



USSOCOM

SOCIAL MEDIA SMARTCARDS

TABLE OF CONTENTS



USSOCOM SMARTCARDS

2	Threats to Identity
4	Self Assessment
8	People Search Opt-Out
11	Data Aggregator Opt-out
14	Google Alerts
16	Online Registration
18	Twitter
25	Instagram
32	Facebook
38	Amazon
50	Pinterest
55	Snapchat
63	TikTok
65	YouTube
69	LinkedIn
72	PlayStation
79	Hidden Apps
81	Pay Apps
83	Dating Sites & Apps
84	Fitness Apps
89	iOS Privacy Settings (14.1)
93	Android Privacy Settings (11.0)
98	Zoom
103	Traveling with Smartphones
104	Identity Theft
106	Child Safety Online
109	Photo Sharing Sites
114	EXIF Removal
116	Lock Down Your Computer
118	Wifi Security
121	Delete Browser Artifacts
126	Additional Resources

THREATS TO IDENTITY



USSOCOM SMARTCARDS

In Case of Identify Theft

- Notify your bank & credit card companies
- Change all passwords including on social media
- Report ID Theft to www.FTC.gov
- Let friends and family know in case the criminal now has access to your emails and social media accounts
- File a Police report

What to Lock Down

- Any PII Information
- Your credit report
- Your child's credit report
- Your social media accounts (recommend using smartcards to lock accounts down)

Actions for the Physical World

- Be aware of your surroundings
- Invest in a home safe Shred documents, bills, and any mail
- Do not give out your SSN
- Be mindful of shoulder surfers (whether on your phone, computer, at an ATM, etc.)
- Be mindful of credit card skimmers at ATMs and Gas pumps
- Use a locked mailbox
- Check financial statements frequently
- Read medical statements
- Use credit cards instead of debit cards
- Be sure to sign the back of any credit or debit card

Actions to Take in 2021

- Recommend turning on Two Factor Authentication for all devices and accounts that allow such an option Update your devices' virus protection and your passwords
- Clear cookies and browser history frequently
- Update , Update , Update!!! Make sure to allow your device to update to ensure you have the most up to date security measures
- Make sure you backup all your devices .
- Encrypt your emails
- Never save credit or debit card information to devices, apps, or accounts for quick and easy checkout
- Verify those emails; most official business emails will not ask for your PII or Password ... check those links
- Don't accept friend requests from strangers
- Consider using a VPN

Note: Be sure to check out <https://haveibeenpwned.com/> to see if your personal data, via your email address, has been compromised in any data breach. Not all data breached are included on this website, but it is a great start to owning your identity.

THREATS TO IDENTITY



USSOCOM SMARTCARDS

- When buying a new car don't leave the paper work in the glove compartment or elsewhere in the car . Criminals who break into cars can use that information to steal your identity, not just your car.
- Consider posting travel (vacation) photos and information after you return from your trip so criminals don't know you are away and your house is empty.
- If you are buying or selling something online and it seems too good to be true, chances are it is. A simple Google search of the situation might end up saving you a lot of time and hard earned money.
- Consider turning off your Wi-Fi as soon as you get into your car to leave your house [#habitscanbegood](#)
- Consider how many people have access to public Wi-Fi, then consider only using privately secured Wi-Fi.
- Consider an open-phone policy with your children so you can access their phone any time and without notice. Remember if you are “friends:” with your kids online that’s only half the battle... it’s important to check on their accounts to see who and what they are talking about. [#keepingourkidssafe](#)
- It's always great to donate, but consider verifying the authenticity of a charity and/ or website first. Perhaps visiting an official website or calling the official number.
- Gamers: consider who you are communicating and sharing information with and perhaps limit online gaming interactions to only people you have met face to face.
- Consider logging off of your email and social media accounts when you are not using especially on your computer. Doing so will limit the access and abilities of an intruder if they are able to hack in. [#protectyourdata](#)

Useful Resources and Links

<https://www.identityforce.com/blog>
<https://www.common sense media.org/privacy-and-internet-safety>
<https://www.ftc.gov/>
<https://identity.utexas.edu/>
<https://www.getsafeonline.org/>
<https://staysafeonline.org/>
<https://www.idtheftcenter.org/>
<https://www.irs.gov/>
<https://www.usa.gov/identity-theft> <https://www.consumer.gov/articles/1015-avoiding-identity-theft>
<https://www.transunion.com/fraud-victim-re-source/child-identity-theft> 75

SELF ASSESSMENT



Your Online Presence

One of the easiest ways for people (e.g. potential employers, criminals, etc.) to get information about you is through your existing online presence. Anyone can learn about you with just a few clicks of the mouse and a quick Internet search. It is important for you to know just what is publicly available about you, and how you might reduce any unwanted information.

Review your social media accounts and available data aggregator websites to determine what, if any, negative or unwanted information is out there about you. Remember, your close contacts (including family members) may have also, unintentionally exposed information about you. It is important to also review what others may have posted about you especially if you have been tagged, directly linking you to a post and making you much easier to find.

Search Engines

Use various search engines to search yourself such as Google, DuckDuckGo, Bing, etc. for the differences and benefits of each (for a few examples of popular search engines, please see the third page). Google appears to yield the most accurate results for people searches and captures more relevant information.

Prior to researching, ensure you are not logged into any of the search engine sites such as Google or Yahoo. Be sure to delete your browser history and clear cookies before you begin and when you have completed all your research. These next instructions are related to the Google search engine, but can be applied to most other search engines.

Start with basic personal information such as First and Last Name. If you have a common name, you may want to search First, Middle, and Last Name, or your name associated with your address, or an associated organization. Search terms within quotations marks " " will yield results that have the same terms in the same order as the ones inside the quotes. So "John Edward Smith" will not necessarily return the same results as "Edward, John Smith."



Boolean Logic

Boolean logic defines logical relationships between terms in a search. The Boolean search operators are "and", "or" and "not". You can use these operators to create a very broad or very narrow search. And combines search terms so that each search result contains all of the terms. Also, if your search results continue to include items that are not relevant, use the dash sign to exclude certain search terms like this: "John Smith" -Pocahontas

Google does support Boolean logic, however you might, instead decide to use its own search operators which can be found here:
<https://support.google.com/websearch/answer/2466433?hl=en>

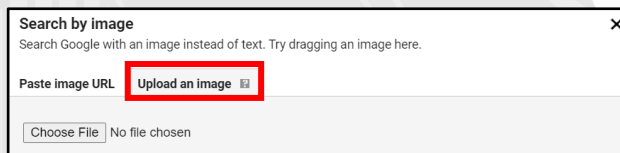
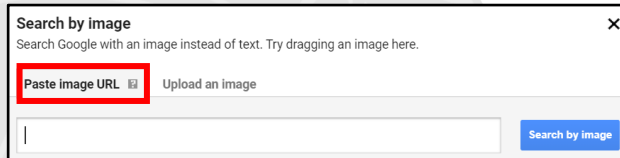
Search engine results will give you an idea of the information that can be quickly collected on you. For example, you may have found and information about previous work experience, hobbies (e.g. sports), or schools (e.g. graduation announcement). Use that information to conduct further searches.

SELF ASSESSMENT



Image Searches

You may want to conduct an image search on any photos you have used as profile pictures on social media accounts or posted to other places online. The reason for this is to ensure that advertisers and/or any other company or individual hasn't taken your picture for their own personal use. To conduct an image search using Google, go to images.google.com, click the camera icon, then select Upload an image. Select the image you want to use to start your search.



Social Media Sites

- www.facebook.com
- www.linkedin.com
- www.myspace.com
- www.twitter.com
- www.tumblr.com
- www.classmates.com
- www.instagram.com
- www.vk.com
- www.pinterest.com
- www.flickr.com
- www.meetup.com
- www.youtube.com
- www.snapchat.com
- www.reddit.com
- www.tiktok.com

Social Media Searches

Take an inventory of the social media accounts that you currently maintain. Some examples include, Facebook, Instagram, LinkedIn, Twitter, etc. First, without being logged in to any social media accounts, conduct open source searches on yourself to see what is viewable to the public. Remember, if your social media accounts don't show up during your open source searches that doesn't mean your account is completely private. It's important to check out the smartcards to help you lock down your accounts to your own personal satisfaction.

Next, login to those accounts and thoroughly review your profile for sensitive information and consider removing unnecessary data: Review your profile to see what data is available to the public (address, employment, phone number, etc.) Check any photos that you have posted or have been tagged in (this can be done through your Activity Log if using Facebook) * See Facebook, Instagram, Twitter and LinkedIn Smartcards to learn how to properly set privacy settings.

If you post something on your social media account, it may show up on search engine search results. Remember to set your privacy settings.

SELF ASSESSMENT



USSOCOM SMARTCARDS

Common Search Engines

www.google.com

Google is a search engine that specializes in Internet-related services and products. These include online advertising technologies, search, cloud computing, and software. The majority of its profits are derived from AdWords, an online advertising service that places advertisements near the list of search results.

www.bing.com

Bing is the second largest search engine in the U.S. Searches conducted using Bing generally yield similar results to Google, however Bing's image search capability (<https://www.bing.com/images>) is considered superior by most.

www.duckduckgo.com

DuckDuckGo is a search engine that distinguishes itself from other search engines by not profiling its users and by deliberately showing all users the same search results for a given search term. Does not store or compile any of your data to include searched data or personal information. DuckDuckGo emphasizes getting information from the best sources rather than the most sources, generating its search results from key crowdsourced sites such as Wikipedia and from partnerships with other search engines like Yandex, Yahoo!, Bing, and Yummly.

www.searx.me

Searx is a metasearch engine, aggregating the results of other search engines while not storing information about its users.

<https://archive.org>

The Internet Archive is an American digital library with the stated mission of "universal access to all knowledge." It provides free access to collections of digitized materials, including but not limited to; websites, software applications, music, videos, moving images, and millions of public-domain books.

Relatives

Though you may have found most of your information conducting your individual search, it might be a good idea to conduct a light search on friends and family members. Remember, they may have posted information about you that an adversary may be able to access.

Ensure nothing posted on any of the accounts indicates or outright displays personal information you don't want discovered.

Ask immediate family members (spouse, children, etc.) to review their account settings and postings to ensure that they have not inadvertently posted personal information about you or themselves.

Provide family and friends with copies of our Smartbook or Smartcards to help them with locking down their accounts and devices.

SELF ASSESSMENT



People Finders

You can conduct an initial search on data aggregators (a.k.a. people finders) for free, but all of these sites require payment to access a full report. These sites require no special authorities; anyone with Internet access and a credit card can purchase reports, so it is a good idea to be familiar with the information that can be discovered through them.

If you find information that you do not want publicly available in any of the reports, contact the organization to request that your information be opted out. Once you've opted out of or suppressed any sensitive information you have found, consider setting up Google Alerts so that you're notified if the information reappears.

People Finder/Fee-Required Sites

- www.ussearch.com
- www.beenverified.com
- www.intelius.com
- www.radaris.com
- www.truthfinder.com
- www.findpeoplesearch.com
- www.privateeye.com
- www.usa-people-search.com
- www.spokeo.com
- www.locateplus.com
- www.peakyou.com
- www.thatsthem.com
- www.familytree.com
- www.instantcheckmate.com
- www.publicrecords.com
- www.whitepages.com
- www.reversegenie.com
- www.social-searcher.com
- www.infospace.com
- www.publicrecordsnow.com
- www.findoutthetruth.com
- www.truepeoplesearch.com
- www.checkpeople.com
- www.peoplefinder.com
- <https://carsowners.net>
- <https://allpeople.com>

PEOPLE SEARCH OPT-OUT



Search Engine Opt-Out

Google

www.google.com/webmasters/tools/removals

While conducting a “Self Assessment” (see the Self Assessment card) you may find Google Search Results (websites) that you wish to remove. Find the URL associated with the “Search Result” you wish to remove and paste the URL in the “Request Removal” box (see URL above and picture to the right). It is important to note that a “Search Result” cannot be removed so long as the information and URL remain active on the original Webmaster’s page. In order to remove your information from Google you must first contact the Webmaster where the information resides and ask that it be removed. Once you obtain confirmation that the information has been removed, you can then “Request Removal” from Google. On the “Search Console” page, you can also track you requests to determine if Google has accepted the removal request.

Remove outdated content from Google Search

Guidelines

- This tool works only for pages or images that have already been modified or removed from the web
- To remove personal information or content with legal issues, [submit a legal request instead](#)
- [Read this doc](#) for more information

New request

New Request

Page Image

Enter page URL

Example: <https://www.foo.com/article>

Bing

www.bing.com/webmasters/tools/contentremoval

To remove a search result or cache from Bing, go to the above URL and follow the steps located on the Bing website, under “Removing Outdated Cache”. Like any search engine, it is important to note that your information cannot be removed from Bing prior to it being removed from the active website via the websites Webmaster. You will also need to create and sign into Bing with your Microsoft account (formerly Windows Live ID) in order to submit your request and track its progress.

Report Broken Links or Outdated Cache Pages

Content URL

Enter URL or Paste if copied

Removal type

- Remove page
- Remove outdated cache

Submit

Once you have reviewed your information and identified what needs to be removed (if any), you should record your findings to facilitate the removal process. Please note, the information presented here about how to remove personal details is subject to change. Opting out will not remove your information indefinitely

PEOPLE SEARCH OPT-OUT



USSOCOM SMARTCARDS

Google Analytics Opt-Out

<https://tools.google.com/dlpage/gaoptout>

To provide website visitors the ability to prevent their data from being used by Google Analytics, they have developed the Google Analytics opt-out browser add-on for the Google Analytics JavaScript (ga.js, analytics.js, dc.js). If you want to opt-out, download and install the add-on for your web browser. The Google Analytics opt-out add-on is designed to be compatible with Chrome, Internet Explorer 11, Safari, Firefox and Opera. In order to function, the opt-out add-on must be able to load and execute properly on your browser. For Internet Explorer, 3rd-party cookies must be enabled.

Get Google Analytics Opt-out Browser Add-on

Available for Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Edge.

People Finders Opt-Out

<https://www.peoplefinders.com/manage>

Upon request, People finders can block the records they have control over in their database from being shown on PeopleFinders.com. Unless otherwise required by law, they will only accept opt-out requests directly from the individual whose information is being opted-out and they reserve the right to require verification of identity and reject opt-out requests in their sole discretion. Of course, they are unable to remove any information about you from databases operated by third parties.

They do not accept optout requests via fax or mail. They are not obligated by law to block the records they have control over in their database from being shown on PeopleFinders.com. Despite this, they will endeavor to comply with any such requests to block the records they have control over as described above.

Please note, they have no control over public records, and do not guarantee or warrant that a request for removal of or change to personal information as described above will result in removal of or change to all of your information from PeopleFinders.com. Further, they are not responsible for informing third parties with whom they have already shared your personal information of any changes. Just because PeopleFinders.com is associated with a separate aggregator does not mean they will contact them on your behalf to remove your information you must visit each site.

A Search for your info
Screenshot of the PeopleFinders search page. The search bar contains fields for 'First', 'Last', 'City', and 'State', followed by a 'SEARCH' button. A hand icon points to the search bar.

B Click on your profile
Screenshot of a search result for 'John Smith' with '100 RESULTS FOUND'. Two profile cards are visible: 'John A Smith' and 'John M Smith', each with a 'VIEW' button. A hand icon points to the 'VIEW' button on the 'John A Smith' card.

C Copy the URL
Screenshot of a profile page for 'John Smith' in 'Portland, OR'. A list of data categories is shown with checkmarks: Address, Phone, Email, Relatives, Workplace, Licenses, Assets, Financial, and Court. Below the list are two 'SELECT' buttons. A hand icon points to the URL bar at the top of the browser window.

PEOPLE SEARCH OPT-OUT



Been Verified Opt-Out

<https://www.beenverified.com/app/optout/search>

Been Verified provides a quick and easy process to allow you to remove your information from their People Search results. Using the above link, you can search their database, select your record, and verify your request to opt out by clicking on the link in their verification email. After you verify, they will send you an email confirming that the record you selected has been opted out and will instruct their data partners not to return the record in future People Search results.

Been Verified uses your email address to send you an email to verify your request to opt out. They will not sell the email address that you provide as part of the opt-out process, or use it for any other purpose, without your prior consent. There is no charge to remove your data from Benzetimide's People Search results. Once you receive their email confirming that they have processed your opt-out request, your request will be reflected in their People Search results the next time their server refreshes. In most cases, this will take 24 hours to take effect and then they encourage you to check for yourself.

Looking To Opt-Out of Our People Search?

Start by searching for your record here. ↓

First Name Last Name All

[Looking To Opt-Out of Our Property Search?](#)

Once you receive their email confirming that they have processed your opt-out request, your request will be reflected in their People Search results the next time their server refreshes. In most cases, this will take 24 hours to take effect and then they encourage you to check for yourself. Once your opt-out has been processed, they will instruct their data partners not to return the record you opted out in future People Search results. At this time, they only provide an opt-out for their People Search service. Therefore, it is possible that your name will appear in search results for the other search services available through Been Verified even after you opt out of People Search.

There may be times when one of their data partners provides a new record that is different enough from your existing, opted-out record that they cannot match this new record to the existing record opted-out record and will create a new one. If you have previously opted-out and see a new record about you appear in their People Search results, contact them at privacy@beenverified.com and they will help you remove that record as well. It is important to occasionally check Been Verified to ensure the opt-out process is continuing.

DATA AGGREGATOR OPT-OUT



USSOCOM SMARTCARDS

- **Do** conduct research to see what records data aggregators have collected about you.
- **Do** research what information data aggregators have about your family under multiple listings; you may need to repeat the removal process described below for each listing.
- **Do** follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator.
- **Do** understand that incorrect information may be a good thing and that it might not be necessary to “fix”.
- **Don't** think removing your information from data aggregators will suppress everything. Information in about family members may still contain information about you.
- **Don't** think you have to delete all your information on these sites. Some information on data aggregator sites is normal.
- **Don't** remove information on other family members. If there is information that you believe is harmful to you, contact your family member and help them to go through the removal process.

Private Eye

USA PEOPLE SEARCH

Confı-Chek

FastPeopleSearch

peoplefindersSM

Individual Data Aggregator Removal Links

PrivateEye, Veromi, People Finders, and PublicRecordsNow, and USAPeopleSearch are all owned by the same parent company, Confi-Chek.com. You must still opt out of each individually. See links below:

Opt-out of PrivateEye by completing the form at:
<https://www.privateeye.com/static/view/optout/>

Opt-out of FastPeopleSearch by completing the following steps at:
<https://www.fastpeoplesearch.com/removal>

Opt-out of People Finders and Public Records Now by visiting:
<https://peoplefinders.com/manage/>

Opt-out of USA People Search by visiting:
<https://usa-people-search.com/manage>

Most opt-out forms/instructions are located at the bottom of each data aggregator site. Look for either the “Do Not Sell My Personal Information” or the “Privacy Policy” links to begin the removal process.

DATA AGGREGATOR OPT-OUT



USSOCOM SMARTCARDS

Radaris

To opt-out of Radaris, follow the instructions at:
<https://radaris.com/control/privacy>



PeopleConnect and Intelius

Peopleconnect, Inc. provides online social network services. The Company offers basic people search, list management, criminal records, employee screening, human resources background checks, and identity theft protection services. Peopleconnect serves customers in the United States and it owns Intelius, Truthfinder, Instant Checkmate, and US Search. Most opt-out links on these sites will redirect you to the Intelius Opt-Out Form located here: <https://www.intelius.com/opt-out/submit/>. However, TruthFinder's Opt-Out Form is located here: <https://www.truthfinder.com/opt-out/>



Family Tree

Family Tree Now allows you to opt-out at: [https:// www.familytreenow.com/optout](https://www.familytreenow.com/optout). The entire process takes place in four simple steps, where you must first select your record and then verify it is in fact your record. After you have found and confirmed your record, you simply click "Opt-Out" and you will have completed the process.



It is important to note that if you found your FamilyTreeNow record on a search engine like Google, Family Tree Now has a process for its remove, which can also be found using the link above where you will find additional information under "Notes".

DATA AGGREGATOR OPT-OUT



USSOCOM SMARTCARDS

TruePeopleSearch

To opt-out of TruePeopleSearch simply go to: <https://www.truepeoplesearch.com/removal> and follow the three step process.



WhitePages



To opt-out of Whitepages, search for your information using your first name, last name, city, and state. Once you have located your record copy the URL and paste it here: https://www.whitepages.com/suppression_requests/. Next, follow the steps to complete the removal process. This process will require a phone call from WhitePages (computer generated) in order to complete the process.

MyLife

To opt-out go to: <https://www.mylife.com/ccpa/index.pubview>. You can also call MyLife at 888-704-1900. Press 2 to speak to an operator. Tell the representative that you want your listing removed and provide the information you want deleted. A second option is to request opt out via email at: privacy@mylife.com. Be sure to specifically request your information is removed from Wink.com as well as MyLife.com.



PeekYou



To opt out of PeekYou, fill out the form at: <http://www.peakyou.com/about/contact/optout/index.php>. Select Remove my entire listing under Actions. Paste the numbers at the end of your profile's URL in the UniqueID field. Fill in the CAPTCHA, and you're all set. You'll get an immediate email confirming you've sent in your opt out form and a second email in a few days or weeks to tell you that it has been deleted.

GOOGLE ALERTS

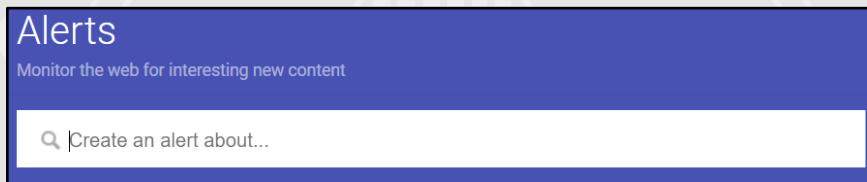


Background

“Google Alerts” is a free Google feature that monitors the internet for mentions of any topic a user specifies. Google collects and packages all instances of these mentions and delivers them to the user continuously (as soon as Google recognizes the mention), daily or weekly. For instance, you may choose to be notified anytime your name is mentioned in an article, when a specific job title is posted, or when your business is mentioned. .

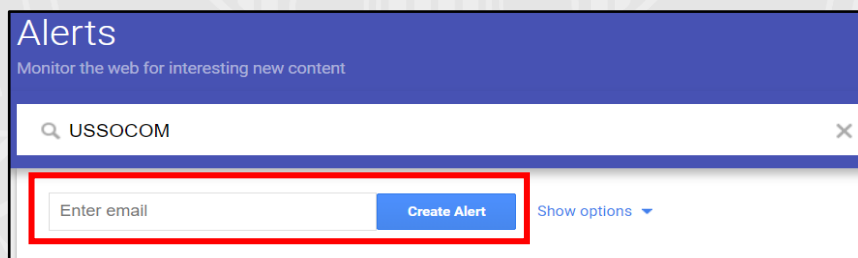
Step 1: Open the Website

To begin, type “Google Alerts” into your search engine, or you can go directly to the website: <https://www.google.com/alerts>. Bookmark this page for easier access in the future.



Step 2: Enter Your Search

Under “Alerts”, enter the topic you would like to receive alerts about. As soon as you begin typing, a sample of your first alert will appear. If you are not getting the results you want, you can change your input right away. You may decide to set an alert for your own name to help monitor what might be out on the internet about you, especially after you have reviewed the “Self-Assessment card”.



Step 3: Create the Alert

Enter a valid email address, where Google will send you the results of your query. Then complete the process by clicking on the “Create Alert” button. (If it doesn’t ask for your email, you are likely already logged into your Google Account, and will receive the emails in the associated email account). You will receive an email from Google Alerts asking you to confirm or cancel this request. Once you confirm the request, you will begin receiving your alerts. Your first basic Google Alert is now complete.

Tip: You can use the search box like you would in Google Search, but avoid general terms or the vast majority of the results will be wildly unnecessary and difficult to sift through. You can use advanced search commands, surround the search in quotes for phrase searches, search on a specific site only, etc.

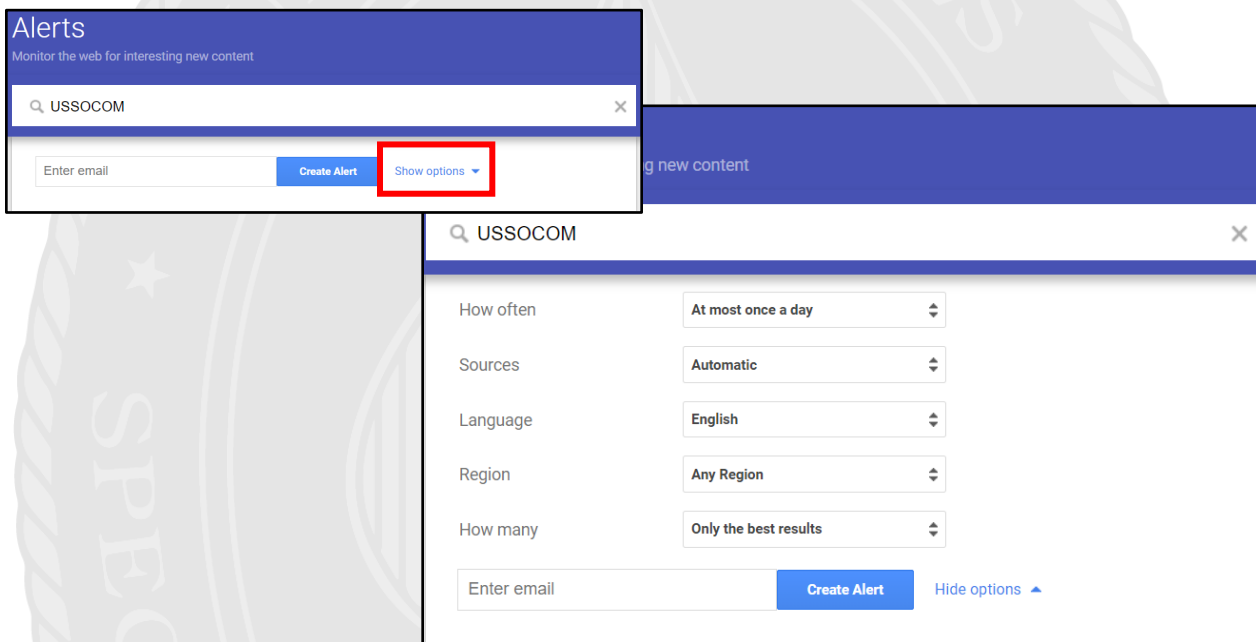
GOOGLE ALERTS



Step 4: Choose Search Parameters

Select “Show options” to adjust:

- How often you want to receive alerts (As it happens, Once per day, or Once per week)
- The source of the search (e.g. Automatic, Video, News, Web, Books)
- The language of the source website
- The region in which the search should take place (like the U.S., Egypt, Spain, etc.)
- How many search results you want to see (Only the best results or all results)
- Where to deliver the Google Alerts data (your email address or an RSS feed)



Modify or Delete Alerts

To modify an alert, select the “Edit” button next to the alert you wish you modify (see the Pencil icon as highlighted below). You may now change the alert keywords, as well as any of the search parameters listed. To finish, select “Update alert” at the bottom.

To delete one or more of your alerts, you can do so easily by clicking the “Trash can” icon next to the alert you wish to delete.



Tip: Emails from Google Alerts are sent from googlealerts-noreply@google.com. You might set up an email filtering rule for messages from that address so that they're sorted into a special folder instead of in your inbox, where they can easily cause cluttering.

ONLINE REGISTRATION



Identify Elements of Social Networking Site (SNS) Accounts

Online services include sites that require users to register and create personal profiles prior to using their service. Best practices include:

- Review the terms of service for each site to determine their privacy policy and data sharing agreements with third party entities.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access to your social security number or physical address.
- Deny options to upload and share your existing contacts during registration.
- Check and, if necessary, change privacy settings to protect your personally identifiable information immediately after completing the registration process.

First and Last Name

First and last name are mandatory for almost all SNS accounts. Some users choose to use their first and middle name instead.

Gender

Gender is a common field to fill out on the registration page, used mostly for future content customization. Whenever possible, avoid making a distinction when signing up.

Email Address

Email is the second most common requirement for creating a SNS account. It is used to verify your account during registration and as a credential for future log-ins.

Sexual Orientation and Relationship Status

These fields are most often required in online dating sites, but are optional on other SNS.

Mobile Phone Number

Registering for email accounts frequently requires a verifiable phone number. Refrain from using services that require phone numbers or opt to use an alternative method to verify accounts.

Username

Username is unique to each user account, unlike first and last name which can be shared across multiple users. DO NOT include personally identifiable information, such as last name or birthday, when creating your username.

Location

Location information is required to various levels of granularity depending on the service. It may include address, zip code, and/or country.

Employment Information

Company and employment information are required for professionally-oriented SNS services.

Birthday

Birthdays are used to verify the user's age and customize age-appropriate content for the user on the site. This information is sometimes published on the SNS profile and must be removed retroactively.

ONLINE REGISTRATION



USSOCOM SMARTCARDS

IDENTITY INFORMATION REQUIRED DURING ONLINE SERVICES REGISTRATION							
	LinkedIn	Amazon	Facebook	Twitter	Instagram	Pinterest	Spotify
First and Last Name	X	X	X	X	X	X	X
Username	*Name by Default	*Name by Default	X	X	X	*Name by Default	Optional
Password	X	X	X	X	X	X	X
Birthday	X	Optional	Optional		Optional		X
Gender	Optional		Optional		Optional	Optional	X
Email Address	X	X	**Optional	X	X	X	X
Phone Number		Optional	**Optional	Optional	Optional		Optional
Country	X	X	X	X	X	X	X
Zip Code	X	X					
Employment	X						
Job Title	X						
Facebook Account	Optional	Optional	X	Optional	Optional	Optional	Optional

*Social media sites default to the "name" provided when settings up the account as your Username, instead of asking Users to create a "handle."
 **Facebook requires a mobile number or email address when registering. Consider using a Google Voice number for two factor authentication.

It is easier to simply sign-up or register on a social media site when you link other accounts to them. Usually, it is a simple click of the button. However, it is NOT recommended to do this.

If someone gains access to your Facebook account and you have signed up for other social media (SM) accounts using Facebook, then that likely gives them access to those other accounts, as well. Treat SM account creation just like your password; create a new and unique one for each site you wish to sign up for.

Additionally, it is always best to use a current email for any social media use. This way, if something were to happen to your account, you're immediately notified and can quickly correct the problem. If you have an email account that you do not check routinely, or that has suffered a major data breach, you might not know if someone hacked into your social media account(s) until it is too late to fix.

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Common identity elements required by SNS for creating accounts and participating in their online services are shown above.

TWITTER

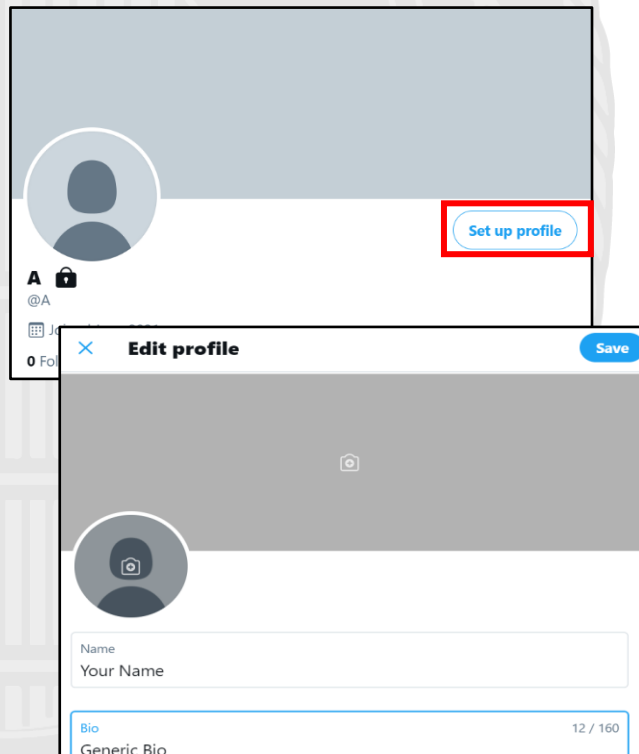


- **Do** be careful when using #hashtags in Tweets as it allows users to index and associate your Tweet with a particular topic.
- Do ensure that family members take similar precautions with their accounts.
- **Do** use caution when posting images and videos of any kind. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- **Do** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- **Don't** provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your Tweets.
- **Don't** link your Twitter account to any third-party applications such as Facebook, LinkedIn, or fitness apps.
- **Don't** allow Twitter to access your location. Disable location services when posting images on whichever device you are using whether it be iOS, Android or uploading them from your computer.
- **Don't** allow people you do not know in real life to follow you. Only maintain connections with people and pages you know and trust.

Your Profile

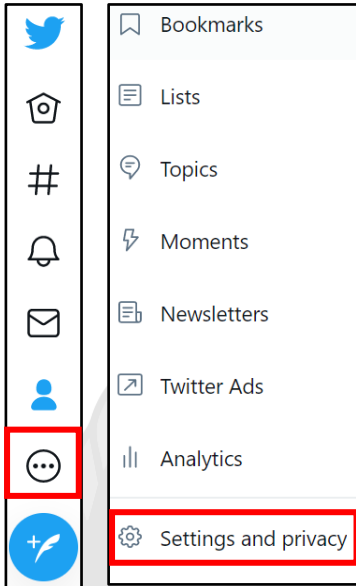
Let's start to lock down your account on your PC (web-based version) by first checking out what your "Profile" says about you. Click the "Profile" icon at the lower left of the screen — this is likely your profile picture. Click "Edit Profile" or "Set up Profile" as shown to the right.

Notice the "Profile Image" and "Header Image" sections. We recommend that you do not use photos of yourself for your profile and header photos. These are viewable to the public and present an unnecessary vulnerability.



Below the "Profile Image" section are the "Name", "Bio", "Location", "Website" and "Birthday" sections. These are not required to be filled in, and it is recommended that you leave them blank or generic.

Even if you use inaccurate location data, it is possible for someone to tie the data back to you by using data aggregator sites. Personally Identifiable Information (PII) is often used as a means to gain access to certain accounts (banks, credit cards, school etc.). Thus, providing even your birthday could help an identity thief steal your identity.



Settings and Privacy

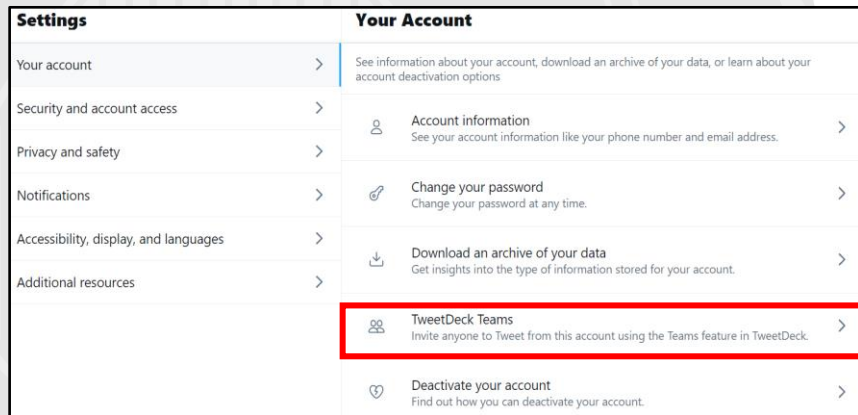
Now, let's move on to the "Settings and Privacy" tab on the same menu at the left-hand side of your screen.

Getting to the "Settings and Privacy" section on your smartphone varies slightly from the computer-based version. These settings need to be updated separately as Twitter is programmed differently on each version. They may not automatically transfer among on your devices.

From here, you will see your setting options and can review your account information, security, privacy and safety, notifications, etc.

TwitterDeck Teams

In "Your Account", identify the "TwitterDeck Teams" section. We recommend you turn the "Twitter for teams" switch off. This will make it so no one can add you to a team without your permission.



Security and Account Access

Next, go to "Security and Account Access". Here you can activate "Two-factor authentication" and "Additional password protection". It is recommended that you chose both.

For the "Two-factor authentication" option, you can choose "Text Message", "Authentication App", or "Security Key".

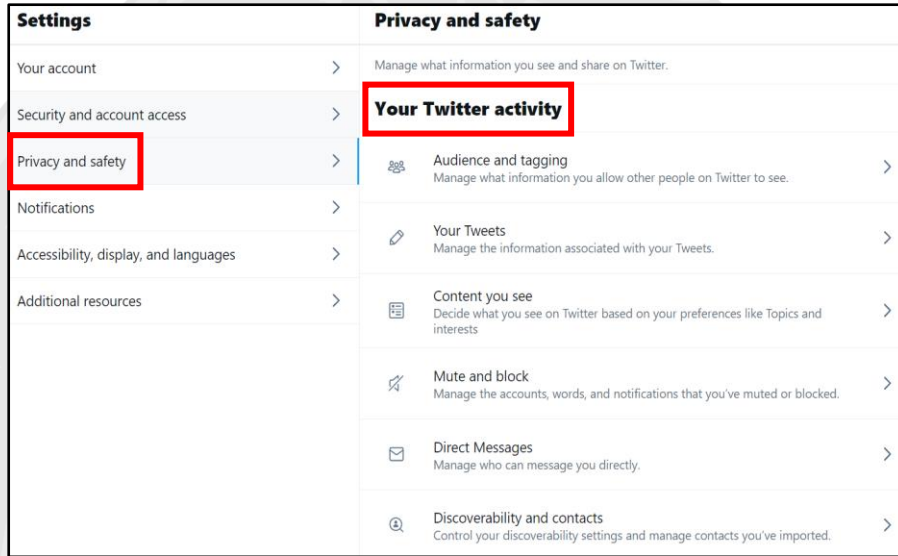
Lastly, ensure "Password reset protect" is checked.

Important Message from Twitter: Changing an account's password does not automatically log the account out of Twitter for iOS or Twitter for Android applications. In order to log the account out of these apps, sign in online and visit "Apps" in your settings. From there you can revoke access for the application, and the next time the app is launched, a prompt will request that the new password be entered.



Privacy and Safety Settings - Your Twitter Activity

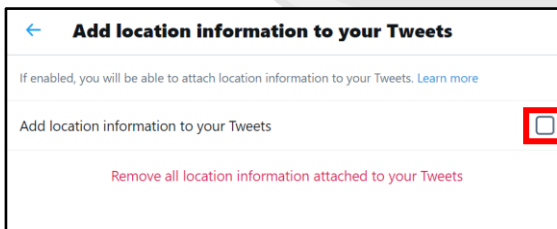
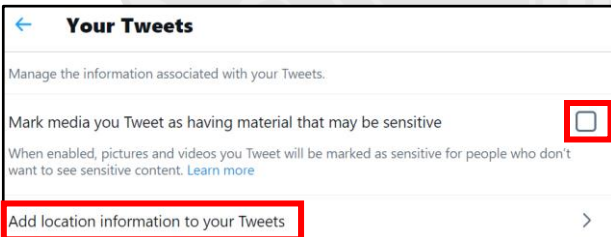
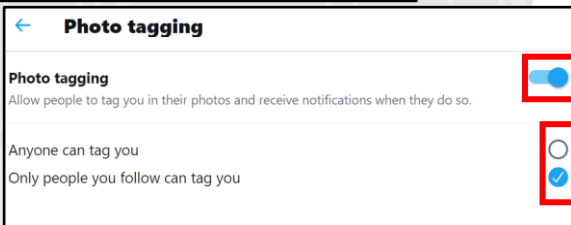
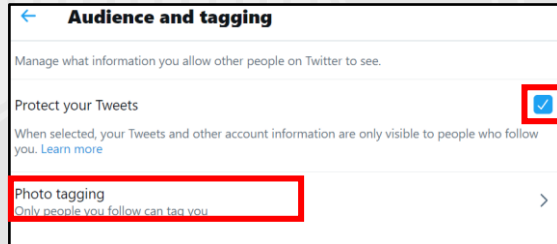
Next, go back to the left column, under “Settings” and select “Privacy and safety” (see below).



Audience and Tagging

First, in the “Your Twitter activity” section, go to “Audience and tagging”. Check the box to “Protect your Tweets” – this makes your account private.

You can also turn off “Photo tagging” options or you can ensure only people you follow can tag you.



Location Information

Next, go to the “Your Tweets” section. Here you can enable or mark your tweets as “sensitive” which will prevent those who do not want to see that type of content from viewing your posts.

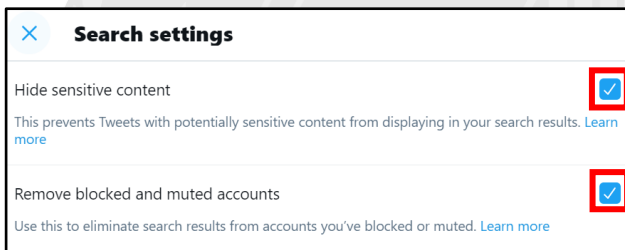
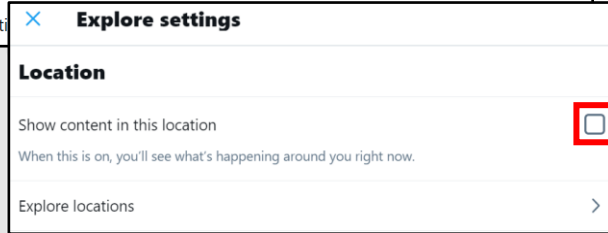
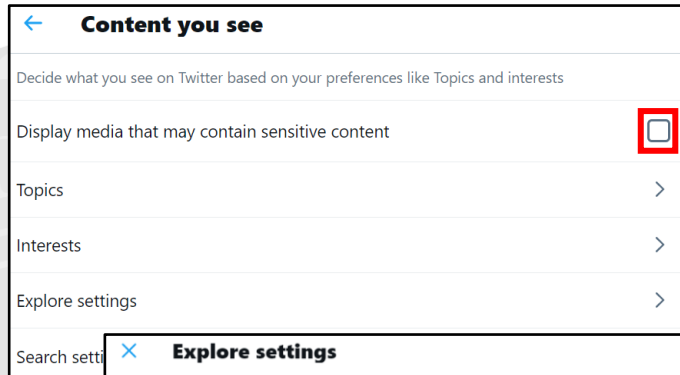
It is also important to remove location data from your tweets. Make sure the box is unchecked in the “Add location information to your Tweets”.

TWITTER



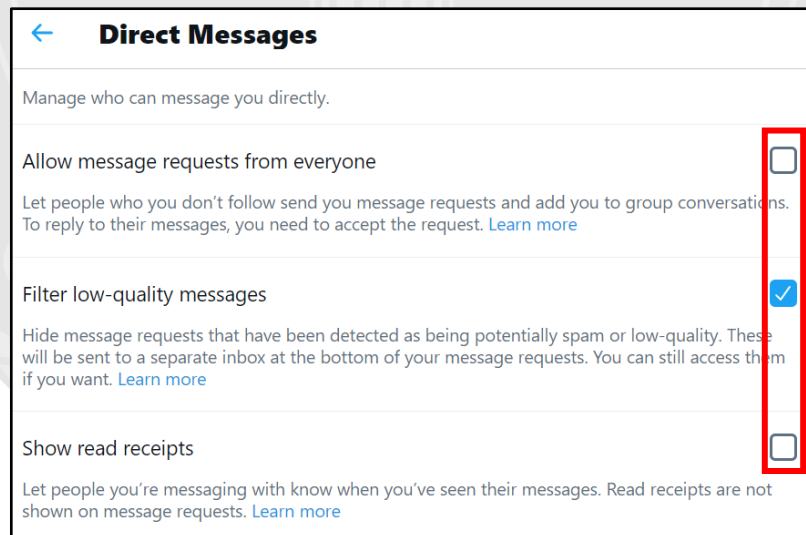
Content You See

Next, you can edit the content you see. This menu is especially helpful if you are locking down your children's accounts. This section also has a location setting in "Explore settings" that uses your location to show you content happening near you. It is best to leave this unchecked. You'll also want to ensure "Search settings" are hiding sensitive content and blocked/muted accounts from view.

