Identity and Privacy: An Owner's Guide

UPDATED DEC 2019

TABLE OF CONTENTS

Err on the side of caution: Assume that the information you post and share is viewable to anyone and everyone.

UPDATED DEC 2019

IDENTITY THREATS SMART CARD

Top Data Breaches of FY 19 That You Should Be Aware Of

- Microsoft Email Services - March 2019
- MoviePass - Aug 2019
- Choice Hotels - Aug 2019
- State Farm - Aug 2019
- Asurion - Aug 2019
- Facebook - Dec 2018, April 2019 & Sept 2019
- DoorDash - Sept 2019
- Disney Plus - Nov 2019
- T-Mobile - Nov 2019
- Zynga - Dec 2019
- Wyze – Dec 2019
- Wawa – Dec 2019

**Two researchers have discovered four billion records on at least 1.2 billion people left open on an unsecured server impacting an estimated hundreds of millions of people. The data however, doesn't include sensitive information such as passwords, Social Security numbers, or credit card numbers. It does, nevertheless, contain profiles of hundreds of millions of people that do include home and cell phone numbers, associated social media profiles like Twitter, Facebook, and LinkedIn, work histories which appear to have been scraped from LinkedIn, almost 50 million unique phone numbers, and 622 million unique email addresses.

Things to Consider

- When buying a new car don't leave all 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 anytime 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 them, especially on your computer. Doing so will limit the access and abilities of an intruder if they are able to hack in. #protectyourdata

What to Lock Down

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

In Cases of Identity 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

Actions to Take in 2019

- Recommend turning on Two Factor Authentication for all devices and accounts that allow such an option
- Update your devices' virus protection
- 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
- Watch what you post online, to include your product and service reviews
- 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

Assume that the information you post and share is viewable to anyone and everyone.

UPDATED DEC 2019

IDENTITY THREATS SMART CARD

Actions for the Physical World

- Be aware of your surroundings
- Use checks sparingly
- 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

Useful Resources and Links

https://www.identityforce.com/blog

https://www.commonsensemedia.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-resource/child-identity-theft

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 breaches are included on this website but it's a great start to owning your Identity.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Checking data breaches monthly or quarterly will help to ensure you do not fall victim to Identity Theft.

UPDATED DEC 2019

HOW TO CONDUCT A SELF-ASSESSMENT

Assume that the information you post and share is viewable to anyone and everyone.

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. There, they can learn about you with just a few clicks of the mouse and a quick Internet search. It is therefore important for you to know just what is out there 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.

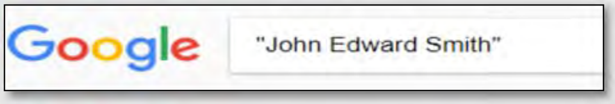
Search Engines

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

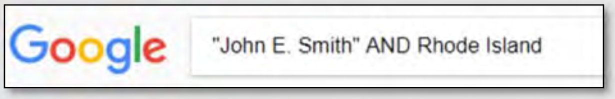
Prior to researching, ensure you are not logged into any of the search engine sites such as Google or Yahoo. Be sure to delete your browser history and clear cookies before you begin and when you have completed all your research.

These next instructions are related to the Google search engine, but can be applied to most other search engines.

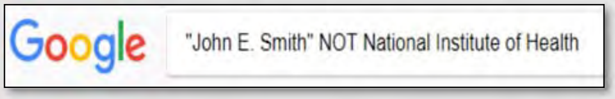
Start with basic personal information such as First and Last Name. If you have a common name, you may want to search First, Middle, and Last Name, or your name associated with a City and State, Home Address, or an associated organization. Please see the examples below:



"John Edward Smith"



"John E. Smith" AND Rhode Island



"John E. Smith" NOT National Institute of Health

Search Engines Continued...

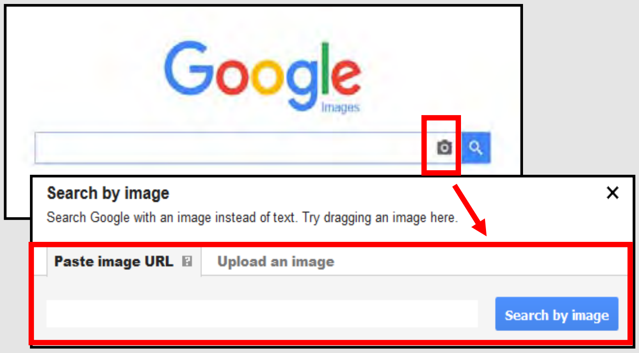
Please note that search terms **within quotations marks** " " will yield results that have the same terms in the **same order** as the ones inside the quotes. So "John Edward Smith" will not necessarily return the same results as "Edward, John Smith."

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**

You will also want to search your email addresses, usernames, and phone numbers within quotation marks.

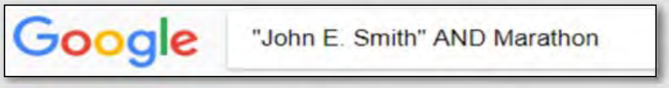
If your search results continue to include items that are not relevant, use the **dash sign** to **exclude** certain search terms like this: "John Smith" -Pocahontas

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.

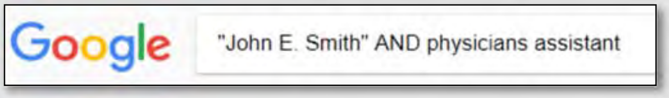


Search Google with an image instead of text. Try dragging an image here.

Collectively the 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. races, sporting events), or schools (e.g. graduation announcement). Use that information to conduct further searches such as:



"John E. Smith" AND Marathon



"John E. Smith" AND physicians assistant

HOW TO CONDUCT A SELF-ASSESSMENT

Search Engine's are the best place to start a Self Assessment. They can help to provide you a quick idea as to how much information there is about you online.

