompressed data. Cable that connects your computer to your monitor, or your DVD player to your TV.

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.

Heat Map
A heat map is a visual representation of data that allows you to see phenomenon as clusters or over space.

Home Screen
The main screen of a computer or mobile device. Home screens are typically personalized by the user so that no two home screens will look alike.

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.

iCloud
Apple's cloud service.

Icon
A graphic representation of a program, file or function.

Information Security
The protection of data and the mitigation of risks, generally on computer networks.

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.

iPad
Apple's tablet computer, running iOS.

iPhone
Apple's cellular phone, running iOS.

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

ISBN
International Standard Book Number. A numeric commercial book identifier that is unique for every edition and variation of a book.

ISP
Internet Service Provider. Company you pay so you can have internet at home.

iTunes
Apple's music service.

JPG / JPEG
Joint Photographic Experts Group. A lossy compression format for digital images.

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

LAN
Local Area Network. A group of computers / devices that share a common communications line.

Last Mile
The service from your local provider to your home.

Latency
The time delay between the sending and receiving computer.

Location Bar
See address bar.

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

Lock Screen
The opening screen or interface of an operating system. A lock screen keeps unauthorized users from accessing the data and information on a device.

Lossless Compression
A form of data encoding that maintains the original quality of the file but at the cost of having a large file size.

Lossy Compression
A form of data encoding used to reduce file size at the cost of data quality.

LTE
Long-Term Evolution, A technology for mobile wireless broadband communication.

Malware
Software is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Mbps
Megabits Per Second. The speed of your internet service.

Messenger
An app that allows users to send text messages and images to other users in a system.

Metadata
A data set that give you information about other data. A card catalog contains metadata.

Micro-SD
Micro-Secure Digital Card. Smaller size SD card, used in phones and lightweight devices. Comes with an adapter that allows for the transfer for files from a portable device to a computer.

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.

MOBI
Mobipocket. The proprietary ebook format for the Amazon Kindle. MOBI files are reflowable.

Mobile Carrier
A wireless service provider that allows users to connect portable devices (such as phones) to the internet through a cellular service.

Mobile Data
Wireless internet access through a cellular data connection.

Modem
Modulator-demodulator. A device that converts data from a digital format to a format for analog transmission.

MP3
Moving Pictures Experts Group Layer-3. A coding format for digital audio.

MP4 / MPEG4
Moving Pictures Experts Group Layer-4. A coding format for digital multi-media, commonly video.

MPEG
Motion Picture Experts Group. A standard for encoding and compressing video.

NDA
Non-Disclosure Agreement. A legally binding contract where parties agree not to share sensitive or confidential information.

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.

News Feed
The main page of Facebook, where you see content posted by users you have chosen to follow. These content can be text or images.

Notification
A message displayed by an electronic device to provide an alert, reminder, or other communication.

Online Chat
Real time communication over the internet through (generally short) text messages.

OS
Operating System. 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.

P2P
Peer-to-Peer

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.

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.

PayPal
A method of online money transfer and payments.

PDF
Portable Document Format. Once an Adobe proprietary format, now one of the most common formats for sharing digital documents.

Peer-to-Peer
A distributed that shares tasks or work between devices of the same level.

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.

Phreaking
An attack on the telephone system

Play Store
Goggle's app store, where users can download or purchase programs to run on their Android devices.

PNG
Portable Network Graphics. A lossless compression type for digital images.

Podcast
A digital audio file made available on the Internet for downloading to a computer or mobile device, typically available as a series, new installments of which can be received by subscribers automatically.

Post
A message, comment, image, or other item that is placed on the internet, generally on a website.

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.

Reflowable
An ebook format that layout depending upon the output device. MOBI and EPUB are reflowable formats, which means the number of words on the page change, depending upon the page / text size.

Repeater
A device that extends the range of Wi-Fi signal.

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

Reply
A response to an electronic 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 networks.

RTFM
Read The *Fantastic* Manual.

Scraping
Web scraping, web harvesting, web data extraction is extracting data from websites—gathering up information available on a public website.

SD
Standard Definition. The lowest quality rating for digital streaming.

SD Card
Secure Digital Card. Removable memory that is used in devices like cameras, because it can be easily switched out when full. Allows for easy transfer of files from device to computer without a cable.

Search
A computer command that allows you to find specific files on your computer that meet a designated category, such as file type, or date modified.

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.

Settings
An app that allows you to customize your computer, device, or program.

Siri
Apple's personal assistant.

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

Smart TV
A television with a network port to allow you to watch streaming services (and other internet content) without having to use an additional device.

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.

Sort
To organize information in a prescribed sequence, such as alphabetically, or oldest to newest.

Spam
Unsolicited electronic messages (especially advertising).

Speed
Download speed is how quickly you can pull down data from the internet. Upload is how quickly you can send data out to the Internet.

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.

SSD
Solid State Drive. A storage device for your computer that saves data on chips instead of a mechanical platters.