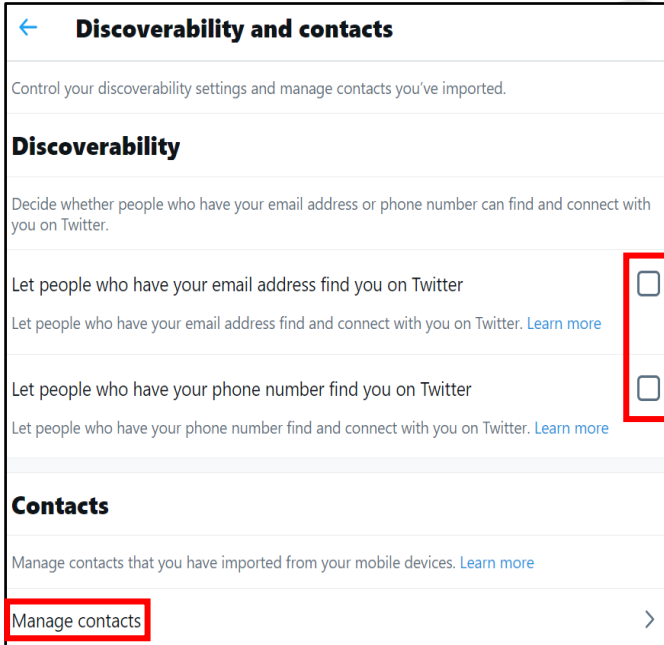


Direct Messages

Another setting to consider is how you're contacted on Twitter. Go to the "Direct Messages" section. Uncheck the first box in this section in order to limit incoming messages from people you do not know. You can also check the "Filter low-quality messages" box which hides messages that are flagged as potential spam.



Hashtags (#) are used to index key words and topics on Twitter, think of them as the topic of your "tweet" or "post". Understand if your account is public, and you use a hashtag on a tweet, anyone who does a search on that hashtag may find your tweet. When you add a hashtag to a tweet, Twitter adds the message to the hashtag group so more users see your "tweet".

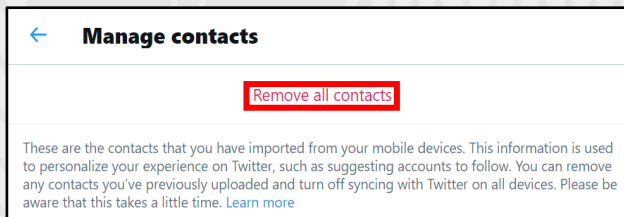


Discoverability and Contacts

In the “Discoverability and contacts section”, ensure both boxes under “Discoverability” are unchecked. It is best to maintain as much control as possible of who is connecting with you.

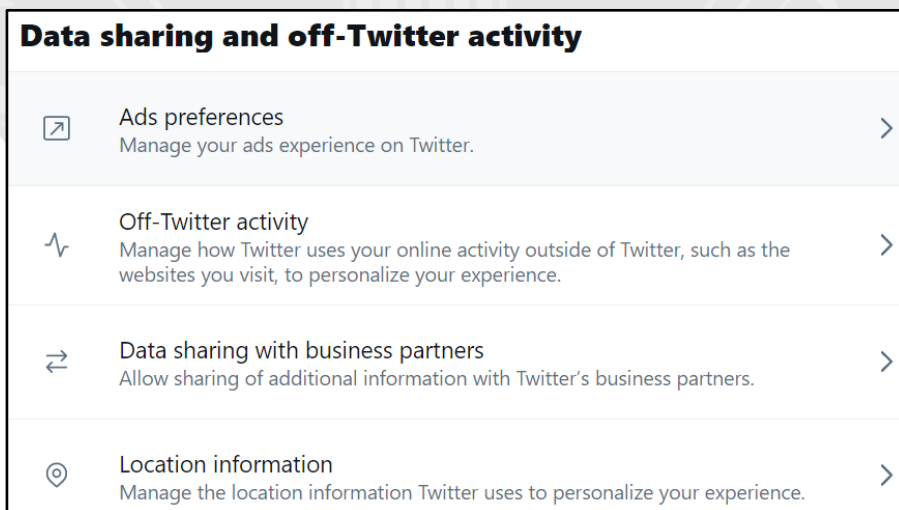
In the “Contacts” section, you can review and remove any contacts Twitter has collected. It is recommended that you not synchronize any of your accounts together, or to include any email accounts with contact information in them. Synchronizing your email accounts allows Twitter to do more than just upload your contacts — Twitter uses the information to learn more about you and your contacts.

“Remove all contacts,” if there are any in this section, and remember to keep your identifying information off your own Twitter account, in case your contacts try to import your data to any of their accounts.



Privacy and Safety – Data Sharing and Off-Twitter Activity

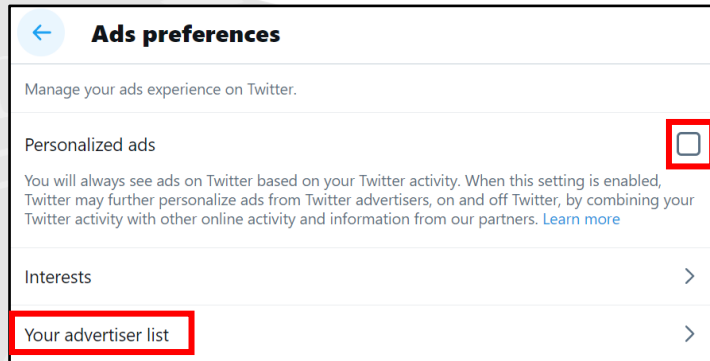
Now, go back to the “Privacy and safety” menu and scroll down. Here, you’ll see “Data Sharing and Off-Twitter Activity”. This is where you can manage ad preferences and other location or data-based information from being used by the application.





Ad Preferences

In the “Ad Preferences” section, make sure you have unchecked the “Personalized ads” box. You can also see the interests that are mapped to you. Lastly, you can see if you are part of a tailored audience in “Your advertiser lists”. Tailored audiences are often built from email lists or browsing behaviors. They help advertisers reach prospective customers or people who have already expressed interest in their business.



Off-Twitter activity

Manage how Twitter uses your online activity outside of Twitter, such as the websites you visit, to personalize your experience.

Allow use of where you see Twitter content across the Web

This setting lets Twitter keep track of your visits to other websites that integrate Twitter content, such as embedded timelines. That information makes Twitter better for you, such as by personalizing your experience. This web browsing history will never be stored with your name, email, or phone number. [Learn more](#)



Personalize based on your inferred identity

Twitter will always personalize your experience based on information you've provided, as well as the devices you've used to log in. When this setting is enabled, Twitter may also personalize based on other inferences about your identity, like devices and browsers you haven't used to log in to Twitter or email addresses and phone numbers similar to those linked to your Twitter account. [Learn more](#)



Data sharing with business partners

Allow sharing of additional information with Twitter's business partners.

Allow additional information sharing with business partners

Twitter always shares information with business partners as a way to run and improve its products. When enabled, this allows Twitter to share additional information with those partners to help support running Twitter's business, including making Twitter's marketing activities on other sites and apps more relevant for you. [Learn more](#)



Off-Twitter Activity

It is also recommended that deny Twitter to ability to track your visits to other websites and your browser history, as well as, turning off the personalization feature.

Data Sharing with Business Partners

Twitter always shares information with business partners. We recommend you change this setting and leave it unchecked, as well.

Location Information

Lastly, you can turn off preferences based on places you've been and can see (and clear) past locations in the app.

Other location settings from previous “Your Twitter Activity” section are also repeated here for you to review and edit as needed.

Location information

Manage the location information Twitter uses to personalize your experience.

Personalize based on places you've been

Twitter always uses some information, like where you signed up and your current location, to help show you more relevant content. When this setting is enabled, Twitter may also personalize your experience based on other places you've been.



See places you've been

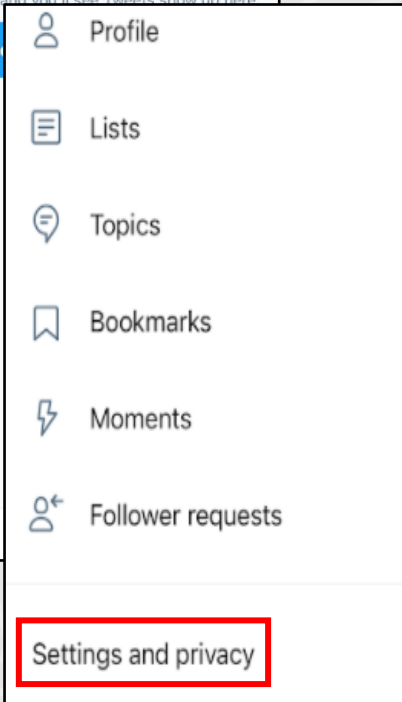
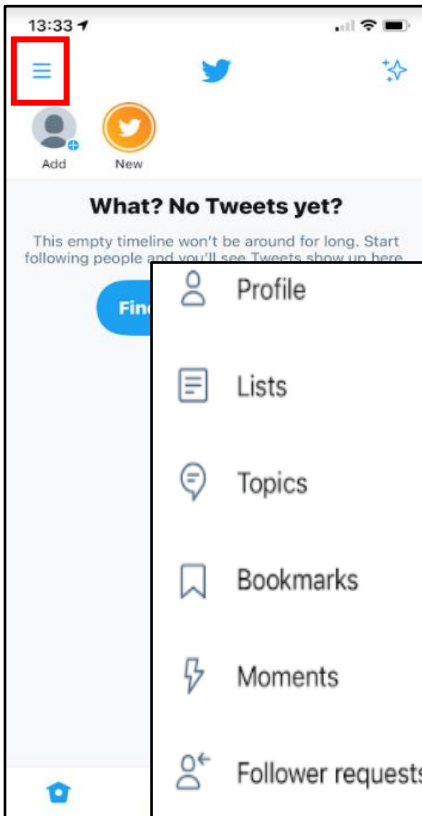
Add location information to your Tweets

Explore settings

TWITTER



USSOCOM SMARTCARDS

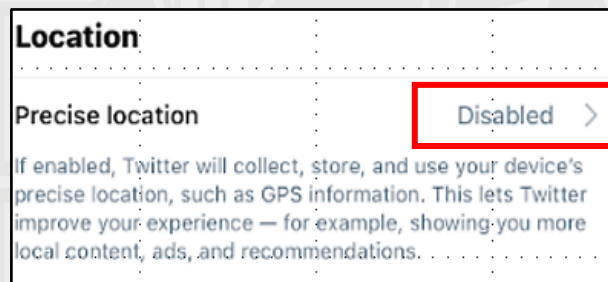
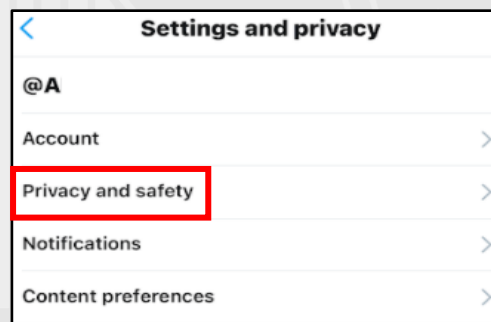


Settings and Privacy

Getting to the “Settings” section on your smartphone is slightly different than the computer-based version. If you frequently access Twitter on your mobile device, you will want to ensure all of the above procedures are completed. Additionally, you will want to accomplish one lockdown feature that is **ONLY** available on your smart device – the “Precise Location” feature.

It is important to turn this feature off because it allows Twitter access to your location for advertisements and photo geo-tagging.

Set your “Location” to “Off” on ALL devices.



iPhone users: select the “Profile” icon at the top left of the screen, then select “Settings and Privacy” at the bottom of the menu. Next, select “Privacy and Safety”, scroll all the way down to “Location”, and “Precise Location” to ensure it is disabled. (see images)

Android users: getting to the “Settings and Privacy” section is similar to the computer-based version. Once you are in the “Settings and Privacy” link, select “Privacy and Safety” then scroll down to the bottom of the page and select “Precise Location.” We recommend that you turn this function to “disable” and then select “done.” (images not provided, but similar).

If you still need help or have questions, you can contact Twitter using their Support handle @TwitterSupport.

INSTAGRAM



USSOCOM SMARTCARDS

- **Do** use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- **Do** remember there are privacy concerns when using your name and birthdate when registering for free services, such as apps and social media. It is not necessary to use your real name or birthdate when creating an account.
- **Do** change your password periodically and turn on Two-Factor Authentication to help keep your account secure.

- **Don't** use geo-location tags—this will prevent others from seeing your location. Instagram deletes metadata from a photo the moment of uploading; however, geo-tags that give your location pose a personal security risk.
- **Don't** establish connections with people you do not know. Understand that people are not always who they say they are online.
- **Don't** forget to remind family members to take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

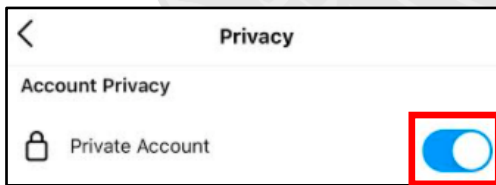
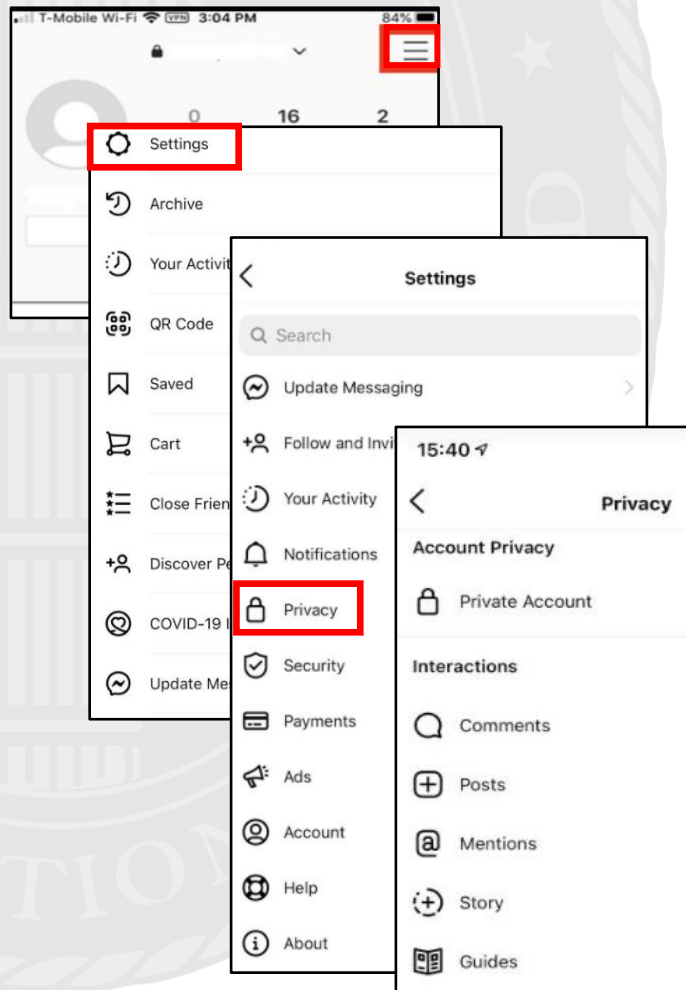
Privacy Settings

It is highly recommended that you set your account to "Private".

Select the "Menu" icon located at the top or the bottom of your screen. Select the first option, "Settings", then select "Privacy."

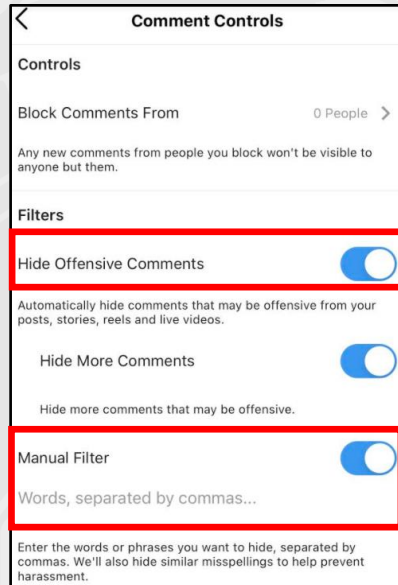
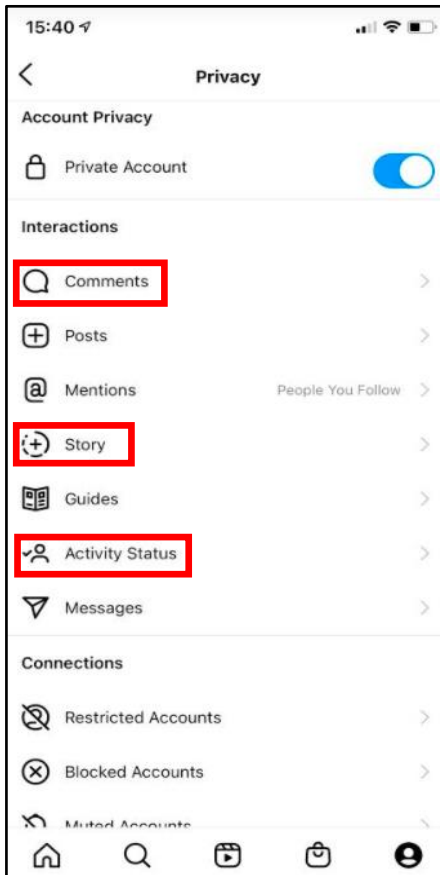
At the top, you'll see the "Account Privacy" section, then toggle "Private Account" to "On." If you are on your computer, the "Settings" tab will be located under your profile icon in the top right.

In "Privacy Settings", you can update settings for "Comments", "Tags", "Mentions", etc.



Instagram now provides you with the ability to update your settings on either your mobile device or computer! It is important to note that some settings are available only on your smart device and a few are only available on your computer, most of the settings are available on your smart device! * Images are of iPhone (iOS)

INSTAGRAM



Comment Controls

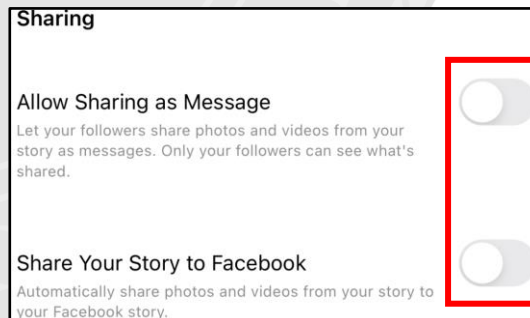
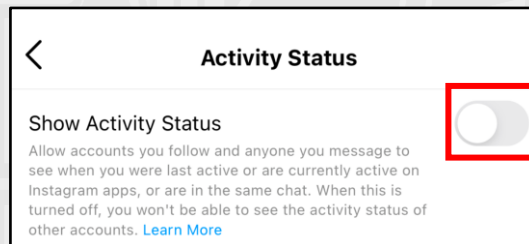
There are many useful features under the “Privacy” tab. First choose “Comments”, then adjust the settings under “Comment Controls”.

Especially for children’s or teen’s Instagram accounts, you may want add and filter the kinds of feedback allowed on their posts. Here, you can block comments from certain people, and filter out offensive comments including specific words you designate yourself.

Sharing and Activity Status

You will also see “Activity Status”. This function allows users to see when you are active on Instagram. If you do not want users to know when you are active you can select “Activity Status” and toggle to “Off.”

In “Story”, identify the section titled “Sharing”, toward the bottom of the page. Here you will be able to turn off the “Allow Sharing as Message” function, which allows others to share stories that you have posted. It is also recommended that you take a second to ensure the “Share Your Story to Facebook” function is “Off”.



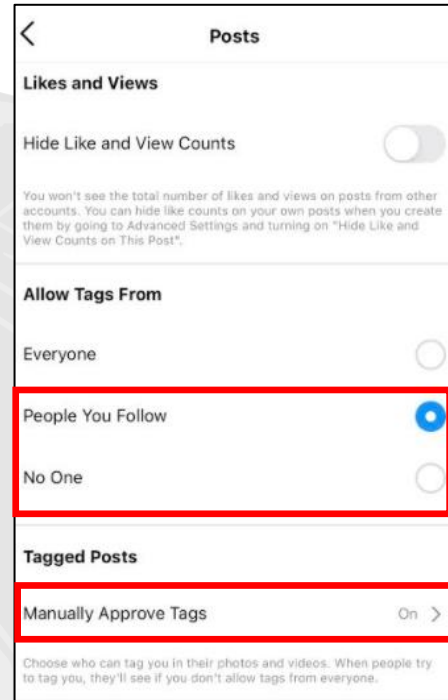
80% of Instagram users are from outside of the US. Therefore, it is extremely important to vet your followers before you trust them with your profile.

INSTAGRAM



Tagging

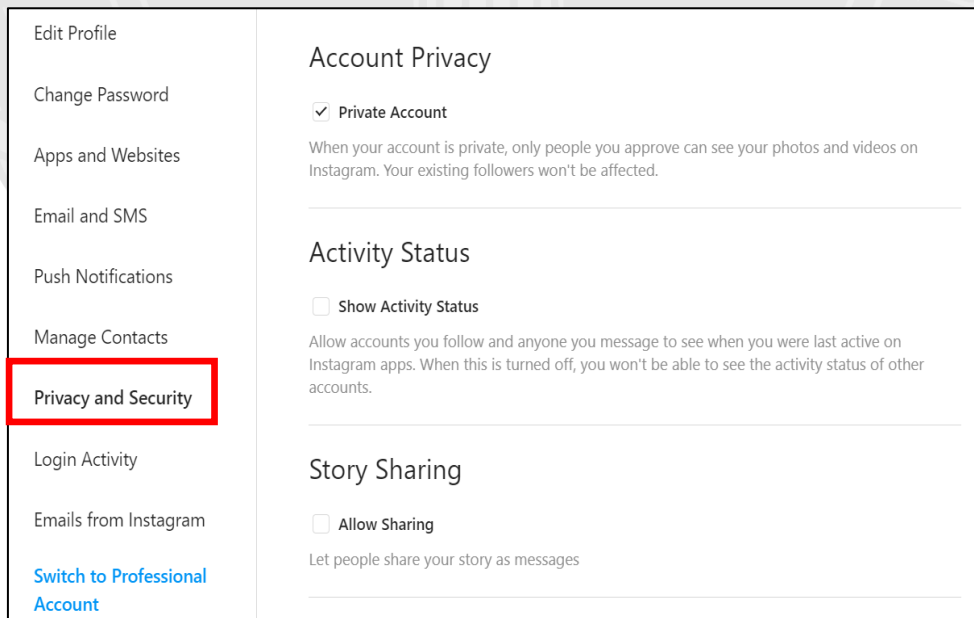
Next, you want to make sure you are in full control of pictures of you that are online - for this, review the “Tags” menu. From the “Privacy” menu, select “Tags”. For best security, identify “Allow Tags From” and select “No One”, which will allow no one to tag you in their photos. Alternatively, choose “People You Follow”. Also, under “Tagged Posts”, ensure that “Manually Approve Tags” is noted “On”, or select this option and toggle it “On”.



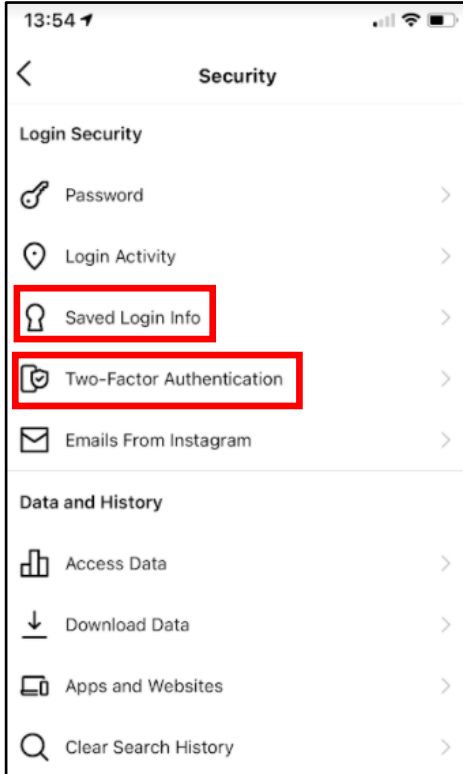
Additional Privacy Setting Considerations

The remaining items under the “Privacy” tab allow you to restrict, block, and mute Instagram accounts as you see fit.

Once you have adjusted the “Privacy” settings on your mobile device, it is a good idea to check them on your computer application as well, to ensure your preferences have been updated.



INSTAGRAM

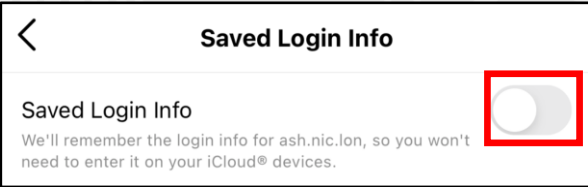


Security Settings

With your “Privacy” secured, the next important feature to address is “Security” on your Instagram account.

Saved Login Information

Back under “Settings”, select “Security”, right under the “Privacy” section you just completed. First, select “Saved Login Info”, then ensure the toggle is set to “Off”. This way, if someone steals your phone, they will not also have instant access to your Instagram account.

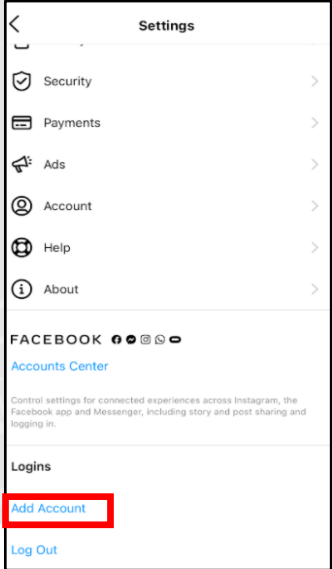


Two-Factor Authentication

“Next, under “Security”, select “Two-Factor Authentication.” It is recommended that you choose this function in order to better protect your account. On the following screen, select “Get Started”, then choose your preferred authentication method, likely “Text Message”.

Adding Accounts

There is a function located in “Settings” called “Add Account”, by which you can add unlimited additional accounts to your mobile device. For instance, a parent would be able to add the child’s account to theirs and monitor activity. Depending on the settings of the account, you may be able to access the added account without entering a password.



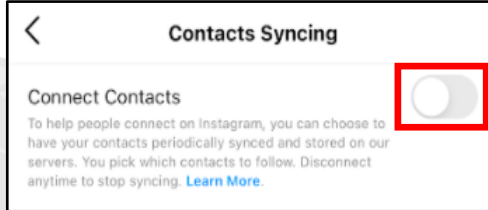
The dangers of the “Add Account” feature is significant for teenagers, who are less inclined to consider security. No one should allow others to “Add Account”. You should not try to access your account on someone else’s mobile device, and always remember to log out, especially when using a different device.

INSTAGRAM



Contact Syncing

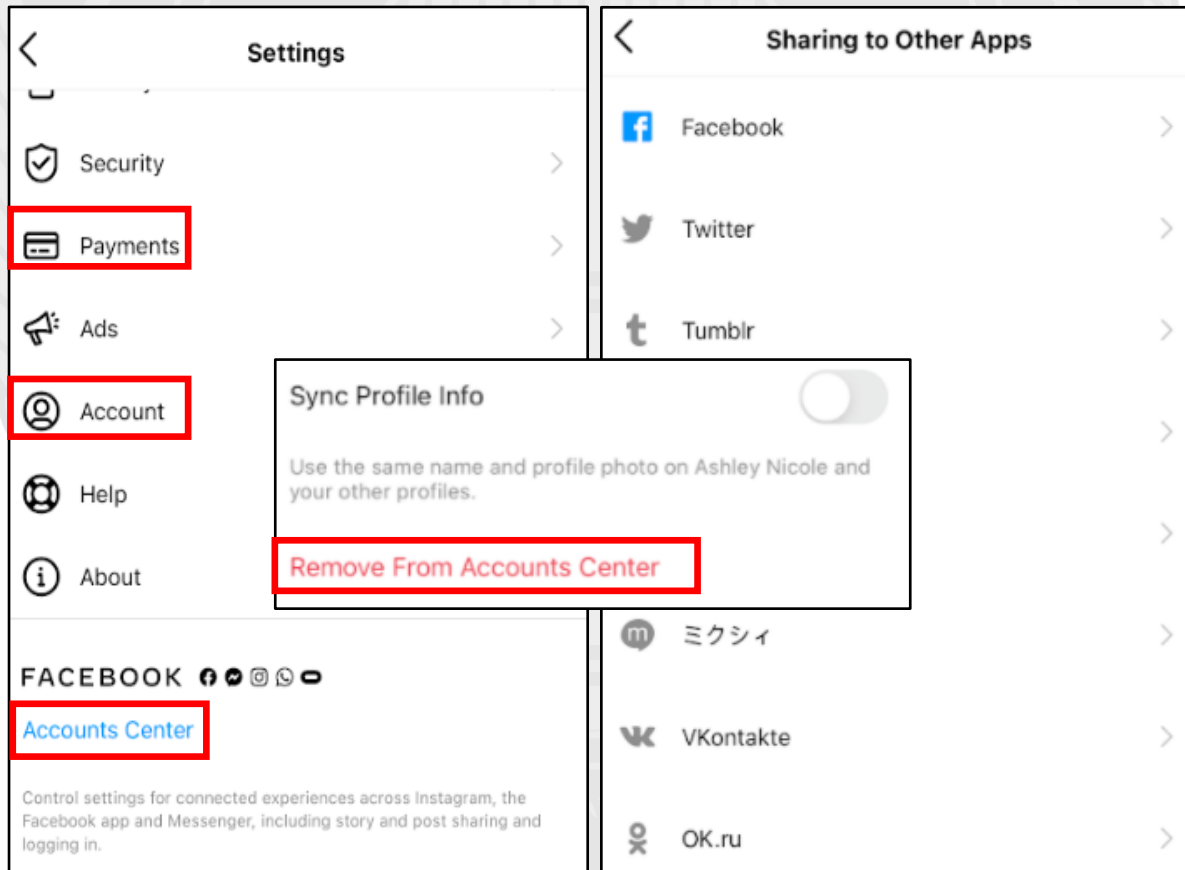
Back in the “Settings” menu, select “Account” then “Contacts Syncing”. It is recommended that you deny Instagram from uploading your contacts by turning “Off” the “Connect Contacts” option.



Additional Account Setting Considerations

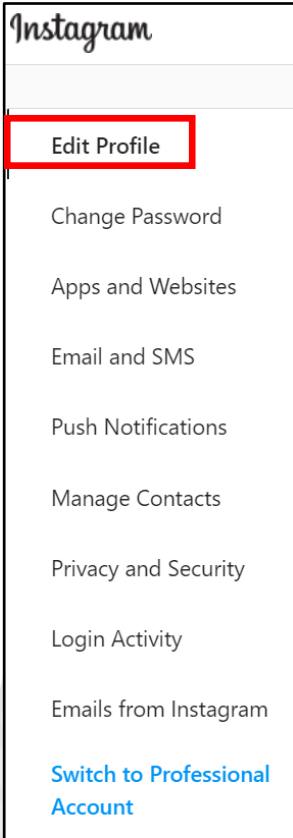
Another option in the “Accounts” tab is the “Sharing to Other Apps” (or Linked Accounts) feature. Here you want to make sure you have not linked any of your social media accounts to Instagram. You can also use the “Accounts Center”.

“Payments” feature allows you to add a payment method to your Instagram account for purchases made in the application. It is not advisable to store credit card or any other payment information on your account.



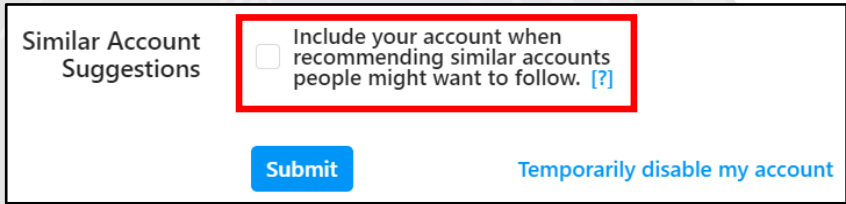
Instagram allows you to have more than one account loaded at a time. Talk to your kids about sharing their usernames and passwords with their friends.

INSTAGRAM



Discoverability

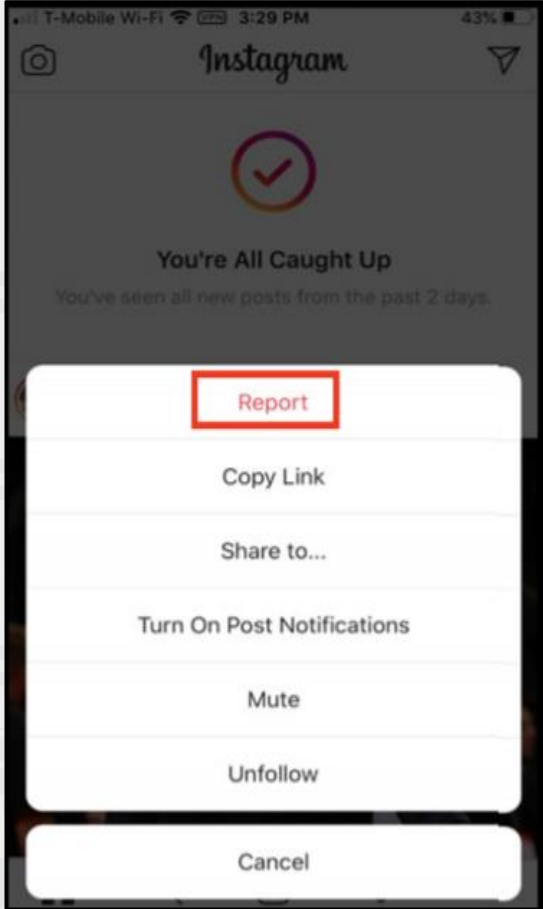
Instagram (personal computer/web-based version) has a feature that allows it to push your profile to other users as “suggested users to follow”. It is recommended you disable this feature. First, select the “Profile” icon, then select the “Edit Profile” button. Once there, scroll to the bottom of the page. *This feature can only be locked down on your computer application.*



Report, Mute, or Unfollow

Instagram allows you to report, or remove from your feed, any offensive post you come across.

Simply select the menu button at the top right corner of the post and select which option best applies to that particular post from the drop-down menu. You have options to “Report” the offensive post, “Mute” the account that posted it for a select period of time, or “Unfollow” the person who posted it. When you report a post, Instagram will ask you for more information as to why you are reporting it, and then offer suggestions to improve your Instagram experience.



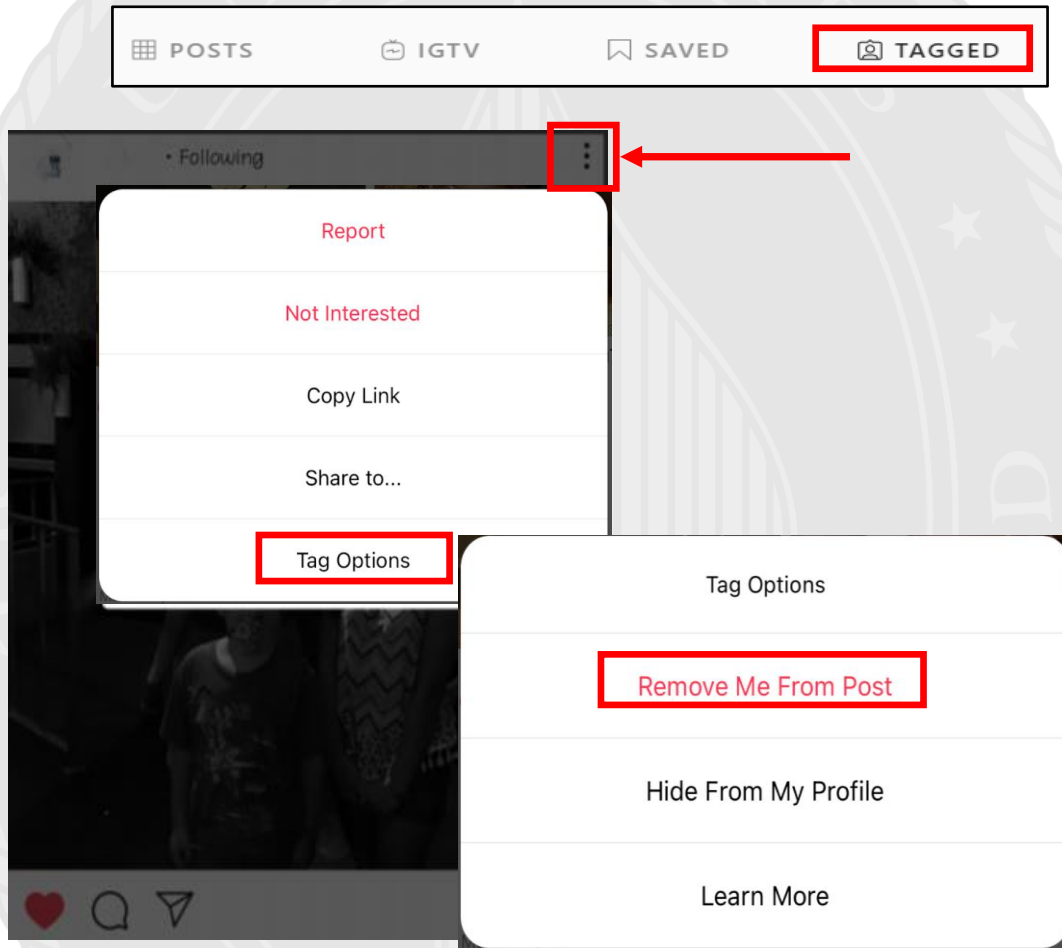
**If you find that someone is impersonating you on Instagram...
Go to <https://help.instagram.com/>, then go to “Privacy and Safety Center”, “Report Something,” and finally select “Impersonation Accounts.”**

INSTAGRAM



Removing Profile from Tagged Content

Removing unwanted tagged photos/posts is important. If you have a profile that is “Private,” you are on the right track to controlling your online image. Understand that even if your profile is private, if you tag or comment on a post from a public profile, your tag or comment will be viewable to all.



First, go back to your “Profile” icon and select the “Tagged” icon. Next, select the post you are tagged in that you wish to un-tag yourself from. Find and select the menu at the bottom of the post (shown to the left of the page by a red box), then select “Tag Options.” Next, you can “Remove Me From Post” simply by selecting the link highlighted here in red.
This may not be available on all devices or the web-based version.

If you still need help or have questions, you can always contact Instagram by:
[https://help.instagram.com/
contact/272476913194545?helpref=faq_content](https://help.instagram.com/contact/272476913194545?helpref=faq_content)

FACEBOOK

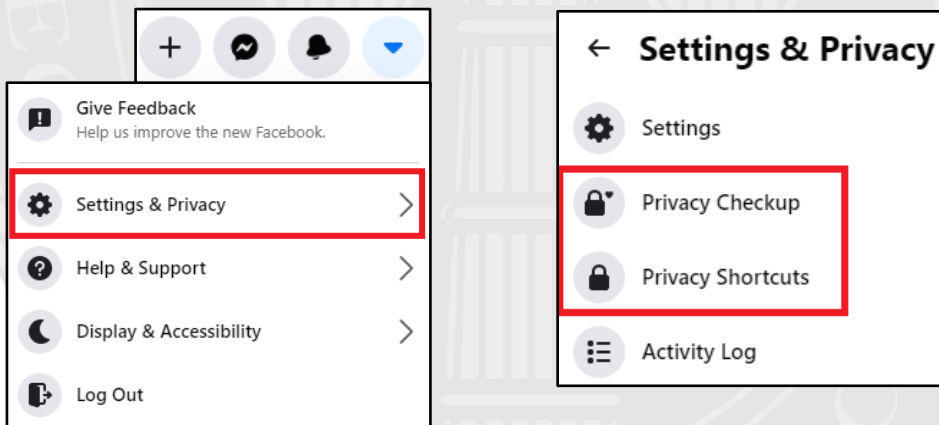


- **Do** use pictures of something other than yourself for cover and profile photos. Cover and profile photos are always Public.
- **Do** use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- **Do** select “Only Me” or “Friends” for all available settings options. Ensure that family members take similar precautions with their accounts.
- **Don’t** add your birthdate, location, phone number, or other personal details to your profile. If you do add this information, make sure its privacy toggle is set to “Only Me.”
- **Don’t** link your Facebook account to any third-party applications such as Twitter, LinkedIn, or gaming apps.
- **Don’t** establish connections with individuals you do not know and trust.
- **Don’t** discuss specific or sensitive details on Facebook, keep discussions general.

Privacy Checkup

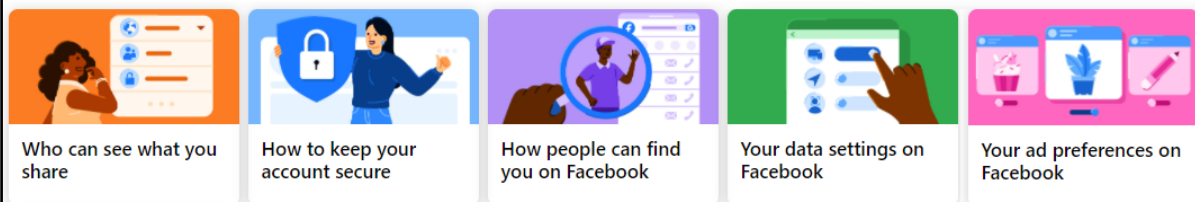
Starting at the Home Page, select the Down Arrow in the top right corner (shown below) and select “Settings & Privacy.” Next, select “Privacy Checkup” and walk through each box on the screen that follows. This is an abbreviated version of the full privacy settings review. You could also use this feature to complete easy quick checks on a regular basis, for instance each month, just to make sure you stay on top of changes. Secondly, you can select “Privacy Shortcuts” to quickly get to additional privacy information and access useful information about Facebook’s ad policy and processes.

In recent years, Facebook has continuously enhanced its privacy efforts to better protect user data. As a result, settings change often, and new settings may be added.



Privacy Checkup

We'll guide you through some settings so you can make the right choices for your account.
What topic do you want to start with?



FACEBOOK



Starting in the “General” section, go through and review your information. Remember, your “Username” (in your profile URL) will be Public, along with your “Name.” In this section you can add a new email address and phone number, direct what happens with your account when you die, and direct Facebook ads to a new email address.

Settings	General Account Settings																		
<ul style="list-style-type: none">GeneralSecurity and LoginYour Facebook InformationPrivacyFace RecognitionProfile and TaggingPublic PostsBlocking	<table border="1"><tr><td>Name</td><td></td><td>Edit</td></tr><tr><td>Username</td><td>https://www.facebook.com/</td><td>Edit</td></tr><tr><td>Contact</td><td>Primary</td><td>Edit</td></tr><tr><td>Ad account contact</td><td></td><td>Edit</td></tr><tr><td>Memorialization Settings</td><td>Decide what happens to your account after you pass away.</td><td>Edit</td></tr><tr><td>Identity Confirmation</td><td>Confirm your identity to do things like run ads about social issues, elections or politics.</td><td>View</td></tr></table>	Name		Edit	Username	https://www.facebook.com/	Edit	Contact	Primary	Edit	Ad account contact		Edit	Memorialization Settings	Decide what happens to your account after you pass away.	Edit	Identity Confirmation	Confirm your identity to do things like run ads about social issues, elections or politics.	View
Name		Edit																	
Username	https://www.facebook.com/	Edit																	
Contact	Primary	Edit																	
Ad account contact		Edit																	
Memorialization Settings	Decide what happens to your account after you pass away.	Edit																	
Identity Confirmation	Confirm your identity to do things like run ads about social issues, elections or politics.	View																	

Under “Security and Login,” look at the “Where You’re Logged In” section and ensure you recognize each location Facebook has you logged in from. Some of these locations can be repetitive based on different sessions, devices, or browsers. If you do not recognize a location, you can select the three dots and choose “Not You?” Facebook will take you through steps to help ensure your account is secure. Next, under “Login”, select “Save your login info”, you have the choice to keep yourself logged in on any device you choose. We recommend that you NOT enable this function, and instead choose to log in each time you open Facebook. This way your account is secure even if you lose your computer or mobile device. Select the “Edit” button to the right, and then select “Remove saved login info”.