Boolean Match Logic

Boolean Search is a way to organize your search using a combination of keywords and the three main Boolean operators (AND, OR and NOT), to produce more accurate and more relevant results.(1)

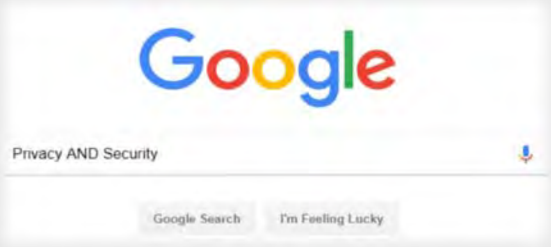
a) AND

b) OR

c) NOT

d) " "

e) ( )

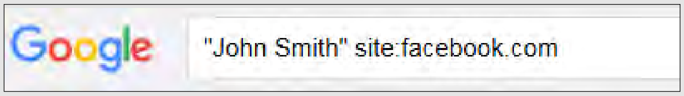


Privacy AND Security

Social Media Search

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.



"John Smith" site:facebook.com

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 Smart Cards to learn how to properly set privacy settings.

People Finder Open Source/Fee Required Sites

Conduct searches on various data aggregator sites.

Examples include:

- www.BeenVerified.com
- www.Intelius.com
- www.Radaris.com

You can conduct an initial search 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.

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 Smart Cards to help them with locking down their accounts and devices.

HOW TO CONDUCT A SELF-ASSESSMENT

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

Examples of 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 (meaning it will not learn from your searches in the same way that Google will). 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.[2]

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.

References:

1. https://www.socialtalent.com/blog/recruitment/the-beginners-guide-to-boolean-search-operators
2. https://searx.me/about

Examples of Common 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

Additional Examples of People Finder Open Source/Fee Required Sites

- ♦ www.privateeye.com
- ♦ www.peoplefinders.com
- ♦ www.usa-people-search.com
- ♦ www.spokeo.com
- ♦ www.lookupanyone.com
- ♦ www.locateplus.com
- ♦ www.peekyou.com
- ♦ www.thatsthem.com
- ♦ www.familytree.com
- ♦ www.instantcheckmate.com
- ♦ www.zabasearch.com
- ♦ www.peoplelookup.com
- ♦ www.publicrecords.com
- ♦ www.phonesbook.com
- ♦ www.whitepages.com
- ♦ www.reversegenie.com
- ♦ www.yasni.com
- ♦ www.social-searcher.com
- ♦ www.infospace.com
- ♦ www.lullar.com
- ♦ www.publicrecordsnow.com
- ♦ www.findoutthetruth.com
- ♦ www.truepeoplesearch.com
- ♦ www.checkpeople.com
- ♦ www.peoplelooker.com
- ♦ www.persopo.com
- ♦ www.peoplefinder.com

UPDATED DEC 2019

OPTING OUT OF SEARCH ENGINES & OTHER DATABASES

Google

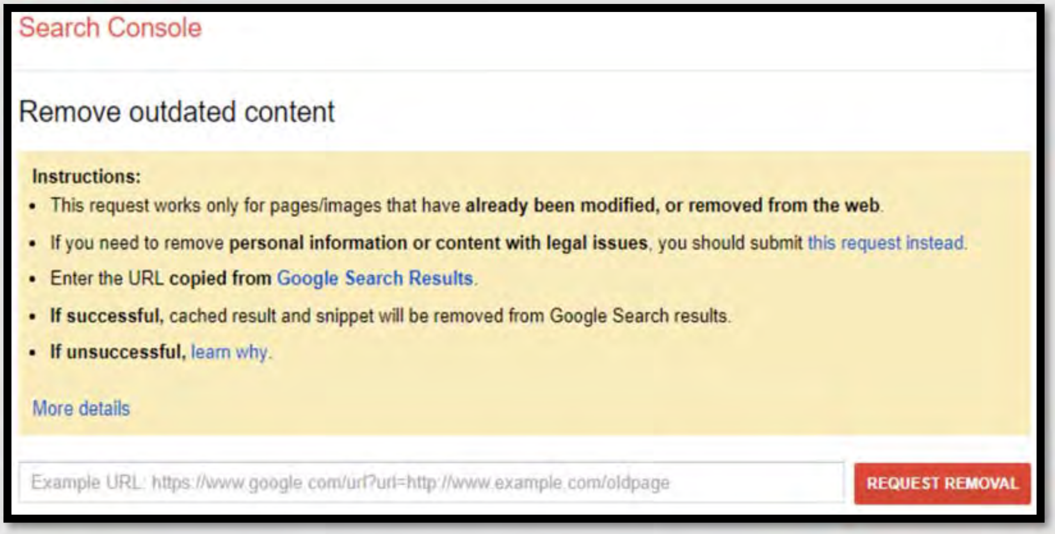
https://www.google.com/webmasters/tools/removals

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.



Search Console

Remove outdated content

Instructions:

- This request works only for pages/images that have **already been modified, or removed from the web**.
- If you need to remove **personal information or content with legal issues**, you should submit this request instead.
- Enter the URL **copied from** Google Search Results.
- **If successful,** cached result and snippet will be removed from Google Search results.
- **If unsuccessful,** learn why.

More details

Example URL: https://www.google.com/url?url=http://www.example.com/oldpage

REQUEST REMOVAL

Bing

https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d

To remove a search result or cache from Bing, go to the above URL and follow the steps located on the Bing website.

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.

Bing webmaster tools

Acxiom

https://isapps.acxiom.com/optout/optout.aspx

What kind of books do you read? What kind of shoes do you buy? What type of information do Marketers have on you?

Acxiom Corporation is a database marketing company. The company collects, analyzes and sells customer and business information used for targeted advertisements. Good news! You can Opt Out of this service simply by following the link shown above. #protectyourdata

acxiom

Google isn't the web; it's only a search engine for finding data on the Web. Find the source of content, and who controls it to remove it.

UPDATED DEC 2019

OPTING OUT OF SEARCH ENGINES & OTHER DATABASES

BeenVerified

https://www.beenverified.com/f/optout/search

Public government records are available from official public records custodians or repositories to anyone who requests them. In addition to public records, personal information may be commercially acquired from credit reporting agencies or utilities. BeenVerified is one of many online data brokers that purchases and collects publicly available information that is resold to anyone as a report.

BeenVerified 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.

BeenVerified 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 BeenVerified'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.

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 BeenVerified 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. Accordingly, 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 BeenVerified to ensure the opt-out process is continuing.