Status Bar
A graphical element, usually at the top or bottom of a device's screen, that displays information about the state of the device. Some settings commonly found on the status bar are sound/volume, time, and battery life.

Streaming Device
An object, such as Roku stick or Fire stick, you purchase that plugs into your existing TV so you watch video through the device on your existing television.

Streaming Service
An online provider of entertainment (music, movies, etc.) that delivers the content via an Internet connection to the subscriber's computer

Switch
A device that connects to a router and provides multiple ports for wired connections.

Sync
See synchronize.

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.

Tag / Tagging
A keyword or term added to the metadata of a piece of information. In social media, when someone is tagged, they are alerted to a post made by another user.

Taskbar
A graphical user interface (GUI) that is typically along the bottom of your window, and usually shows you what programs are actively running as well as important information about the operating system.

TB
Terabyte. A measure of computer storage equal to 1000 gigabytes or trillion bytes. The prefix tera means 10^{12}.

TCP
Transmission Control Protocol. The main protocol used on the internet that allows computers to send and receive data.

TCP/IP
Transmission Control Protocol/Internet Protocol

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.

Thumb Drive
USB Flash Drive

Thunderbolt
Interface reconfigured to be compatible with USB-C that carries data, video (PCIe and DisplayPort), sound, and power over a single cable.

TIFF / TIF
Tag Image File Format. Lossless digital image format that was developed originally for scanners as an alternative to multiple proprietary formats.

Timeline
A display of items in chronological order. Twitter has a timeline; Facebook has a news feed.

TL;DR
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.

Unfollow
To stop seeing a user's posts in your timeline or news feed. On Facebook, you can unfollow someone by still remain friends with them.

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.

Unique Identifier
A piece of data that is unique to a record. Telephone numbers and email addresses are often used as unique identifiers, because no two individuals have the same ones. Unique identifiers allow data records to be linked across databases.

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.

URL Bar
See address bar.

USB
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-A, USB-A 3.0, mini-USB, micro-USB, and the newest standard, USB-C.

USB Flash Drive
Also: USB thumb drive. A small USB data storage device that is removable, rewritable, and can be easily carried in a pocket.

User Data
Any type of data generated by people interacting with software programs. User data includes: Explicit Data, which is given by a user directly such as name, address, email, and phone number; Implicit Data, which is not provided by the user directly but gleaned through analysis of user interactions, such as pages visited, session duration, or type of device; and finally External Data which has been gathered from third parties with whom an organization has a relationship.

Username
Also called account name, login ID, 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.

VGA
Video Graphics Array. A connector that takes video signal from a computer and takes it to the monitor (or projector).

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.

WAV
Waveform Audio File Format. An audio file standard for uncompressed audio.

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.

Web Cookie
See Cookie.

Website
a location connected to the Internet that maintains one or more pages on the World Wide Web

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

Widget
A graphical element that displays information or provides quick access to certain parts of an app. Mobile devices frequently have a weather widget that is linked to your weather app, and which tells you the current temperature and forecast.

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.

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.

WWW
World Wide Web. An information system on the Internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another.

Acronyms

AF: As (naughty word)
AFK: Away from Keyboard
ATM: At The Moment
BTW: By the Way
B/C: Because
BFD: Big *Freaking* Deal
BFF: Best Friends Forever
BRB: Be Right Back
CU: See You
CYT: See You Tomorrow
DGMW: Don't Get Me Wrong
Diss: Disrespect
EOD: End of Discussion
EOM: End of Message
F2F: Face to Face
FAQ: Frequently Asked Questions (pronounced fak to rhyme with pack)
FFS: For *Freaks* Sake
FREX: For Example
FTW: For the Win
FWIW: For What It's Worth
FYI: For Your Information
GOAT: Greatest of All Time
GR8: Great
HTH: Hope This Helps
HMU: Hit Me Up
IANAL: I Am Not A Lawyer
ICYMI: In Case You Missed It
IDC: I Don't Care
IDK: I Don't Know
IIRC: If I Remember/Recall Correctly
IKR: I Know Right
IMHO: In My Humble Opinion
IMO: In My Opinion
IOW: In Other Words
IRL: In Real Life
IYKYK: If You Know, You Know
JK: Just Kidding
L8R: Later
LMK: Let Me Know
LOL: Laugh(ing) Out Loud
MYOB: Mind Your Own Business
NGL: Not Gonna Lie
noob / n0ob: Newbie
NNTR: No Need to Reply
NOYB: None of Your Business
NP: No Problem
NRN: No Reply Needed
NSFW: Not Safe for Work
NVM: Never mind
OMG: Oh My God
OMY: On My Way
OOTD: Outfit Of The Day
OTOH: On the Other Hand
OT: Off Topic
OTP: On the Phone
PM: Private Message
RL: Real Life
RN: Right Now
ROTFL: Rolling on the Floor Laughing
RTFM: Read the *Fantastic* Manual
RQ: Real Quick
RU: Are You
SFLR: Sorry for Late Reply
SO: Significant Other
SMH: Shaking My Head
STFU: Shut the *freak* up
TBC: To Be Continued
TBH: To Be Honest
THX: Thanks
TIA: Thanks in Advance
TL;DR: Too Long Didn't Read
TMI: Too Much Information
TTYL: Talk to You Later
TUVM: Thank You Very Much
TYT: Take Your Time
UR: You Are / Your
woot / WooT: Hooray! Yay! Yippee!
Wo: WithOut
W8: Wait
WFM: Works for Me
WRT: With Regard To
WTH: What the *Heck*
WTF: What the (naughty word)
YMMV: Your Mileage May Vary

Be careful with emojis, as many have multiple meanings besides the obvious. Don't send eggplant or peach unless you are *definitely* talking about foods.