Where You're Logged In

	Windows PC · Merrifield, VA, United States Chrome · Active now	
	Google Pixel 4 XL · Merrifield, VA, United States Facebook app · 14 hours ago	Not You? Log Out

[See More](#)

Save your login info
It will only be saved on the browsers and devices you choose [Edit](#)

We recommend that you enable Two-factor Authentication which will give your account the highest level of security available. Click on the “Edit” button to the right of “Use two-factor authentication” and choose the security method you prefer or are most familiar with. A security code will be sent to you for verification each time you log in.

Two-Factor Authentication

Use two-factor authentication On • We'll ask for a code if we notice an attempted login from an unrecognized device or browser. Edit
Authorized Logins Review a list of devices where you won't have to use a login code View
App passwords Use special passwords to log into your apps instead of using your Facebook password or login codes. Add

FACEBOOK



Next, go back to the column on the left-hand side and select “Your Facebook Information.” Select “Off-Facebook Activity” and clear your history. It is highly recommended that you forbid Facebook from tracking your “Off-line Activity. Select “Clear History” and click on the “Clear History” button on the pop-up. Also consider selecting “More Options”, then “Manage Future Activity” in order to limit the kinds of information Facebook can collect from your “Off-Facebook Activity” in the future. Follow the prompts to “Manage Future Activity”.

Now head back to your “Settings” page and select “Privacy” from the tabs on the left side. Completing this section is one of the most important aspects to keeping your information safeguarded on Facebook. This section puts you, the user, in charge of decisions about where your data goes and who can see it. Take some time to ensure each section is set to your preference. It is recommended no category be set to “Public”. If you have friends on your Facebook that you do not fully trust, it is a good idea to select “Only Me” where your personal information is concerned.

We recommend choosing “Only Me” wherever possible but understand that this sometimes undermines the social purpose of Facebook. We strongly recommend you leave the “Only Me” setting for “Who can see your friends list” to protect yourself and your social network. Where you cannot leave “Only Me” selected, the next best option is to choose “Friends.” Finally, we recommend you do not allow Facebook to link other search engines to your profile.

Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Who can see the people, Pages and lists you follow?	Custom	Edit
How People Find and Contact You	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Custom	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

FACEBOOK



Next, head back over to the left side “Settings” menu and select “Face Recognition.” It is recommended here that you not allow Facebook to recognize your face in videos or photos. Simply select “Edit” and from the drop-down menu that appears and then select “No”.

Face Recognition Settings

This setting allows Facebook to recognize whether you're in a photo or video. For more information about how and when we recognize you, visit the [Help Center](#).

Face Recognition Do you want Facebook to be able to recognize you in photos and videos? **No** [Edit](#)

Now select “Profile and Tagging” from the side “Settings” menu. It is recommended that all items be updated from “Public” to either “Friends” or “Only Me.” Make sure to turn “On” each section under “Reviewing” so that any tag created with your name on it is reviewed by you in case you do not agree with the content and want the tag removed.

Under “Reviewing”, you can also view your profile from the perspective of the public. Select “View As” next to “Review what other people see on your profile.” While reviewing your profile from the public perspective, take note of anything you want to lock down or delete, such as old profile pictures.

Profile and Tagging

Viewing and Sharing	Who can post on your profile?	Friends	Edit
	Who can see what others post on your profile?	Friends	Edit
	Allow others to share your posts to their stories?	Off	Edit
	Hide comments containing certain words from your profile	Off	Edit
Tagging	Who can see posts you're tagged in on your profile?	Friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends	Edit
Reviewing	Review posts you're tagged in before the post appears on your profile?	On	Edit
	Review what other people see on your profile		View As
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

In the “Location” section make sure Facebook shows your location as “Off.” You must also turn your location settings to “Off” on each of your mobile devices to ensure you do not share location data with Facebook.

Location Settings

To help explore what's around you, Location History allows Facebook to build a history of precise locations received through Location Services on your mobile devices. Only you can see this information, and you can delete it by viewing your Location History on your mobile device or on your computer. [Learn More](#)

[View Location History](#)

Location History Turn on Location History for your mobile devices? **Off** [Edit](#)

FACEBOOK

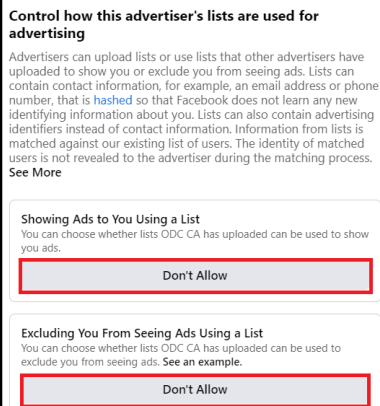
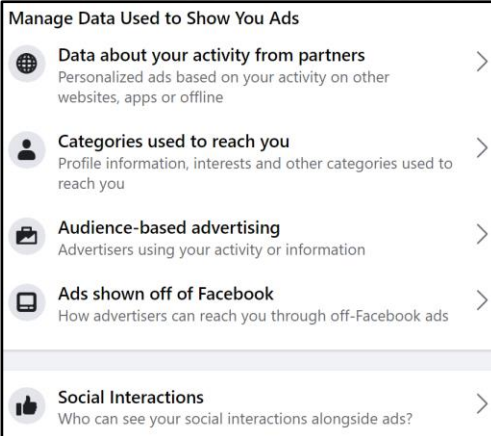
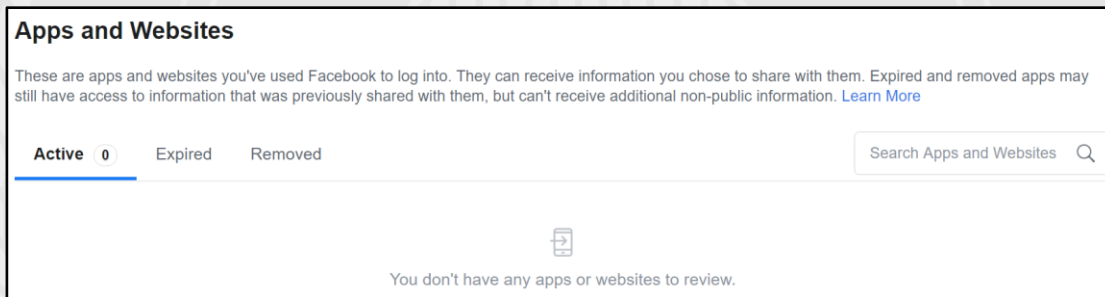


Since the “Stories” function has become more popular, it is important to remember it also needs to be locked down. Facebook has created a new feature that prohibits others from sharing your Stories. Select “Stories” from the Settings menu and set both “Sharing Options” to “Don’t Allow.”



Now is the “Apps and Websites” section. For security purposes, this section should have zero apps or websites listed. If there are any apps or websites listed, it means you have allowed them log you in with your Facebook account or to share data between platforms.

If you have allowed apps or websites access to your Facebook account, you can remove and delete that access here. Make sure to check the “Active” and “Expired” section tabs at the top of this box.



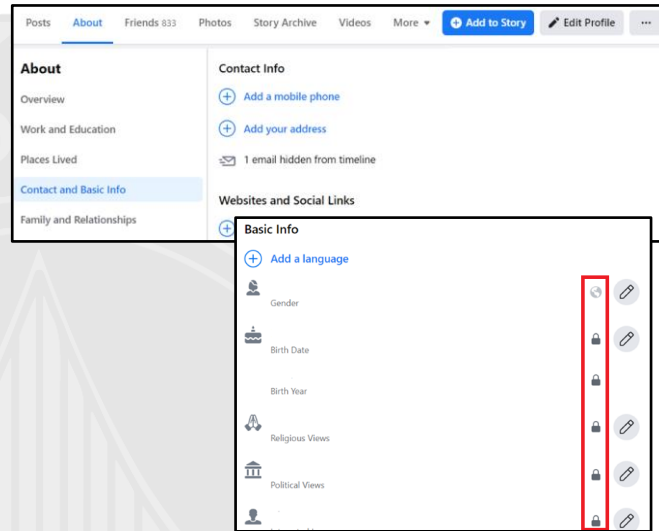
On the left side “Settings” menu select “Ads” where you will be redirected to the “Ads Preference” section. Most important is the “Ad Settings” section. In this section you can manage where Facebook allows ads to pull information from about you. It is recommended that you do not allow Facebook to personalize ads for you on any account you may have linked to Facebook (which ideally should be none). Next in “Categories used to reach you” it is recommended that you toggle each section to off so that Facebook ads cannot use your personal information to provide ads to you. In this same section it is also important to review the “Interest Categories” and the “Other Categories,” both of which have additional information to be limited. Now, select “Audience-based advertising” to review each advertiser that uses your information to generate ads. It is best practice to go through each listed advertiser who is using your information. Select the advertiser then select the section under “Why are you in this advertiser’s audience?” and select “Don’t Allow” (shown to the right highlighted in red) in each section where it is permitted. Finally, select “Ads shown off of Facebook” where it is recommended you select “Not Allowed” to prevent advertisers from pushing ads to you off of Facebook.

FACEBOOK

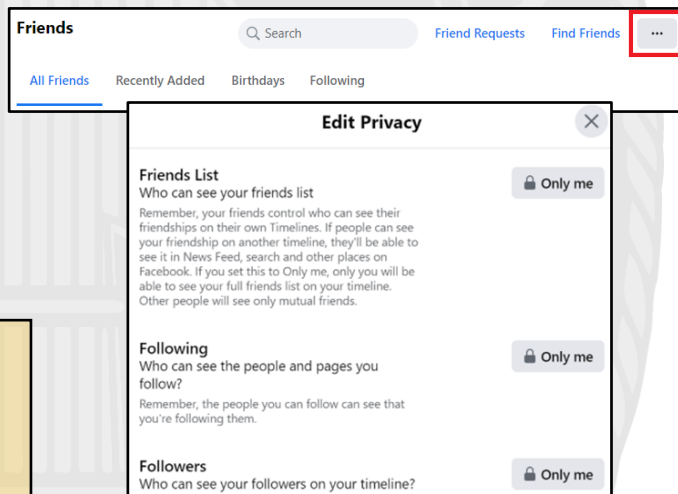


USSOCOM SMARTCARDS

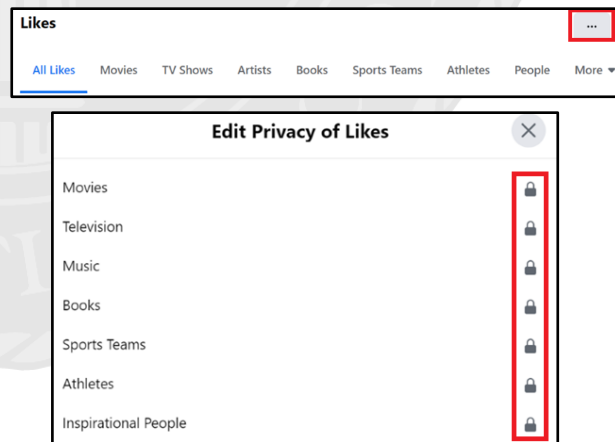
Now that you have completed the “Settings” sections, let’s secure your personal profile information. From the “Home” screen, select your profile picture or username to take you to your profile page. Next, select “About” on your profile page. You should go through each topic in the “About” section and make sure the privacy settings are as secure as possible. You will see two update opportunities for each item: privacy and edit. For whom the information is seen by, we recommend you choose “Only Me” as much as possible, and “Friends” as a second choice. When editing, remember to include the least amount of information possible wherever you can. You can leave some inputs blank but when you need to provide information, keep it vague.



Next to this is the “Friends” section. Here, select the ellipsis button in the upper right corner of the section. Select “Edit Privacy” and then adjust the settings in the pop-up box (see right). We recommend setting all three options to “Only Me.”



The things you “Like” on Facebook can be analyzed to create an accurate profile of you. This information can be a lot more dangerous than you might imagine. In the “About” section, scroll down to the “Likes” section and you will be able to control who sees each category by selecting the ellipsis button to the right of each interest (e.g.: sports, music). Select “Edit Privacy” and set your “Likes Privacy” icon to “Only Me” or “Friends” on each section. “Only Me” is the most secure choice and recommended whenever possible.



Although you have enhanced the security of your “Likes” categories, you will need to repeat the process in each section that is currently visible on your profile. If you do not need people to be able to view your “Like”, it is highly recommended that all topics be “Only Me” in order to prevent unknown users from gaining information about you.



- **Do** take time to clean up old credit cards from your account.
- **Do** use Two-Factor Authentication to protect all your information on Amazon. With all the information that Amazon captures it is important to make sure it is protected by every means available.
- **Do** frequently update your password for Amazon.

- **Don't** link any other accounts to your Amazon account. This will limit what outsiders can find out about you, to include your pattern of life and hobbies.
- **Don't** fall for scams on Amazon or from emails that appear to be from Amazon.
- **Don't** buy from international sellers. Avoiding this will help protect you from identity theft and scams.

Your Account

In order to lock down your Amazon account you will need to access “Your Account,” located on the upper right side of your screen. You will notice, to the right, a visual representation of the Amazon Drop down menu and all three sections within the “Account” section. Each of these sections will be noted periodically throughout this guide please take note of them here as a reference point.

Looking towards the upper right of your screen, see “Account & Lists” and select the down arrow. From this list, select “Account.”

Hello, Sign in
Account & Lists ▾

Your Account

Account

Orders

Recommendations

Browsing History

Watchlist

Video Purchases & Rentals

Kindle Unlimited

Content & Devices

Subscribe & Save Items

Memberships & Subscriptions

Prime Membership

Amazon Credit Cards

Music Library

Start a Selling Account

Register for a Business Account

Your Account



Your Orders
Track, return, or buy things again



Login & security
Edit login, name, and mobile number



Prime
View benefits and payment settings



Gift cards
View balance, redeem, or reload cards



Your Payments
Manage payment methods and settings, view all transactions



Your Profiles
Manage, add, or remove user profiles for personalized experiences



Your devices and content
Manage your Amazon devices and digital content



Your Messages
View messages to and from Amazon, sellers, and buyers



Archived orders
View and manage your archived orders



Your Lists
View, modify, and share your lists, or create new ones

Ordering and shopping preferences

Your addresses
Your Payments
Your Transactions
Your Amazon profile
Download order reports
1-Click settings
Amazon Fresh settings
Language preferences
Manage saved IDs
Coupons
Product Vouchers
VAT registration number

Digital content and devices

All things Alexa
Manage content and devices
Your apps
Prime Video settings
Amazon Music settings
Manage Amazon Drive and photos
Digital games and software
Twitch settings
Audible settings
Amazon Coins
Digital gifts you've received
Digital and device forum

Memberships and subscriptions

Kindle Unlimited
Prime Video Channels
Music Unlimited
Subscribe & Save
Amazon Kids+
Audible membership
Your Essentials
Magazine subscriptions
Other subscriptions

Communication and content


Email subscriptions
Advertising preferences
Communication preferences
Shipment updates via text
Alexa shopping notifications
Deals Notifications
Videos you've uploaded

Shopping programs and rentals

Third Party Credit Card Installment
Manage Your Profiles
Rentals by Amazon
Amazon Household
Shop the Kids' Store by age
No-Rush rewards summary
Teens Program
Pet Profiles
Shop with Points
Amazon Second Chance

Other programs

Account Linking
Amazon credit cards
Your seller account
Login with Amazon
Amazon Pay
Manage your trade-ins
Amazon Business registration
Amazon Web Services
Amazon tax exemption program



Login & security
Edit login, name, and mobile number

Login and Security

Let's look at the "Login & Security" settings first. The "Login & Security" settings are located in the first section of the "Account" page. First, review the general login information provided to ensure its accuracy. Next, head to the "Two-Step Verification (2SV) Settings" section and select "Edit." Now, select "Get Started" (highlighted in red to the right) and follow the steps provided.

Since Amazon retains some of your most sensitive information, like your credit cards and address, this feature is important to help secure your account. Here, you can set up "Two-Step Verification" for your account. It is highly recommended throughout this guide that, where possible, you turn on "Two-Step Verification" in order to help prevent others from gaining access to your account.


Login & security

Name:	Edit
Email:	Edit
Mobile Phone Number:	Edit
Password: *****	Edit
Notice suspicious activity?	
Two-Step Verification (2SV) Settings: Manage your Two Step Verification (2SV) Authenticators	Edit

Devices and Content

Now, let's go back to the "Account" page and select "Your devices and content", then select "Change your digital and device settings" which will likely open the "Preferences" section if not select "Preferences" from the top menu.

You may want to review the settings to make sure the content agrees with your needs. We recommend that you review "Saved Wi-Fi Passwords" to make sure there are no passwords saved that you do not want Amazon to retain. There is a plethora of other settings to check within this section and it is recommended periodically that users revisit this site to ensure all settings have remained intact.



Your devices and content
Manage your Amazon devices and digital content

Things you can do

View or cancel your digital orders	Manage devices
Ask the Amazon Community	Manage digital content
Change your digital and device settings	Install or remove apps

Your Saved Wi-Fi Passwords
All Devices



Alexa Voice History

Now look to the “Manage Your Content and Devices” header menu and select “Privacy Settings” and either select “Alexa Privacy” from the drop menu or simply select the full menu and then select “Alexa Privacy.” Here users can review the privacy settings associated with any of their Alexa devices.

First look to the right (shown here to the left) to find the “Alexa Privacy” menu and select “Review Voice History.” Here you can review every sound detected by Alexa, which includes but is not limited to, any/all commands you have ever ask of Alexa. It is recommended that periodically users visit this section and clear your command history the same way you would clear your cookies and cache from the internet. Select the time frame you wish to review/delete and then select “Delete Detected Sounds History.”

Next, locate “Review History of Detected Sounds” from the side menu to review any sound Alexa may have picked up over the course of her “life”. It is recommended here also that this section be periodically deleted.

Manage Your Content and Devices Content Devices Preferences **Privacy Settings**

Overview
Review Voice History
Review History of Detected Sounds
Review Smart Home Device History
Manage Skill Permissions
Manage Your Alexa Data

Review Voice History

Review and manage your voice recordings.

Displaying: **Today** , **All devices**

Delete all recordings from today

Review History of Detected Sounds

History of Detected Sounds shows events you have opted to have Alexa detect, such as Smart Alerts for the sounds of glass breaking or smoke/CO alarms. You can filter by date and choose an entry to see details, listen to and delete recordings.

To learn more about the events you have opted to have Alexa detect, and the devices on which Alexa is detecting them, [click here](#).

Date Range

All History ▾

Delete All Recordings for All History



Smart Home Device History

Now, select “Review Smart Home Devices History” here users can review all devices that are connected to Alexa, which also means they are connected to Amazon and can potentially make purchases on that connected account. This section should be reviewed quarterly to ensure only trusted devices are connected to Alexa and all others are deleted.

In the next section, “Manage Skill Permissions,” users can review any “skills” they may have enabled Alexa to have, such as accessing a devices street address or email address. It is not recommended that any of these “skills” be enabled. Finally, select “Manage Your Alexa Data” and review any information here that you do not wish Alexa to have or you can set how long information such as recordings are kept. Once you have completed this section head back to the main Account section.

The screenshot shows the 'Smart Home Device History' settings page. A red box highlights the 'One-time deletion of all history' option, which is described as 'Allows you to delete all of your third-party smart home devices history'. A modal dialog box titled 'Delete Smart Home Devices History' is overlaid on the page, containing the following text: 'You can choose to delete information about third-party smart home devices connected to Alexa. Deleting this information from Alexa may degrade your Alexa experience and certain smart home features. It will not delete other information we have about your smart home devices, such as device type or name, and will not delete information about requests you made to Alexa regarding your smart home devices. Are you sure you want to proceed?' The dialog has 'CANCEL' and 'DELETE' buttons.

Smart Home Device History

Alexa receives information about the status and use of third-party smart home devices connected to Alexa, such as the state of your connected switches (on/off) and thermostats (set temperature, household temperature).

Alexa uses this information to better personalize your experience and to help Alexa better for you and other smart home customers.

You can review this information for the most recent 30 days in [Review Smart Home Devices History](#) page. To delete this information, you can use the deletion options below.

Choose how long to save history

Save history until I delete it

One-time deletion of all history

Allows you to delete all of your third-party smart home devices history

Delete Smart Home Devices History

You can choose to delete information about third-party smart home devices connected to Alexa.

Deleting this information from Alexa may degrade your Alexa experience and certain smart home features. It will not delete other information we have about your smart home devices, such as device type or name, and will not delete information about requests you made to Alexa regarding your smart home devices.

Are you sure you want to proceed?

CANCEL **DELETE**

Manage Your Alexa Data

The more you use Alexa, the smarter the service gets by adapting to your speech patterns, vocabulary, and personal preferences. Data from a diverse range of customers also helps ensure Alexa works well for everyone.

Voice Recordings

Voice recordings are used to better understand requests and personalize the Alexa experience. Listen to and delete voice history [here](#).

Enable deletion by voice

Allows you to delete recordings by saying "Alexa, delete what I just said" or "Alexa, delete everything I said today."

Choose how long to save recordings >

Save recordings until I delete them

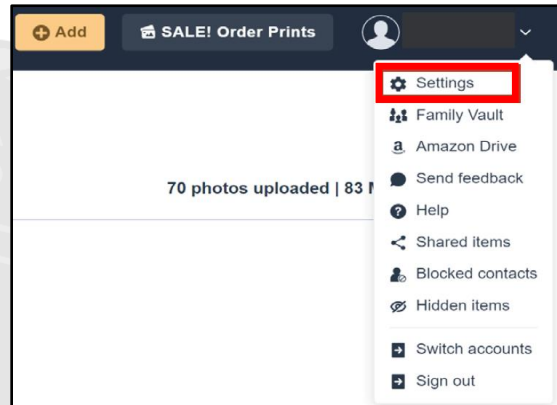


Amazon Drive

Each Amazon account comes with an “Amazon Drive”. In order to lock down your “Amazon Drive,” look to the second section on your “Account” and select “Manage Amazon Drive and Photos.”

On the top right of the screen, select the profile picture to open the “Drive” menu. Next, select “Settings” and review each section present on your screen.

It is important to note there is a new section titled “Use your Alexa Contacts.” It is not recommended that users allow Alexa to obtain access to your contacts, be sure this function is “off”. Other sections to be sure and visit here are “Find People, Places, and Things,” “Add Uploads to Family Vault” as well as the “Manage Third-Party Apps” section.



Use your Alexa Contacts OFF

If you already imported contacts to use with Alexa, you can use these contacts in Amazon Photos. This allows you to share with these contacts whenever you tap the “share” button.

Find People, Places, and Things OFF

Automatically tag your photos by keyword, group together photos of the same people and places, and more.

[Learn more](#)

Turn on image recognition to use Search or People. Image recognition organizes and lets you search for photos based on things in your pictures. This setting applies to all members of your Family Vault.

Illinois residents, by turning on image recognition features, you agree to [this important legal information](#).

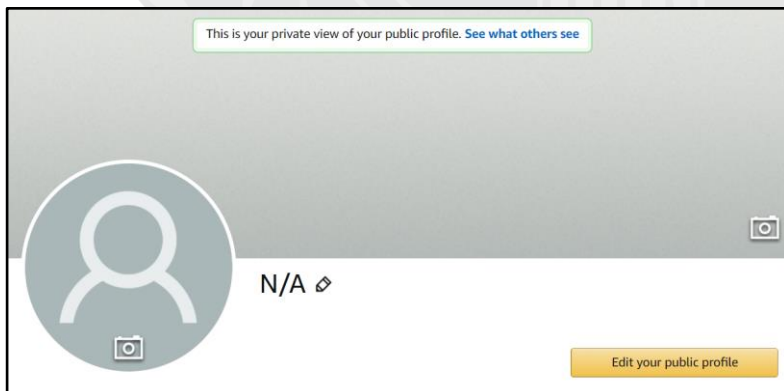
Add Uploads to Family Vault OFF

Automatically add your uploads to the Family Vault so others can see them.

Manage Third-Party Apps

Login with Amazon allows you to log in to registered third-party websites or apps using your Amazon user name and password. It also allows you to opt-in to letting third-party websites or apps read or modify content in your Amazon Photos account. [Learn more](#)

[Manage Login with Amazon](#)



Your Public Profile

Amazon provides you with your own “Public Profile”. This “Profile” and your entire “Amazon Account” can be linked to any of your social media accounts. It is important to review your profile and its settings to ensure it is locked down, not linked to other social media accounts, and not searchable by the public.



Your Public Profile

In order to lock down your public profile, go back to “Your Account”, then select “Your Amazon Profile” under the “Ordering and shopping preferences”, or you can choose the “Your Profiles” icon at the top of the page. From there, follow the steps below and on the remaining pages to best secure your profile.

Select “Edit your profile”. In the “Profile page settings” review all your information to make sure only information you want on public profile is filled in. We recommend you not display your full name in the “Your public name” section.

Scroll down on the page and find the “Add social links to your profile” section to make sure you have not linked any of your social media accounts to your Amazon account.

Ordering and shopping preferences

- Your addresses
- Your Amazon Day
- Your Payments
- Your Transactions
- Your Amazon profile**



Your Profiles

Manage, add, or remove user profiles for personalized experiences

Manage your Profiles

Amazon programs may use these profiles to provide a personalized experience.

Your Name >

Kids >

Looking for your Amazon Public Profile?

Public Profile page settings

View your public profile as visitor

Edit public profile

Edit privacy settings

Your public name

N/A

This will not change the name associated with your account (Ashley Lonergan) [Edit](#)
Your public name will be visible on your public profile page and elsewhere on Amazon.
[Learn more about your public name](#)

Your public information (optional)

Bio

Share a little something about you

Occupation

Share your current job

Add social links to your public profile (optional)

Location

Share where

Facebook

Pinterest

Twitter

Instagram

Youtube

Your public information will be visible on your public profile page.

We will never share what you browse or purchase on Amazon. Amazon will never ask for your account login or password, billing information, or any other account details via your Public Profile page.

[Learn more about your public information](#)



Public Profile – Privacy Settings

Now let's go to the "Edit privacy settings" to review and make sure they are set. Select "Edit privacy settings" to review how they are presently configured. We recommend that you select the box "Hide all activity on your profile" as well as "Hide sensitive activity." Users can view their "Profile" as a visitor, by selecting "View your profile as visitor" from the top right of the "Profile page settings." This capability allows users to ensure their profile is properly locked down so that information specific to the User is not readily available to anyone. Next, scroll down to the bottom of the "Edit privacy settings" and make sure the box titled "Allow customers to follow you" is not checked. It is also important to click on the "See who is following you" link to make sure you have not allowed anyone to follow you up to this point..

Public Profile page settings [View your public profile as visitor](#)

[Edit public profile](#) [Edit privacy settings](#)

What's public on your public profile

When checked, the below settings will be applied to your Public Profile page. Privacy settings that apply to individual activities will always override your general privacy settings chosen here. Changes you make will be reflected across all experiences that you log into using this Amazon account. These settings may not be reflected elsewhere on Amazon. For example if you remove reviews from your Public Profile page they will still be viewable on the product page.

Top Contributor Status (This requires reviews and customer follow to be turned on.) [Learn more](#)

Public activity	Following and badges	Lists
<input type="checkbox"/> Reviews	<input type="checkbox"/> Who You Follow	<input type="checkbox"/> Public Wish Lists
	<input type="checkbox"/> Top Reviewer Badges	<input type="checkbox"/> Wedding Registry
		<input type="checkbox"/> Baby Registry

Hide all activity on your public profile [Read more](#)

Hide sensitive activity [Read more](#)

Follow Settings

If you have any followers, you can delete them from this link and then update your privacy settings to preclude any future followers. We recommend you do not let people follow you on Amazon, especially if you do not know them.

Follow settings:

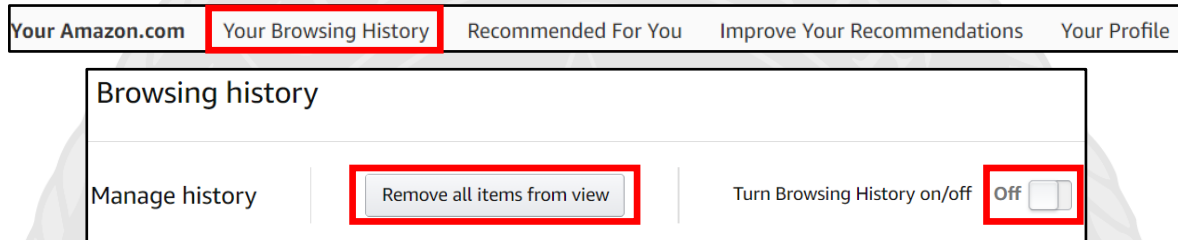
Allow customers to follow you

When customers follow you, they will be notified of your new content, such as reviews or articles. You can turn this off at any time and customers will no longer be following you. We will not share what you browse or purchase on Amazon with your followers.



Browsing History

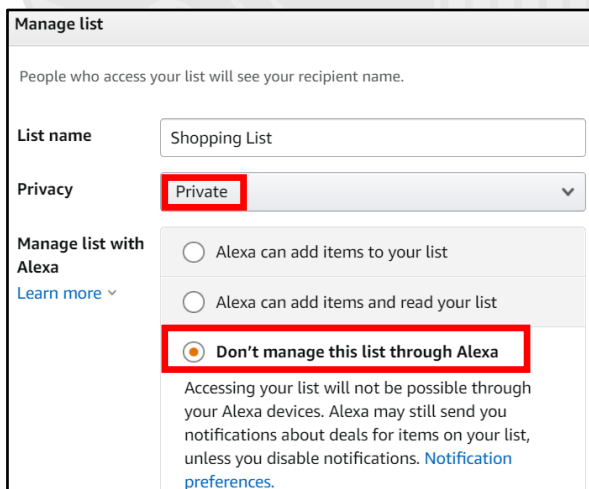
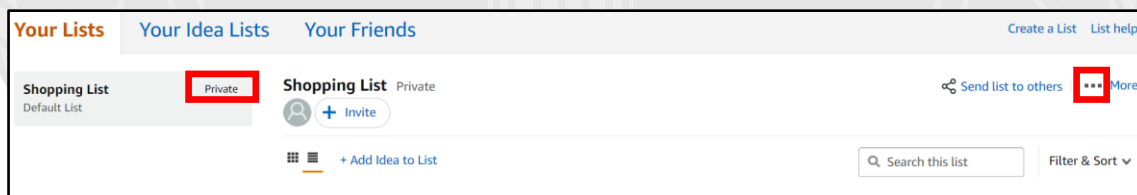
Now let's take a look at "Your Browsing History". Go to the top menu bar, from either the "Your Profile" section or the "Your followers" page and select "Your Browsing History". From here, look at the right side of your screen and select the drop-down arrow next to "Manage history." From here, it is recommended you remove all items and "Turn Browsing History" to "Off."



Wish Lists

One of the most public sections of Amazon is the "Wish Lists." If not made private, anyone can view your lists and gain information about who you are or who the people in your family are (how many, gender, age, etc.). People use "Lists" for making Christmas lists, birthday lists, or even grocery lists. The titles of these lists are revealing (i.e., a child's name for a birthday or Christmas list). These bits of information could be useful to a social engineer or identity thief when combined with other bits of data on you.

Amazon has recently changed its privacy options for "Wish Lists", requiring users to enter an email address in order to access any "Wish List", so make sure that information is locked down. New to the "Wish List", is the option to provide Alexa with access to your "Lists". We do not recommend you provide such access but instead set each list to "Private".



Select the "Your Lists" icon on the "Account" screen in order to begin the process of locking down your lists. Once there, your "Wish Lists" will be on the left-hand side of the screen (see above). In order to review and change these settings, select the ellipses and select "Manage List." From there, select "Privacy" and select "Private" from the list. Be sure to select "Save Changes."



Registries

Much like a “Wish List”, your registries can also be displayed publicly unless, it is therefore important that you go through the “Settings” for any registry you may build on Amazon.

While still in your “Wish List”, go to the top menu and select a Registry to create. To create your “Registry” select “Create a new Registry” from the center of your page. Scroll down to “Who can see your registry” and select “Shared” or “Private” for the visibility of your registry. It is important to note that if you decide to make your registry “Public”, it may be shared on a third-party website – TheBump or TheKnott - unless you “Unselect” that option.

Amazon has created a new registry for birthdays which has many of the same lock down features as the Wedding and Baby registries. Once you have completed the registry and time has passed for its use, it is recommended that you go in remove the data and delete the registry from Amazon.

Happily Ever After

Create a registry that celebrates who you are as a couple. Shop the world's largest selection to find everything you need to build your new life together.

[CREATE YOUR REGISTRY](#)

Do you want your registry to be public or private?

If you change your mind, you can update your preferences in Settings.

Public
I want it searchable on Amazon.com

Private
I want it visible only to myself

Make my registry searchable on TheKnot.com

Audible

Head back to the “Account” section and select “Audible Settings” from the “Digital content and devices” menu. Note: this section is only for users who have also signed up and use Audible. In the “Audible Settings” review each section but pay special attention to the “Profile & Preferences” section.

Here users will want to ensure that the “Allow other Audible members to see my hoisted location on the Audible” is toggled to the “off” position. At the bottom off this page you can also review what devices are registered and authorized to use your Audible account. If you notice any device that you do not recognize simply select “Deregister” next to that devices name.

PROFILE & PREFERENCES

Audible.com Community

[Edit your Audible profile](#)

Allow other Audible members to see my listed location on the Audible Listener Page and with my reviews.

Amazon.com Community

[View your profile](#)

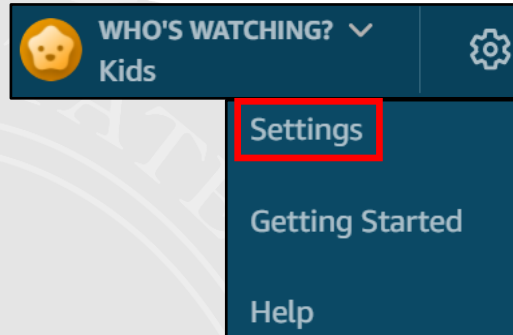




Parental Controls

Let's take a look at the "Parental Controls" and settings located in the "Video" section of Amazon. To do that you will need to go back to "Your Account" and select "Prime Video Settings" under "Digital content and devices."

At the top of the page select "Parental Controls". For parents, it is always important to monitor and protect our children from age-inappropriate material on the internet and television screen. Amazon allows parents to set "Prime Video PINs" and "Viewing Restrictions". Here you can select at what age rating you would like a PIN to be required.



Account & Settings

Your account Player **Parental Controls** Subtitles Your devices Watch History Hidden videos

Prime Video PIN

Your PIN is used to authorize Prime Video purchases and to bypass Parental Controls. [Learn more](#)

Purchase restrictions

To help prevent accidental charges, enable the Prime Video PIN for purchases. [Learn more](#)

Note: Restrictions for Fire devices and Xbox 360 must be set on the device.

 On
 Off

Viewing restrictions

① Viewing restrictions **only** apply to the devices selected below. Restrictions for **Fire TV** and **Xbox** devices must be set on those devices. [Learn more](#)

Videos with these ratings require a PIN: 13, 16, 18

Tap age to set restrictions

- | | |
|----|---|
| G | Videos suitable for General Audiences are available. |
| 7 | Videos suitable for General Audiences and older children are available. |
| 13 | Videos suitable for general audiences, older children and teens are available. |
| 16 | Videos suitable for general audiences, older children, teens, and young adults are available. |
| 18 | All videos, including those not rated or for mature audiences, are available. |



Communication and content

Email subscriptions

Advertising preferences

Communication preferences

Shipment updates via text

Alexa shopping notifications

Deals Notifications

Amazon Advertising Preferences

Interest-based ads are sometimes referred to as personalized or targeted ads. Our [Interest-Based-Ads](#) notice.

Submit Your Preference

- Show me interest-based ads provided by Amazon
- Do not show me interest-based ads provided by Amazon

Submit

Ad Preferences

Now let's check the security and privacy settings regarding advertising and communications on your account. Go back to "Your Account" and in the "Communication and Content" section, select "Advertising Preferences" so we can review what Amazon provides to you and to advertisers.

Personalized ads, sometimes referred to as targeted or interest-based ads are built on information about you, such as the products you view, the purchases you make on Amazon, or websites you visit where Amazon might provide ads or content.

Communication Preferences

Go back to "Your Account" and select "Communication Preferences." Select the down arrow to the right of "Marketing Information by Post" and select "Do not send me marketing information by mail" (highlighted in red to the right). This will help to eliminate spam and other marketing emails from cluttering your inbox. Be sure to select the "Update" button to save these changes.

Communication Preferences Center

We'd like to stay in touch, but only in ways that you find useful.

Mail Preferences

Marketing Information by Post Don't miss out on our best recommendations and deals. Subscribe now to receive personalized mails and newsletters. ▼

Email Preferences

Do not send me marketing information by mail.

General Settings Email is currently being sent to alonerga@mail.usf.edu in HTML (Text and Images). ▼

Promotional Emails You're receiving emails for 0 departments.

Do not send me any marketing email for now



Other Account Considerations

Finally, Amazon has different profiles to help you manage your account and any account you may want to create for your children. For instance, a teenager can have their own log in and purchase ability, while parents maintain control over purchases. Parents can also add any children under 12 to their accounts to help manage the content displayed on certain devices, such as the Fire TV. In order to create these accounts or manage these accounts, select “Amazon Household” or “Teens Program” from the third and final section under “Account.”

The screenshot shows two main sections: 'Teens' and 'Children'. The 'Teens' section is titled 'Teens' and 'Available for ages 13 to 17'. It features a profile icon for 'Abbey' with an 'Add a teen' button and an 'Add a teen' button with a plus sign. Below this is a 'Teen Shopping' section with a house icon and a list of bullet points: 'Teens can shop from their own login and parents approve purchases', 'Parents with Prime share select Prime benefits with their teen at no additional cost', and 'Don't want to approve every order? Skip the approval with teen spending limits'. There is also a 'Teen settings' link. The 'Children' section is titled 'Children' and 'Suggested age: 12 and under'. It features an 'Add a child' button with a plus sign and an 'Add a child' button with a plus sign. Below this is an 'Amazon FreeTime' section with the Amazon FreeTime logo and text: 'Children have access to FreeTime and FreeTime Unlimited on Fire Tablets, Fire TV, Kindle eReaders, and Android phones and tablets. When you create a child profile, we enable a kid-safe web browser in the FreeTime experience. Learn more about the FreeTime web browser and change the web browser settings in the Parent Dashboard.' There are three bullet points: 'FreeTime Unlimited is an all-in-one subscription for children that offers unlimited access to more than 15,000 kid-friendly books, movies, TV shows, educational apps, and games.', 'To select individual titles to share with the children in your Household, go to Your Content and Devices.', and 'To discover the books, videos, educational apps, and games your children enjoy in FreeTime, visit the Amazon Parent Dashboard.'

“Ships from” and “sold by” [seller]: Third-party seller that ships an item from them directly to you. Amazon doesn’t touch the item. This is where scammers thrive.

“Sold by” [seller] and “Fulfilled by” Amazon: A third-party seller sends the product to Amazon’s warehouse, then Amazon ships . These items can be “Prime” eligible, but are still third-party.

PINTEREST



USSOCOM SMARTCARDS

- **Do** use Two-Factor Authentication to protect all your information. Like all social media accounts, it is important to make sure your Pinterest is as secured as possible. Two-Factor Authentication is one of the best ways to control your information.
- **Do** make sure your email is up to date! If Pinterest suspects nefarious activity on your Pinterest account, they will lock your account down and send your new password to the email address on file.
- **Do** monitor what your children and teenagers are looking at on Pinterest. Pinterest does have inappropriate content that, if not specifically tagged as such, will not be flagged or removed by Pinterest.
- **Do** monitor what your children and teenagers are looking at on Pinterest. Pinterest does have inappropriate content that, if not specifically tagged as such, will not be flagged or removed by Pinterest.
- **Do** make your boards private once you create them so that they are not searchable by any and all Pinners.
- **Don't** put personal information on the title of your Pinterest boards. A lot of information can be obtained simply by reading a title (whether or not you have children, rent or own a home, marital status, etc.).

Your Profile

Since there aren't many privacy settings to manage on Pinterest, it is especially important to ensure the ones we have are locked down. In order to change your Pinterest settings on your PC, look to the top right of your screen and select "Settings" (three horizontal ellipses, or a down arrow). Once you are on the "Settings" page you will be able to go through each of the settings provided by Pinterest.

First, let's review the "Edit Profile" page, which provides your basic information on Pinterest. We recommend you avoid using your full name as your "Username", and instead use parts of your name or a nickname. We also recommend leaving the "Bio" and "Location" sections blank. This information is not required. Select "Done" if you make any changes.

A series of overlapping screenshots from the Pinterest mobile app. The top screenshot shows the top navigation bar with a red box around the profile icon and a dropdown arrow. The second screenshot shows the "Settings" menu with "Settings" highlighted by a red box. The third screenshot shows the "Edit profile" screen with "Edit profile" highlighted by a red box. The bottom screenshot shows the "Edit profile" form with red arrows pointing to the "First name", "Last name", "Username", and "Location" fields. The Pinterest logo is also visible in the middle of the screenshots.

PINTEREST



Account settings

Set your login preferences, help us personalize your experience and make big account changes here

Basic information

Email

Password

Change

Country/Region

United States ▼

Language

English (US) ▼

Gender

Male Female Non-binary

Login options

Use your Facebook or Google account to log in to Pinterest.

[Learn more](#)

- Use your Facebook account to log in
- Use your Google account to log in

Account Settings

Next, let's review your "Account settings". Under "Account settings" you will find options to change your email address and password, set your login options, and delete or deactivate your account in the case you decide you no longer want to use Pinterest.

We recommend you always log in with a unique password used only for Pinterest, and never login via Facebook or Google. Ensure the toggles next to these options are set to "Off". If you decide to deactivate your account or delete it altogether, follow the prompts after selecting the correct option. Select "Done" at the top to save your changes.

Deactivate account

Hide your Pins and profile

Deactivate account

Delete account

Delete your account and account data

Delete account

Linking Accounts

The next few settings have to do with linking your other social media accounts to Pinterest. As always, we recommend that you do not link any other social media accounts to Pinterest. If someone gains access to one of your social media accounts, keeping them separate prevents an intruder from accessing all your other accounts.

First, see the "Claim" section. This option allows you to connect Instagram, Etsy, or YouTube accounts, with the purpose of gaining more popularity for your posts across all platforms. We recommend not claiming these accounts.

Claim

Get credit for all your content on Pinterest. When you claim your content, your name and profile picture will show up next to any Pins that come from your site or external accounts.

 Websites


Claim

 Instagram

Claim

 Etsy

Claim

 YouTube

Claim

PINTEREST



Privacy and Data Settings

Next, continue down the screen to find “Privacy & data” and review the settings. First, you will see “@Mentions”, which allows other Pinterest users to mention you in their comments and pins. It is recommended that this function be turned off or that “Only people you follow” be allowed to mention your name.

You will also see “Search Privacy”, which left unchecked, will allow your account to be searchable on Google. We recommend you make your account private by checking the box next to “Search Privacy”.