People Finders

https://www.peoplefinders.com/manage

Upon request, Peoplefinders 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 opt-out 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.

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

Consider including your internet footprint to your list of items that need to be cleaned out during your annual Spring Cleaning event. #internetspringcleaning

UPDATED DEC 2019

Opting Out of Public Records and Data Aggregators

This process will not delete your data but instead suppress it. In addition, these sites update periodically with new information, it is important to repeat this process every six to nine months.

- Conduct research to see what records each data aggregator has collected about you and your loved ones.
- Some data aggregators may have information about you and your family under multiple listings; you may need to repeat the removal process described below for each listing.
- Have ALL the required information prepared before you begin the removal process. Also, follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator.
- Understand that incorrect information may be a good thing and that it might not be necessary to "fix".
- Do not think removing your information from certain data aggregators will suppress everything that's available about you. Information in data aggregators about family member and associates may still contain information about you.
- Don't think you have to delete/suppress all your information on these sites. Remember, some information on data aggregator sites is "normal" since it is collected from places such as Public Records and Credit Bureaus.
- Do not 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.

Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames using some of the data aggregator links below. 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 from data aggregators is subject to change. Opting out will not remove your information indefinitely.

Individual Data Aggregator Removal Links

PrivateEye, Veromi, PeopleFinders, and PublicRecordsNow are all owned by the same parent company, Confi-Chek.com. You must still opt out of each individually.

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 **and** by visiting the Peoplefinders opt out (url below).
- Opt out of PeopleFinders and Public Records Now by visiting: **https://peoplefinders.com/manage/**
- Opt out of USA People Search by visiting: **https://usa-people-search.com/manage**
- Opt out of Veromi by visiting: **http://veromi.net/Help** and finding solution #20 .

Radaris

To opt out of Radaris follow the instructions at: **http://radaris.com/page/how-to-remove**

Group Removal Data Aggregator Links/Information

Intelius owns, or is affiliated with, the below sites. When you request removal of your records, also request removal from this network of sites. Opt-out of Intelius online at **https://www.intelius.com/optout**. Of the Intelius affiliates, the following require a separate opt out process where you must fax your ID and a letter containing the information you want removed to **425-974-6194**:

- Peoplelookup, and Phonesbook

Use the following language on the coversheet:

"As per your privacy policy, please remove my listing from iSearch, ZabaSearch, Public Records, PeopleLookup, PhonesBook, LookupAnyone, and all other affiliated people search sites. Thank you for your help with this personal security issue."

US Search/Spock/Lookupanyone

Opt out of US Search by visiting **http://www.ussearch.com/privacylock**. Here you will be redirected back to Intelius.com. Search for your name and click on the appropriate listing. Print the cover sheet and mail or fax a state issued ID or drivers license to the listed address or fax number.

UPDATED DEC 2019

Opting Out of Public Records and Data Aggregators

Family Tree

FamilyTreeNow allows you to opt out at: **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, FamilyTreeNow has a process for its remove, which can also be found using the link above where you will find additional information under "Notes".

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.

http://www.whitepages.com

MyLife

Call MyLife at **888-704-1900**. Press 2 to speak to an operator. Have the following ready: name, age, date of birth, email, current address, and a previous address. Tell the representative that you want your listing removed and provide the information you want deleted. Be sure to specifically request your information is removed from Wink.com as well as MyLife.com. Once they confirm the removal, the listing will be off the site in 7-10 days.

http://www.mylife.com

Been Verified

BeenVerified allows you to opt out at **https://www.beenverified.com/faq/opt-out/**. Search for your listing and claim it by selecting the "**>**" on the right side of your record . Enter your email address. You must click the opt out link within the email sent to your account. **http://www.beenverified.com/**

PeekYou

To opt out of PeekYou, fill out the form at: **http://www.peekyou.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.

http://www.peekyou.com

USA People Search

To opt out of USA People Search, go to **https://www.usa-people-search.com/manage/** and search for your information. Once you have located your record select "That's the One." The next page will be a confirmation that you would in fact like to Opt Out of the USA-people-search database, click the agreement blocks at the bottom of the page and it will complete the Opt Out Process.

InstantCheckMate

To opt out of InstantCheckMate, follow the instructions at: **http://instantcheckmate.com/optout**
You can opt out by mail or online.
You must provide them an email address to send the record removal to.

http://www.instantcheckmate.com/

Changing or suppressing information could be detrimental to your ability to obtain credit. It is important to know what is worth suppressing and what is worth keeping. #themoreyouknow

HOW TO SET UP GOOGLE ALERTS

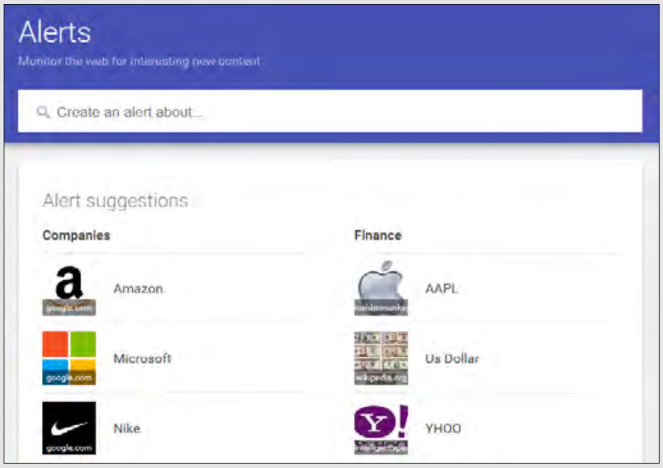
Help keep your identity safe by staying up to date on new Data Breaches – create an Alert for "Recent Data Breach" and monitor results for your information. #databreach

Background

Google Alerts is a service that generates search engine results, based on criteria provided by you, and delivers the results to your e-mail account. This service is useful for many reasons, such as monitoring the web for specific information about your employment, your kids, your online content's popularity or your competition. Google does not require a Gmail account in order to use the service; any email will work.