References

7 Actionable Tips to Secure Your Smart Home and IoT Devices Institute of Electrical and Electronics Engineers

70TB of Parler users' messages, videos, and posts leaked by security researchers CyberNews

Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock "Experimental evidence of massive-scale emotional contagion through social networks" (2014) *PNAS* 111 (24) 8788–8790

AirTag Stalking Attacks Are on the Rise. Here's How To Protect Yourself (2022) Popular Mechanics

Alexa and Siri Can Hear This Hidden Command. You Can't (2018) Seattle Times

Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments (2021) The Verge

An Absurdly Basic Bug Let Anyone Grab All of Parler's Data (2021) Wired

An Ugly Truth: Inside Facebook's Battle for Domination (2021) Sheera Frenkel and Cecilia Kangm

Apple Siri Eavesdropping Puts Millions Of Users At Risk (2019) Forbes

Are your smart home devices secure? (2021) UW–Madison Information Technology

Big Banks Blink on Zelle Scams (2022) The Observer

Big brother brands report: which companies might access our personal data the most (2021)

Cybersecurity 101: Protect your privacy from hackers, spies, and the government (2022) ZDNet

Dynamic pricing tech may brighten retail bottom lines and put consumers in the dark (2024) Marketplace

Facebook turned over chat messages between mother and daughter now charged over abortion (2022) NBC News

Health advisory on social media use in adolescence American Psychological Association

How the cookie became a monster (2022) NPR

I Agree by Dima Yarovinsky (2018) My Modern Met

If These Apps Are Still on Your Phone, Someone May Be Spying on You (2022) Readers Digest

Information flow reveals prediction limits in online social activity. *Nature Human Behaviour* volume 3, pages 122–128 (2019)

Instagram & Copyright (2022) Copyrightlaws.com

Internet of Things and Privacy – Issues and Challenges Office of the Victorian Information Commissioner

Mindf*ck: Cambridge Analytica and the Plot to Break America (2019) Wylie, Christopher

Personalization or Price Discrimination? (2020) Open Markets

Political Advertising on Social Media Platforms (2020) American Bar Association

Ring Changed How Police Request Door Camera Footage: What it Means and Doesn't Mean (2021) Electronic Frontier Foundation

Social Media and Mental Health NAMI

Social Media and Mental Health, Braghieri, Luca, Ro'ee Levy, and Alexey Makarin. 2022. American Economic Review, 112 (11): 3660-93.

Social Media and the Transformation of Public Space (2015)

Social Media and Youth Mental Health US Surgeon General

Social Media Use and Its Connection to Mental Health: A Systematic Review. Karim F, Oyewande AA, Abdalla LF, Chaudhry Ehsanullah R, Khan S. , Cureus. 2020 Jun 15;12(6)

Social media use of adolescents who died by suicide: lessons from a psychological autopsy study. Balt, E., Mérelle, S., Robinson, J. et al. Child Adolesc Psychiatry Ment Health 17, 48 (2023)

Stalking Apps: What To Know FTC

The Cost Of Getting Your Money Back (2019) Planet Money

The Dangers of Cheap USB Cables (2016): Make Use Of

The Many Identifiers in Our Pockets: A primer on mobile privacy and security (2015) University of Toronot

The most invasive apps: which apps are sharing your personal data? (2021)

The Soviets' Unbreakable Code: The hidden history of the Fialka espionage machine (2019) Anna Borshchevskaya. Foreign Policy

The Strava Heat Map and the End of Secrets (2018) Wired

This USB-C Lightning cable should terrify you (2021) PC World

Top 50 Impersonated Brands (2023) Cloudflare

Trends in the Incidence of Eating Disorders Among Active Component Service Members, 2017 to 2021 Jessica H. Murray, MPH; Sithembile L. Mabila, PhD, MSc; Alexis A. McQuistan, MPH. Health.mil

What Companies Does Facebook Own? (2023) Dataromas

What Companies Google & Alphabet Own: Visuals & Full List Kamil Franek

What Is Dynamic Pricing, and Why Has It Made Everything So Expensive? (2024) US News & World Report

What Parler Saw During the Attack on the Capitol (2021) (some video may be disturbing)

What to Do If the Police Ask for Your Video Doorbell Recordings (2021) Consumer Reports

Your Technology Is Tracking You. Take These Steps For Better Online Privacy (2020) NPR

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