Next look at “Personalization” and see the list beneath it. These settings allow Pinterest to collect information about you in order to personalize ads and other content for you. We recommend leaving all boxes in this section unchecked.

Privacy and data

Decide whether your Pinterest profile will be hidden from search engines, and what kinds of data you want us to use to improve the recommendations and ads you see. [Learn more](#)

@Mentions

Choose who can @mention you

- Anyone on Pinterest
- Only people you follow
- Turn off - no one can @mention you

Search Privacy

Hide your profile from search engines (Ex. Google). [Learn more](#)

Personalization

- Use sites you visit to improve which recommendations and ads you see. [Learn more](#)
- Use information from our partners to improve which recommendations and ads you see. [Learn more](#)
- Use your activity to improve the ads you see about Pinterest on other sites or apps you may visit. [Learn more](#) in Help Center.

Reset Save

Security

Now let’s visit the “Security” section, which allows you options for better account security. The first section is for “Two-factor Authentication”, which we strongly recommend you enable. Select the box next to “Require code at login”, and you will have the option of having a code sent to your mobile device that you will need to enter when you log in - a new code will be sent each time you log in.

Under “Two-factor Authentication”, you will see “Connected devices”. Select “Show sessions” in this section and you will be provided the opportunity to “End Activity” for all sessions that may seem suspicious or are not needed.

Security
Turn on two-factor authentication and check your list of connected devices to keep your account, Pins and boards safe. [Learn more](#)

- Edit profile
- Account settings
- Claim
- Notifications
- Privacy and data
- Security**

Two-factor authentication
This makes your account extra secure. Along with your password, you'll need to enter the secret code that we text your phone each time you log in

Require code at login

Connected devices
This is a list of devices that have logged in to your account. Revoke any sessions that you do not recognize. [Learn more](#)

Hide sessions

Last accessed:	Current Session
June 7	
Location: Florida, United States (Approximate, based on IP)	
Device: Chrome	
Last accessed: October 24, 2018, 11:46 PM	End Activity

PINTEREST



Third-Party Applications

Finally, the “Apps” section allows you to disconnect any third-party apps you might have linked to your account. Again, we recommend keeping all accounts separate for the best security. If you were to lose your mobile device or computer, you do not want someone to have full access to all of your accounts, including Pinterest. If there are any apps listed in this section, we recommend deleting them.

[Edit profile](#)

[Account settings](#)

[Home feed](#)

Apps

[Claim](#)

Keep track of everywhere you've logged in with your Pinterest profile and remove access from apps you're no longer using with Pinterest. [Learn more](#)

[Notifications](#)

You have not approved any apps

[Privacy and safety](#)

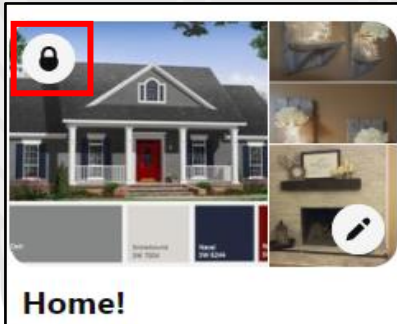
[Security](#)

[Apps](#)

Visible Content

Everything that you “Pin” is public. Not just your followers, but everyone can see your profile and what you pin. Pinterest has no means of limiting the visibility of your “Pins” or your “Comments” like there are on other social media platforms (unless you make them “Secret”, which is discussed next).

There is only one way to ensure full control over your “Boards” and “Pins”, which is by setting them to “Secret”. When you use this feature, no one can see your content unless you specifically invite them to. We recommend you consider setting some or all of your “Boards” to “Secret” in order to limit the amount of information someone can gather about you.



To create a “Secret Board”, select your “Profile Icon” in the top right corner of the page. Then select the “+” icon to create a new “Board”, name the board, and set the toggle next to “Keep this board secret” to “On”. Select the “Create” button. Only the creator of the “Secret Board” has control over its features, and with whom content is shared. You must invite “Collaborators” via email in order for others to see the content. When you “Pin” content to a “Secret Board”, the “Pins” are also private.

In order to change a “public” board to a “Secret board” simply open the board you wish to change, then select the three dots next to the board title. From the drop down select “Edit board.” Scroll down to select “Keep this board secret” then hit “done.”

Create board

Name

Like “Places to Go” or “Recipes to Make”



Keep this board secret

So only you and collaborators can see it. [Learn more](#)

Create

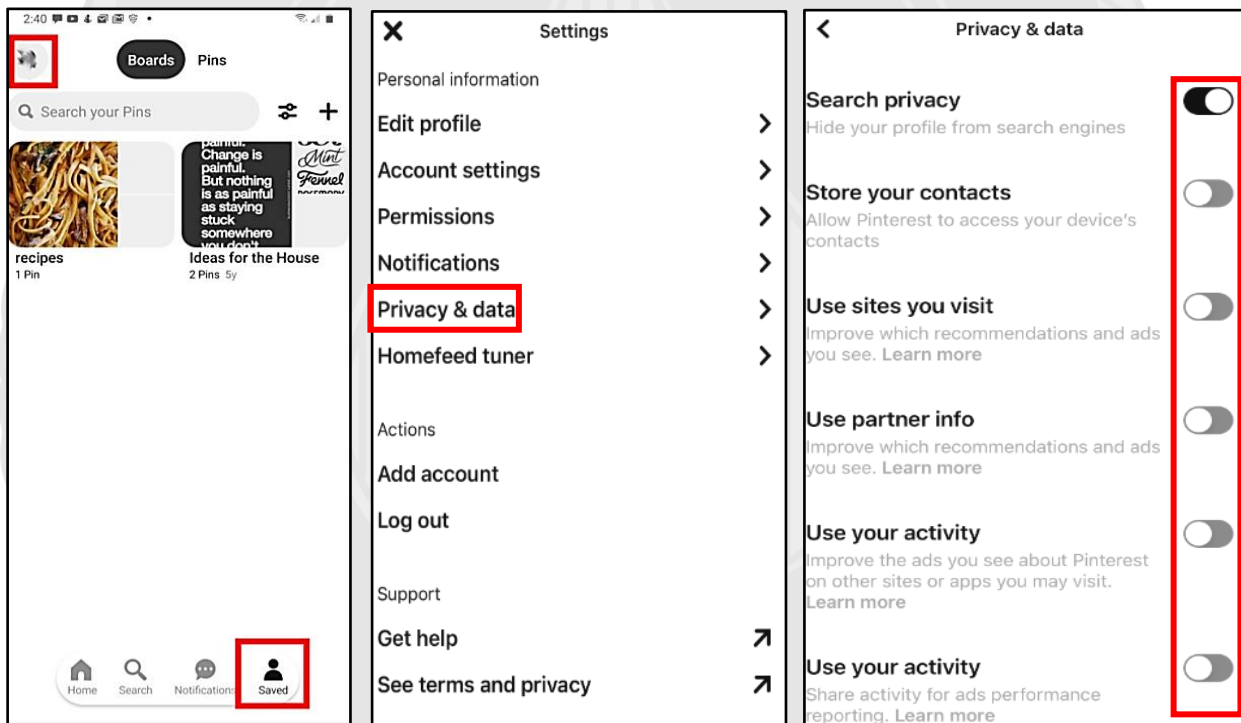
PINTEREST



Security and Privacy Settings

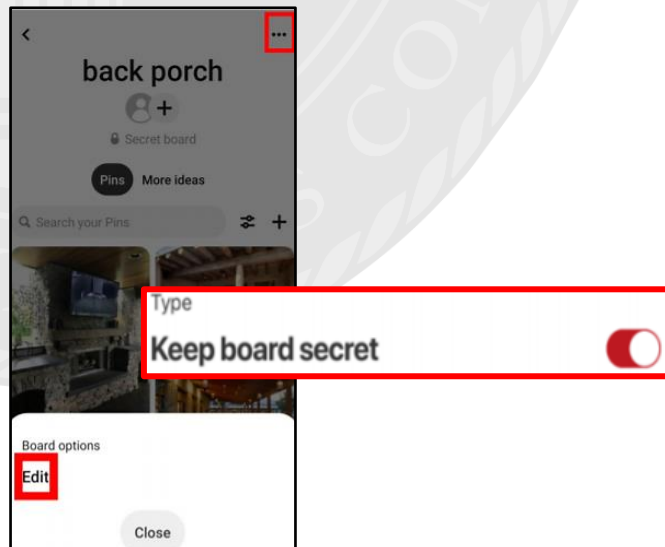
On your mobile device, you will begin at your “Profile” screen by selecting the “Profile” icon at the bottom right of the screen or locating your “Profile Picture” on the page. Then select the “Settings” icon at the top right. The “Edit profile” and “Account settings” are the same as the computer version.

However, the “Privacy & data” section is a little different on the mobile version. If you select “Privacy & data”, then see “Store your contacts”, and ensure the toggle is set to “Off”. Additionally, make sure that all your privacy settings are set the way you want them, in case the settings you chose via computer did not transfer to the mobile app.



Edit Board Privacy

Select the “Board” you want to make private, then select the “Menu” icon, or “. . .” at the top right of the screen, select “Edit”, then scroll down to “Keep board secret”, and set the toggle to “On”. To save your changes, select the “Done” button at the top right of the screen.



SNAPCHAT



- **Do** set up privacy and security settings on your Snapchat and help your teenager to do the same.
- **Do** assume ALL information and images you share are publicly viewable, regardless of your settings.
- **Do** talk to your teenager about the dangers inherent to Snapchat. Make sure they know to come and tell you if someone they don't know tries to contact them or sends them inappropriate material.
- **Don't** add your birthdate, location, or other personal details to online profiles.
- **Don't** allow users you do not know personally to contact you via Snapchat.
- **Don't** believe that all pictures and videos are automatically deleted. There are ways to save and share content despite Snapchat's efforts to make all communications disappear.

Understanding the App

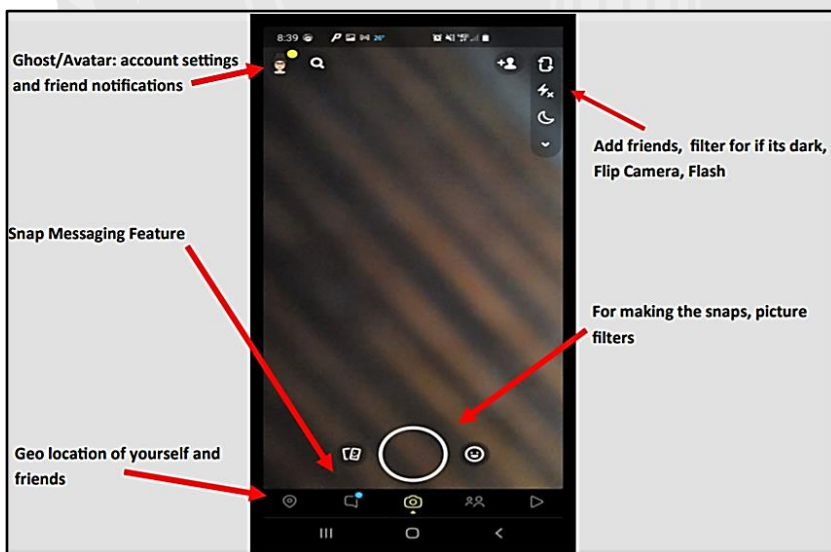
Snapchat is an image and video messaging app that allows users to share multimedia messages that will “self destruct” in up to 10 seconds. Its communication style is meant to mirror real life face-to-face interactions that are temporary. Content is designed to delete automatically (from user view), but most users are becoming aware that content can be saved using screen shots, screen recording, or other software.

NOTE: All of your data is saved and stored by the application and can be downloaded by any individual with your username/email and password! [See last page for more details.](#)

The Basics

This is your “Home Screen”. You know you are there when you have a “Camera View”. One of the main features of the app is making “Snaps”, via photos/videos, which you would do from this screen, then share with your “Friends”.

Next, identify your “Profile” picture at the top left of the box (highlighted in red), this icon will take you to your Snapchat statistics and the “Settings” icon.



SNAPCHAT



USSOCOM SMARTCARDS

Still a link to your account page

The personal message and new stories screen: AKA what you get by swiping right or pressing the little blue button on the bottom left

Create a new text chat

Filled in squares means you have content to watch

Blue circles mean your friend has shared a new public story

Empty squares mean you have already watched/read

Chat and Settings

Above is an overview of the “Chat” feature. Select the “Chat” icon on the lower left corner of the home screen. Here you can see if someone has sent you a message, posted a story, or reviewed your posts. You can also start a “Chat”.

From here, you can select your “Profile” icon at the top left and head to your Snapchat stats and “Settings” section.



In order to delete a chat you already sent: 1) hold down the chat, and then 2) select “Delete”. Once selected, Snapchat will provide another message box to confirm that you would like to delete the chat you have just selected, and to remind you that, although the message is being deleted, your friends will still be able to see that something was deleted, if not the deleted content itself.

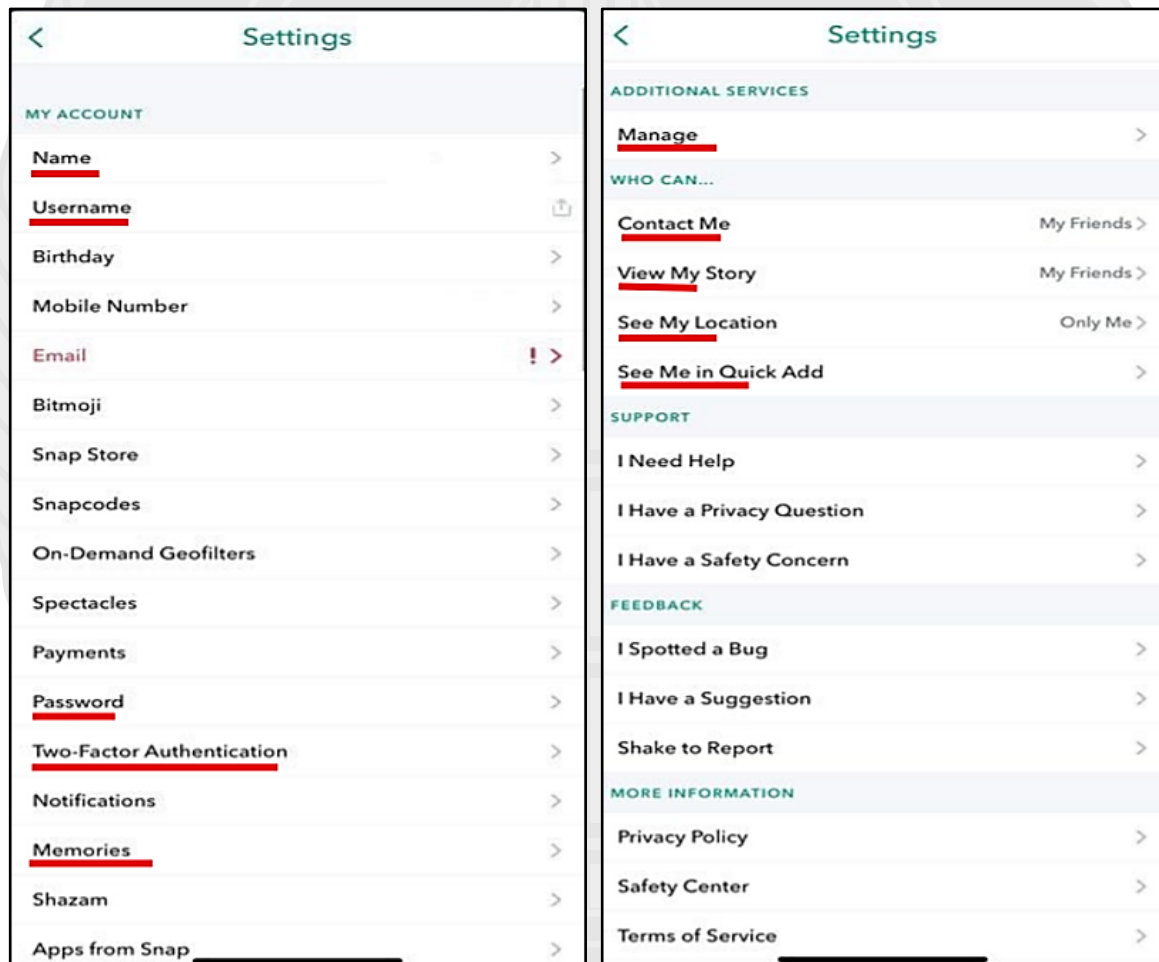
SNAPCHAT



Settings

First, check your “Name” and “Username”, and make sure they don’t give too much information about you. We recommend you use a nickname or a mixture of names instead of using your full name, and never add birthdays or other significant information to your name. You do not need to put your real birthday on your account and should consider using an inaccurate one.

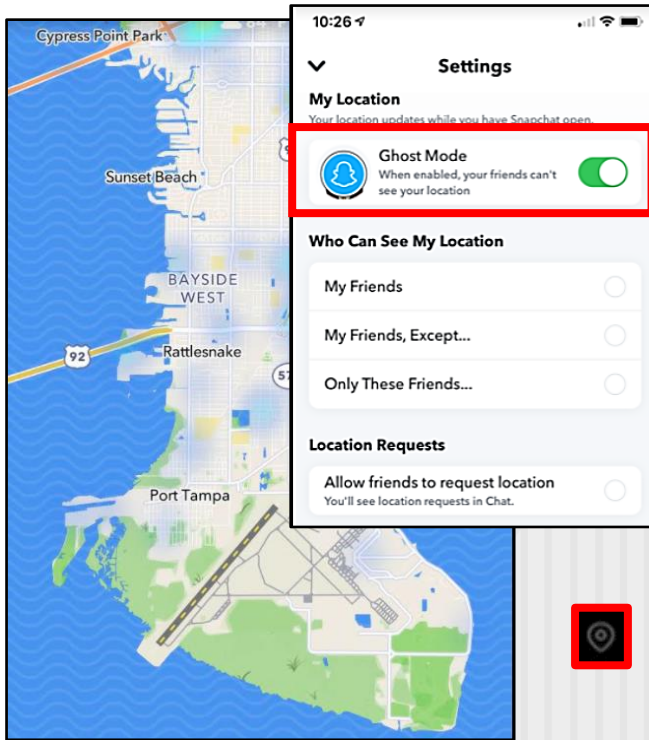
Next, we recommend using a “Password” that is unique to Snapchat. As with all of your social media accounts, reusing passwords creates an unnecessary vulnerability, and you should use unique passwords for each account



Two-Factor Authentication

It is recommended that you choose this function in order to better protect your account.

SNAPCHAT



Location Settings

You can find the “Snap Map” icon on the bottom left your camera screen or by swiping right on the “Chat” screen. This feature shows “hot spots” that were geo-tagged (or adding location-based filters) by other Snapchat users which are public. You can also view the location of your friends if they are broadcasting their location publicly.

To prevent your location from being shown, you can change your location setting to “Ghost Mode” in the Settings menu under “Who Can... See My Location” or on the “Snap Map” in the upper righthand corner.

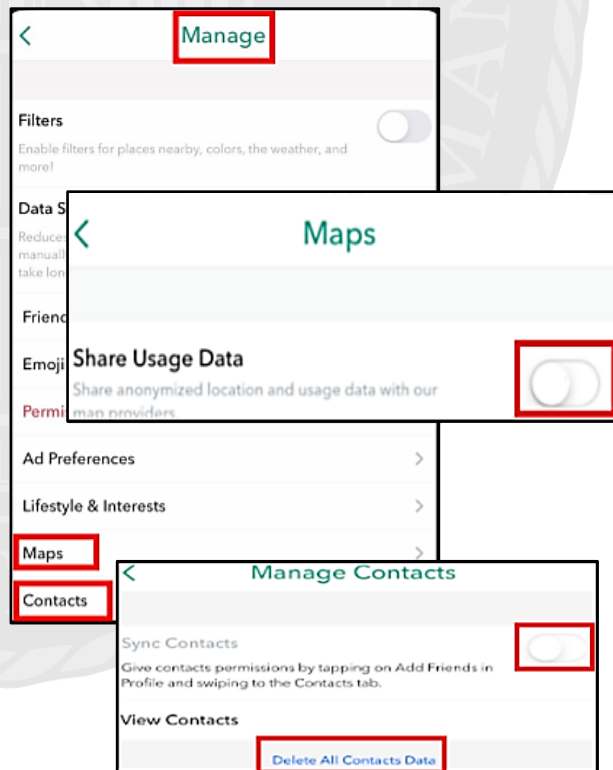
You should also turn off sharing your Map Usage Data in the “Manage” menu

Contact Settings

It is recommended that you lock down who can contact you, view your stories, and turn “Off” your discoverability in the “Quick Add” feature in the “Settings” menu. You should also turn prevent or clear Contact Syncing.

On iPhone: under “Manage”, select “Contacts”, then set toggle to “Off”, and “Delete All Contacts Data”.

On Android: under “Settings”, scroll down again to “Privacy”, select “Contact Syncing”. Ensure this feature is “Disabled” by identifying the space to the right of “Sync Contacts”, and see that there is “No Checkmark” visible. Also, select “Delete All Contact Data” below “View Contacts” as well

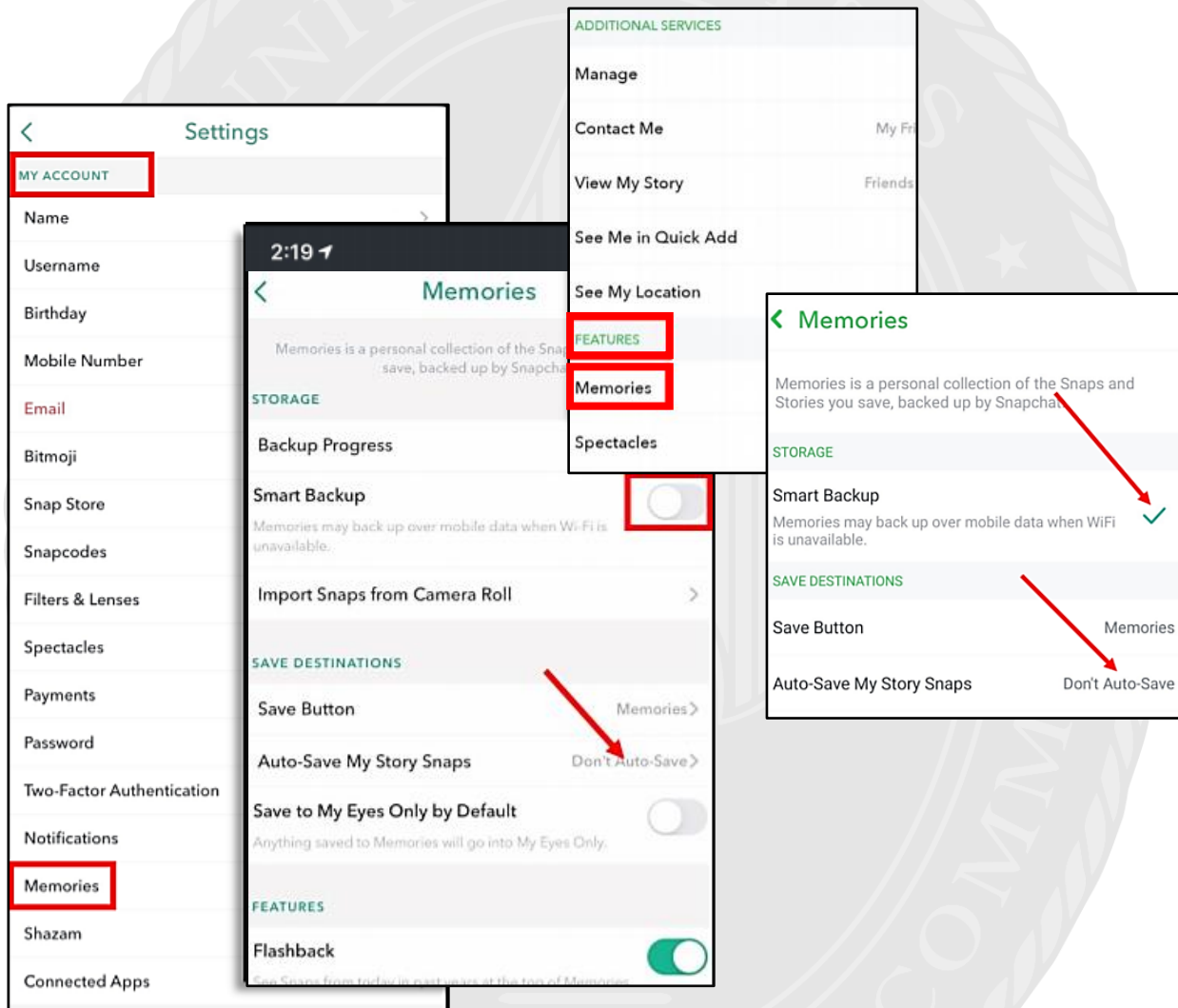


SNAPCHAT



Memories

“Memories” are Snapchat’s storage function. Snaps are saved on Snapchat’s servers, but are searchable and visible only to you. We recommend you not allow Snapchat to store your photos, and instead choose manually when you want a “Snap” saved to your “Memories” as needed. It is important to know that snaps of all kinds do not truly delete on Snapchat.



On iPhone: in “Settings”, select “Memories” under “My Account”. Set the “Smart Backup” toggle to “Off” and select “Don’t Auto-Save” next to “Auto-Save My Story Settings”.

On Android: in “Settings”, scroll down to “Features”, then “Memories”, and “Uncheck” the “Smart Backup” option. Also, ensure “Auto-Save My Story Snaps” is set to “Don’t Auto-Save”.

When does Snapchat delete “Snaps”? Snapchat servers are designed to automatically delete all “Snaps” (on their servers) after they have been viewed by all recipients. All unopened “Snaps” are deleted after 30 days.

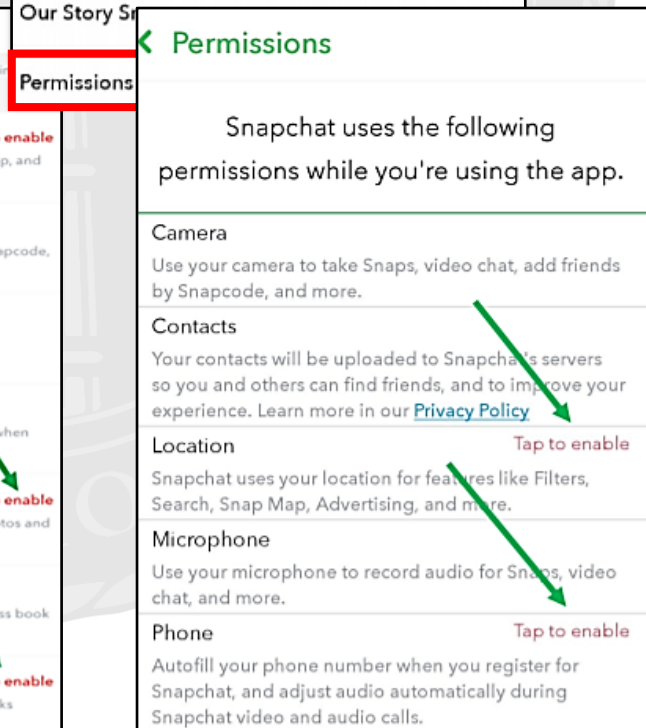
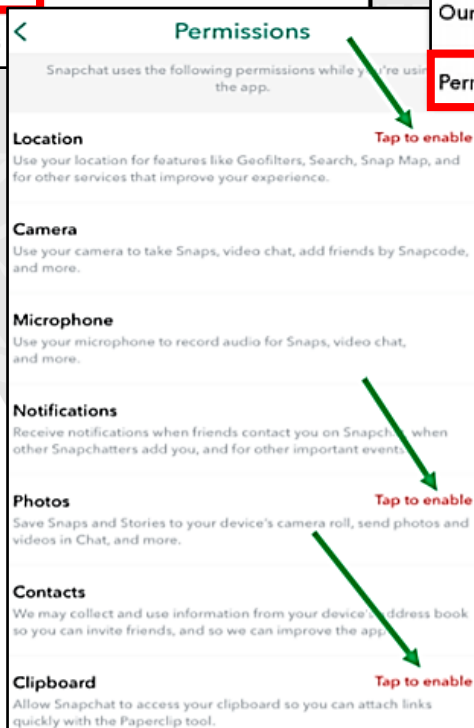
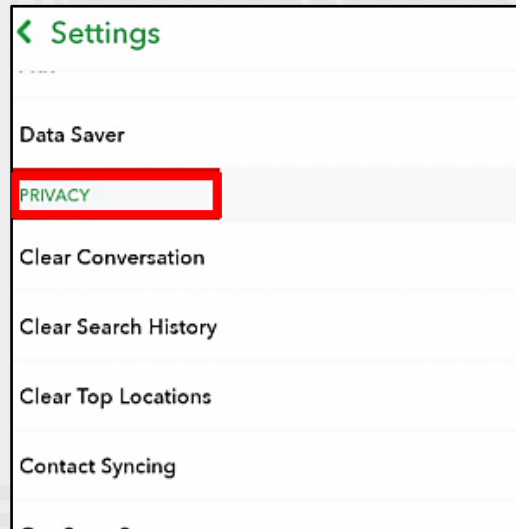
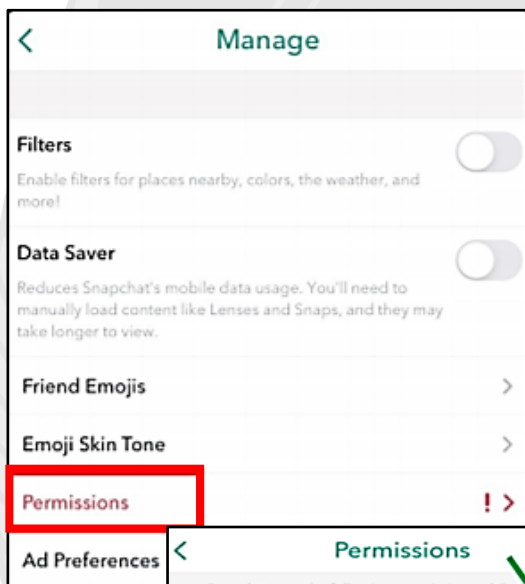
SNAPCHAT



Permissions

On iPhone: select “Manage”, then “Permissions”, and ensure “Location”, “Photos” and “Clipboard” are not enabled. Each of these features allows Snapchat to capture and store information from your mobile device in some way.

On Android (yellow): under “Settings”, scroll down to the section titled “Privacy”, then select “Permissions”. You can adjust “Location” and “Phone”. We recommend you leave them “Disabled”.



SNAPCHAT

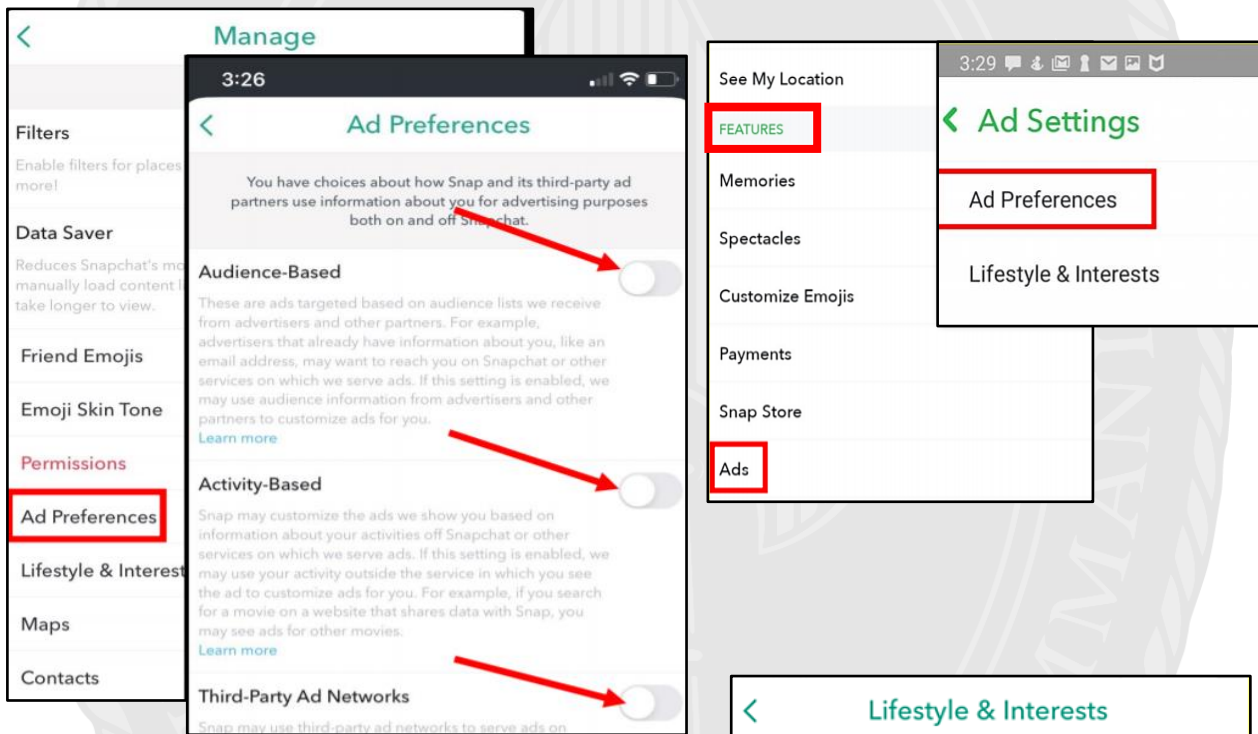


Ad Preferences

Next, let's lock down what kinds of information Snapchat can capture from you in order to support advertising.

On iPhone: go back to the "Manage" section, select "Ad Preferences", ensure all three toggles are set to "Off".

On Android (yellow): under "Settings", scroll down to the section titled "Features", then select "Ads". Select "Ad Preferences" on the next screen, then ensure "Audience -Based", "Activity-Based", and "Third-Party Ad Networks" are all "Unchecked".



Lifestyle and Interests

Next, go back to the "Manage" section ("Ad Settings" on Android) and select "Lifestyle & Interests," its recommended that you unselect any section that is enabled. You can also periodically clear any tags that may have specified your interests by selecting "Clear Content Interests Tag" located at the very bottom of the "Lifestyle & Interests" screen.

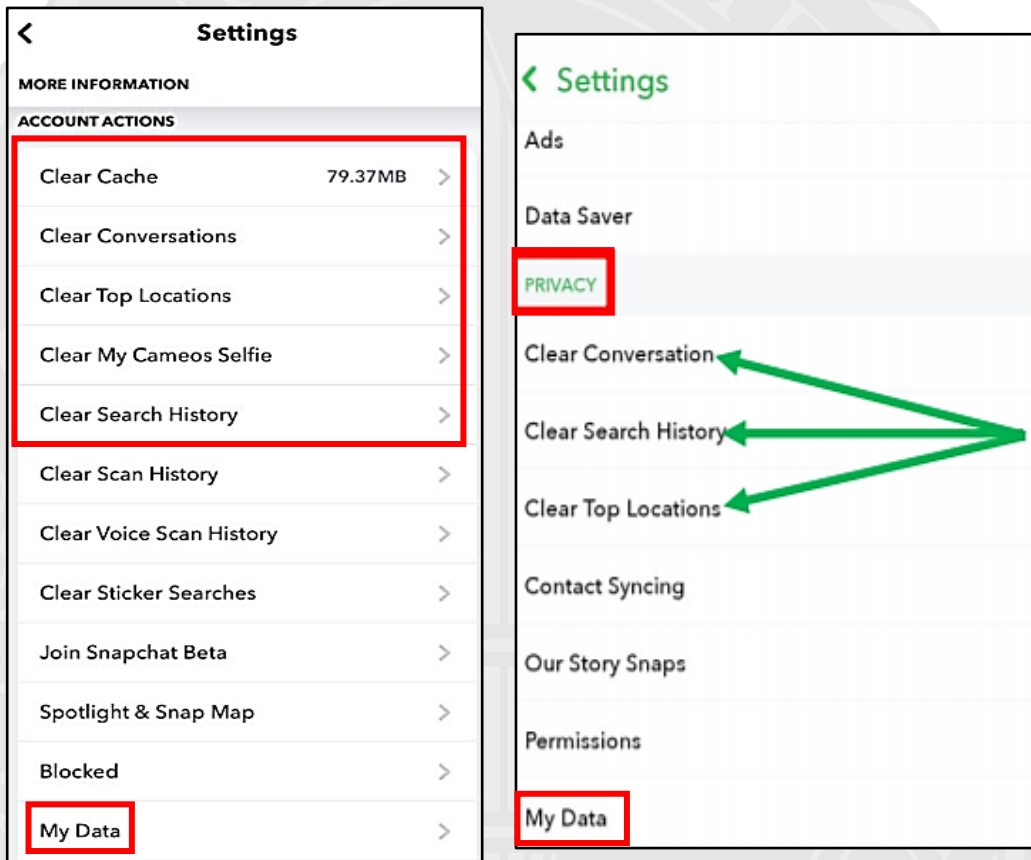
Clear Content Interests Tag

SNAPCHAT



Clear Caches

Finally, we recommend clearing out old data periodically on your Snapchat account, as well as your other social media accounts, whenever this feature is available. Snapchat provides you the capability to “Clear Cache”, “Clear Conversations”, Clear Search History, and “Clear Top Locations” (in addition to others on iPhone). You will clear these and the other options listed, the same way you would clear your Internet browser cache.



Download Your Data

When you use Snapchat, they collect information from and about you. You can submit a request to download your data and within 24 hours, you will receive a zip file with said data. See the types of information you can download below.

- | | | |
|--|--|--|
| <ul style="list-style-type: none"> ✓ Login History and Account Information <ul style="list-style-type: none"> · Basic Information · Device Information · Device History · Login History · Account Deactivated/Reactivated ✓ Snap History <ul style="list-style-type: none"> · Received Snap History · Sent Snap History ✓ Chat History <ul style="list-style-type: none"> · Received Chat History · Sent Chat History | <ul style="list-style-type: none"> ✓ Location <ul style="list-style-type: none"> · Frequent Locations · Latest Location · Business and public places · Areas you may have visited ✓ Search History ✓ Terms History ✓ Subscriptions ✓ Bitmoji | <ul style="list-style-type: none"> ✓ Story History <ul style="list-style-type: none"> · Your Story Views · Friend and Public Story Views ✓ Account History <ul style="list-style-type: none"> · Display Name Change · Email Change · Mobile Number Change · Password Change · Snapchat Linked to Bitmoji · Spectacles · Two-Factor Authentication |
|--|--|--|

TIKTOK



USSOCOM SMARTCARDS

- **Do** opt out of personalized data. TikTok is owned by a company based in China, opting out helps prevent your data from being gathered and redistributed without your knowledge.
- **Do** ensure family members take similar precautions with their accounts. Their privacy and settings can expose your personal data.
- **Do** use a picture of something other than yourself for your profile photo. Profile photos are publicly viewable.
- **Don't** provide any identifiable information (name, hobbies, job title, etc.) on your profile or in your videos.
- **Don't** link your TikTok account to any third-party applications such as Facebook, LinkedIn, Instagram or Twitter.
- **Don't** use identifiable locations, backgrounds or relatable images, when posting videos.
- **Don't** participate or appear in other users' videos

Privacy Settings

By default, all accounts are set to "Public" which means anyone can see what you post on TikTok. We recommend you set your account to "Private" which will ensure that all videos can only be seen by the creator and no one else on the platform. With a private account you can approve or deny users and limit incoming messages to "Friends" only.

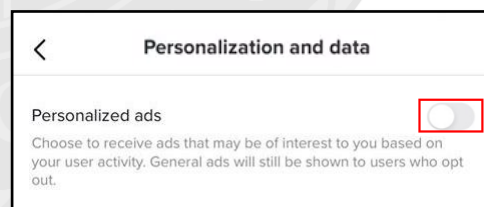
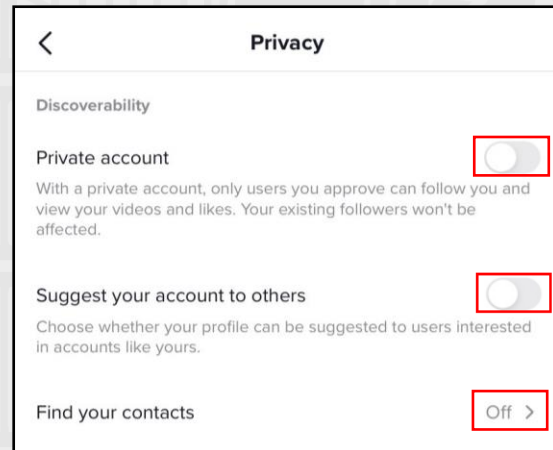
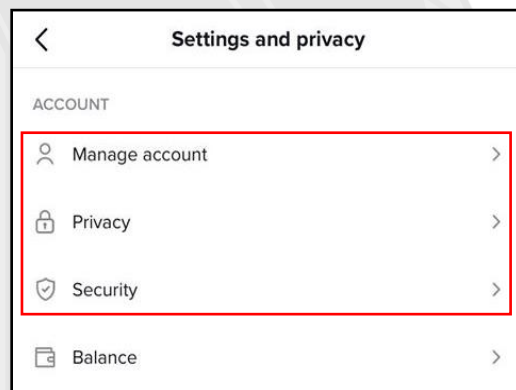
Even with a Private account, your Photo, Username, and Bio are still visible to all users of the platform.

To make your account Private, go to "Privacy" under "Settings and privacy" and set the "Private account" toggle to "On".

We recommend you set "Suggest your account to others" to "Off", which will prevent others from being directed to your account.

It is recommended that you do not allow TikTok or any other social media account to have access to your contacts. Toggle "Find your contacts" to "Off".

Next, review the "Personalization and data" section. Here you will toggle "Personalized ads" to "Off" which will minimize the amount of personal data collected by the application.

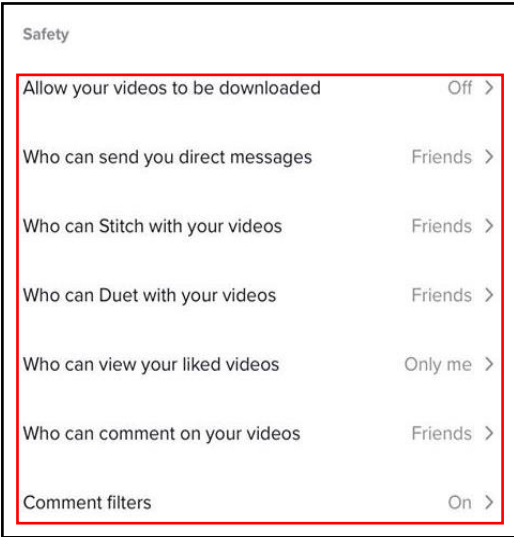


TikTok is owned by the Chinese company ByteDance. TikTok is influenced by the Chinese government, data created in the app is subject to Chinese censorship, and it is likely that personal data is collected on US citizens using the app.

TIKTOK

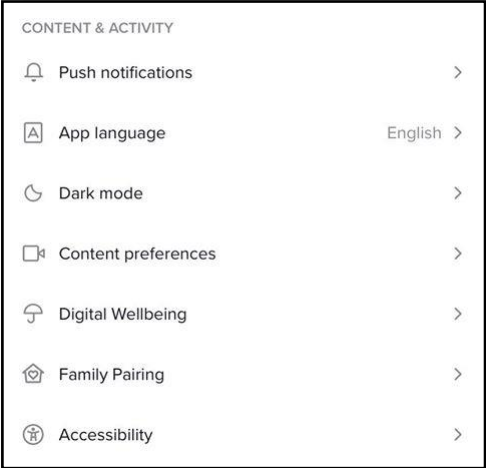
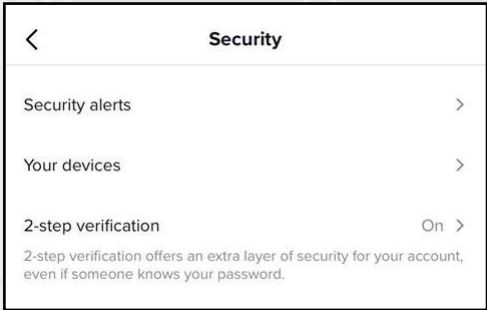


USSOCOM SMARTCARDS



The next group of settings falls under the “Safety” section within the “Privacy” menu. Here you will want to go through each section to maintain privacy on your videos. It is highly recommended that the highest level of privacy is set to “Friends” and no setting is set to “Everyone.” This will limit unknown profiles from being able to contact you and access your videos. In addition, it is strongly recommended that you do not allow others to download your videos, so that they are unable to leave TikTok and be shared on other platforms.