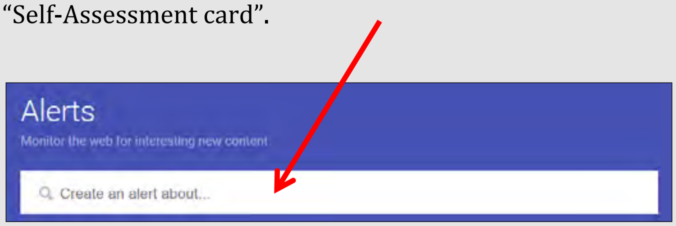
Step 1: Open the Website

Once you have a web browser open, type "Google Alerts" into your search engine, or you can go directly to the website "http://www.google.com/alerts". It might be useful to bookmark this page for easier access in the future.



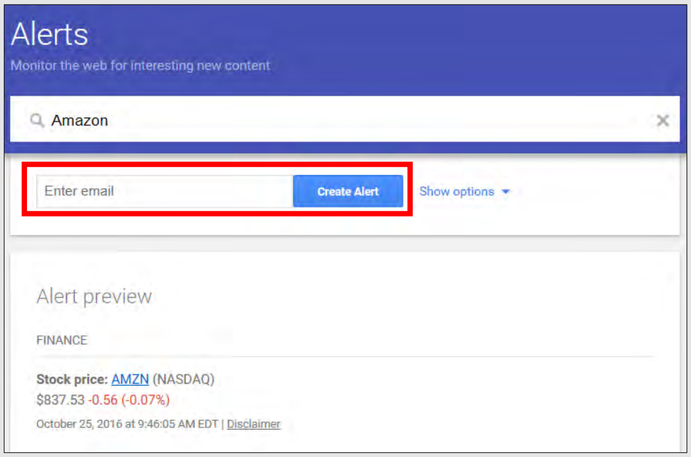
Step 2: Enter Your Search

Under "Alerts" (highlighted below), enter the topic you would like to receive alerts on. As soon as you begin typing, a sample of your first alert will appear. If you are not getting the results you expected, you can change your input right away. It might be a good idea 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

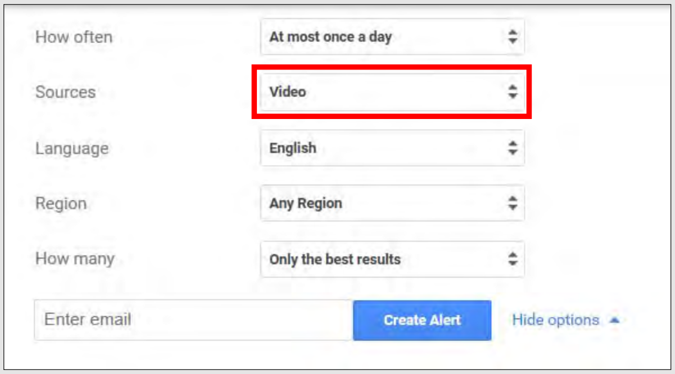
Enter a valid email address, where Google will send you the results of your query. Then complete the process by clicking on the "Create Alert" button. You will receive an email from Google Alerts asking you to confirm or cancel this request. Once you confirm the request, you will begin receiving your alerts. Your first basic Google Alert is now complete. It is recommended that you select "Show Options" and see Step 4 after completing this process.



Stock price: AMZN (NASDAQ)
$837.53 -0.56 (-0.07%)
October 25, 2016 at 9:46:05 AM EDT | Disclaimer

Step 4: Choose Source Type

There are some additional options available to tailor your search to your particular needs. Click the "Show options" drop down menu (highlighted in **red**), to customize your alert. For instance, you may choose the type of source you wish to search or how often you wish to receive each alert. The default is "Automatic", which is a good choice if you are not entirely certain what you are looking for. Otherwise it might be a good idea to select a more specific "Source" to narrow your search results. The example below *(Amazon)* is the same topic previously selected, but the source was changed to video. By changing the source, the type of results you receive will vary.

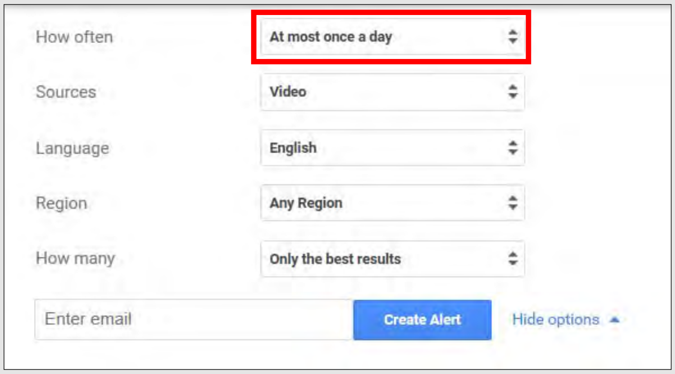


How often	At most once a day
Sources	Video
Language	English
Region	Any Region
How many	Only the best results

HOW TO SET UP GOOGLE ALERTS

Step 5: Choose the Frequency

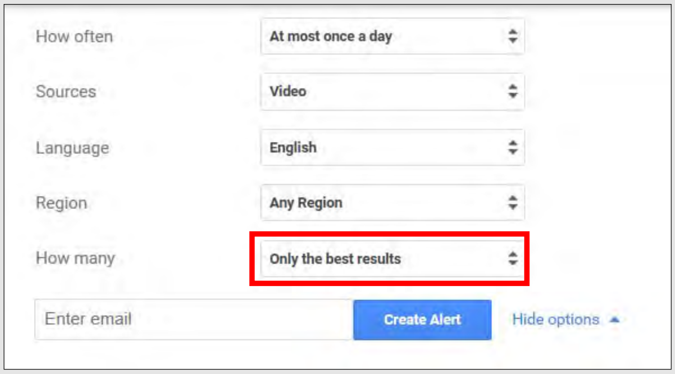
You can now indicate how often you would like the results to be delivered to your inbox. You have the options of “once a week”, “once a day”, or “as-it-happens”. The default for this option is once a day. The “as-it-happens” setting may deliver the results to your inbox multiple times a day, depending on how often the query appears in the news stream. If that happens you can modify your “Alert” to decrease how often it is sent to your email (see “Modify Alerts” to the right). Once a day and once a week will stockpile the results and only deliver them according to the chosen schedule.