Now, head back to the “Settings and privacy” and select “Security.” Here you can check if there has been any suspicious activity on your TikTok account and set up 2-step verification. 2-step verification is an important additional secure layer to help reduce unwarranted access and account fraud.



Much like YouTube, TikTok has a “Restricted Mode” for children or teenagers whose parents want to limit the type of content they can see and follow.

To turn the “Restricted Mode,” go back to the main menu, “Settings and privacy,” and select “Digital Wellbeing.” From there select “Restricted Mode” then choose “Turn on Restricted Mode” from the bottom of your screen. A passcode can be enabled to prevent “Restricted Mode” from being disabled.



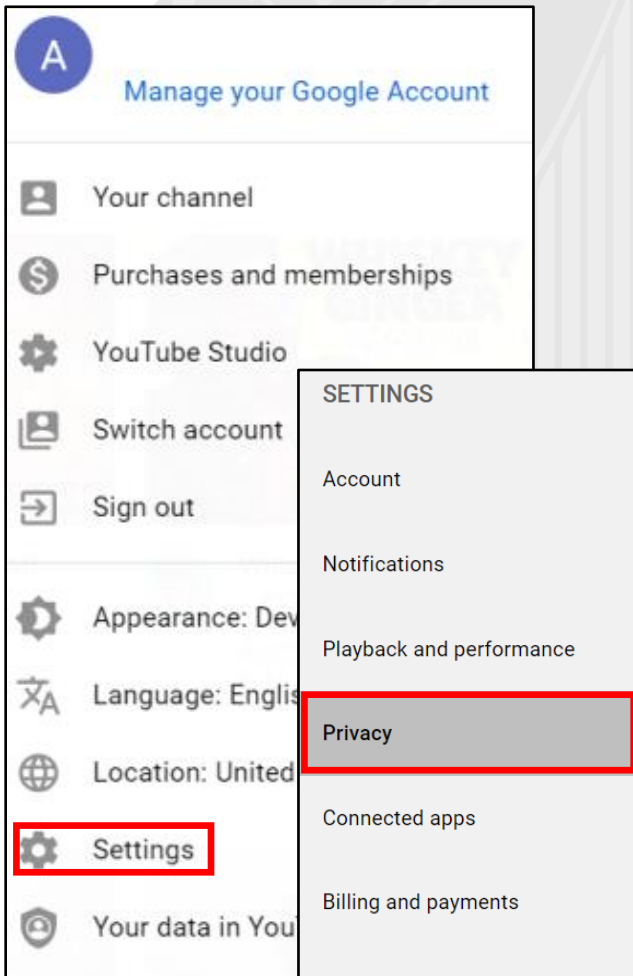
We recommend you do not link your TikTok account to any other social media platform (Twitter, Instagram, Facebook, etc.). If linked, TikTok will pull personally identifiable information (PII) and pictures from linked platforms. You are not required to put any personal or biographical information into your profile, and it is recommended you leave optional sections blank.

YOUTUBE



- **Do** monitor the videos that your children are watching, even if they are in “Restricted Mode.”
- **Do** use Two-Factor Authentication to protect all your information. Enable this function via your Google Account.
- **Do** set all your videos to “Unlisted” or “Private” so that you maintain full control over who can see them.

- **Don’t** allow your children to post “Public” videos to their YouTube account. Posting public videos allows “subscribers” (strangers) to follow your children on YouTube.
- **Don’t** ignore the “Comments” and feedback on your published videos. Review them to make sure they



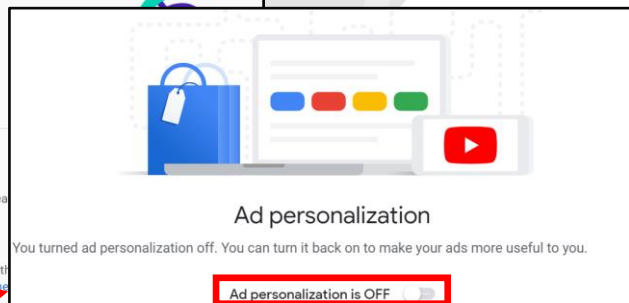
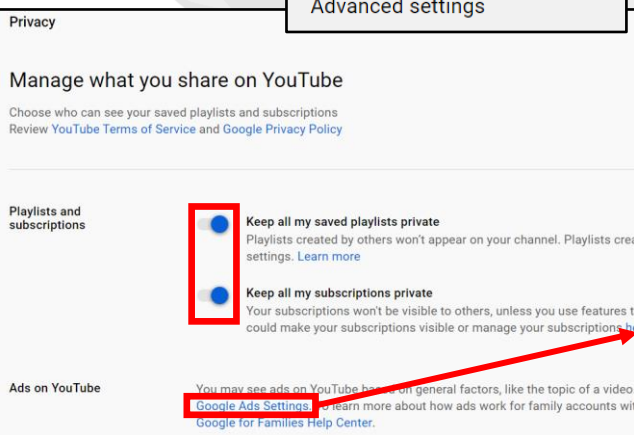
Privacy and Ad Settings

Your “YouTube Account” (if you have one) is connected to your “Google Account”, meaning your Google email and password are used to sign into YouTube. To set your security and privacy settings on YouTube, let’s begin with “Settings”.

Look to the top right of your screen and select your “Google Profile” picture (see left). From the dropdown menu, select “Settings”, and the “Settings” menu will appear. Select “Privacy”.

In the “Privacy” section, scroll through each setting to make sure it is locked down. We recommend you keep all sections in “Manage what you share on YouTube” private, set the toggles to “On” or “Check” the boxes.

In the section “Ads based on my interest”, we recommend turning this feature off, because it must collect data from you in order to work properly. Disable the “Google Ads Settings” by selecting “Google Ads Settings”, then set the toggle to “Off” as seen below.



YOUTUBE



Restricting Mature Content – PC and Mobile

Back in the “Settings” menu and select “Account” then “Contacts Syncing”. It is recommended that you forbid Instagram from uploading your contacts by turning “Off” the “Connect Contacts” option.

On iPhone: go back to “Settings”, then set the “Restricted Mode” toggle to “On”

On Android (yellow): under “Settings”, select “General”, scroll down to “Restricted Mode” and set the toggle to “On”.

The image contains several screenshots from the YouTube mobile app. On the left is the 'Manage your Google Account' screen with 'Restricted Mode: Off' highlighted. In the center is the 'Settings' menu with 'Restricted Mode' highlighted. To the right is the 'General' settings screen with 'Restricted Mode' highlighted. At the bottom is the 'Restricted Mode' toggle screen with the 'ACTIVATE RESTRICTED MODE' toggle highlighted. The background features a large, faint watermark of the USSOCOM seal.

Manage your Google Account

- Your channel
- Purchases and memberships
- YouTube Studio
- Switch account
- Sign out
- Appearance: Device theme
- Language: English
- Location: United States
- Settings
- Your data in YouTube
- Help
- Send feedback
- Keyboard shortcuts

Restricted Mode: Off

Settings

- Get YouTube TV
- Paid memberships
- YOUTUBE
- Remind me when it's bedtime
- Dark theme
- Restricted Mode
- Play HD on Wi-Fi only

Settings

- Get YouTube TV
- General
- Autoplay
- Watch on TV
- History & privacy

Restricted Mode

This helps hide potentially mature videos. No filter is 100% accurate. This setting only applies to this browser.

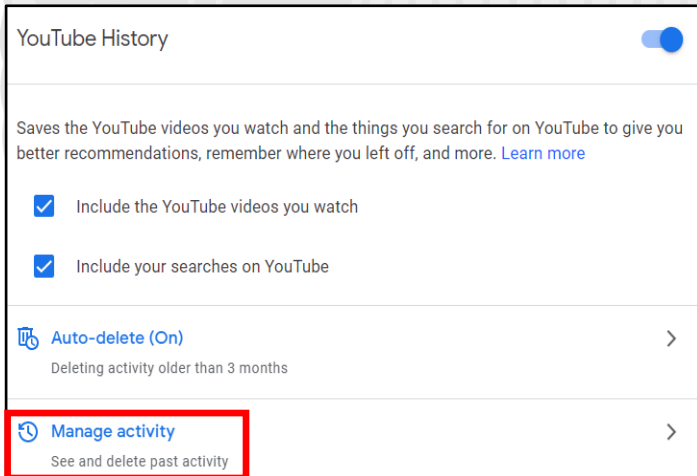
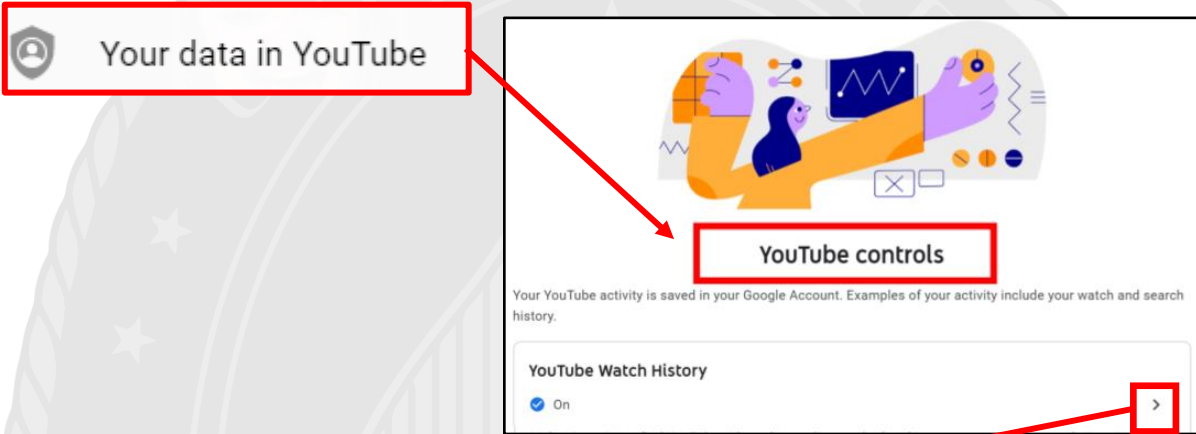
ACTIVATE RESTRICTED MODE

YOUTUBE

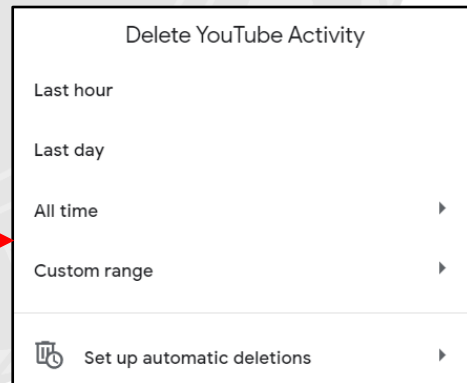
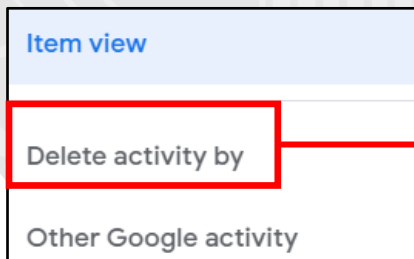


Delete History

Another important feature located at the bottom of your “Account Menu” (from your “Google Profile” icon) is the “Your data in YouTube” tab. Just as it is important to clear your browser history on your search engines, it is important to manage and clear your history on your YouTube account. Select “Your data in YouTube”. On the next page, scroll down to “YouTube Controls”, select “Manage your YouTube Watch History”.



Look to the left of your screen to see a menu of available options to manage and delete your history. We recommend you select “Delete activity by”, then select “All time”, which will delete your entire history. You can also set up automatic deletions,



You can also delete history on your mobile phone. Select your “Google Profile” icon, then select “Settings”, then “History & privacy”. Follow the prompts to “Clear watch history” and “Clear search history”.

YOUTUBE



Who Can See Your Videos?

One of the main uses for YouTube is of course uploading and watching videos. In order to upload your videos and create privacy settings you must first locate your “Video Manager.” Select the “Google Profile” icon, and on the drop-down menu select “Your Channel.” Then press the blue “Customize Channel” button (“Manage Videos” on mobile app). Here you will be able to upload and edit videos.

Manage your Google Account

Your channel

Purchases and memberships

YouTube Studio

Switch account

Sign out

Dashboard

Content

Playlists

Analytics

Comments

Subtitles

Settings


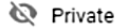
CUSTOMIZE CHANNEL





MANAGE VIDEOS

Visibility Settings

In order to edit the “Visibility” of a video, or who can see the video, simply hover over the “Visibility” column next to the video and select the “Down Arrow” or the “Edit” icon. From the pop-up menu that appears, you can choose “Private”, “Unlisted”, or “Public” - we recommend you select “Unlisted”.

On your phone, you will select the menu button on the right of the video, hit “Edit” and select “Private”.

Video	Visibility	Date
<input type="checkbox"/>  Country Road Add description	 Private	Oct 17, 2018

Visibility	Date
   Private 	Oct 17, 2018 Uploaded

The “Unlisted” privacy setting on YouTube means that your video is only visible to viewers who have a link to the video. “Private” means only you can view the video.

And “Public” means anyone can search for the video and view it, react to it, and comment on it. Once a video is uploaded to YouTube and made “Public” there is no real way to pull it back from comments, shares, likes, etc.

LINKEDIN



- **Do** review your connections often to ensure that they are current and that you are not providing your information to individuals who no longer need it.
- **Do** consider your profile picture. Posting a profile picture is optional, and we recommend that if you decide to post a picture, you dress in professional business attire.
- **Do** ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- **Do not** use an email account that is associated with your banking, finances, or other important contacts. Instead, consider creating an email account specific to this site.
- **Do not** establish connections with people you do not know and trust. Not everyone is who they say they are.
- **Do not** register, log in, or link third party sites (e.g., Facebook, Twitter, etc.) using your LinkedIn account. Third party sites may aggregate and misuse your personal information and data.

Settings & Privacy

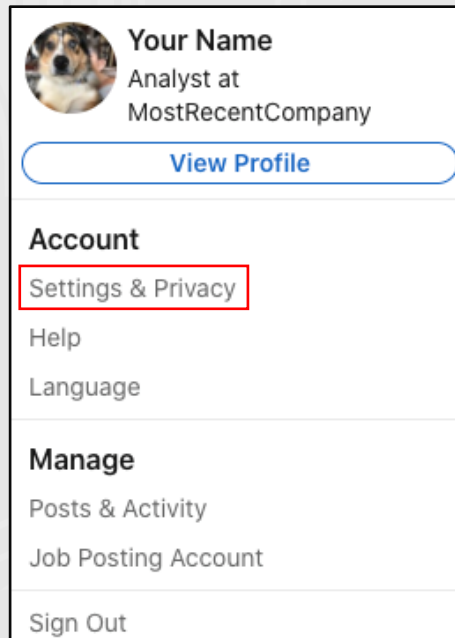


It is recommended to review personal information in LinkedIn profiles. To adjust settings, select **"Me"** in the top right corner of the website. Select **"Settings & Privacy"** > **"Account Preferences."**

Under "Profile Information" > "Name, location, and industry." It is recommended to limit the information visible to all LinkedIn members to ensure privacy. Review personal information. It is highly recommended to not add a maiden or former name. Select "Save." Under "Site Preferences," select "People also viewed." While utilizing LinkedIn for employment purposes it is helpful to leave "on" the "People also viewed" preference. Once employment has been secured, it is recommended to change this setting to "No."

Under "Syncing options," choose "Sync calendar." Remove all synced calendars or contact information if any are currently synced. Linking calendars or contacts could inadvertently reveal PII.

Under "Partners & services," ensure other services are not connected. Under "Account management," do not transfer connections from a compromised account.



LinkedIn is a social network and online platform intended to allow users to find business or career opportunities, connect with others, and find information. There is no guarantee that personal data may not be accessed, disclosed, altered, or destroyed by breach of any of LinkedIn's physical, technical, or managerial safeguards.



Settings & Privacy (Continued)

Select **“Me”** > **“Settings & Privacy”** > **“Sign in & security.”** Review emails and phone numbers associated with your account. One of the first things a hacker will do, aside from changing a password, is change the associated email address preventing the user from regaining access. Review “Where you’re signed in” to ensure there are not fraudulent active sessions. Activate “Two-step verification” for additional security.

Select **“Me”** > **“Settings & Privacy”** > **“Visibility.”** Under “Profile viewing options,” it is recommended to select “Private mode.” Also select “Private mode” under “Story viewing options.” Under “Edit your public profile,” it is recommended to turn public visibility off. Under “Who can see or download your email address,” select “only visible to me” for the tightest security and do not allow connections to download email addresses in their data export. It is not recommended to allow visibility of “Representing your organization and interests.” Under “Profile visibility off LinkedIn,” select “No.” Under “Profile discovery using email address” and “Profile discovery using phone number,” it is recommended to select “Nobody.” However, “2nd degree connections” may be selected while searching for employment. Under “Manage active status,” it is recommended to choose “Your connections only” since they are trusted. Under “Mentions or Tags,” it is recommended to choose “No.” Under “Followers,” select “Your connections” to prevent non-network individuals from viewing any public updates.

Account preferences
Sign in & security
Account access
Visibility
Communications
Data privacy
Advertising data

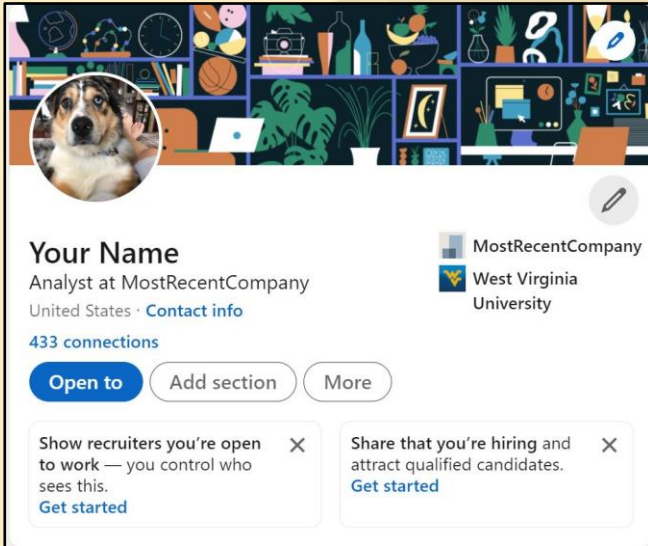
Select **“Me”** > **“Settings & Privacy”** > **“Communications.”** Under “Invitations to connect,” select “Only people who know your email address or appear in your “Imported Contacts” list.” Even though it is not recommended to import a contact list, this is the most secure and feasible option. Under “Messages,” select “yes” to enable message request notifications and control incoming messages. Select **“Me”** > **“Settings & Privacy”** > **“Data privacy.”** Under “Manage your data and activity” you can review all changes made to your account since joining LinkedIn. It is a good idea to check this periodically to ensure unsolicited changes have not been introduced. Under “Salary data on LinkedIn,” it is not recommended to provide salary data. It is also not recommended to provide “Personal demographic information.” Do not enable “Social, economic, and workplace research” allowing LinkedIn to share this data with third-party partners. Under “Job application settings,” it is not recommended to upload a resume to LinkedIn. It is recommended to go to the company website to apply for a position. Under “Commuter preferences,” do not enter a complete address. Under “Other Applications,” review “Permitted services” and “Microsoft Word” preferences. In these sections, verify services have not been granted access to the LinkedIn profile or network data and Microsoft Word does not have access to work experience descriptions.

Select **“Me”** > **“Settings & Privacy”** > **“Advertising Data.”** Under “Profile data for personalizing ads” and “Interest categories,” select “No” to prevent LinkedIn from accessing profile information to personalize ads or job postings. Under “Data collected on LinkedIn,” each subcategory collects data to personalize ads. It is recommended to select “No” for each subcategory to deny LinkedIn the capability of using personal information. Under “Education,” “Job information,” and “Employer” unselect each category as there are multiple. Under “Third-party data,” select “No” under each subcategory to prevent LinkedIn from pushing personal information to or pulling personal information from other services.

LINKEDIN



Profile



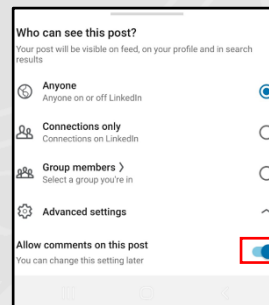
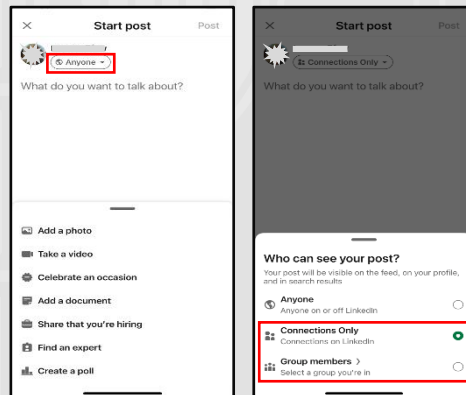
Review LinkedIn profile to ensure generality while still serving the purpose of the account. Select **“Me”** > **“View Profile.”** Select the pencil icon in the upper right corner to edit the profile. It is not recommended to use photos of yourself for the profile or header photo. These are viewable by the public and present an unnecessary vulnerability. If using a personal picture, ensure that it is visible only to **“Connections.”** Review profile visibility to others by selecting the picture icon then your picture icon. Select **“Visibility”** located at the lower right of the pop-up box. It is recommended to select **“Your connections”** for visibility. It is not recommended to add a phone number, birthdate, or address as they are not required. Select **“Save”** to keep selected settings.

LinkedIn on Mobile Devices

Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal.

On iPhone: Select **“Post”** at the bottom center of the screen, then under your name select the arrow on the dropdown menu. From the popup menu, select **“Connections only”** or **“Group members.”** Select **“Advanced Settings”** to **“Disable comments on the post.”**

On Android: the process of locking down visibility of posts on Android is the same as on iPhone, except the **“Advanced Settings.”** When selecting **“Advanced Settings,”** set the toggle to **“Off”** in order to disable comments on this post.



To remove a mention - Select More icon in the top right corner of a connection's post > Remove mention from the list of options > Remove. The post will no longer link to your profile.

To remove a tag - Select the Tag icon on the photo > Click the X icon next to the tag with your name to remove the tag.

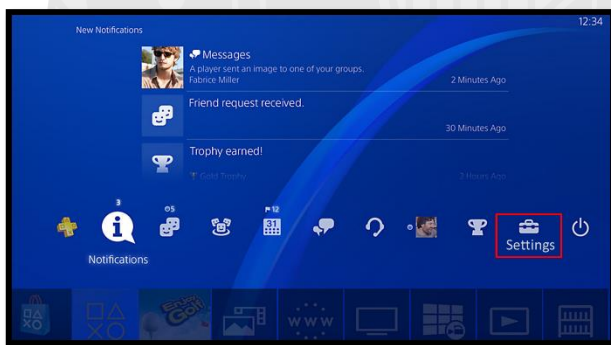
PLAY STATION



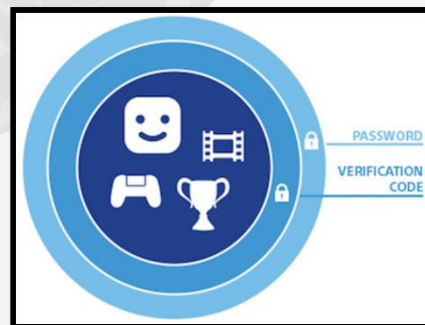
Do's and Don'ts

- **Do** use caution when sharing Gameplay when messages, video, audio, and personal data may be available to other users participating in your game experience.
- **Do** select "Friends Only" for all available settings options. Ensure family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- **Do** use parental controls to restrict access to questionable content and features for children using the PS4.
- **Do** refer to privacy policies / user agreements of individual games and third-party applications to see if they use the PS4 camera, and to understand other privacy information.
- **Don't** forget to update your PS4 system to the latest version of the system software.
- **Don't** use pictures of yourself for your profile photos. Instead, use avatars or photos of something else. Profile photos are potentially viewable to other users and the public depending on your privacy settings.
- **Don't** discard or transfer ownership of your PlayStation without using "Initialization". Initialization sets your PS4 back to factory mode and erases the system data.
- **Don't** establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.

PlayStation allows you to manage a host of settings in order to take ownership of your system security and privacy, and determine what information other users can see. You must first access the "Settings" button from the "Dashboard Menu", highlighted below in red. From there, go to "Account Management".



Two-Factor Authentication: The Two-Factor Authentication process has slightly changed. After you go to "2-Step Verification", select ACTIVATE to switch on 2-Step Verification. Next, select how the verification will be received; whether, via Authenticator App or Text Message. For user's that select verification via authenticator app, open an authenticator app on your mobile device and scan the QR code. If the QR code fails, copy and paste the alphanumeric code. You'll then see a verification code in the app. For users that select verification via text, enter a mobile number or select an existing one. Enter the verification code that was sent to your mobile device. **Recommendation:** Save your backup codes in a secure location. Backup codes allow access to your system when your mobile phone is not available; therefore, if the backup codes are compromised, a hacker can use these to circumvent the intended protections of 2-step verification.



PLAY STATION



2-Step Verification

PlayStation's two-factor authentication is an added layer of security to ensure only authorized individuals have access to the system, accounts, and privacy information.

The sequence of screenshots illustrates the process of enabling 2-Step Verification:

- Account Management:** The 'Account Information' option is highlighted in red.
- Account Information:** The 'Security' option is highlighted in red.
- Security:** The '2-Step Verification' option is highlighted in red.
- Set Up 2-Step Verification:** The 'Set Up Now' button is highlighted in red.
- Verify Your Mobile Number:** The input field for the verification code is highlighted in red.

Privacy Settings

Next, let's take a look at privacy settings. From the "Account Management" screen, select "Privacy Settings" as seen on the right highlighted in red. The "Gaming | Media" subcategory allows you to determine which activities are viewable by others. The "Friends | Connections" subcategory allows you to decide which status of individuals (e.g. friends, followers, etc) can view established connections. The "Personal Info | Messaging" subcategory allows you to choose who can see your real name and who can communicate with you. View the picture on the bottom right to see the privacy setting subcategories.

The screenshot shows the 'Account Management' menu with 'Privacy Settings' highlighted in red.

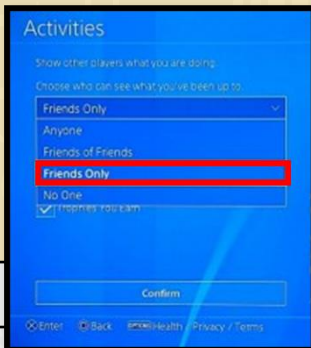
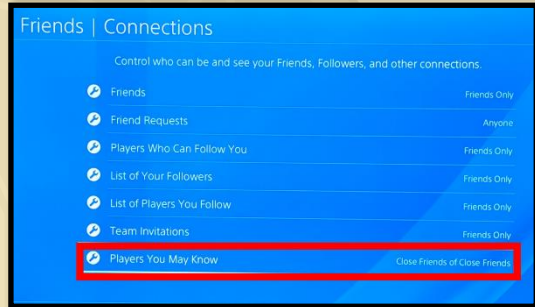
The screenshot shows the 'Privacy Settings' menu with 'Gaming | Media' highlighted in red.

PLAY STATION



Privacy Setting Recommendations.

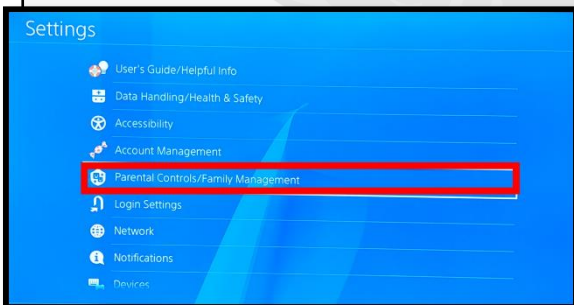
We recommend that you set your privacy settings to “Friends Only” for most sections, in order to prevent the general public from seeing information pertaining to the user. See “Recommended Privacy Settings” on the privacy settings graphics for “Gaming | Media”, “Friends | Connections”, and the “Personal Info | Messaging” subcategories. We recommend the primary user and family members be mindful of who they become friends with and connect to on the system. It is important to remember not everyone on your family and friends “Friends List,” should be trusted. Parents, it is important to know not all users have good intentions, and are accurately portraying themselves online. For this reason, we recommend that you review your child’s “friends” periodically. Other users on the system may utilize gaming systems to connect with potential victims or use social engineering against other users. If you do not know someone, we recommend you not add them to your “Friends List”.



After going through “Gaming | Media”, the “Activities” box shows different setting options you can choose from for privacy. We recommend that you select the “Friends Only” option as shown here in the example picture on the right, highlighted in red.

Parental Controls

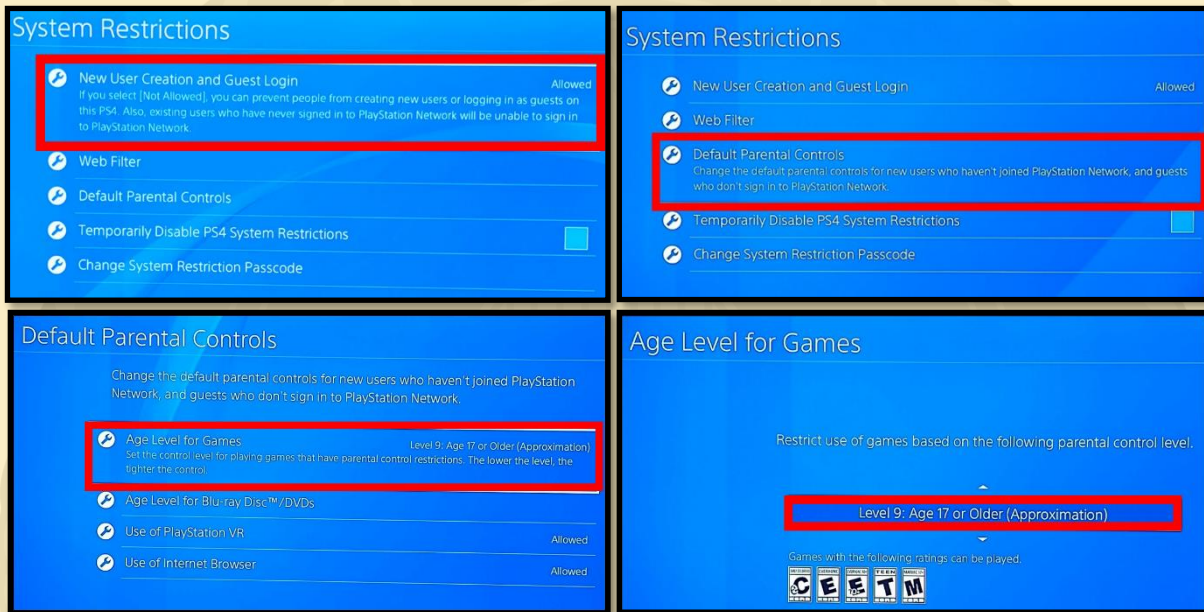
PlayStation allows you to manage numerous parental control settings with the ability to limit playing time, restrict user account creation, set maturity levels for games, and change systems passcodes. To get to “Parental Controls/Family Management” settings, select the “Settings” tab on the front “Dashboard Menu” and scroll down to “Parental Controls”. The subcategories are “PS4 System Restrictions” and “Family Management”.



PLAY STATION



From the “System Restrictions” section, you can select “New User Creation and Guest Login” to restrict who can log into the PlayStation and whether guests can access the system. From the “System Restrictions” section, you can click “Default Parental Controls” for the purpose of setting age and maturity restrictions for your users. See the graphics below highlighted in red for the pathways of these features within the settings. Parents are recommended to implement the various system restrictions and the age appropriate parental controls.

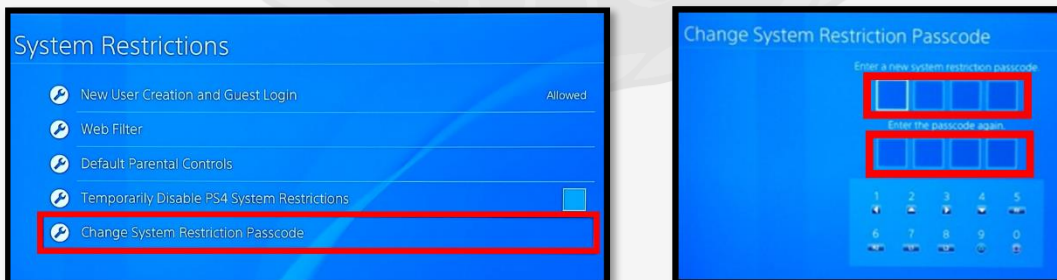


See below for the approximate user ages that match up to the parental control levels available in the user settings.

Parental control level	1	2	3	4	5	6	7	8	9
Approximate age of user	0	3	6	10	12	-	15	17	18
North America/Central America and South America*1									
					*2				*3

Passcode

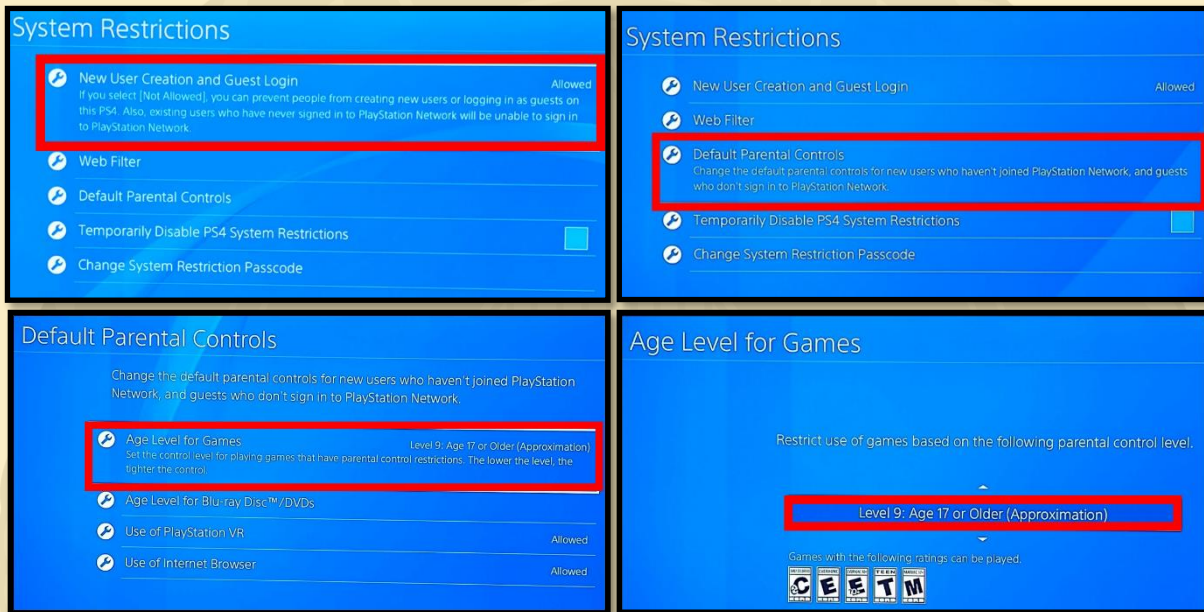
The PlayStation Passcode is defaulted to “0000”. We recommend you change the system passcode to enhance the security of your device. To change the passcode, go to the “System Restrictions” section, and select “Change System Restriction Passcode” as illustrated in the bottom left graphic below, highlighted in red. Next, type in a new system restriction passcode. Verify the passcode by entering it twice.



PLAY STATION



From the “System Restrictions” section, you can select “New User Creation and Guest Login” to restrict who can log into the PlayStation and whether guests can access the system. From the “System Restrictions” section, you can click “Default Parental Controls” for the purpose of setting age and maturity restrictions for your users. See the graphics below highlighted in red for the pathways of these features within the settings. Parents are recommended to implement the various system restrictions and the age appropriate parental controls.

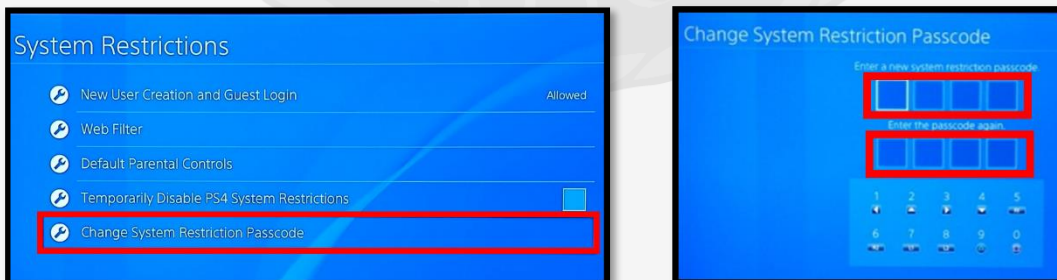


See below for the approximate user ages that match up to the parental control levels available in the user settings.

Parental control level	1	2	3	4	5	6	7	8	9
Approximate age of user	0	3	6	10	12	-	15	17	18
North America/Central America and South America*1									
					*2				*3

Passcode

The PlayStation Passcode is defaulted to “0000”. We recommend you change the system passcode to enhance the security of your device. To change the passcode, go to the “System Restrictions” section, and select “Change System Restriction Passcode” as illustrated in the bottom left graphic below, highlighted in red. Next, type in a new system restriction passcode. Verify the passcode by entering it twice.



PLAY STATION



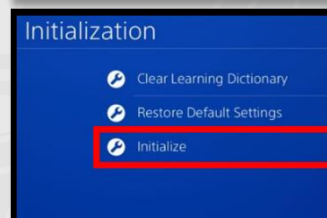
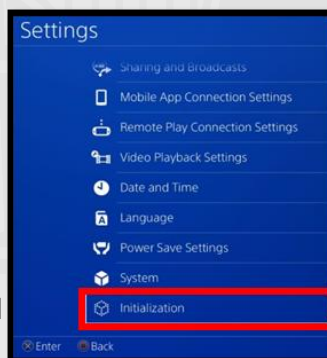
Family Management

Go to the “Parental Controls/Family Management” section. On the PS, select “Family Management” (as seen on the right, highlighted in red) and click “Set Up Now” (as seen below, highlighted in red). Within the “Family Management” area, parents can identify all the family members that will use the PlayStation system, manage play time limits, and set restrictions for children. A parent, guardian, or family manager can set the parental controls.



Initialization

Next, we recommend you use the “Initialization” feature whenever you are discarding or transferring the PlayStation system to another person. Initialization of your PS system restores system settings to default values. It deletes data saved on system storage and deletes all users and their data from the system. When you initialize the system software, all settings and information saved on your PS system are deleted. This cannot be undone, so make sure you do not delete any important data by mistake. Deleted data cannot be restored. Initialization helps ensure the removal of your privacy information after you are done with the system. In order to “Initialize” the PS, first go to “Settings”, then “Initialization” as seen to the right, highlighted in red. Next, select “Initialize” as illustrated on the bottom left, highlighted in red. Finally, click “Full”, as depicted on the bottom right graphic, highlighted in red. Selecting “Full” completely initializes the system. If the “Quick” feature is selected, the system will not be completely restored to a default system - some data will still remain on the PS. Be sure you are doing a “Full” initialization.



PLAY STATION



Potential System Compromise:

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- Unexpected charges from financial institutions tied to your PlayStation accounts.
- Primary email and password have been changed without your authorization.
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.).
- Primary console changed to another device without your consent.
- Receive a special character in a private message, immediately followed by the system crashing or frequent glitches.

If you said “Yes” to any of the above, you are recommended to take the following actions:

- Change your password immediately and use strong/complex passwords.
- Enable two-factor verification.
- Notify the financial institutions about fraudulent purchases resulting from the hack.
- Set your “Messages” privacy setting to “Private” and adjust other privacy settings as well.
- Restrict who has access to create new accounts and logins.
- Contact PlayStation Support or the Sony Customer Service line immediately.

If you need to report **Spam/Fake Accounts/Harassment**: Contact the PlayStation Support Site at 1-800-345-7669 or the Sony Customer Service Line.

Also, you can report that your account has been hacked by going to <https://www.playstation.com/en-us/support/>

If you have additional questions about responding to system compromise, contact <https://twitter.com/AskPlayStation/>.

Important Message on PlayStation: you are responsible for all activities your PlayStation Network, so it's very important you do your best to ensure you are the only person using it.

The PlayStation System is an entertainment system that enables users to enjoy multiplayer online gaming, stream live TV, provides a social and messaging network for friends to connect, allows for video streaming services such as Netflix, Amazon Video, Hulu, YouTube, HBO Now, NBA TV, and more. Each application has its own privacy concerns and is susceptible to being breached or hacked.

Sony/PlayStation Users recently received a notification like the one on the right here. This notification is to let users know that there has been a change in their policy and they are now allowing users to record party conversations. This does not mean however, according to Sony, that Sony or PlayStation themselves are recording your conversation. These recordings must be initiated by an individual in the “Party” and then submitted for possible violations to Sony. This feature is also only available to PS5 users but can be used in parties where PS4 users are also in attendance.

About Party Safety

We want PlayStation Network to be fun for everyone, which is why we have a Community Code of Conduct.

Please be aware that voice chats in parties may be recorded and sent to us by other users. By participating in voice chats, you agree to your voice being recorded.

When behaviors that violate the Community Code of Conduct are reported, PlayStation Safety will review the reports to check if there have been genuine violations.

These recordings will be used only for safety and moderation purposes by PlayStation Safety.










HIDDEN PHONE APPS



- **Do** periodically check your child’s smart devices to ensure they have not downloaded anything you have not approved.
- **Do** think about using a monitoring service (as discussed in the Keeping Children Safe Online Smartcard) for your child/teens smart devices, especially if you have given them the ability to download apps themselves.
- **Do** talk to your teens about the dangers of taking and sending nude photos or videos on their smart devices and make sure they understand the serious consequences.
- **Don’t** give your child/teen the password or authorization to download apps in their respective “App Store”. Having them ask you for the password allows you to review any app they might want to put on their device.
- **Don’t** allow your child to use “Messaging Apps” that instantly delete the content they hold. Allowing such apps will take away from your ability to help your kids navigate through smart device social norms.
- **Don’t** allow children to set private passwords without sharing them with you. Always ensure that you can access your child/teen’s phone.

What are Hidden Apps?

“Hidden” apps, “Vault” apps, or “Ghost” apps are apps that look innocuous, perhaps like a calculator, but are actually used to hide pictures, videos and messages on a smart device. Teens often use these apps because they want to hide their activity from their parents. Often times, these apps require a password to be entered in order to gain entry into the hidden area of the app. Some Vault apps go a step further and if the password is entered incorrectly, a picture of the individual attempting to gain access will be taken.

Android Hidden Apps (examples)		iPhone Hidden Apps (examples)	
	Gallery Vault – hide photos/videos, strong encryption		Calculator# – hide photos/videos, strong encryption
	LockMyPix – hide photos/videos, AES encryption		Private Photo Vault – hide photos/videos, AES encryption
	Vaulty – hide photos/videos		Secret Calculator Browser – hidden internet browser
	Keepsafe Photo Vault – hide photos/videos		Keepsafe Photo Vault – hide photos/videos
	Secret Calculator Vault – hide photos/videos		Secret Vault – hide photos/videos

HIDDEN PHONE APPS



How to Find Hidden Apps

One of the easiest ways to search for hidden apps on a smart device is to visit the devices respective App store (Apple or Google Play Store).

- Android device: In the “Google Play Store” select “Menu” (3 vertical lines in the “Search” box), then select “My apps & games.” Next, select the “Installed” tab in the middle of your screen. Here you can review all the apps that have been downloaded to the device. Additionally, from your “Account” (under the same “Menu”) you can review “Purchase History” which will provide you an overview of all purchased apps.
- iPhone device: In the “App Store” find and select the “Account” icon, or “Profile Picture” at the top right of your screen. Then select “Purchased” and the account you want to review purchases from (if you have an “Apple Family Sharing Plan”, more than one account will appear).

Another way to review purchase history on a smart device is to find the “App Store” and search for “Hidden Apps.” Once a list of available apps appears on the screen, you can scroll through the list. If any “Hidden Apps” are downloaded on the device, it will be noted to the left side of the screen. This method may return inaccurate results due to some apps being miscategorized.

Red Flag Indicators

▲ If your child seems to have more than one of any kind of app it may indicate that one of those apps is not what it appears to be. Redundancy in apps may indicate that one is a “Hidden App”.

▲ If your child seems to try and hide his / her screen any time you enter the room, it may indicate he / she is trying to hide his / her phone activity from you.

How to Prevent Your Downloading Hidden Apps

- iPhone: iOS has an “Apple Family Sharing Plan” that allows parents to turn on a feature called “Ask to Buy”. When this feature is enabled, your child will not be able to download any apps without your approval. iOS has a built in feature that can be controlled through the “Settings” of your iPhone. Simply go in to your “Settings” section and find “Screen Time”. Select “Turn On Screen Time” > “Continue” > “This is My Child’s iPhone” > “Not Now” > “Not Now”. From there you can go in and set “Content & Privacy Restrictions” as well as a “Use Screen Time Passcode” to make sure that your settings are not changed by anyone who doesn’t have a password.
- Android: Android users can setup parental controls in the “Google Play Store” by creating a PIN and choosing the maturity levels you want to allow. Go to the “Google Play Store” > “Menu” > “Settings” > under “User Controls”, you will find “Parental Controls”, and other settings you can review to control what your children download. It is also important to note that where many of the “Hidden Apps” are concerned, “Google Play Store” rates them “E” for everyone. Android users can also create a password for authentication to authorize purchases. This feature is located in the “User Control” section of your “Google Play Store” “Settings”

PAY APPS



USSOCOM SMARTCARDS

- **Do** review all privacy settings and set them in accordance with your personal preference and acceptable risk level. Some mobile pay apps have a social side to them which may display your payment activity if not locked down.
- **Do** make sure you have an anti-malware app on your phone to protect your phone, and the information on your phone from getting into the wrong hands.
- **Do** make sure to periodically check transactions made on mobile pay apps. Make sure they are accurately showing up on the payment device you have linked to the app.
- **Do not** visit online banking or online shopping websites by clicking on a link you have received in an email or from a text message. Doing so may lead to fictitious websites and possible identity theft.
- **Do not** use unsecured Wi-Fi or public Wi-Fi networks while using mobile pay apps or for any online banking purposes.
- **Do not** download mobile pay apps from unofficial sites. It is recommended for all apps, not just mobile pay apps, that you use official stores such as the Apple and Google Play stores.

DEFINITION

Mobile wallets utilize technology the user already owns — a smartphone, for example — to allow the user to make in-store payments quickly and securely without having to use a credit or debit card. The term “digital wallet” may refer to either an electronic device that stores payment information (such as a smartphone) and the program or app used to make the payment, such as Apple Pay, Google Wallet, Samsung Pay, or PayPal.

RISKS

Using mobile pay apps means that losing a smartphone essentially becomes equivalent to losing a wallet. Whoever finds the smartphone holds the keys to using mobile pay apps via a smart device means having to be on the alert for cyber criminals.

the owner’s identity.

Using mobile pay apps means running the risk of malware infecting the smart device and gaining access to the owner’s payment and identity information.

GAINS

Unlike a traditional wallet, if the smart device is stolen, there are levels of security that may limit or even prevent access to the contents of the device.

A user may have the ability to delete all personal information or “wipe” the device remotely if it has been lost or compromised. A physical wallet becomes compromised immediately.

Using physical debit or credit cards means the owner runs the risk of the card being copied upon scanning if the machine being used has been tampered with.

Even if relying solely on mobile pay apps to make purchases, it is important to have some other form of payment in the event the mobile device is inaccessible.

PAY APPS

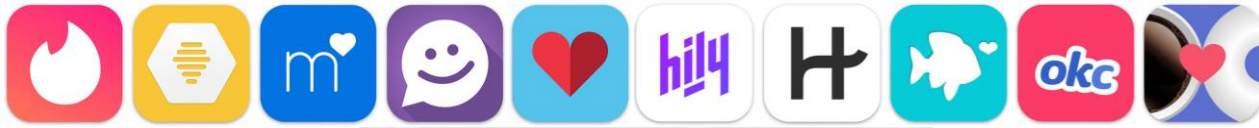


USSOCOM SMARTCARDS

	APPS					
	Apple Pay	Venmo	Facebook Messenger	Cash App	Zelle	Google Pay
Security	High	Low-Medium	Medium-High	Medium-High	High	Medium-High
International Pay Feature	Yes, User must manually turn this feature on	No	Yes, limited	Yes, UK	No	Yes
Linked to Bank Account	Transfer to Bank account	Yes	Yes, only through a Visa or Mastercard debit card or PayPal account	Yes	Yes	Yes
Linked to Debit Card	Yes	Yes	Yes	Yes	Yes	Yes
Linked to Credit Card	Yes + Fee	Yes +Fee	Yes	Yes + Fee	No	Yes
Paying on the Web	Yes, if accepted and while using an Apple device.	Yes, if accepted and while using a smart device where App is loaded.	Yes, thru Facebook ads, Marketplace and groups. **See Cons	Yes, with Cash Card or other payment system such as Google Pay	No	Through PayPal
In Store Payments	Yes, where accepted	Limited acceptance at retailers.	No	Yes, with Cash Card or other payment system such as Google Pay	No	No
Pros	Rated most secured payment app. Accepted at some major universities	User friendly. owned by PayPal	Secure payment method for friends and family. User friendly.	Easy to use and friends do not need the app to receive money. Can purchase and sell Bitcoin.	Works directly with your bank app.	Offers a money back guarantee, pay bills and reload mobile phones. Powered by PayPal.
Cons	Transfers can only be made to other Apple device users. Only works with Apple devices.	Default privacy setting shares your payment history with the world. Scammers are known to take advantage of Venmo.	Limited use. No ability to stop a payment on your end once you send it (however, receiver can reject it). Payment protection only applies to payments made to family and friends.	Not widely accepted. Customer service limited to messaging in app, no call center.	If money is sent to the wrong person or user becomes a victim of fraud or scam, Zelle will not reimburse you.	There is a minimum payment for use. Requires Gov. issued ID as well as a proof of residents. They may also require a bank statement.

The privacy policy for each “Pay App” states what agreements a user consents to when signing up for the application. While each app has different information that is stored and/or shared, they all have a common theme. Many applications collect your name, date of birth, email address, telephone number, name of financial institution, financial account numbers, additional information from consumer reporting agencies, people you invite to use the application, the operating system on the device, etc. The company may be able to keep your information for an indefinite period of time, depending on what the privacy policy states.

DATING SITES & APPS



- **Do** protect your information and set limits on what and when you provide information to people you meet on dating sites.
- **Do** provide your own transportation when meeting someone for the first time.
- **Do** use more popular dating apps and stay away from less popular sites, which may have less security in place.
- **Do** list your age but not your full date of birth.
- **Don't** use dating app sites on public Wi-Fi. Always make sure you are connected through a secure internet connection.
- **Don't** sync social media accounts with dating accounts.
- **Don't** use photos associated with other online or social media accounts.
- **Don't** give out personal information to include phone numbers or addresses.

Signs of a Scam

- Professes love quickly or claims to be overseas for business/military service.
- Asks for money or sends links to follow off the dating site.
- Claims to need money for emergencies, hospital bills, or travel to visit.

Tips and Tricks

- Be anonymous: Do not include your last name or any other identifying information in your profile. During initial communications, do not provide any PII such as phone number, email address, home address, place of birth, etc.
- Use a unique email address and username not associated with other accounts.
- Keep your financial information private.
- Do not meet at your house or place of work.
- Choose a first date location that is public.
- Do not provide specific personal questions while chatting, save that for the date. This will help to prevent giving away too much information, too early.
- Online dating scams are known to run for months at a time. Always be on the lookout for unusual conversations and behavior, such as requesting you to follow unknown links or send money.

Be aware of fake accounts and bots on dating apps. If a profile looks incomplete or too good to be true, it probably is. When messaging someone on a dating app, do not follow unknown links or send money.

FITNESS APPS

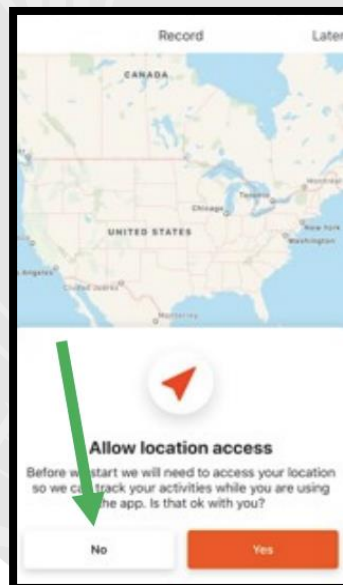
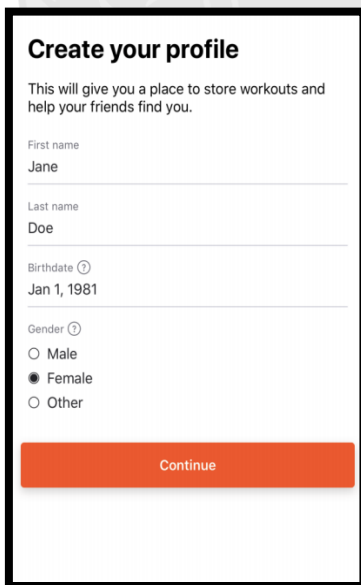


- Do make sure that your profile is not set to “public”. Also, limit what information you put on your profile even if it is set to “private”.
- Do keep your fitness app activity set to “private” by default, so that your routes cannot be tracked online.
- Do ensure that family members take similar precautions with their accounts.
- Do use a picture of something other than yourself for your profile. Profile photos are viewable to the public.
- Do not link your fitness app to any of your social media accounts. Doing so allows your routes and the times you exercise to be published to your social media accounts for others to see.
- Do not track exercises that begin at your own home, workplace, or school.
- Do not choose the same route every time you go for a run or walk. It is important to mix it up so that any potential stalker won't be able to track your whereabouts.

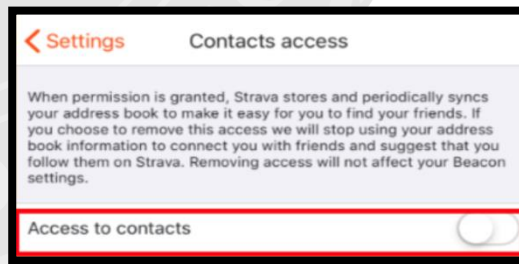
Create Your Profile

When creating an account put only the required personal information. Strava is a fitness tracker as well as a social network, its key feature is that its members can locate the most popular bike and running paths in their areas, follow their friends' routes, and log group exercises. For these key features to work, an optimal number of members must continuously share location data. If you leave your location data for people to see, you become vulnerable to victimization such as; physical attack, stalking, or theft of your belongings when you are away from your home.

When asked to access location data, although this is a big part of the app, we strongly recommend not allowing Strava to have access to location data. It is also recommended that you not share your contacts with Strava, though it will be asked multiple times.



It is recommended that you turn off the function that allows Strava to have access to your “Contacts” - the default for this function is set to “On”. Go back to “Settings”, scroll to the middle of the menu, select “Contacts”. Set the toggle to “Off”.

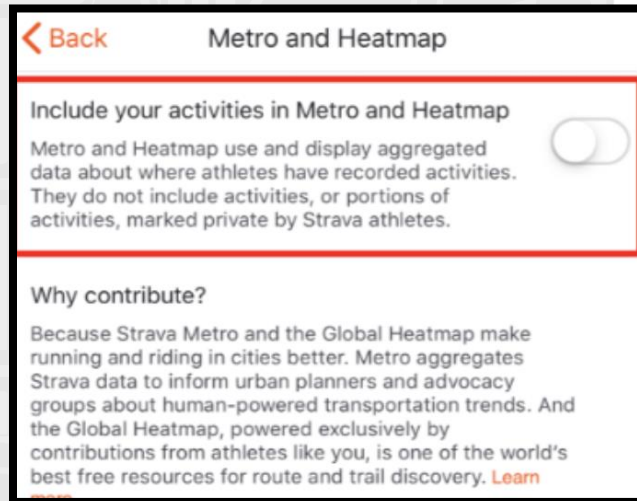
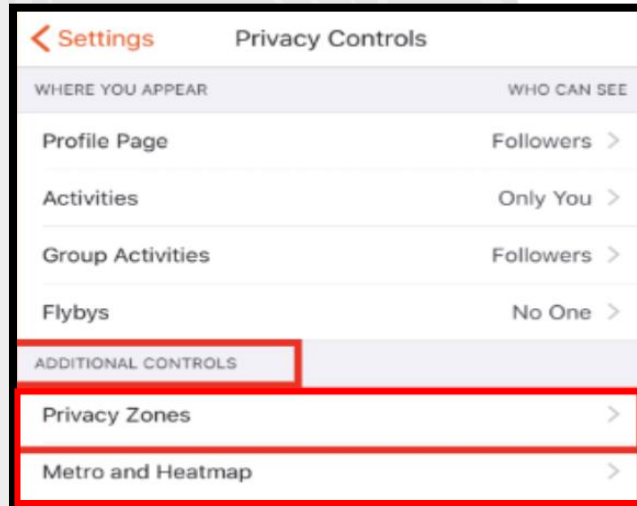
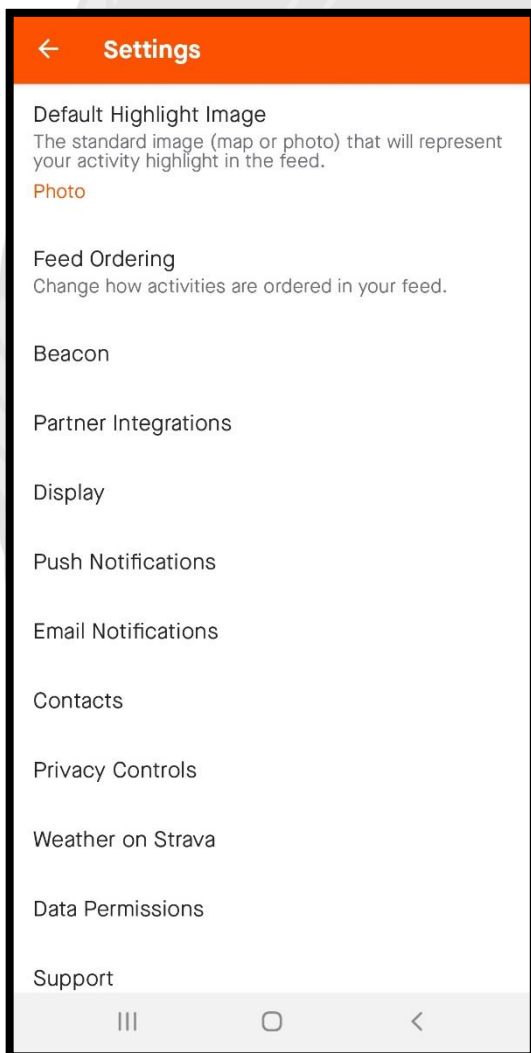


FITNESS APPS



At the top of the screen select the “Settings” icon. Scroll to find and select “Privacy Controls”. Here make sure each block in the “Where You Appear” is locked down to a comfortable level. It is recommended only “Followers” or “Only you” be selected to best protect your privacy. Now, locate the “Privacy Zones” tab. It is recommended that this function not be used, however if you allow others to track your movements on Strava already, this may be a great privacy function. Next, locate and select the “Metro and Heatmap” then be sure to turn this function off.

Heading back to the “Settings” tab, locate “Data Permission” where it is recommended Strava is denied access to “Health-Related Data”.



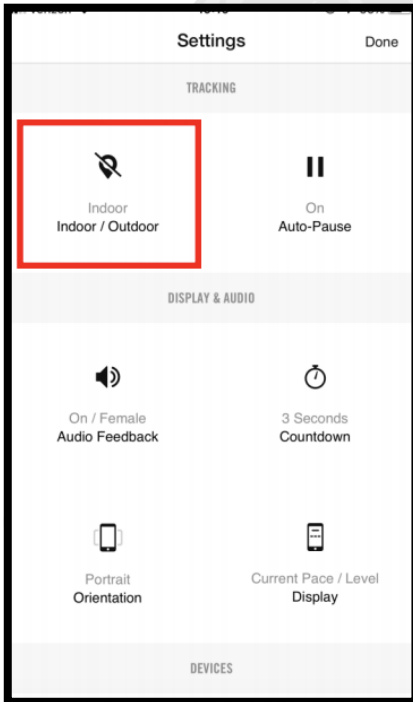
On iPhone: we recommend you scroll to the “Siri & Shortcuts” tab, under “Settings” (see left) and review the current settings there. Ensure your “Siri” function is off.

FITNESS APPS



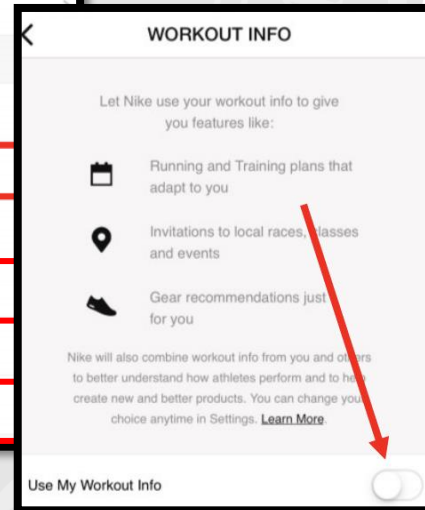
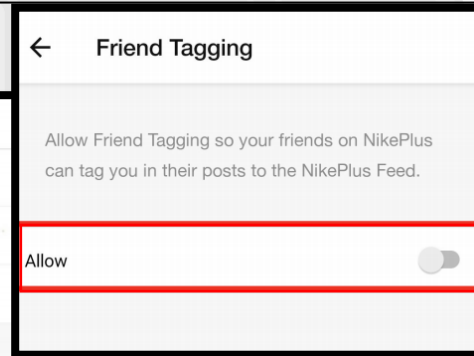
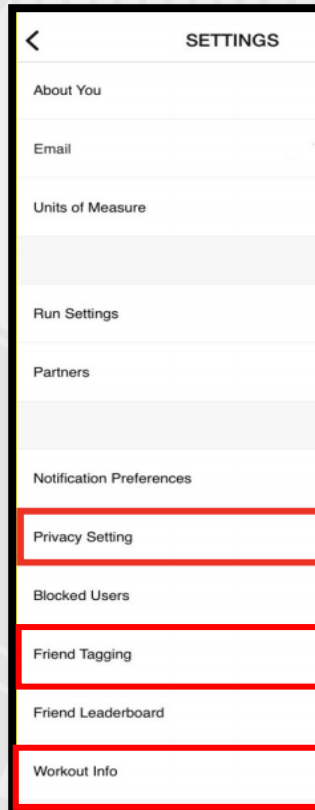
Create a Nike Run Club Account

As you create your Nike Run Club account, provide the minimum amount of personal information possible. It is recommended that you not link any other social media account to your fitness apps. Instead, use an email and password unique to this account. When setting up the account it is not recommended that Location data be accessible to the app, be sure to turn that function “off”.



Different Settings

This app contains two different “Settings” functions; the first is the Account Settings function and the second is the “Run Settings”. First look at the middle of the home screen and select the “Settings” icon to take you to your “Run Settings”. Here select “Indoor/Outdoor” to taggle the function to “Indoor”. These settings can also be found in the Account Settings as well.



Privacy Settings

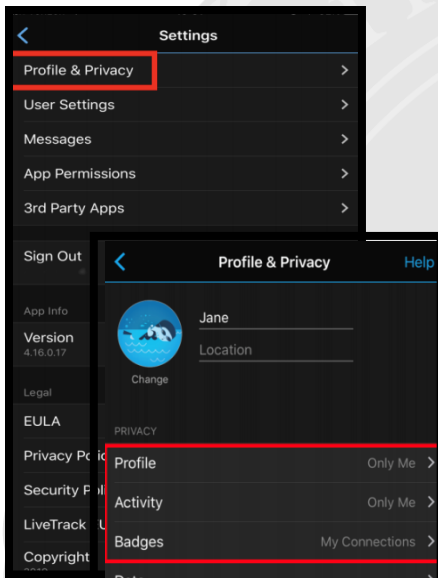
Now head back to the home screen and select the menu in the top left of the screen. Now select “Settings” to access the Account Settings. Scroll to find and select “Privacy Setting”. It is recommended that “Only Me” or “Friends” be selected here. Next head down to “Friend Tagging” to turn this feature off. Finally, scroll to and select the “Workout Info” tab, still in the “Privacy Settings”. We recommend you set the toggle to “Off” in order to secure your data and personal information.

FITNESS APPS



Creating a Garmin Account

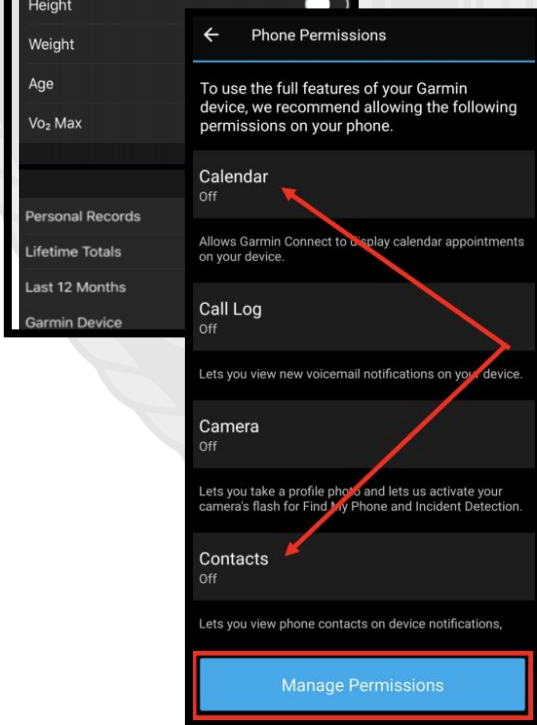
As you create your Garmin account, provide the minimum amount of personal information possible. It is recommended that you not link any other social media account to your fitness apps. Instead, use an email and password unique to this account. When setting up the account it is not recommended that Location data be accessible to the app, be sure to turn that function "off".



Create Your Profile

Select the menu icon from the top left-hand side of the screen, then select "Settings". Locate and select "Profile & Privacy". In the first section, labeled "Privacy", go through and change each setting to your comfortability. It is recommended "Only Me" or "My Connections" be selected.

In the same section review the "Data" tab. These functions allow Garmin to collect data from your account and device in order to build and reinforce databases that hold popular routes. We recommend you turn this function off by setting the toggle to "Off". Next, select "Insights" and read through the consent policy provided before you decide if you want to "Agree" or "Do Not Agree", this is your choice. Finally, select "Device Upload" and decide whether you want to Garmin to connect your Garmin devices to "Garmin Connect", set the toggle to "On" or "Off" based on your preference here. Review each data collection section under this tab to change each to your comfortability.



Phone Permissions

Head back to the "Settings" menu and select "Phone Permissions". Review each setting and change to your comfortability. It is recommended that, where possible, phone permissions be limited to any app.

FITNESS APPS



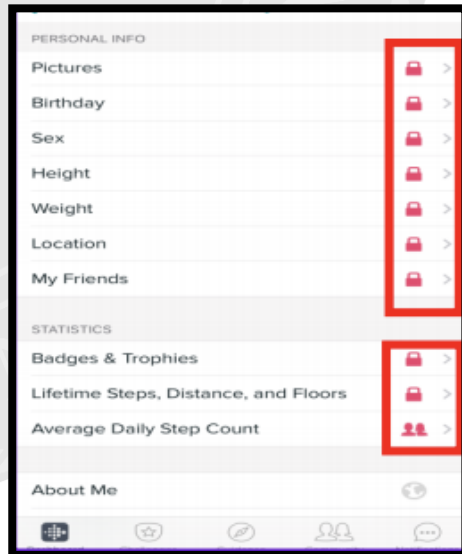
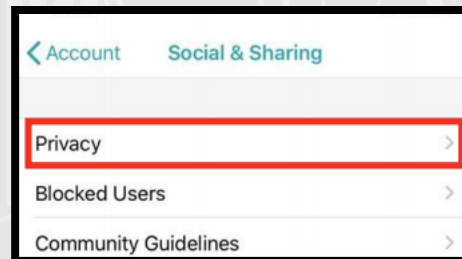
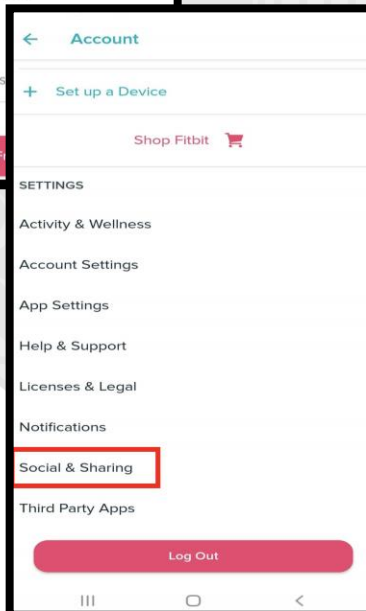
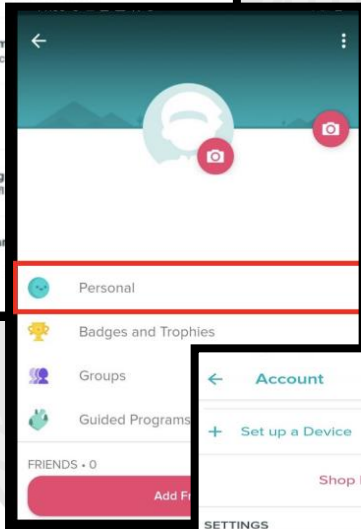
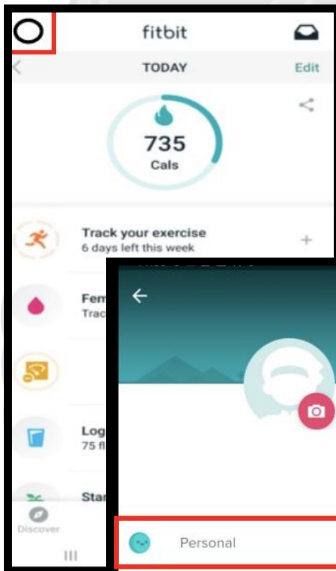
Creating a Fitbit Account

As you create your Fitbit account, be sure to provide the minimum amount of personal information possible. It is recommended that you not link any other social media account to your fitness apps. Instead, use an email and password unique to this account. When setting up the account it is not recommended that Location data be accessible to the app, be sure to turn that function “off”.

From your “Home” screen select your “Profile Picture” icon in the top left corner. Then select your “Account”, noted by your name, and your “Profile Page”, select “Personal” and ensure that “Location” is not turned on. The “About Me” section is always set to “Public” so you may want to review what other information is in this section.

Social & Sharing

In the “Account” section, select “Social & Sharing” then select the “Privacy” section. Select the icon to the right of the category for each section. Select the icon and make the change, then select “Save” in the upper right corner of the screen. It is recommended that “Private” or “Friends” be selected here and not “Public”.



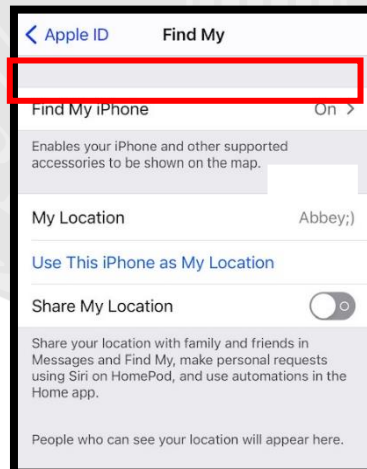
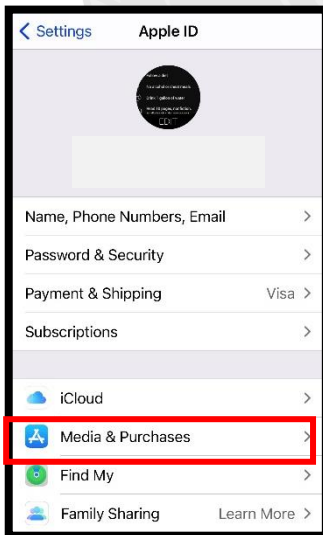
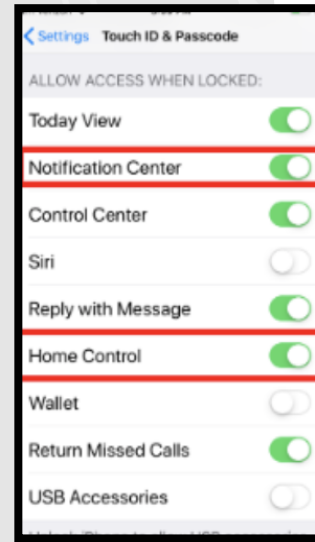
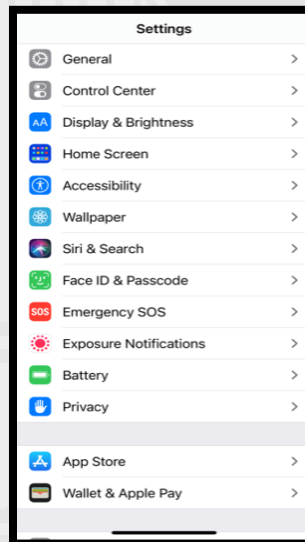
iOS PRIVACY SETTINGS (14.1)



- Smartphones and tablets are not impenetrable. Secure your smartphone with a password and use apps such as “Find My iPhone” to locate lost or stolen devices.
- All smartphones and tablets have cameras and micro-phones that can be remotely activated. Caution should be used when device is near anything of personal importance.
- Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible and avoid public wireless networks. It is advisable to turn these services off if not immediately needed.
- Prior to downloading apps on your device, read the developers permissions. Many apps require permission to access your camera, microphone, text messages, and contacts.
- Turn off location services until they are needed. Otherwise, your daily movements may be tracked by various apps and vendors. Whether turned on or off, location services are always available to 911 and first responders.

Physical Security

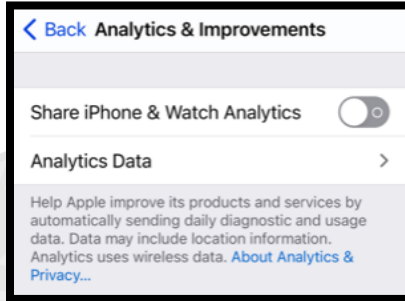
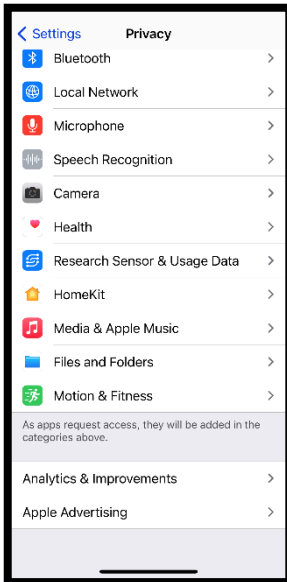
In the iOS “Settings” app find and select “Touch/Face ID & Passcode”, then select “Add a Finger-print” and “Turn Passcode On”. Ensure the password is strong such as an alpha-numeric passcodes. Note: iPhone 11 has taken off the feature “Touch ID” and replaced it with “Face ID”. Additionally, it is recommended that you turn off “Siri” due to its listening capabilities and bugs associated with accessing your phone. Finally, scroll further down in this section to find, “Allow Access When Locked” and go through to ensure comfortability with each.



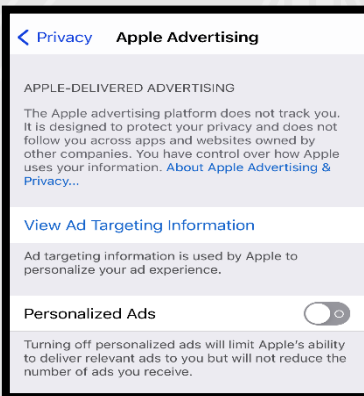
Find my iPhone

Next go to “Settings” and select your account at the top of the list. Now select “Find My,” then “Find My iPhone”. Be sure this function is turned “On”. This way if you lose your phone, you can access your account online and geo-locate where it is.

iOS PRIVACY SETTINGS (14.1)

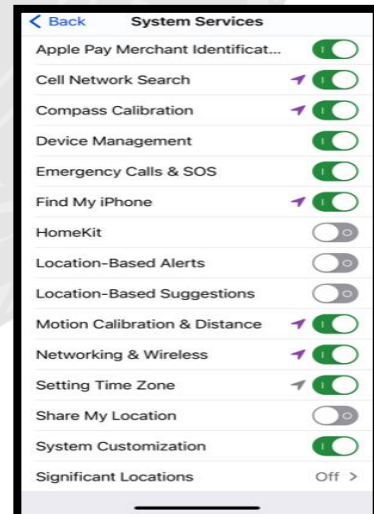


Analytics and Advertising
Locate and select “Privacy” under “Settings” then select “Analytics” & “Improvements”. Here it is recommended that “Share iPhone & Watch Analytics” be turned off. Next, under “Privacy” select “Apple Advertising”. Here it is recommended that “Personalized Ads” be turned “Off”.



Location Based Services
“Location-Based Apple Ads” and “Apple Ads” allow Apple to serve you with ads, based on your location. “Location-Based Ads” do not use your exact location and Apple does not give this information to advertisers. Under “Privacy”, locate and select “Location Services” then scroll down to select “System Services.” Here a list of location-based selections can be toggled to off. While in “System Services,” it is also recommended you scroll to the lower portion of the screen and select “Significant Locations”. From there be sure the “Significant Locations” is toggled to the “off” switch, so that your Wi-Fi and iPhone are not capturing your location data. It is also recommended that any previous data collection be deleted.

Adding Accounts
Now navigate to “Share My Location” and tap on the toggle to disable “Share My Location.” Note: If you turn off “Location Services” in the “Privacy Setting” menu, you cannot use location services for things such as “Navigation” or “Find My iPhone” if lost or stolen. You can still wipe your phone, using the “Find My iPhone”, if “Location Services” are off. “Alternatively, you can leave “Location Services” on in “Privacy Settings” but turn it off for installed apps you don’t want to have access. Just scroll down to find which apps use your location. Go back to “Location Services” to disable your location from being saved with photos and tap on “Camera” to change this setting. Note: The “Location Services” toggle must be on to find the camera option. Perform the same steps to disable location services for other apps listed in the “Location Services” setting. Navigation and maps apps are examples of those that require “Location Services.”



iOS PRIVACY SETTINGS (14.1)

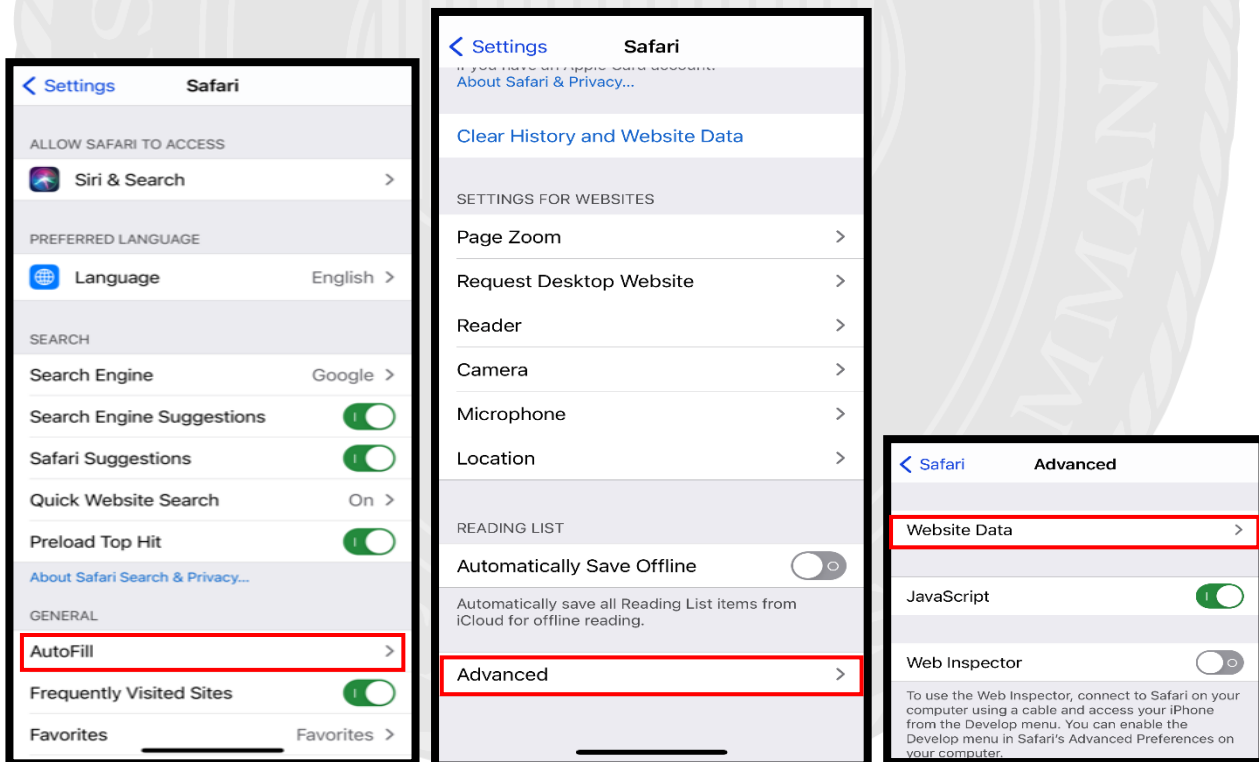


Safari

Safari’s “Do Not Track” is a universal web tracking opt-out initiative that allows users to prevent advertisers from tracking your browsing habits. The Safari browser on iOS 13.0 allows users to opt-out to prevent advertisers from seeing users mobile web browsing history. To opt-out, open the “Settings” app, scroll down and select “Safari”. There are several sections to look through and adjust the settings, but definitely turn off “Frequently Visited Sites” under the section titled “General”. This prevents Safari from tracking sites you regularly visit. Next, under the “Privacy & Security” section on the “Safari” page, turn on “Prevent Cross-Site Tracking” and “Fraudulent Website Warning.”

It is also a best practice to clear the browser history periodically. To do so, continue to scroll down in the Safari settings, at the very bottom select “Advanced” then select “Website Data”. From there select “Remove All Website Data”.

Clear the AutoFill to protect passwords and credit card information. To do so, open “Settings” and select “Safari” then click on “AutoFill”.



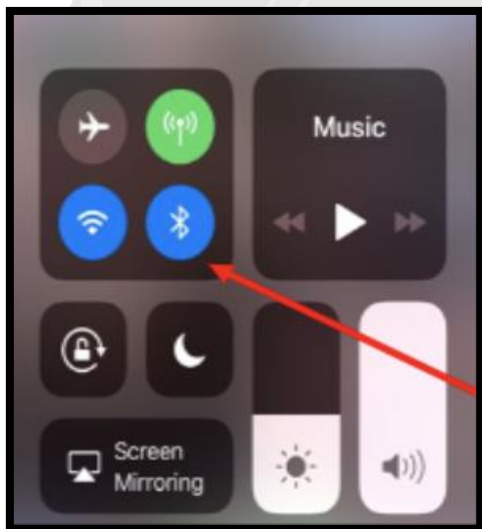
iOS PRIVACY SETTINGS (14.1)



WiFi and Bluetooth

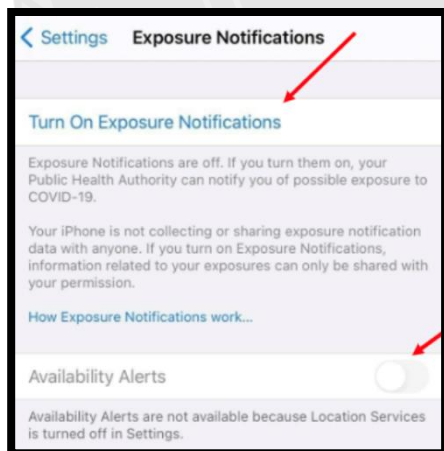
“Wireless Networks” Where possible, public WIFI networks should be avoided due to the vulnerabilities they present to your personal data. If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt on-line transactions. There are two ways to turn off WIFI: 1) Scroll up from the bottom of your phone and tap the icon on the control screen; or 2) In “Settings”, Select “WIFI”, and it turn off.

Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your iPhone or tablet, hackers can gain access to your device and obtain contacts, messages, calendars, photos, and notes without your knowledge. It is therefore recommended that you only use Bluetooth, when necessary, like in your car, and that you turn it off after you are done using it each time.



COVID 19 Contact Tracing Apple and Google have partnered on offering a secure and private coronavirus contact tracing implementation on iOS and Android. You can see whether this is activated by going to “Settings” then locate and select “Exposure Notifications” and “Exposure Logging”. When you see “Exposure Logging”, you will notice a toggle to the right that is probably “Off”.

If you decide at any point that you want to disable the “Exposure Notifications Logging” tool on your iPhone, you can take the following steps. First, on iOS 13.5 and later, go to “Settings” on your iPhone. Next, swipe down and select “Exposure Notifications”. You can also delete the exposure logs manually at any time by going to the bottom of the “Exposure Logging” page and selecting “Delete Exposure Log”. If you have opted-in to the “Exposure Logging” system, you may be interested to know who is trying to access your exposure information. To find out, select “Exposure Checks” on the “Exposure Logging” page. This is a record of all requests to check your “Exposure Log” from the past 14 days.



Note: The “Exposure Logging” toggle is disabled by default in iOS 14.1. It does not connect any data without you in-stalling and authorizing a local health authority app, which will be available soon. Apple and Google’s exposure notification system will be completely opt-in.

ANDROID PRIVACY SETTINGS (11.0)



Best Practices

- Smartphones and tablets are not impenetrable. Secure your smartphone with a password or biometrics, and utilize apps such as Find My Device or Prey Anti Theft to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Consider your device when you are in certain places or conversations.
- Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible, and always avoid public wireless networks.
- Prior to downloading apps on your device, read the developer's permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- Keep location services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked. Don't worry, location services are always available to 911 and first responders, even when turned off.
- If you have a google account, you can use your google credentials to login at [maps.google.com/location history](https://maps.google.com/location-history) to see your device location history for the last year or more.