How often: At most once a day
Sources: Video
Language: English
Region: Any Region
How many: Only the best results

Step 6: Select Search Volume

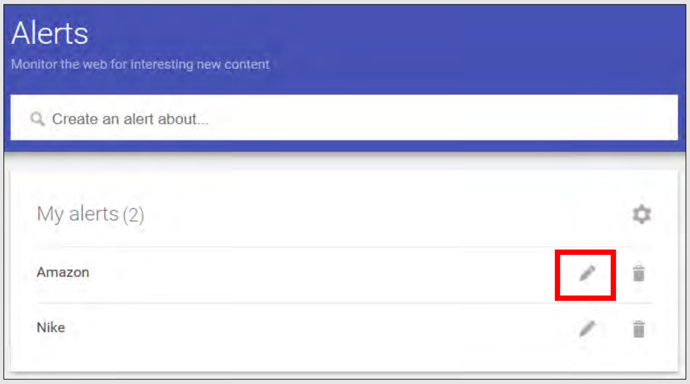
The last choice you have is to set the “How many” of the results you want delivered. This allows you to switch the volume between only the best results, in which Google filters your results for relevance to the topic, and all results. If you are not yet certain what you looking for, or perhaps do not have a specific time period in mind, you may want to select "All Results." Once you are able to narrow down what you are looking for, you can always go back and modify your settings to “Only the best results.”



How often: At most once a day
Sources: Video
Language: English
Region: Any Region
How many: Only the best results

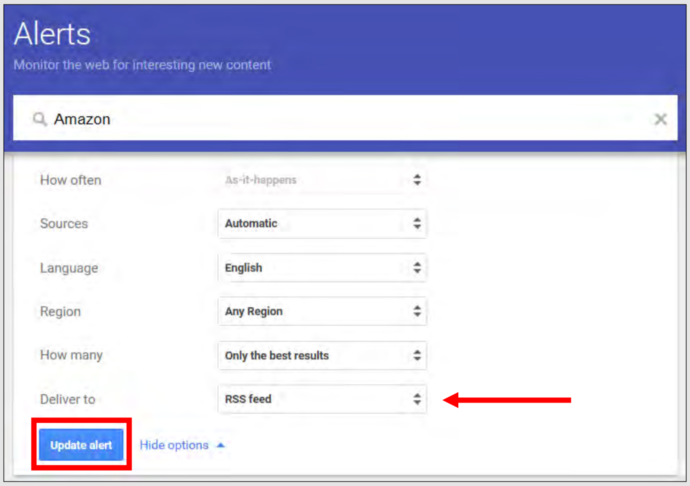
Modify Alerts

If you would like to modify your current Alerts, it's fairly simple to do by just following a few steps. Next to each alert is an "Edit" button (see the Pencil icon as highlighted below). This allows you to modify your keywords as well as the volume and frequency of how alerts are delivered. You also have the choice of having the alert delivered to your inbox or directly into an RSS feed. Click the “Update alert” button to save your changes.



Alerts
Monitor the web for interesting new content

My alerts (2)
Amazon
Nike



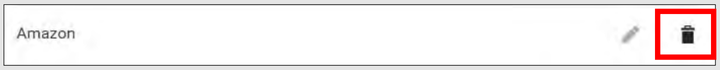
Alerts
Monitor the web for interesting new content

Amazon

How often: As-it-happens
Sources: Automatic
Language: English
Region: Any Region
How many: Only the best results
Deliver to: RSS feed

Delete Alerts

If you ever wish to delete one or more of your alerts, you can do so easily by clicking the "Trash can" icon (highlighted below).



Amazon

Identity thieves often wait up to a year or more before attempting to use stolen personal information in an attempt to evade identity protection services . #stayuptodate

ONLINE REGISTRATION SMART CARD

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.
- Turn down 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.

Identify Elements of Social Networking Site (SNS) Accounts

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 below.

First & Last Name

First and last name are mandatory for almost all SNS accounts. In order to better protect yourself, it is important to make sure your account is locked down and perhaps consider having a profile picture that is something other than your photo.

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.

Birthday

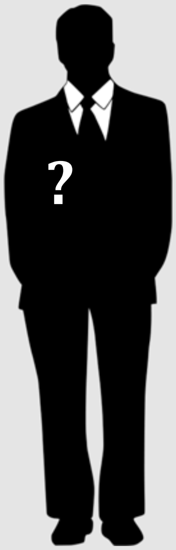
Birthdays are used to verify the user’s age and customize age-appropriate content for the user on the site. This information is sometimes published on the SNS profile and must be removed retroactively.

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 for your account.

Location: Address, Zip Code, Country

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



Company/Employment Information

Company and employment information are required for professionally-oriented SNS services, where the main purpose is to meet and build your network with other people in your field.

Sexual Orientation / Relationship Status

These fields are most often required in **online dating sites**, where the main purpose is to meet people.

Email Address

Email is the 2nd most common requirement for creating a SNS account. It is used to **verify your account** during registration and often used as a credential during future log-ins.

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.

Only fill in the minimum required identity information to help limit what human hackers can find out about you. #stopidentitytheft

ONLINE REGISTRATION SMART CARD

Identity Information Required During Online Services Registration

	LinkedIn	Facebook	Twitter	Instagram	Spotify	Amazon	Pinterest
First and Last Name	X	X	X	X	X	X	X
Username	*Uses name by default	x	X	X	Optional	*Uses name by default	*Uses name by default
Password	X	X	X	X	X	X	X
Birthday	X	X		X	X	Optional	
Gender	X	X		X	X		X
Email Address	X	**Optional	X	X	X	X	X
Phone Number		**Optional	Optional	Optional	Optional	Optional	
Country	X	X	X	X	X	X	X
Company/Employment Info	X						
Job Title	X						
Zip Code	X					X	
Facebook Account	Optional	X	Optional	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 an account. Consider using a Google Voice number for two factor authentication for additional security.**

It is a lot 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 recommended that you DO NOT do this. If someone gains access to your Facebook account and you have signed up for other 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.