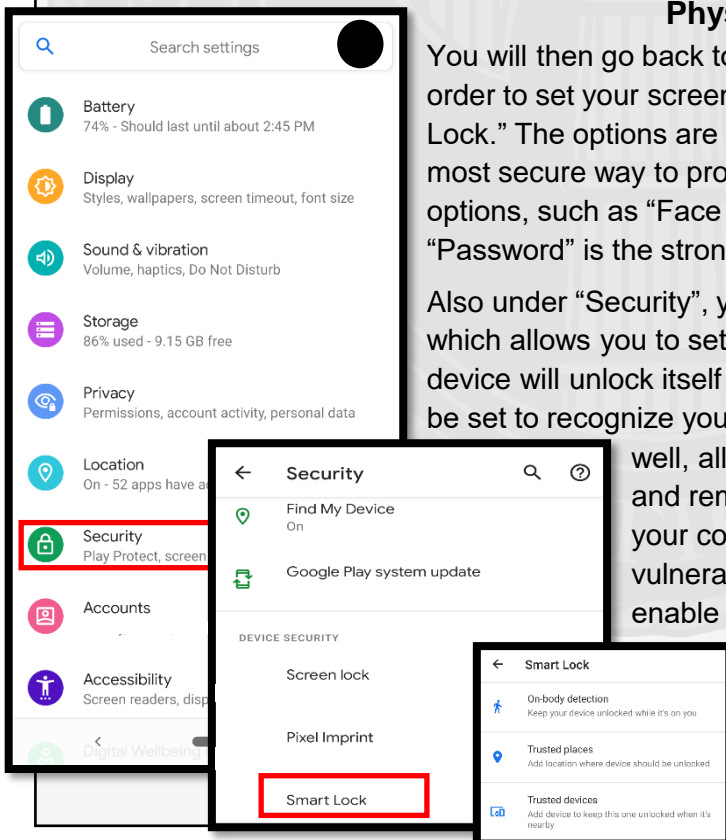
***NOTE:** Due to varying Android manufacturers, the instructions in this Smart Card may vary slightly depending on the device being used.*

The most important thing you can do to keep your information secure is to keep your device up to date. In order to make sure your Android is up to date with the latest Android Version, first go to "Settings" then "System," scroll to the bottom and select "Advanced." From there you will see the "System Update" tab, select the tab. (On some versions, you may go to "Settings", then "Software update" toward the bottom of the "Settings" list).

Physical Security

You will then go back to "Settings" and select "Security" in order to set your screen-lock preferences. Tap the "Screen Lock." The options are Swipe, Pattern, PIN, Password. The most secure way to protect your phone is to use the **biometric** options, such as "Face Recognition" and "Fingerprints". A "Password" is the strongest backup solution.

Also under "Security", you will see the feature "Smart Lock", which allows you to set "Trusted Places" inside of which your device will unlock itself and remain unlocked. This feature can be set to recognize your face and "Trusted Devices" as well, all of which trigger your device to "Unlock" and remain unlocked. This feature is meant for your convenience, but presents obvious vulnerabilities. We recommend you do not enable any "Trusted Features".

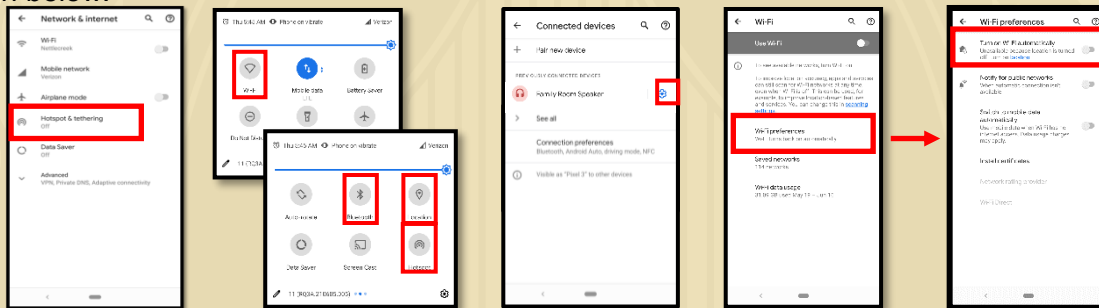


ANDROID PRIVACY SETTINGS (11.0)



Mobile Hotspot, Bluetooth and Wi-Fi

Mobile hotspots devices can be purchased and used for connecting to the internet remotely, but without connecting to public Wi-Fi, which is always discourage. Most Android Smartphones have a “hotspot” feature that allows you to connect to your internet (for instance on your laptop) remotely. By turning on this feature, your phone uses its cellular data to create a “Wi-Fi hotspot”. You can turn this option on and off under “Settings” > “Network & Internet” > “Mobile Hotpot and Tethering”. **Bluetooth** is a wireless technology for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your device, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes, or install malware without you even knowing. To disable Bluetooth go to “Settings” > “Connected Devices > “Connection Preferences”. When using **Wi-Fi** on your Android it is important to ensure the “Turn on Wi-Fi automatically” feature is turned off. To do this head to the Wi-Fi screen then select “Wifi Preferences”. If this function is turned on simply toggle the switch to the “off” position as shown below.



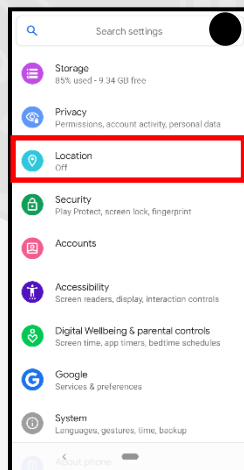
Note: We always recommend avoiding public Wi-Fi networks because they are unsecured. If you must use one, avoid logging into accounts that require passwords and use a VPN client to encrypt on-line transactions.

Note: In order to delete Bluetooth sessions you no longer need, go to “Bluetooth”, select “Previously Connected Devices” then select the “Settings” icon, select “Forget.”

Location Services

Whenever you take a photo, data on your location is saved inside of the photo’s called EXIF data. When you send that photo to someone or post it online, data on where you took the photo may be available to those who know how to view it. If you post a picture that you took from your home, anyone that can view it may be able to figure out where you live and more.

To disable your location from being shared, select “Settings” and scroll down to “Location.” Disable your location services by switching the toggle to “off”.



Near Field Communication (NFC)

NFC is technology that allows you to “bump” your smartphone with other NFC devices to exchange information or pay for items using a Pay app. A malicious user can tamper with the data being transmitted between two NFC devices if they are within range with malware.

Turn off NFC when not in use by tapping “Settings” > “Connected Devices” > “Connections Preferences” > “NFC”. Then tap the toggle switch for “NFC and payment” so that it is in the “off” position.



ANDROID PRIVACY SETTINGS (11.0)



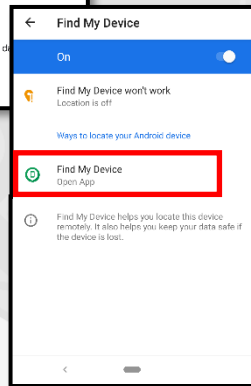
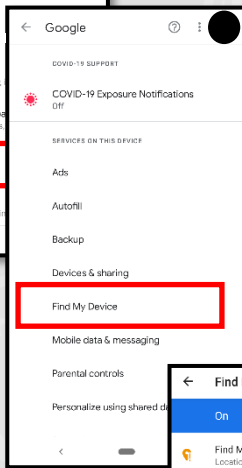
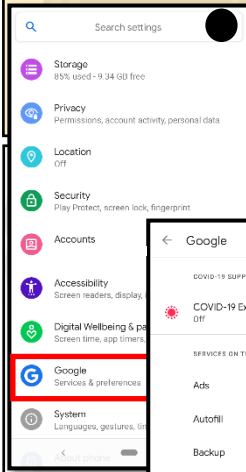
Lost/Stolen Phone

Over 100 cell phones are lost or stolen in the U.S. every minute, which shows how necessary it is to keep your device secure and locked with biometrics or a passcode. All Android phones work by syncing a phone to a google account, so if you lose your device, you can go to android.com/find in order to locate it. This is the native “Find My Device” tool for Android, and is automatically enabled on your Android Smartphone. Alternatively, you can download the “Find My Device” app from Google Play Store.



- ◆ Locate Android devices associated with your Google account.
- ◆ Reset your device's screen lock PIN.
- ◆ Erase all data on the phone.

Note: If you turn off “Location Services” in the “Location Setting” menu, you cannot use “Location Services” for apps that locate lost or stolen devices. You can still wipe your phone if the “Location Services” are “off”. If you wish to use some “Location Services”, be sure to go into each app and set the “Location Settings” as desired rather than turn off the main “Location Services” setting.

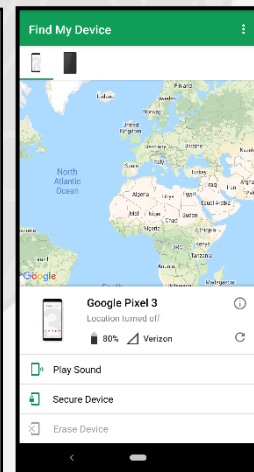


What should you do if your device is lost or stolen? Google can help you locate it. Let's enable the settings on your device so that in case you need to, you can locate your lost phone. Go into “Settings” > “Biometrics and security” > “Find My Mobile”. Ensure the Toggle is set to “On”

If your device is lost or stolen, you can then go to “Google Find My Device” page and see where your phone was located last. You can make the (android.com/find) device ring at full volume to help you find it or remotely lock or erase all data on it.

In order to test this feature, let's go to android.com/find and see if it works.

Can Android phones get viruses? The traditional “virus” is common on personal computers, Androids don't get these traditional viruses, but they do get other malware. This malicious software can be designed to secretly control the device or even steal private information. An example of this Android malware is Triout. Triout was originally founded in 2018, bundled with a legitimate application on the Google Play marketplace. This malware could hide on your Android and record phone calls, save text messages, record videos, take pictures and collect your location. Although this original version was only active from May 2018 to Dec 2018, there are new variations being discovered. In order to help prevent malware from getting onto an Android device it is important to turn off your Wi-Fi, Bluetooth, and sharing capabilities whenever you are not actively using them.



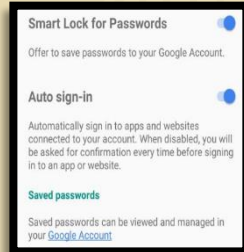
ANDROID PRIVACY SETTINGS (11.0)



Smart Lock for Passwords

From the same Google Settings section, select “Smart Lock for Passwords”. You will then see the screen where you can turn off the options to save your passwords and automatically sign-in to web pages and other account-oriented sites. You can also add apps for which you don’t want passwords to be saved.

Alternately, you can select specific accounts and delete the saved password by tapping the “Google Account” hyperlink. All saved passwords are encrypted and stored in the Google cloud storage that comes with your account. Although it is recommended that you turn off the above options, only you can balance your security with the convenience of saved passwords.

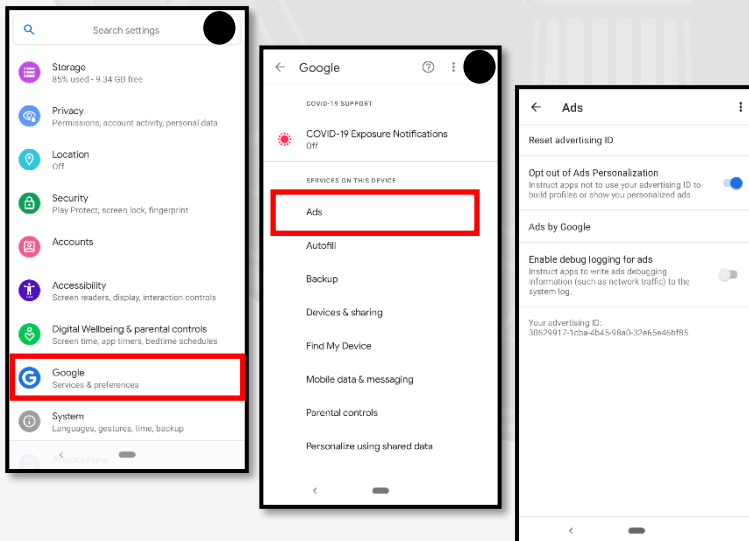


Ad Tracking

Ads can track everything you do. Not all Android devices and OS versions have settings to turn Ad tracking off. If your device does not have this setting, you can download ad blocking / privacy-oriented browsers or browser add-ons. Here are just a few examples:



If your device has the option to control advertisements, the following directions show you how to disable the feature: Go to “Settings” > “Google” > “Ads”. Tap the toggle switch to the “On” position for “Opt out of Ads Personalization”.



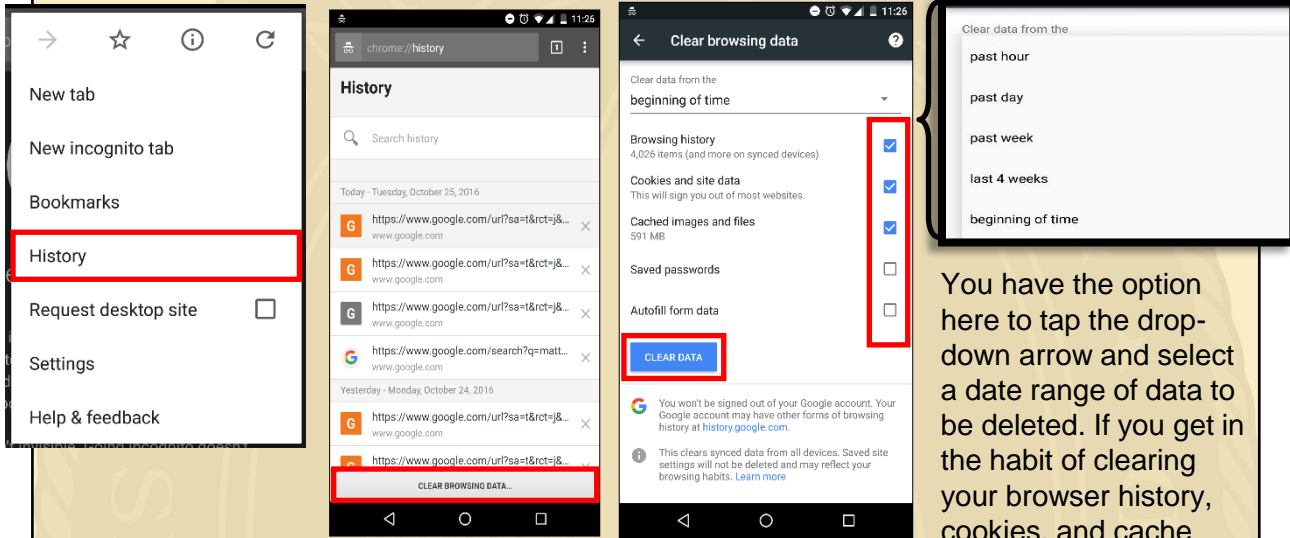
Safe Browsing: Android devices have a “safe browsing” mode that is built into them and enabled by default. While using Google Chrome, this feature will give warnings before entering a suspicious site. As long as your Chrome and Android are updated to the most recent versions, this feature should work to protect you from malicious sites.

ANDROID PRIVACY SETTINGS (11.0)



Internet Privacy Settings

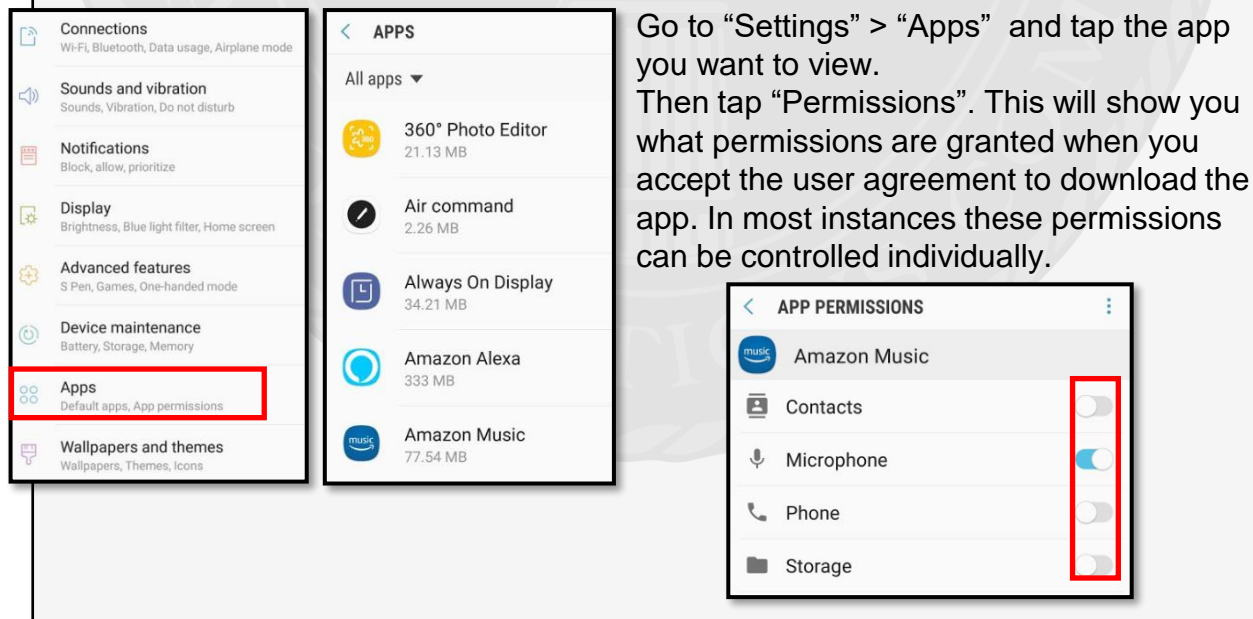
Browser history and cookies are tracked when browsing the web from your mobile devices. To ensure privacy, open your browser (Chrome) and tap the three dots in the upper right-hand corner. Tap “History” then “Clear Browsing Data” at the bottom (or top) of the screen. On the next screen, select the applicable boxes (use the below screen shot as an example) and tap the blue “Clear Data” button.



You have the option here to tap the drop-down arrow and select a date range of data to be deleted. If you get in the habit of clearing your browser history, cookies, and cache then taking this step will become less important.

Application Manager

The applications you load access different capabilities on your device, regardless of whether they are active or working in the background. You can see, and to some degree control, what access each application has in the “Application Manager”.



Go to “Settings” > “Apps” and tap the app you want to view. Then tap “Permissions”. This will show you what permissions are granted when you accept the user agreement to download the app. In most instances these permissions can be controlled individually.

ZOOM



USSOCOM SMARTCARDS

• **Do** require a password for all meetings and webinars conducted in Zoom. This will help to minimize intruders from gaining access to your conferences.

• **Do** make sure to control screen sharing capabilities within Zoom. We recommend you never give up control of your personal screen to anyone you are in a meeting with.

• **Do** have all attendees register prior to meeting on Zoom in order to dissuade Zoombombers from entering your meetings.

• **Do** discuss potential security and privacy concerns with your participants or company prior to using Zoom.

• **Do** review updated security notes posted by Zoom.

• **Don't** use video call if it is not required. When possible, it is recommended to refrain from using video conferencing in Zoom. Instead, simply dial into meetings, which limits the information you are required to provide.

• **Don't** allow participants to share their screen during any of your meetings.

• **Don't** forget to lock your meeting once you have confirmed all known participants have entered your meeting domain. Doing so will prevent intruders from gaining access during your meeting.

The screenshot shows the Zoom web interface. At the top, there are links for "REQUEST A DEMO", "1.888.799.9666", "RESOURCES", and "SUPPORT". Below these are "SCHEDULE A MEETING", "JOIN A MEETING", and "HOST A MEETING" with a dropdown arrow. A red box highlights a green "A" icon in the top right corner. On the left sidebar, under the "PERSONAL" section, the "Settings" option is highlighted with a red box. The main content area shows the "Meeting" settings page, with tabs for "Meeting", "Recording", "Telephone", and "Collaboration Devices". The "Security" section is expanded, showing a toggle for "Require that all meetings are secured with one security option" which is turned on. Below this, there is a note: "Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or 'Only authenticated users can join meetings'. If no security option is enabled, Zoom will secure all meetings with Waiting Room. [Learn more](#)".

The following steps are for the computer web based application, followed by the Android and iPhone.

Once you are signed into your Zoom account, look to the left of your screen and below "Personal", select "Settings" (shown here highlighted in red to the left). On the screen you will see three tabs; "Meeting", "Recording" and "Telephone". In the "Meetings" tab scroll down until you see the section shown below. We recommend you always authenticate users and require a password when scheduling any meeting.



Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Meeting Passcode

All instant, and scheduled meetings that users can join via client, or room systems will be passcode-protected. The Personal Meeting ID (PMI) meetings are not included.

Require a passcode for meetings which have already been scheduled

Require passcode for participants joining by phone

A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.

Embed passcode in invite link for one-click join

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

Only authenticated users can join meetings from Web client

The participants need to authenticate prior to joining meetings from web client

Require a passcode for Personal Meeting ID (PMI)

Only meetings with Join Before Host enabled

All meetings using PMI

Embed passcode in invite link for one-click join

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

In response to criticisms of weak security and privacy, Zoom has modified passcode options. Zoom has pre-selected and locked user ability to toggle “Off” passcode options, thus making it more secure for users. We recommend you still verify these options are toggled “On”, as shown to the left. The last portion, “Only authenticated users can join meetings from Web client” allows users the option to toggle “On” or “Off”. We recommend you keep it toggled “On”.

To the left you will see a continuation of the password requirements and recommendations located in “Meeting.” We recommend you require meeting attendees to input the provided password and **not** to embed the password into the meeting link. We also recommend you use a “Pre-meeting Password” and not your “Personal Meeting ID”.

Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants

Prevent participants from saving chat

Private chat

Allow meeting participants to send a private 1:1 message to another participant.

Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

File transfer

Hosts and participants can send files through the in-meeting chat.

Only allow specified file types

Screen sharing

Allow host and participants to share their screen or content during meetings

Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications.

Also, we recommend you use end-to-end encryption whenever possible when using any device that holds your personal information, Zoom is no different.

Note: Zoom’s encryption capabilities have been called into question on several occasions. Therefore, we recommend you watch what is documented on Zoom when in a meeting, as the meeting host’s encryption may not keep your information secure.

While using chat features on Zoom, we recommend you not allow other attendees to save chats. In order to do this, scroll down until you see “Chat” (shown here to the left). All configurations to the left are recommended for the “Chat” section. Scrolling past “Chat” you will find “File transfer” next in your “Meeting” tab. Due to Zoom’s lack of acceptable encryption and recent security issues, we recommend you not send files of any kind on Zoom.

Next, scroll down to “Screen sharing”. We recommend you not allow the ability to screen share when in a meeting on Zoom. If you must allow screen sharing, we recommend that users control who can share screens and who can take control of those screens.



As you continue to scroll down, we recommend you disable the sections “Whiteboard” and “Remote control” (highlighted here in red). It is never recommended that Users give up control of their own computer to any other individual, whether it is a personal computer or company computer.

Whiteboard
Allow participants to share whiteboard during a meeting

Remote control
During screen sharing, the person who is sharing can allow others to control the shared content

Allow removed participants to rejoin
Allows previously removed meeting participants and webinar panelists to rejoin

Allow participants to rename themselves
Allow meeting participants and webinar panelists to rename themselves.

New to Zoom is a feature that allows participants to rejoin a meeting if they have been previously removed. It is important you turn this function to “off” in order to prevent users that might hack into your meetings, to continue to rejoin after you have identified and removed them. In order to do so simply scroll down past “Remote Control” and find “Allow removed participants to rejoin” and toggle it to “off”. It is also a good idea to not allow individuals to rename themselves in order to prevent any confusion from other participants.

Remote support
Allow meeting host to provide 1:1 remote support to another participant

Closed captioning
Allow host to type closed captions or assign a participant/third party device to add closed captions

Save Captions
Allow participants to save fully closed captions or transcripts

Far end camera control
Allow another user to take control of your camera during a meeting

Virtual background
Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

Identify guest participants in the meeting/webinar
Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.

Once you have set the above recommendations, continue to scroll down until you find the “In Meetings (Advanced)” section. Here you will find a series of settings that need to be updated/checked to ensure they meet your specific security requirements. However, we recommend meeting attendees **not** participate in any third party activities while on Zoom. We also recommend users **not** allow other users to take control of their camera while using Zoom. When setting up a meeting or webinar, it is important to ensure you are able to see “guests” who might be participating for both you and your contacts. If you scroll down, still in “In Meetings (Advanced),” you can enable the “Identify guest participants in the meeting/webinar” (shown to the left).

If you scroll all the way to the bottom of this section you will find yet another new section on Zoom. This final section will allow you to blur any photos that are being made from users on smart devices in order to control proprietary information or other individuals who might be in attendance. If you are using Zoom for business functions it is important that you enable this function to ensure your companies privacy.

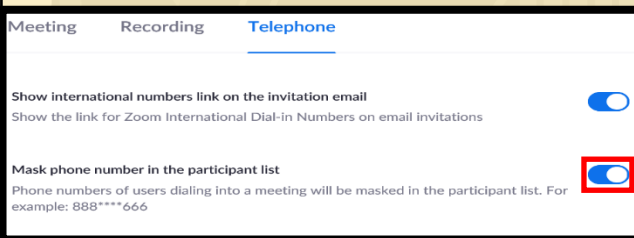
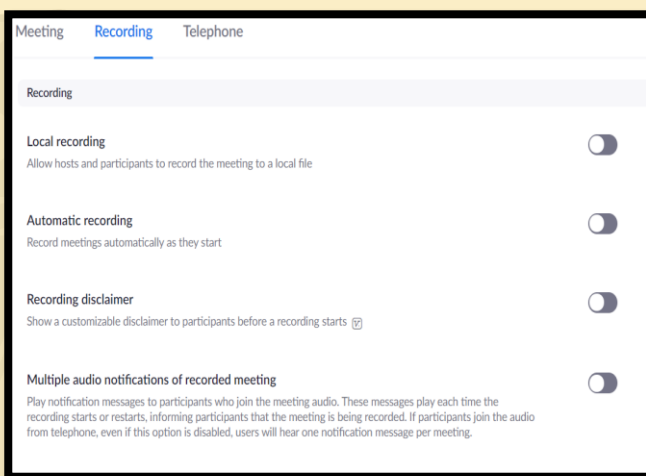
Other

Blur snapshot on iOS app switcher

Enable this option to hide potentially sensitive information on the app switcher screen from Zoom. This screen will be shown only when multiple apps are open.

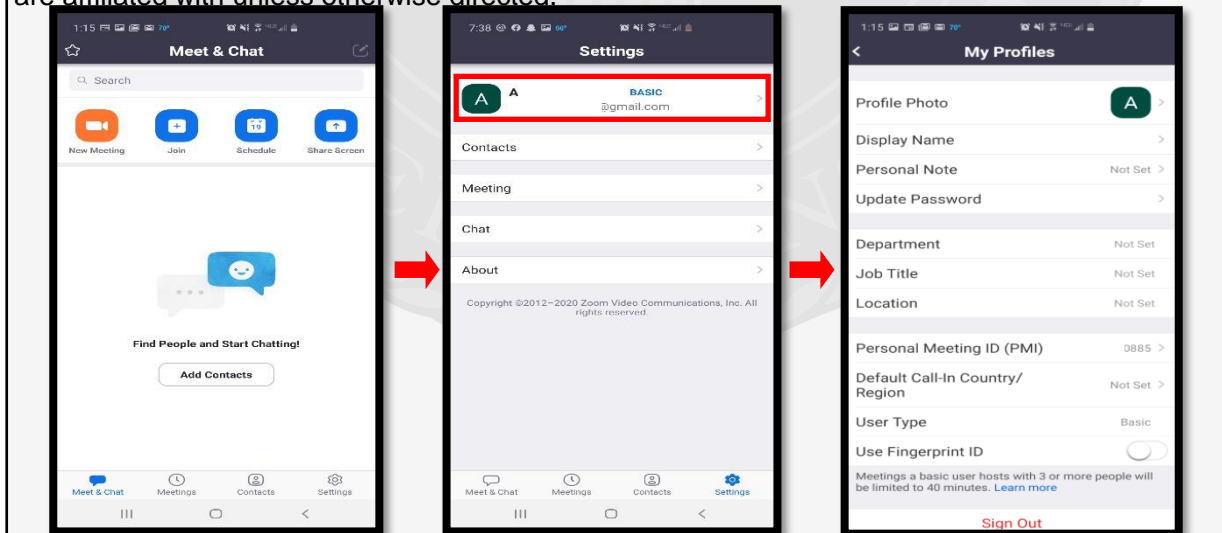


Now, scroll back to the very top of the screen and select “Recording” from the menu option (shown to the right, selected in blue). Though there are not very many selections to go through, it is still very important to review all your settings here and enable or disable any features you see fit. We recommend you disable most, and preferably all, features located in the “Recording” section. The only exception here would be the very last feature, which is more of a personal preference than a security issue. We recommend you *not* allow anyone to record your meetings.



Head back up to the menu and select “Telephone” to review the final settings here. First, we recommend that you mask meeting attendees’ phone numbers. In order to do this, simply toggle the “Mask phone number in the participant list” to enable (shown to the left in red).

When using Zoom on your smartphone there are a few security and privacy settings that should be considered for safe use. Though it is not recommended for use on your smart phone, should you chose, there are a few settings to consider here. On both the Android and iPhone, look to the lower right of your screen and select “Settings” (shown below to the left in red). Next, select your name/email from the top of the screen to take you to your profile page. NOTE: iPhone Users, before selecting your name/email you can look to the lower portion of your screen to “Enable” or (recommended) “Disable” any “Siri Shortcuts” related to this application. In your “My Profiles” section, review each individual section and ensure no personal information has been provided. It is recommended you use initials for your “Display Name,” write no “Personal Notes” about yourself and not fill in any other personal information about yourself or the company you are affiliated with unless otherwise directed.





Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- Unexpected calls or messages made or received from your account
- Any Direct Messages sent from your account you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Zoom stating your account may be compromised
- A notification from Zoom stating your account information (bio, name, etc.) has changed
- Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended you sign-in online and change your password immediately

If you said "Yes" to any of the above, it is recommended you immediately do the following actions:

- Delete any unwanted messages that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure you and only you can access your Zoom account. Note: Two Factor Authentication for Zoom ONLY works on the web based app and only if you are an admin or if the admin has set it up for you.
- Be sure to check your email is secure. It may be worth changing the password to both your Zoom account and the email associated with your Zoom account.

If you need to report a violation of Zoom's Terms of Services follow this link:
<https://support.zoom.us/hc/en-us/articles/200613919-Report-Terms-Of-Use-Violation>

If you would like to terminate your account follow this link: <https://zoom.us/account>

If you still need help or have questions, you can always contact Zoom using their Support site at: <https://support.zoom.us/hc/en-us/articles/201362003>

Important Information Regarding Zoom: If your Zoom meeting gets "Zoombombed" there are a few things that can be done. First you can lock them out by going to the "Participants List" in the navigation bar and select "more." Next click "Lock Meeting" to prevent any additional intruders from entering your meeting, which will also allow you to remove individuals without them being able to regain access.

If you are less worried about the intruder and more worried about the disruption follow the same path but to the "Participants List" and scroll down to select "Mute All Controls." This option is not recommended for privacy and security concerns.

TRAVELING WITH SMARTPHONES



- **Do** enable password and fingerprint locks on your device. Also, protect “Settings” changes on your phone by requiring a password.
- **Do** assume that all information on your device can be accessed remotely. Don’t store passwords and sensitive information on your phone.
- **Do** always use complex passwords, the stronger and longer the password the more difficult it will be for someone to hack into.
- **Do** delete emails that are old or no longer needed prior to travel. Remember emails contain a lot of personal information. Think about what a hacker might gain if they were able to access your email?
- **Don’t** become stagnant upon returning from your travels. Examine your smartphone as soon as you return to your home. If it is acting up or repeatedly making you put your password in there may be malware on your device and you may want to take it in or consider getting a new device.
- **Don’t** link apps and social media accounts together (i.e. using one SM account to login to another). Remember if someone hacks into one of your accounts, it is better if they only get access to that one. Linking accounts together makes all of them vulnerable.
- **Don’t** leave GPS, Bluetooth, and Wi-Fi turned on when traveling. Any of these left on could allow a hacker to connect to your phone if they were able to get within a certain distance from you.

Wi-Fi Safety Tip

Avoid Public Wi-Fi at all costs, hackers will name the network the same thing as the hotel or other public network. Hackers in Europe have been caught making Public Wi-Fi networks to resemble the public network name. Do not assume all networks are secure, just because it says the name of a company does not mean it is a legitimate network, check with the company to be sure. Also, be sure to turn your Wi-Fi off when you are not using it in order to prevent tracking or hacking of your phone.

Precautionary Tips

- Be aware that your phone may be scanned forensically when entering a foreign country.
- Set your phone to lock automatically and make sure you have a complex password or fingerprint enabled while traveling. This will help to limit an intruders ability to break into your phone if you happen to misplace it.
- Consider installing a VPN to ensure more secure online activity.
- Turn off Wi-Fi and Bluetooth when traveling. Only turn these capabilities on when absolutely necessary, then turn them off when done.
- Purchase SIM Cards for international travel in the U.S. prior to departure. This will ensure not only your security but functionality with your device. If you do decide to use a SIM card make sure to turn off “Auto Sync” to conserve your battery and data plan.
- Make sure all the software is updated on your phone, this will in turn ensure the most up to date security patches are installed on your device.
- Make sure to backup all your data before traveling, so that if your phone or data is lost you can easily restore the information and won’t be without important contacts and travel information.
- When feasible, recommend purchasing a pay-as-you-go phone for travel, especially travel overseas. This is probably the single best way to prevent any of your personal information from getting into the wrong hands should you lose the phone.
- Make sure to use your own charger and cables, try not to purchase them from your destination.

IDENTITY THEFT



Practices to Avoid Identity Theft

- **Do** avoid paper billing by requesting secure electronic statements instead, or have them mailed to a Commercial Mail Receiving Agency (CMRA).
- **Do** lock your mailbox.
- **Do** keep your information safe, both online and offline, by shredding documents containing personal information and passwords and protecting sensitive computer files.
- **Do** use unique, hard-to-guess passwords that include a combination of letters, numbers, and symbols.
- **Do** install and update antivirus, anti-malware, and security programs on all computers, tablets, smartphones and operating systems.
- **Do** disable Bluetooth on devices when not in use.
- **Do** watch out for “phishing” scams.
- **Do** fight “skimmers” by touching ATMs to see if all the parts are solid and not add-ons, cover the keypad/screen with your hand while typing the password, and always look for suspicious holes or cameras.
- **Don’t** disclose your full nine-digit Social Security number.
- **Don’t** use the same password across multiple accounts.
- **Don’t** disclose information commonly used to verify your identity on social network sites such as: date of birth, city of birth, mother’s maiden name, and name of high school.
- **Don’t** make purchases, pay bills, or send sensitive information over unsecured WiFi networks.
- **Don’t** trust unsolicited offers and ads.

Suspended Social Security Number: Consumers are reporting a new “government related scam.” The consumer receives a call and is told that their SSN was used in criminal activity. The caller will claim that the SSN has been suspended and they can help the victim get the situation cleared up. The Social Security Administration does NOT suspend SSNs, ever! Do not give personal information out to callers. If you feel you’ve been scammed, report it to the FTC immediately. Also, personally look up the number of and call the agency the scammer(s) claim to represent. Make a detailed record of the interaction and be prepared to provide as much information as possible.

Mobile Phone Scams: This scam was identified when a consumer received an email from their mobile phone provider. The email stated, “Your new mobile phone is on its way” and listed a delivery address that didn’t belong to the consumer, it was actually the address of a local hotel. Further investigation revealed that someone had used a fake identity to obtain the consumers account information and ordered the additional phone on the consumer’s account.

**Report fraud & identity theft scams to the FTC at 1-877-FTC-HELP
(1-877-382-4357) or online: [ftc.gov/complaint](https://www.ftc.gov/complaint).**

IDENTITY THEFT



USSOCOM SMARTCARDS

What to Do if Your Identity is Stolen

The FTC has put together a great, step-by-step guide on what to do if you think your identity has been stolen (link below). Here's where to start: <https://www.identitytheft.gov/steps>

Take action immediately! Keep records of your conversations and all correspondence.

Flag Your Credit Reports. Contact the fraud department of the three major credit reporting agencies. Tell them you are an identity theft victim. Ask them to place a "fraud" alert in your file. An initial fraud alert is good for 90 days.

◆ Equifax 1-800-525-6285 ◆ Experian 1-888-397-3742 ◆ TransUnion 1-800-680-7289

Order Your Credit Reports. Each company's credit report about you is slightly different, so order a report from each company. They must give you a free copy of your report if it is inaccurate because of fraud. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact your creditors about any accounts that have been changed or opened fraudulently. Ask to speak with someone in the security or fraud department.

Create an Identity Theft Report and Report it to the Local Police. An Identity Theft Report can help you have fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- ◆ File a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- ◆ Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

For more information regarding identity theft, visit the following websites:

Federal Trade Commission (FTC) <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>
FTC Identity Theft Online Complaint Form <https://www.ftccomplaintassistant.gov/>
www.fraud.org (You can also call: 1-800-876-7060)

Preventing Other IRS Scams and Fraud: It is very common for criminals to file IRS Tax returns using stolen identities. The fraudsters will typically file early and claim their tax refunds before the victim is aware. It is only when the victim attempts to file their own, valid tax forms that they are informed a refund has already been issued. Victims of identity theft can request a PIN to prove their identity when they file their tax return.

Children also Victims of Tax Fraud and Identity Theft: Increasingly children are becoming victims of identity theft and tax fraud. Criminals will obtain Social Security numbers or will attempt to obtain credit cards in the names of minor children. It is only when parents attempt to obtain legitimate cards for their children that they discover their children have been targeted. To prevent this, parents may place freezes on accounts for their children to ensure no new credit is issued until they are ready.

You can get free copies of your credit report once a year from each agency, get one every four months to monitor your credit.

CHILD SAFETY ONLINE



USSOCOM SMARTCARDS

- **Do** only connect with gamers and online profiles of people you know and trust. Review connections often.
- **Do** assume ALL information and images you share are publicly viewable, regardless of your settings.
- **Do** use a picture of something other than yourself for your profile photo.
- **Do** tell kids to let parents or responsible adults know anything online makes them uncomfortable.
- **Don't** use location services.
- **Don't** add your birthdate, location, phone number, or other personal details to online profiles.
- **Don't** forget your children have online privacy rights as well. If you are unsure what those rights or laws are you can find them here:
<https://www.ftc.gov/consumerprotection/childrens-privacy>

Stats and Resources

- An April 2015 Pew Research Center study revealed that 92% of teens report going online daily – including 24% who say they go online “almost constantly.” A separate study showed that nearly 40% of 3-4 year olds and two thirds of 5-7 year olds go online.
- Cyber-bullying, malware, and predators are a few dangers that make the Internet an unsafe environment for unsuspecting children. In 2012, the FBI launched Safe Online Surfing (SOS), a challenging but fun and informative game that educates children about online safety. See more at <https://www.fbi.gov/fbi-kids>
- In half of all sex crimes against a minor involving a social networking site, the social networking site was used to initiate the relationship. 55% of teens have given out personal information to someone they don't know, including photos and physical descriptions. <https://www.guardchild.com/social-media-statistics-2/>
- 67% of teenagers say they know how to hide what they do online from their parents. 43% of teens say they would change their online behavior if they knew that their parents were watching them.

Parental Controls

One of the best ways to help protect your child online is to monitor what applications they are using.

For iOS users it is recommended that parents keep the Apple ID password and not provide it to the child using the device. Also, make sure that the iPhone requires the password before any downloads can take place.

This can be done on your Android devices, as well.

CHILD SAFETY ONLINE



Security Applications

A variety of paid software packages are available for monitoring your child's online activities. The following packages are effective tools for monitoring or preventing access to content.

Blocksi Web Filter

Blocksi Web Filter is a web filter and parental control extension for Google Chrome. It can be configured to protect your family from inappropriate content on the Internet.

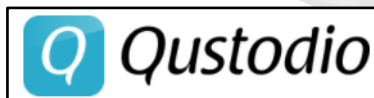


Microsoft Family Safety

Microsoft family is a free service that helps families stay connected, and keep kids safer on Windows 10 and Xbox One devices, along with Android devices running Microsoft Launcher. You'll find settings like activity reporting, screen time limits, location sharing, and content restrictions on account.microsoft.com/family.

Net Nanny

Net Nanny Social lets you keep track of all your children on social media including Facebook, Twitter, Google+, Instagram, Pinterest, and LinkedIn. Features include: detecting any new accounts created, ability to identify cyberbullying, cyber-stalking, or grooming, access to view photos and videos child has published, alert notifications, and daily/weekly reports.



Qustodio

Free and premium parental control app that offers simple tools to manage kids' screen time, filter content and monitor or block apps kids use. Premium features include: SMS Messages & Call Tracking, Location Tracking & Panic Button. ability to view social media activity including Facebook, Twitter, Instagram, and Whatsapp, block pornography, set multi-device time limits, control games and apps, and browser-independent content filter that handles HTTPS traffic.

CHILD SAFETY ONLINE



USSOCOM SMARTCARDS

My Mobile Watchdog

This must be installed on your child's phone. Features include: web filtering, time restrictions, app blocking, real time alerts when a stranger calls the child's phone, location tracking (up to 99 locations) and know exactly where your child is at any time, and Daily Watch summaries! A daily breakdown of your child's activity conveniently packaged and sent to your email.



Norton Family Premier

Includes support across Windows, Android and iOS devices (no MAC support). Includes: web supervision that allows warnings, blocking, or monitoring of sites based on your own site category choices, video tracking, control SMS contacts on Android, email alerts, online time limits, Activity Tracker to view device internet history, and location tracking.

YouTube

Let's give this app another look. YouTube Kids has just pushed their parent-approved content, a control that lets you select every video and channel available to your child. It is available today on Android and iOS.

On Android: Open "Settings" and scroll down to the bottom just past your child's (or your) profile. Select "approved content only" or "Restricted Mode On."

On iPhone: Open "Settings", then "General" and toggle "Restricted Mod" to On.

Next, you may want to also Lock "Restricted Mode" on your browser. "Restricted Mode" lock prevents others from changing the settings on that browser.



Additional Sources

Disney+ parental controls information can be found here:
https://help.disneyplus.com/csp?id=csp_article_content&sys_kb_id=36628f4bdbd66c50055cea4c13961909

Setting up router controls for your kids: <https://kb.netgear.com/25687/How-do-I-set-up-Live-ParentalControls-on-my-NETGEAR-router-using-the-genie-desktop-app>

Google has its own Safety Center to help ensure your kids remain safe here:
www.google.com/safetycenter/families/start/

PHOTO SHARING SITES



- **Do** share photos only with known and trustworthy people.
- **Do** use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- **Do** ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose personal data.
- **Do not** tag geolocations. The information in these tags can disclose location of where the photo was taken.
- **Do not** give apps permissions to access the cellphone location services.
- **Do not** post photos of others, especially children, without getting permission beforehand.

Choosing the right photo sharing service will depend on intent and audience. Key questions to ask:

- Are you sharing photos primarily for yourself, your friends and family, or for public consumption?
- Are your contacts and viewers already using a specific service?
- How much control and privacy do you want over your images? Is the retention of EXIF data problematic?

Although photo sharing services allow you to remove images, not all of them allow you to delete your account. Deleting content and/or an account does not ensure removal from the internet or the service provider's systems. Those with access to the photos on a photo sharing service can acquire and redistribute photos as they please.

What is EXIF data?

Exchangeable Image File Format (EXIF) is metadata stored in the captured image. This data can include date, time, camera settings, and possible copyright information. If the image is captured with a camera phone or digital camera with GPS capabilities, it can record EXIF geolocation metadata.

For more information refer to the EXIF Removal Smartcard.