Rewards

- Join Social Communities
- Connect Instantly
- Self-Expression
- Collaborate With Others
- Real-Time Information

Risks

- Cyberbullying
- Identity Theft
- Overuse
- Posts are Permanent

Only fill in the minimum required identity information to help limit what human hackers can find out about you. #privacymatters

ANONYMOUS INTERNET & MESSAGING SERVICES

Anonymous email accounts offer no overt or obvious connection to your identity, typically require no personal information to register, and retain little data usage**.** These accounts should be accessed and used in conjunction with an anonymous IP address.

"Do's and Don'ts"

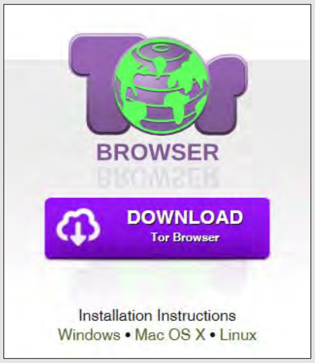
- *Do always use a secure browser and VPN that anonymizes your IP address when accessing anonymous email services. Be sure your browser is updated regularly.*
- *Do remember, although the tools anonymize you, if you have to pay with traditional means, you can be identified through that transaction.*
- *Do use VPN services. They anonymize your IP address, although you will have to submit personal data to sign up for the service.*
- *Do **not** access more than one account in a single browser session, and never access popular services such as Google or Yahoo in the same session.*
- *Do **not** include personal details in your communication that can be used to identify you, such as your name, phone number or address.*
- *Do **not** use anonymous email services on any device that requires personal logins, such as a smart phone with linked accounts.*

"Using Tor to Anonymize Your IP Address"

Tor Browser is a free, open source web browser that uses a volunteer network of virtual tunnels and a layered encryption process to anonymize your IP address. Note that Tor anonymizes the origin of your traffic and encrypts everything inside the Tor network; however, it *cannot* encrypt the data after it comes out of Tor at the destination. Tor can be installed according to the instructions below

1 Visit **torproject.org.**

Download and Install the **Tor Browser Bundle** to your hard drive or a flash drive.

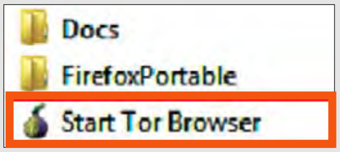


BROWSER

DOWNLOAD Tor Browser

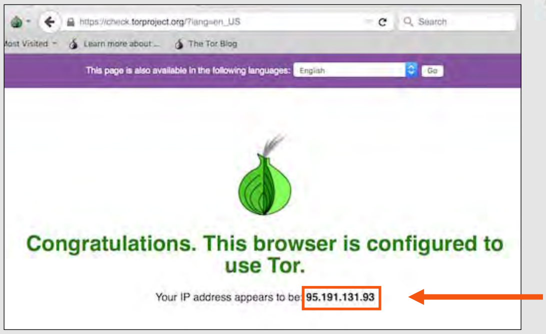
Installation Instructions
Windows • Mac OS X • Linux

2 Launch the **Tor Browser** which can be found at the location you saved the bundle to. Double-click "**Start Tor Browser**".



Docs
FirefoxPortable
Start Tor Browser

3 Ensure your Tor Browser is providing you with an anonymous IP address.



https://check.torproject.org/?lang=en_US

Most Visited · Learn more about... · The Tor Blog

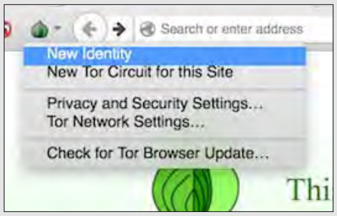
This page is also available in the following languages: English Go

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 95.191.131.93

IP address

4 To use a new IP address, click the 🧅▾ and select "**New Identity**". Please note that doing this will close all of your currently opened tabs.



Search or enter address
New Identity
New Tor Circuit for this Site
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
Thi

No matter how many tools you use to mask your IP, your payment or signup information could identify you

ANONYMOUS INTERNET & MESSAGING SERVICES

There are many email and messaging options out there that can provide a means to send and receive messages anonymously or semi-anonymously. The right service for you will depend on the primary nature of your communications , the cost, and the information you are willing to provide.

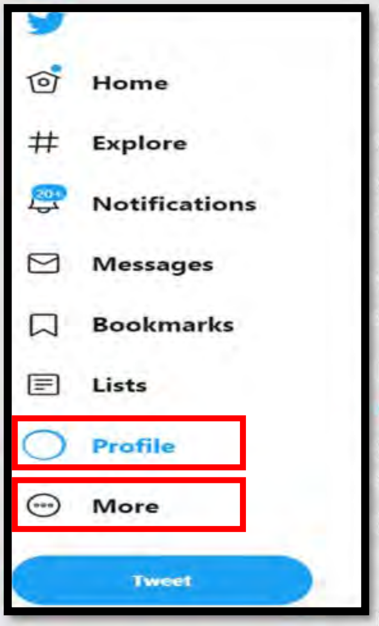
Provider	Service	Primary Use	Data Retained	Data Sharing	Cost
Hide My Ass!	VPN Temporary Email	Freely surf the web (VPN). Receive emails and use the inbox for websites that you do not necessarily trust that require you to provide an email address.	IP address, cookies, payment details, username, password, and actual emails. HMA asks for an existing email address at signup but this is optional.	They do not sell personal data to 3rd parties unless required by law. They do share information with members of AVG Group.	VPN as low as $6.99. Email is free.
CloakMy	One time message and chat service	CloakMy is accessible through Tor, it is one time messaging and chat. You have to send the recipient a unique URL to go retrieve the message.	None, no personal information required	None, there is no data retained	Free
Proton Mail	End to end encrypted email	Fully encrypted email, emails are encrypted client side so they are fully encrypted when they get to the Proton servers in Switzerland	Optional additional email upon sign up for account recovery purposes.	Proton if compelled, which they never have been could only hand over encrypted emails. They do not retain the keys to encryption, the client does.	Free
HushMail	Email host	HushMail is an email host just like Gmail or Yahoo. It is accessible through Tor and it does not require personal information to register.	No person information retained, although there is a payment required so you can be identified that way.	Hushmail logs user IP addresses. They have also turned over user data to U.S. authorities in the past due to court orders.	$49.98/ year
Signal	Encrypted text messaging	Send one-to-one and group messages, which can include files, voice notes, images and videos, and make one-to-one voice and video calls	Signal users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message	Free
Wickr	Encrypted text messaging	End-to-end encryption and content, expiring messages, including photos, videos, and file attachments and place end-to-end encrypted video conference calls	Wickr users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message	Free
Mailinator	Temporary Disposable Email	Use the Mailinator address anytime a website asks for an email address. Can only receive email.	No signup required.	Mailinator is a public domain so anyone can read an email if they know what address was used. Use odd names to avoid heavily used inboxes.	Free

Disposable email services allow you to send untraceable , disappearing emails

TWITTER SMART CARD

Do's and Don'ts

- 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.
- Do***n't*** allow follower's access to your profile that you do not know. Only maintain connections with people and pages you know and trust.
- 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. Their privacy and share settings can expose your personal data.
- 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 use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.

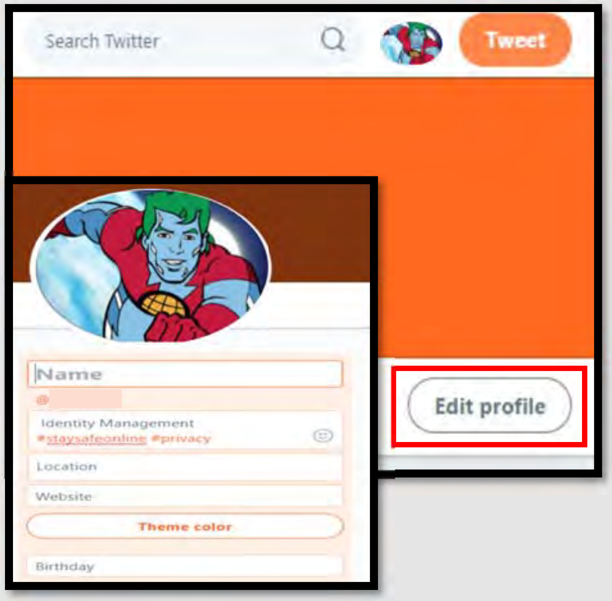


Let's start to lock down your account by first checking out what your "Profile" says about us.

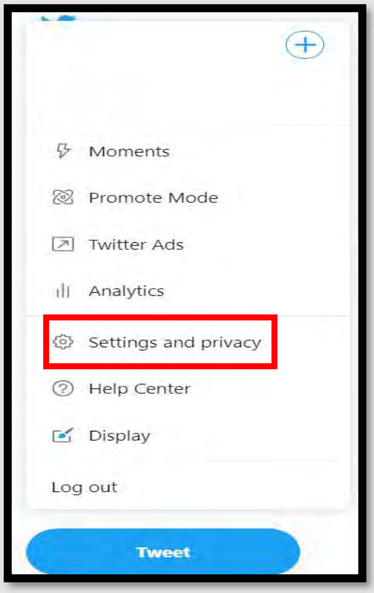
Click the "Profile" icon at the lower left of the screen (this is likely your profile picture). Then click "Profile".

Click "Edit Profile" as shown to the right.

It is highly recommended that you do ***not*** use photos of yourself for your profile or header photo. These are viewable to the public and therefore presents an unnecessary vulnerability.



It is also recommended that no PII or information that may identify you specifically be included in your profile. The "Bio", "Location", "Website", and "Birthday" areas of the profile do ***not*** have to be filled in. Even if you use old location data, it is still possible for someone to tie that back to you utilizing data aggregator sites. PII information is often used as a means to gain access to certain accounts (banks, credit cards, school etc.), providing even your birthday could help an identity thief steal your identity.

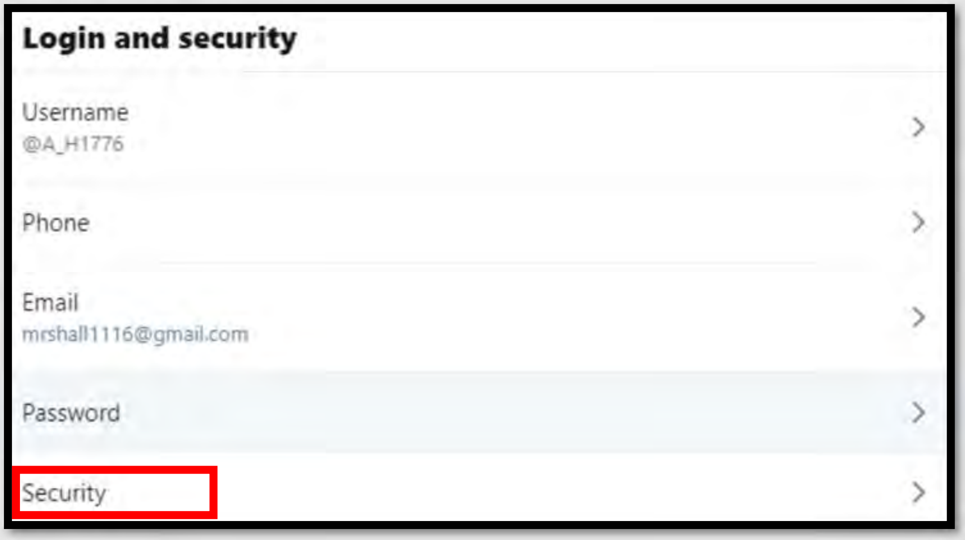


Now, let's move on to the "Settings and Privacy" tab on the same menu at the left hand side of your screen. It is important to remember that these setting should be updated on every device you use to access Twitter, to include your home computer. As with any social media account and mobile device, it is also important to ensure your "Location" is set to "Off."

Twitter accounts are hacked all the time. Make sure to use a strong password that is changed periodically as well as 2FA #safetyfirst

TWITTER SMART CARD

Here you can review your account information, including "Security" settings and how data, such as your "Username" is displayed. Remember to stop and think about what your "Username" says about you, what is it giving away? In the "Security" section, it is highly recommended that you "Set up login verification" as well as the "Password reset verification". This way if someone does try to access your account there are layers of security that will help to prevent them from gaining accessing as well as notify you should any of that occur.