PHOTO SHARING SITES



Six Popular Photo Sharing Services

SERVICE/ DETAILS	Instagram	snapchat	facebook	Google Photos	Flickr	photobucket
PRIMARY USE	Share photos and videos from camera enabled mobile devices	Share photos and videos that “disappear” after viewed or a period of 24 hours	Social network	Photo and video sharing and storage service	Photo and video hosting site used for sharing and embedding on blogs and social media	Photo and video hosting site used for sharing and embedding on blogs and social media
IMAGE PRIVACY OPTIONS	Public ; Private (other users must request to follow you)	Public ; Private (other users must request to follow you)	Public ; Only Me; Friends; Friends of Friends	Private ; Shared Albums allow anyone with the unique web link to view your photos	Public ; Only You, Your Friends, Your Family	Public ; Private (optional password protection)
RETAINS EXIF	No	No	No	Yes	Yes, for original uploaded file (not for resized file) ; You can also hide EXIF data	uploaded file (not for resized file)
GEO-LOCATION OPTIONS (NON-EXIF)	GPS-based device location and customizable location (both removable)	Snapchat Geofilters use location services on your mobile device (Using Geofilters is optional)	Free-form text; location suggestions; map-based (removable)	GPS-based from camera and Google’s Estimated Location (both can be disabled in the phone settings)	Editable location; map-based (both removable)	Location data is available unless you disable it
ALLOWS REPOSTING	Yes, only with third party applications	No, but note that viewers can still screenshot your Snaps	Yes	Yes, photos can be downloaded from a Shared Album.	Yes	Yes ; No
POPULATES IN GOOGLE SEARCHES (INDEXED)	Profiles are indexed, but not photos	No	Public profiles are indexed	Shared photos may possibly be open to public search in the future	Public albums are indexed; Offers opt-out for 3rd party searches	Public albums are indexed

Privacy Settings

*Default settings are in bold.

Instagram

If the account is set to private, only approved users can view images and videos. From a smartphone, tap the person icon at the bottom right corner of the screen > tap the menu icon (three bars) in the top right corner of the screen > click “Settings” > tap “Privacy.” Ensure the toggle is on for private account.

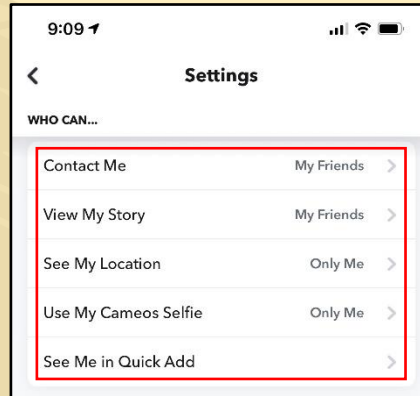
PHOTO SHARING SITES



Privacy Settings (Continued)

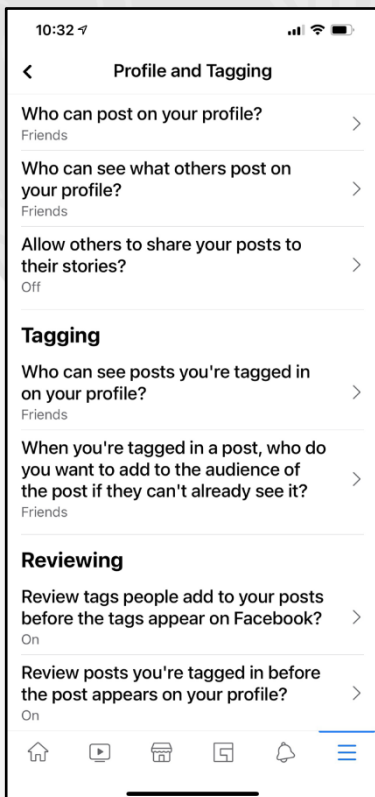


Verify who can view images or videos on Snapchat to ensure privacy. From a smartphone, tap the person icon at the top left corner of the screen > Tap the gear icon at the top right corner of the screen > scroll down to **“WHO CAN...”** Ensure that “Contact Me” and “View My Story” are set to “My Friends.” Ensure under “See My Location” the toggle is set to enable “Ghost Mode” and displays as “Only me.” When “Ghost Mode” is enabled, your location is not revealed to anyone. Ensure “Use My Cameos Selfie” is set to “Only Me.” It is not recommended to toggle on “Show me in Quick Add.”



facebook

It is recommended to review who can view or share your photos on Facebook. From a smartphone, tap the menu icon (three bars) in the bottom right corner of the screen > tap the down arrow next to **“Settings & Privacy”** > tap **“Settings”** > scroll down and tap **“Profile and Tagging”** to adjust who can view your posts and photos..



Google Photos

Review privacy settings in Google Photos. From a smartphone, tap the user icon in the top right corner of the screen > tap **“Google Photo Settings.”** Under **“Sharing,”** tap “Hide photo location data.” Tap “Group similar faces” and ensure the “Face grouping” toggle is turned off. Ensure the toggle is on and the setting displayed is “Other people won’t see where photos were taken.”

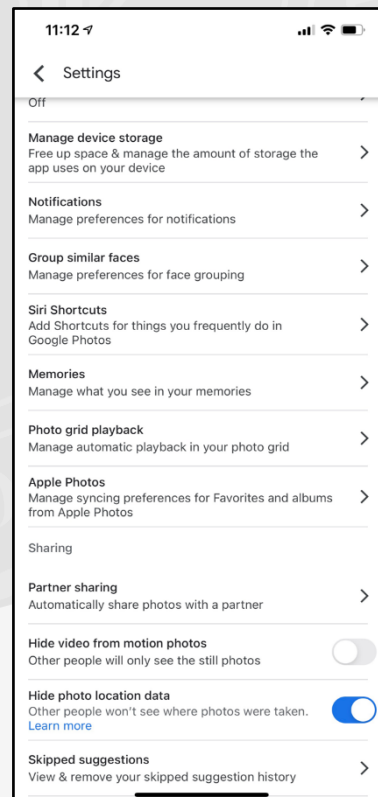
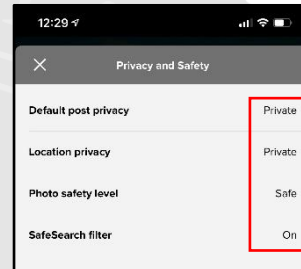


PHOTO SHARING SITES

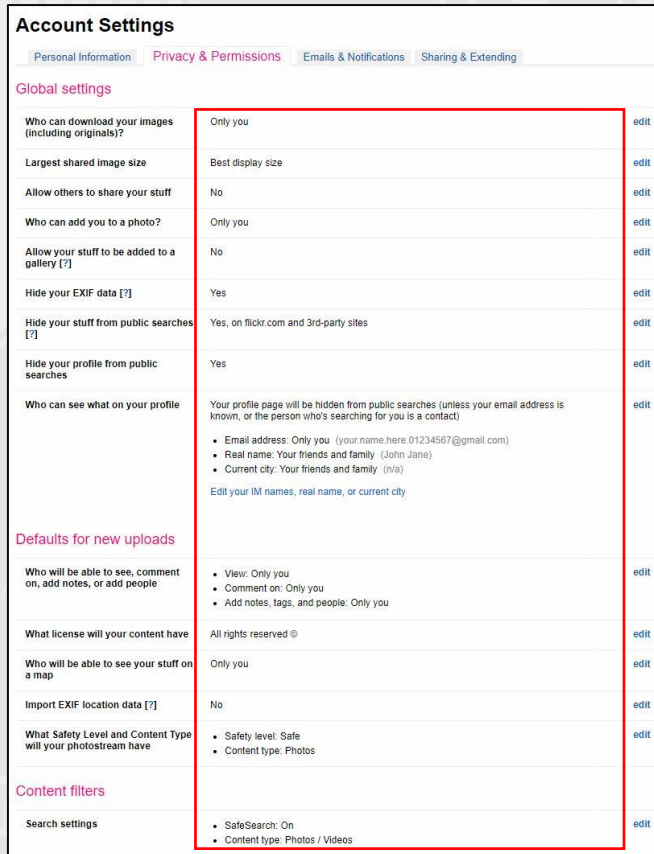


Privacy Settings (Continued)

You can adjust the default photo privacy settings to control who can see your photos and videos. Default settings will affect all your Flickr content whether you upload it from a computer or your mobile device. From a smartphone, tap the person icon in the bottom right corner of the screen > tap the gear icon in the top right corner of the screen > tap **“Privacy and safety.”** Ensure “Default post privacy” and “Location privacy” are both set to “Private.” Set “Photo safety level” to “Safe” and “Safe search filter” to “On.” You can also change the privacy level of a specific photo or video: Click the info icon on the specific photo or video. Choose an option in the drop-down: “Public,” “Private,” “Friends,” “Family,” or “Friends & Family.” It is recommended to only permit family or close friends to view photos.



Comprehensive Flickr account settings can be modified via computer. Click the camera icon. Select **“Settings”** > **“Privacy & Permissions.”** The recommended settings are presented in the screen capture to the right. Click **“Sharing & Extending.”** Ensure third party applications are not linked as demonstrated in the image below.



Account links

You have no third-party applications linked to your account, but [here are some you might like to try](#)

For a comprehensive Flickr security walkthrough, visit the following URL:
<https://safety.yahoo.com/SafetyGuides/Flickr/index.htm>

PHOTO SHARING SITES



Privacy Settings (Continued)



Click the person icon in the top right corner of the screen > select **"Settings"** > Select **"Privacy"** tab. Use the image to the right as an example for security settings. Select the **"Apps"** tab. Use the image at the bottom of the page as an example for security settings. Ensure third-party applications, such as Twitter and Facebook, are not linked to the Photobucket account.

Privacy

Personal Albums **Privacy** Apps Notifications Mobile Account

Followers

Allow others to follow me. You currently have no followers.

Content Privacy

Allow others to copy, download and/or print my photos & videos

Allow comments in my albums

Show where my photos were taken

When I upload, permanently remove information about where my photos were taken

File Name Scrambling

To protect your privacy, we recommend that you select the options to scramble both future and past upload file names. However, if you intend for your photos to be public or used for business purposes, we recognize that you may not want to scramble.

For Future Uploads **For All Previous Uploads**

(Recommended) During upload, scramble file names to make links hard to guess

Scrambling file names changes links.
You will need to re-establish published links once the scramble is complete.

Album Privacy

Applications

Personal Albums Privacy **Apps** Notifications Mobile Account

Connected Services

Connect your social profiles to Photobucket for quick sharing and for finding friends.

Facebook

Twitter

Although it is possible to set Photobucket albums to "private," this does not prevent the photos within being accessed by someone who knows or can guess the URL.

EXIF REMOVAL



- **Do** prevent your device(s) from capturing geo-location data when taking pictures. Remove EXIF metadata from images taken by smartphones or digital cameras.
- **Do** use privacy settings from the app to limit the audience to only yourself or close friends and family, before uploading pictures.
- **Do** assume that anyone can see, copy, or forward photos that are posted online. Even with no EXIF data, the content of images may contain identifying information, including people and locations.
- **Don't** allow apps to automatically upload and share captured images (e.g. Instagram, Flickr).
- **Don't** assume that device settings remain the same after updates or over time. Verify the settings frequently.
- **Don't** upload pictures with landmarks, easily identifiable structures, or signs indicating location.
- **Don't** give apps used for sharing photos permission to access your device's location or other information.

EXIF

Exchangeable Image File Format (EXIF) is a standard format for capturing, storing and exchanging image metadata. Metadata is the description and context of files that allows computers to organize, find, and display information about a file. For example, when a music app displays the artist, year, album, and song name of an mp3 being played, it uses the mp3s metadata to display that information. Images and videos also contain metadata that can show time, date, camera settings, copyright information, and location. Some social networks and photo-sharing sites, such as Flickr, Google+, and Dropbox, have features that display EXIF data alongside images. Facebook, Instagram, Twitter and Reddit, do not share EXIF data publicly. EXIF metadata are listed as tags that store information that can be used to identify an individual. The chart below shows the tag categories, the metadata included in each category, and the potential security risks associated to each piece of metadata.

Tag Category	Important Tags	Security Implications
Geo-location	GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSTimeStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	Ability to reveal the exact location of private places, such as homes or offices. Some photo sharing sites, including Google+ and Flickr, publicly display image GPS coordinates on a map.
Timestamps	ModifyDate, DateTimeOriginal, CreateDate	Creates a log of behavioral patterns and personal timelines.
Camera	Make, Model, Serial Number	A unique serial number identifies the particular device for an image or set of images.
Authorship	Artist, Owner Name, Copyright	Links images with a name or organization.
Image Summary	ImageDescription, UniqueImageID, UserComment	Potentially reveals identifying information about the content of the images, such as captured persons or locations.

Prevent the Capture of Geolocation Data

iOS

If iOS location services are turned off, images captured with the native iPhone camera app will not contain geo-location EXIF data.

1. Select the "Settings" app. Click "Privacy" > "Location Services".
2. Turn off location services altogether or for the iPhone's camera applications.
3. Return to the "Settings" app. Click "Privacy" > "Photos".
4. Disable permissions for other apps to have access to the photos stored in the device's camera roll.

Android

Turning off location storage in the Android camera application prevents captured images from containing EXIF data.

1. Open the camera app and go to "Settings" by tapping the gear icon. This varies from phone to phone since there is no standard camera app on Android devices.
2. After that, scroll down until you see 'location tags' and touch the toggle switch to disable geotagging of photos. The wording may vary slightly between devices.

EXIF REMOVAL



Prevent the Capture of Geolocation Data Continued

- Taking a screenshot of a photo on a device running iOS or Android will create a new image containing no EXIF data. To take a screenshot on an iOS device, simultaneously press the lock and home buttons or google how to take a screenshot on your specific android.
- Even photos taken in airplane mode contain geo-location data. It is recommended to turn off location services/storage on your smartphone camera application, as shown on the previous page.
- Remember that uploading or sharing a lower quality image will contain EXIF data. EXIF data and image quality have no correlation.
- It is important to not only lock down Apps such as Snapchat, Instagram and Twitter (see corresponding Smartcard), but to also remove the meta data from them as best as possible.

EXIF Removal Apps and Programs

Reviewing & Removing EXIF Data for iOS

1. Download the free US-based Photo Investigator app from the App Store.
2. Open the app and tap the gallery icon on the bottom left.
3. To view EXIF data, you can tap on the various icons below the image.
4. To remove exif data tap "Metadata" and then select "Remove".
5. An easy way to identify photos that have EXIF data with geolocations is to view your "Places" folder. Any images that appear in this folder have geolocation data, once you disable the geotagging feature and remove your EXIF data, this folder should be empty.

Metadata Remover for Android

Metadata Remover is a free US-based app that deletes all EXIF data from image files stored on your Android device.

1. Download a Photo Exif Editor app from the Play Store.
2. Open the app and select an image.
3. The EXIF data will be removed.
4. Processed images will be saved separately from the original file.

Reviewing & Removing EXIF Data in macOS

Use the Image Optim (UK based) application (available at <http://imageoptim.com/>) to remove EXIF data on your OS X device.

1. Drag the photos for EXIF removal into the app window and wait for a green check mark to appear next to the file name.
2. Check that the EXIF data has been removed by right clicking the image and selecting "Get Info". EXIF data is listed under "More Info".

Reviewing & Removing EXIF Data in Windows

Use the Windows OS to verify EXIF data has been removed.

1. Navigate to an image in File Explorer. Right click the image and select "Properties".
2. Select the "Details" tab. You can examine EXIF metadata that is available.
3. Click "Remove Properties and Personal Information".
4. You can click "Create a copy with all possible properties removed" to remove all potential properties or select individual properties such as GPS information. Click "OK".

Geo-localization

Even with EXIF metadata removed, images containing vegetation, addresses, business names, road markings, and landmarks allow someone to identify the location a photograph was taken. Geo-localization, the determination of a location of an image through visual information, is currently being developed. This will allow computers to compare a picture without EXIF metadata to millions of other pictures found on the internet that do have location metadata. Once the computer discovers a close match between two pictures, it can apply the location metadata of one structure to its match that does not have location metadata.

LOCKDOWN YOUR LAPTOP

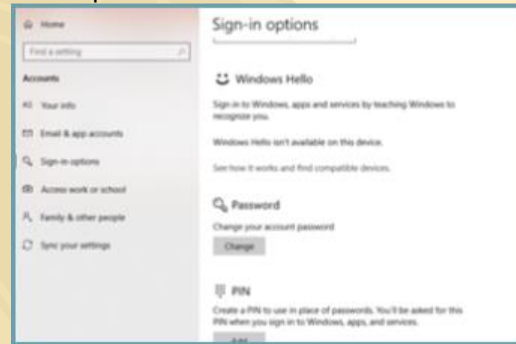


Creating a Windows Log-in Password

Although a log-in password won't protect against a competent hacker, it can be enough to dissuade unsophisticated criminals from snooping through your personal files and accessing your online accounts. Protecting each account (Guest, Admin, and User) with different passwords helps prevent a hacker from getting access to everything on your computer should they gain access to any one account. It is recommended you create and use a "User" account, not the "Admin" account for all daily activity. This way hackers would be limited in the damage they can do to your computer.

Windows 10 offers a number of enhanced log-in and security features.

Navigate to Start Button > Settings > Accounts > Sign-in Options to setup your 'Sign-in Options'.



Practical Password Tips

If you have files on your computer that you don't want anyone else to access, you can use password-protected file or folder encryption to keep them safe. However, encrypted files are only as secure as the strength of the password protecting them.

For this and the rest of your security measures to be maximally effective, make sure you follow these simple password rules:

- Use a password that's at least 12 characters long and includes a mix of lower and upper case letters, symbols, and numbers. Try not to use complete words, but if necessary avoid common words that can be found in a dictionary. Not all devices, systems, or accounts allow these combinations, but do what you can within the available options.
- Avoid sharing passwords across multiple platforms, especially for sensitive accounts like a Windows logon, bank account, and email account.
- Change your passwords frequently - every 6 months for important passwords, at a minimum.

Additional Security

Windows 10 also has a number of additional log-in security features. At the "Settings," "Accounts" and "Sign-in Options" menu you can select "Picture Password" to enable secure log-in based on your unique mouse movement responses.

Note: You can use a PIN to sign into Windows, apps, and services. However, this option is not as secure as the "Picture Password."

Windows 10 also has a feature which allows you to pair your laptop with a Bluetooth-enabled device and automatically lock your computer once the device is out of range. You can enable this feature from the "Settings," "Accounts" and "Sign-in Options" menu by pairing your laptop to a Bluetooth device with the "Dynamic Lock" slider.

For personal accounts you can also enable two-factor authentication (2FA). 2FA requires users to authenticate access through a supported device, i.e. a text to a phone number or an email to a backup address, before accessing an account.

LOCKDOWN YOUR LAPTOP



Virtual Private Network (VPN)

A Virtual Private Network (VPN) connection is the safest way to connect to the Internet and also safeguard your information.

Unsecured networks present a major threat to your personal information, especially when using your device on a public WIFI network. When connecting to public WIFI, we don't know who else is on the local network, which leaves our personal data vulnerable to snooping. Even when connecting to the wider web, our data is increasingly collected, inspected and exploited.

One sensible solution is to use a VPN. We recommend using a VPN whether you are connecting to the internet from home (even with a secure WIFI connection) or in public. This is simply the most secure way to access the Internet.

VPN For Beginners

When you connect to a VPN, you access a site or service directly from your laptop, which acts as a secure launchpad into the World Wide Web. Once connected to the service, your data is encrypted and sent to a third-party server. There it is combined with other traffic before being integrated into the "normal" traffic flow on the World Wide Web. Since your information is jumbled up with other information, it becomes difficult to identify as *your* specific information, it is like a needle in a haystack.

A Few VPN Perks

- VPN services are cheap, with some starting around \$5 per month.
- A VPN can help protect your data from identity theft and fraud.
- VPN providers often allow users significantly increased privacy protections from advertisers and hackers alike.
- VPN providers allow you to enjoy services that require connections from certain countries, regions or time zones.
- If your Internet Service Provider blocks some applications, such as Skype or other VoIP (Voice over Internet Protocol) applications, use of a VPN may help.

Where To Find VPN Services

Not all VPN services are created equal. Depending on your typical Web usage, you will want to shop around for a service that fits your profile. If you need a fast connection for rapid-fire browsing or streaming services and your VPN provider doesn't have enough servers, you may experience poor Internet speeds or be unable to make a connection at all. Others might offer some privacy protections but require you to give up some control of your anonymity.

Before subscribing to a VPN service, be sure to look at reviews. The VPN market is competitive and expanding which means VPN providers often offer free trial periods to new users.

For additional information on current VPN providers see:
www.pcmag.com/article2/0,2817,2403388,00.asp

WIFI SECURITY



Best Practices

- Create passwords that are sufficiently long and complex to include; upper and lowercase letters, numbers, and symbols. Consider a multi-password phrase that does not consist of dictionary-based words. An example would be lLuvF00tb@77 from the phrase “I love football.”
- Turn off your wireless network when you will not be using it for an extended period of time.
- If you have guest-access set up for your network, ensure that it is also password protected.
- If possible, turn on automatic updates for your network device’s firmware. If they are not offered, periodically check for firmware updates on the network devices’ website(s) and manually download and install them.
- If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button usually located on the back of the router.
- Position the router away from windows and as far into the interior of your house as possible to limit the range of the WiFi signal outside your home.

Wireless Router	Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identification (SSID)	Public name of a wireless network.
Pre-Shared Key (PSK)	Authentication mechanism that mandates a password. Adds additional security to wireless networks.
Hypertext Transfer Protocol Secure (HTTPS)	Uses various encryption protocols to add additional security to HTTP
Media Access Control (MAC) Address	Unique, individual identifier assigned to computers and devices.

WiFi Security Level	Level of Security	Explanation
WEP	Low	Old encryption protocol. No longer considered a standard. Highest risk next to an “open” network
WPA	Low-Moderate	Old encryption protocol. Better than WEP but should not be used when more modern encryption is available.
WPA2	Moderate-High	WPA2-PSK (AES) is the most secure option which uses the latest WiFi encryption.
WPA3	High	Approved and replacing WPA2 as the new and more secure option for WiFi security.

WIFI SECURITY



Accessing Your Router

To change your WPA2 password log on to the router online. To do so enter the appropriate IP address, username, and password. If you do not have this information, contact your Internet Provider.

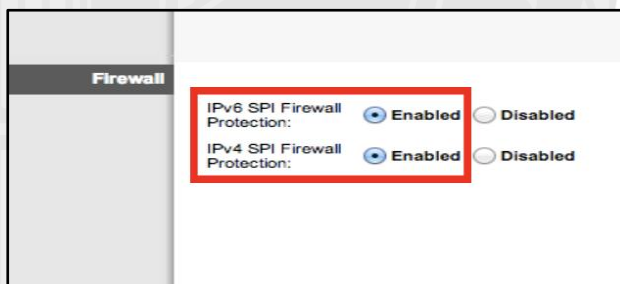
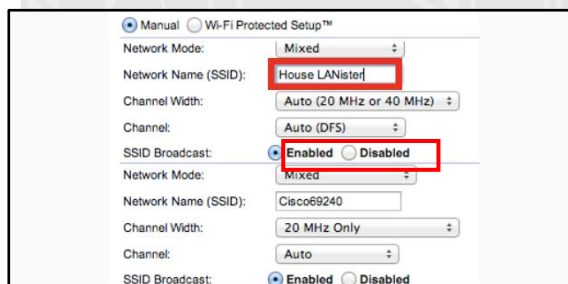
It is **important** to understand that when your internet is set up by the Internet Provider, they are not required to set it up using WPA2. It is recommended that you ask it to be set up with WPA2 and acquire the username and password at the time of service.

When changing your username and password for the WiFi, it is important to use a strong password unrelated to any family attributes.

Lastly, it is important to create a "Guest Account" password separate from the "Admin/Family Account" password.

Creating a Unique SSID

When creating a name for your Wi-Fi (SSID), it is important to consider who will be seeing it. For instance, if you decide on the family last name and number of family members, then anyone within range will be able to see your last name and likely piece together what the numbers represent. Alternately, if you name your SSID "FBI Van," that may call attention to your network and entice nefarious activities. It is recommended that you choose a name for your SSID that is generic in nature. If you would like to hide your SSID so that it does not broadcast to the public, simply select "Disabled" from the "SSID Broadcast" section. Note that, while it is nice to be able to disable the broadcasting of your SSID, it can be "unhidden" by any individual requesting "hidden Wi-Fi's".



Firewall/ Internet Protocol

Internet Protocol (IP) is the infrastructure protocol that provides an identification and location system for computers on networks and routes traffic on the Internet. IPv4 is slowly being replaced with IPv6. It is important to understand that if you are running a VPN on your system, IPv6 may not be covered. Check the VPN company website to see if both versions are supported. You can also visit a "What is my IP address" site that pulls both IPv4 and IPv6 to check if you are properly covered. If IPv6 is not covered, you can choose to disable it from your system.

Children's Learning Devices: If you have children who play with devices like the Leapfrog or Vtech games, and you disable your SSID broadcasting, these devices will not be able to locate your WiFi network.

WIFI SECURITY



Enabling HTTPS

HTTPS is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit. HTTPS enables encrypted communication and secure connection while on the internet. It is used by websites to provide enhanced security for customers OR financial transactions OR where personally identifiable information (PII) is shared. Enabling HTTPS on your servers is a critical step in providing security for your web pages. It is recommended that you enable HTTPS in order to further protect you and your family while navigating the internet.

A screenshot of a router's web interface. The "Access via:" section is highlighted with a red box, showing the "HTTPS" option selected with a checkmark, while "HTTP" is unselected. Below it, "Access via Wireless:" is set to "Enabled".

Encryption

In between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select WPA2-PSK and also AES (a cryptographic cipher that is responsible for a large amount of the information security that you enjoy on a daily basis) for encryption. The PSK password should be long and complex, but different from the administrative router-access password.

A screenshot of a router's web interface showing encryption settings. The "WPA-PSK/WPA2-PSK" option is selected. The "Version:" dropdown is set to "WPA2-PSK" (highlighted with a red box), "Encryption:" is set to "AES", and the "PSK Password:" field contains "RRatJlsSJaKH%1798".

MAC address filtering allows you to define a list of devices' MAC addresses so that only those devices can access your Wi-Fi. In order to do so, follow the steps below: Add the MAC address of each device you want to authorize access to your network. Next, enter the MAC address and a brief description of the connected device for filtering. Finally, enable MAC address filtering to ensure that only approved computers and devices can connect to your router. Click the 'Add' button when done entering authorized devices.

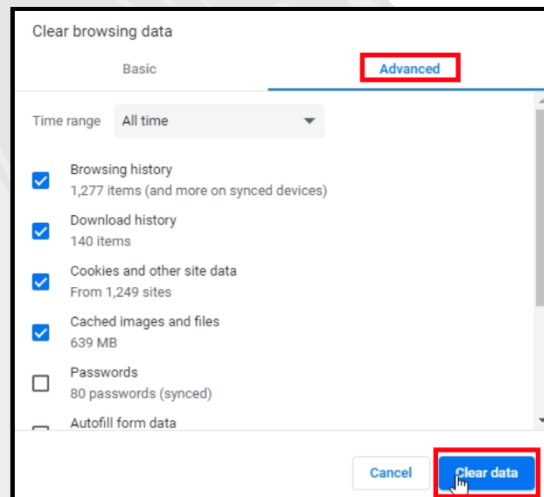
DELETE BROWSER ARTIFACTS



Information such as browsing history, cache, and cookies are saved on your computer while you surf the Web. They are used in various ways to improve your browsing experience. These private data components, while resulting in conveniences such as faster load times and auto-populated fields, can be used by nefarious actors. Whether it be the password for your email account or your credit card number and address, much of the data left behind at the end of your browsing session could be dangerous in the wrong hands. In order to protect yourself, we recommend you delete these artifacts on a regular basis.

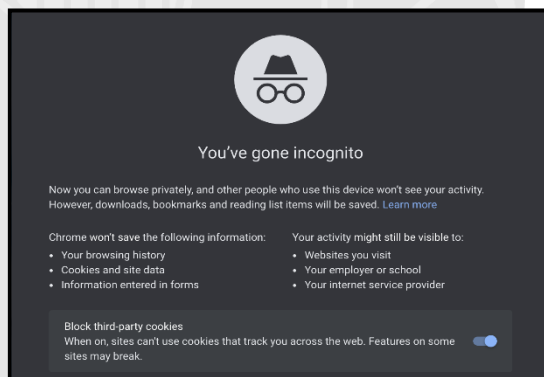
Delete Google Chrome Browser Artifacts

Click the menu icon in the upper right corner.
Click "History" or hold Ctrl-H.
Click "History" again on the menu on the upper left-hand side.
Click "Clear Browsing Data" or hold Ctrl-Shift-Delete.
Click the "Advanced" tab from the pop-up window.
Select the time range you desire.
Select the boxes next to the history you wish to remove and then select "Clear Browsing Data".
Exit all browser windows and restart browser.



Delete Google Chrome Browser Artifacts from Mobile Device

Click the menu icon.
Click "Settings".
Select "Privacy and Security".
Select "Clear Browsing Data".
Select the boxes you wish to remove and then select "Clear Data".



Google Chrome Incognito Mode

Chrome's Incognito mode will **not** save a record of sites visited or downloaded. Incognito is not available if you are using Windows 10's "Family Mode."
Click the menu icon at the upper right of the screen.
Select "New Incognito Window".
To use Incognito via the Chrome app on your iOS or Android device, follow the same steps as above.

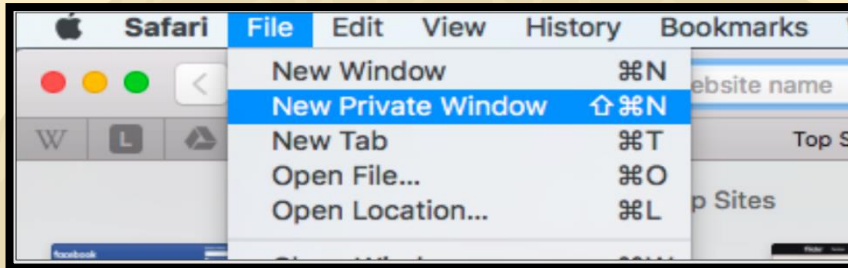
Like Microsoft Edge's InPrivate Browser, Chrome's Incognito mode will require you to constantly type in your password for logins.

DELETE BROWSER ARTIFACTS



Safari Private Mode

Select "File" from the menu at the top of the screen.
Select "New Private Window" from the drop-down menu

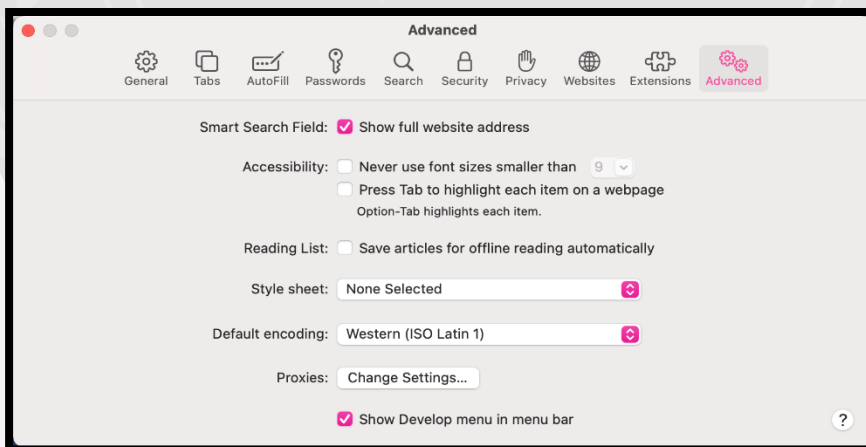


Delete Safari Browser Artifacts

Click the "Safari" menu icon in the upper left.
Click "Preferences".
Click the "Advanced" tab.
Select the box at the bottom titled "Show Develop menu in menu bar".
Click the "Develop" menu at the top of the screen, then click "Empty Caches".
Now click on the "History" menu at the top and select "Clear History". **This can also be done from the "Safari" menu.**
Right click on the "Safari" icon in the App Tray and select "quit" to restart the browser.

Delete Safari Browser Artifacts from Mobile Device

Open your iOS "Settings" application.
Scroll down and tap "Safari".
Tap "Clear History and Website Data" in blue.
Exit all browser windows to restart the browser.



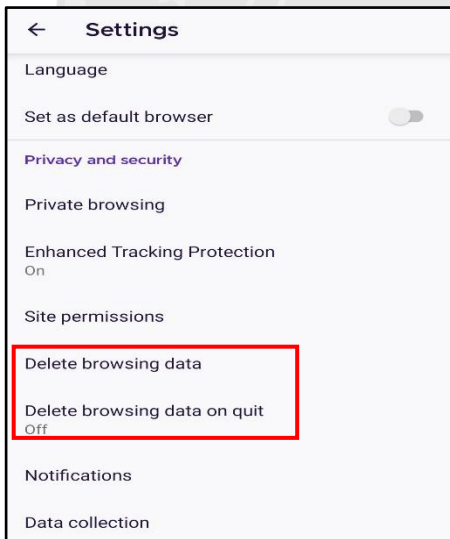
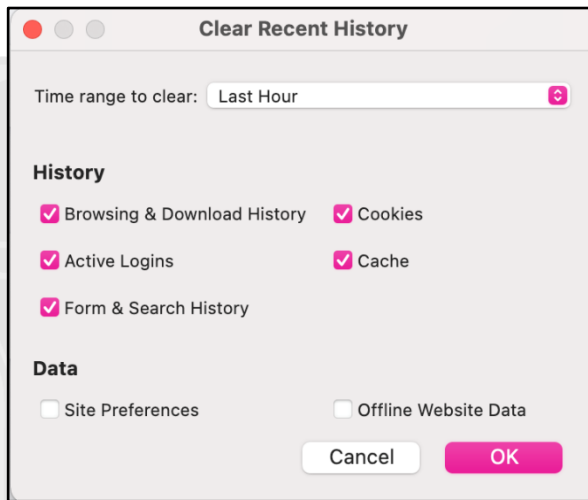
Safari automatically prevents cross-site tracking, and requests that sites and third-party content providers don't track you as a rule. Additionally, the privacy mode stops sites from modifying any information stored on your iOS device, and deletes cookies when you close the associated tab.

DELETE BROWSER ARTIFACTS



Delete Firefox Browser Artifacts

Click on the menu at the upper right corner of the browser.
Select "History" from the drop-down menu.
Select "Clear Recent History" then select all boxes needing to be deleted.
Select "OK" then close all open pages and restart browser.
**This function can also be preformed by click on the menu icon on the top right. Selecting "Settings" then "Privacy & Security" and scrolling to "Cookies and Site Data". **

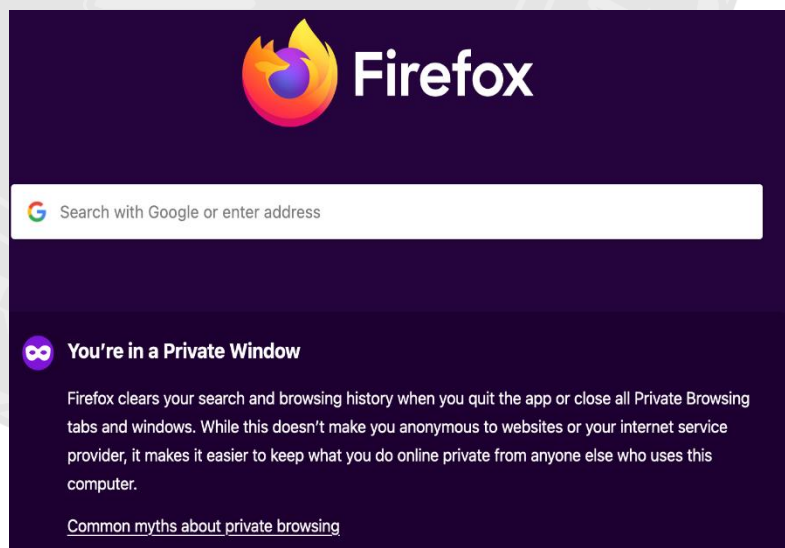


Delete Firefox Browser Artifacts from Mobile Device

Select the menu icon on the lower right of the screen.
Scroll to find "Settings" and select it.
Scroll to "Privacy and security" and select "delete browsing data".
Select each box needing to be cleaned then select "Delete browsing data".
It is recommended that you select "Delete browsing data on quit". To limit caches and collected cookies.

Firefox Private Mode

Select the menu button on the top right.
Click "New Private Window".
Alternatively, after opening Firefox you can use the shortcut "Ctrl-Shift-P".
In the mobile version select the "Mask" Icon in the upper right.



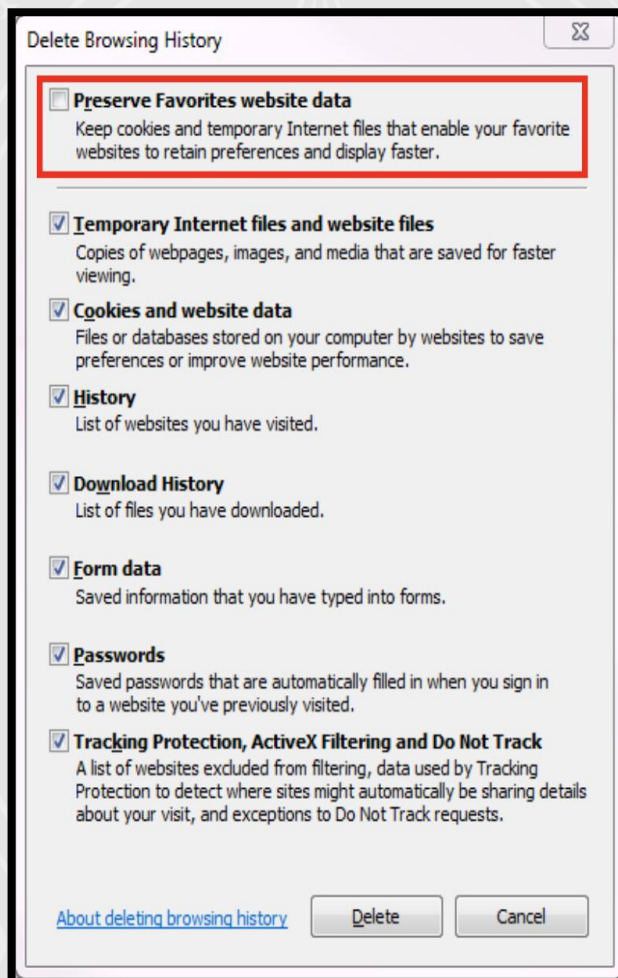
DELETE BROWSER ARTIFACTS



USSOCOM SMARTCARDS

Delete Internet Explorer Browser Artifacts

Click the menu drop down from the upper right corner.
Click "Internet Options".
Click on the "General" tab, locate "Browsing History".
Click "Delete".
Deselect "Preserve Favorites website data".
Select the boxes next to the history needing to be cleaned and select "Delete".
Exit/quit all browser windows and re-open the browser.



Internet Explorer InPrivate Mode

Click the menu drop down from the upper right corner. Select "Safety" then select "InPrivate Browsing".

As of March 2017, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on its Windows 10 devices. As of February 2020, IE version 10 is no longer in support. If you are still using IE, be sure to upgrade to IE 11.

DELETE BROWSER ARTIFACTS

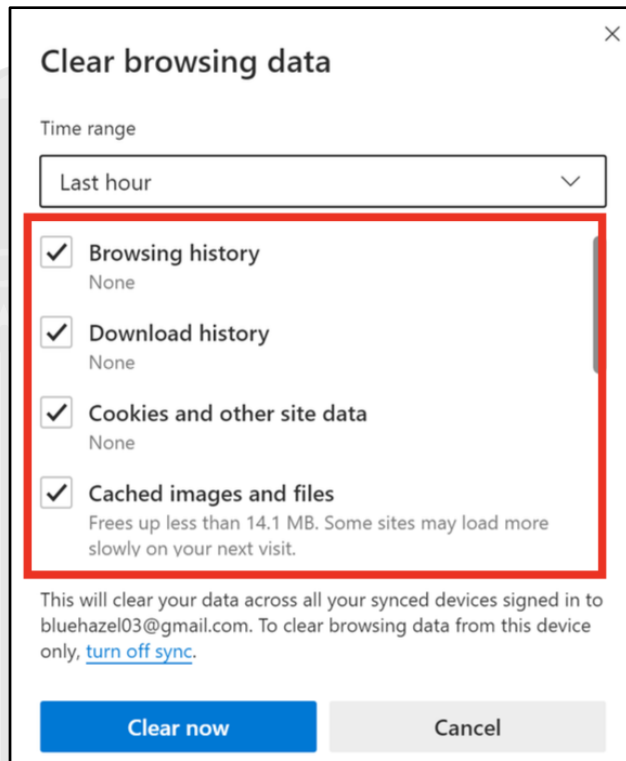


Delete Microsoft Edge Browser Artifacts

Click on the menu icon at the top right of the screen.
Select "History" then select the "History" menu at the top.
Click on "Clear Browsing Data" and select the boxes needing to be cleaned.
It is recommended that the "Tracking Prevention" be set to "Balanced".

Delete Microsoft Edge Browser Artifacts in Mobile

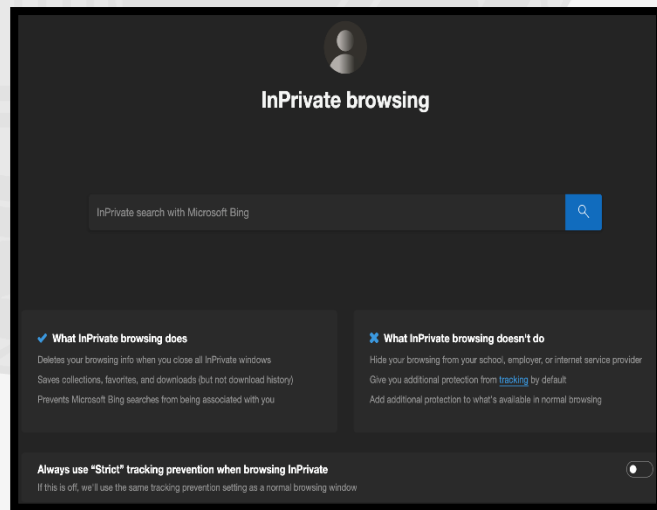
Select the menu from the middle of the lower screen.
Click on "History" then select the trash icon located on the upper right of the screen.
Select "Clear" then click "Advanced," and select all boxes needing to be cleaned.
Select "Clear".



Microsoft Edge InPrivate Mode

Click the menu drop down from the upper right corner.
Select "New In Private Window".

On the mobile application select the menu from the lower middle of the screen and scroll down to find "New InPrivate Tab"



ADDITIONAL RESOURCES



USSOCOM SMARTCARDS

Free Annual Credit Report

www.annualcreditreport.com

USA.Gov

<https://www.usa.gov/identity-theft>

Stay Safe Online

www.staysafeonline.org

On Guard Online

www.onguardonline.gov

Equifax—ID Protection Kit

<https://www.equifax.com/personal/identity-theft-protection/>

Child Identity Theft- Transunion

<https://www.transunion.com/fraud-victim-resource/child-identity-theft>

Opt Out Prescreen -

<https://www.optoutprescreen.com/>

Federal Trade Commission—ID Protection Tips

www.consumer.ftc.gov/topics/protecting-your-identity

IRS—ID Protection, Prevention, Detection and Victim Assistance

www.irs.gov/Individuals/Identity-Protection

Netsmartz Workshop for Parent & Guardians

<https://www.missingkids.org/NetSmartz>

Organization for Social Media Safety

<https://www.ofsms.org/>

FBI Parents Guide to Internet Safety

www.fbi.gov/stats-services/publications/parent-guide

Kids Games

<https://sos.fbi.gov/>

Safety Reviews for Games, Websites, & Apps

www.common sense media.org

Opt Out of Interest-Based Advertising

www.networkadvertising.org/choices

Google Privacy

<https://policies.google.com/privacy>

DMA Choice

<https://dmachoice.thedma.org>

Social Media Help (for updated Privacy information)

<https://www.facebook.com/help>

<http://search.twitter.com>

USSOCOM
SOCIAL MEDIA SMARTCARDS
AS OF JULY 2021