Login and security

Username
@A_H1776

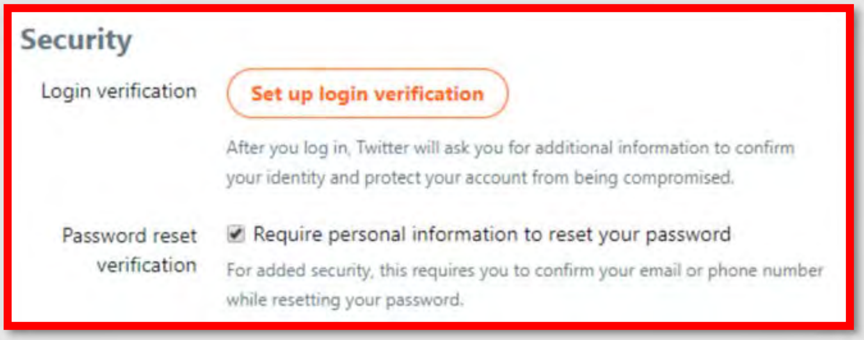
Phone

Email
mrshall1116@gmail.com

Password

Security

Next, go back to the left column and select "Privacy and Safety". Here it gets a bit tricky, but it's important to review what should and what should not be selected. All the sections in RED below are recommended settings that should be selected. Remember it's always better to control your information than it is to allow someone else to decide for you.



Security

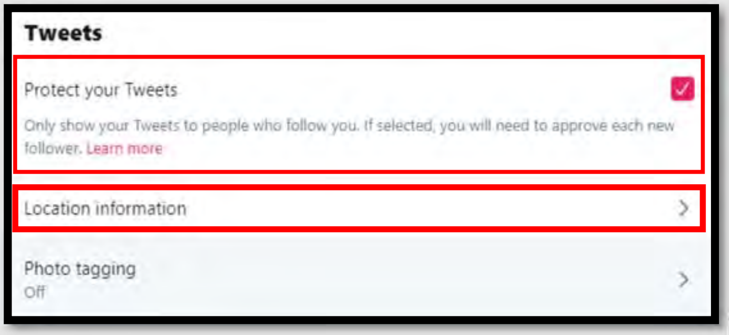
Login verification — Set up login verification

After you log in, Twitter will ask you for additional information to confirm your identity and protect your account from being compromised.

Password reset verification — ☑ Require personal information to reset your password

For added security, this requires you to confirm your email or phone number while resetting your password.

Let's scroll to the bottom of the page and select "Twitter for teams." It is recommended here that you stay in control of who has access to your profile, therefore select "Do not allow anyone to add you to their team". Directly below that it is recommended that you not check any of the "Direct Messages" section, which will help to limit incoming messages from people you do not know.



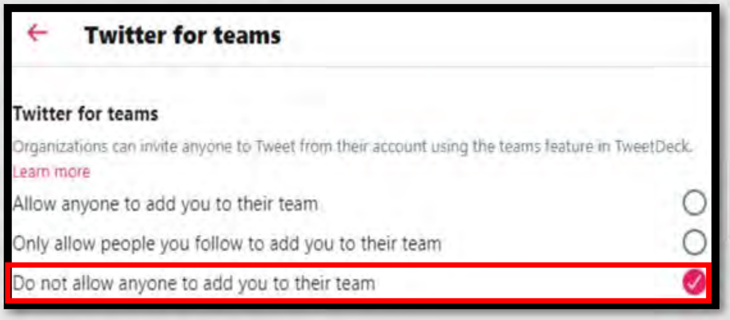
Tweets

Protect your Tweets ☑

Only show your Tweets to people who follow you. If selected, you will need to approve each new follower. Learn more

Location information

Photo tagging
Off



Twitter for teams

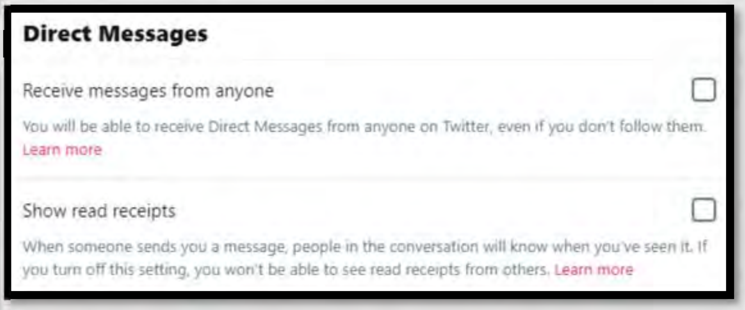
Twitter for teams

Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. Learn more

Allow anyone to add you to their team ○

Only allow people you follow to add you to their team ○

Do not allow anyone to add you to their team ●



Direct Messages

Receive messages from anyone ☐

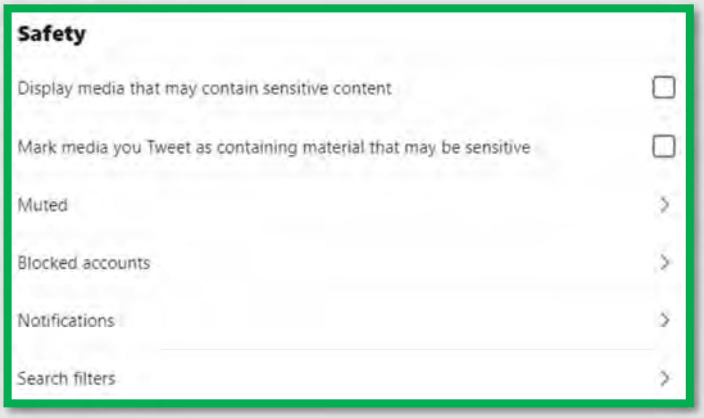
You will be able to receive Direct Messages from anyone on Twitter, even if you don't follow them. Learn more

Show read receipts ☐

When someone sends you a message, people in the conversation will know when you've seen it. If you turn off this setting, you won't be able to see read receipts from others. Learn more

Parents! Following your child's school is important for updates but if your account isn't locked down anyone can see which school your child attends. #lockitdown

TWITTER SMART CARD



Safety

Display media that may contain sensitive content ☐

Mark media you Tweet as containing material that may be sensitive ☐

Muted ›

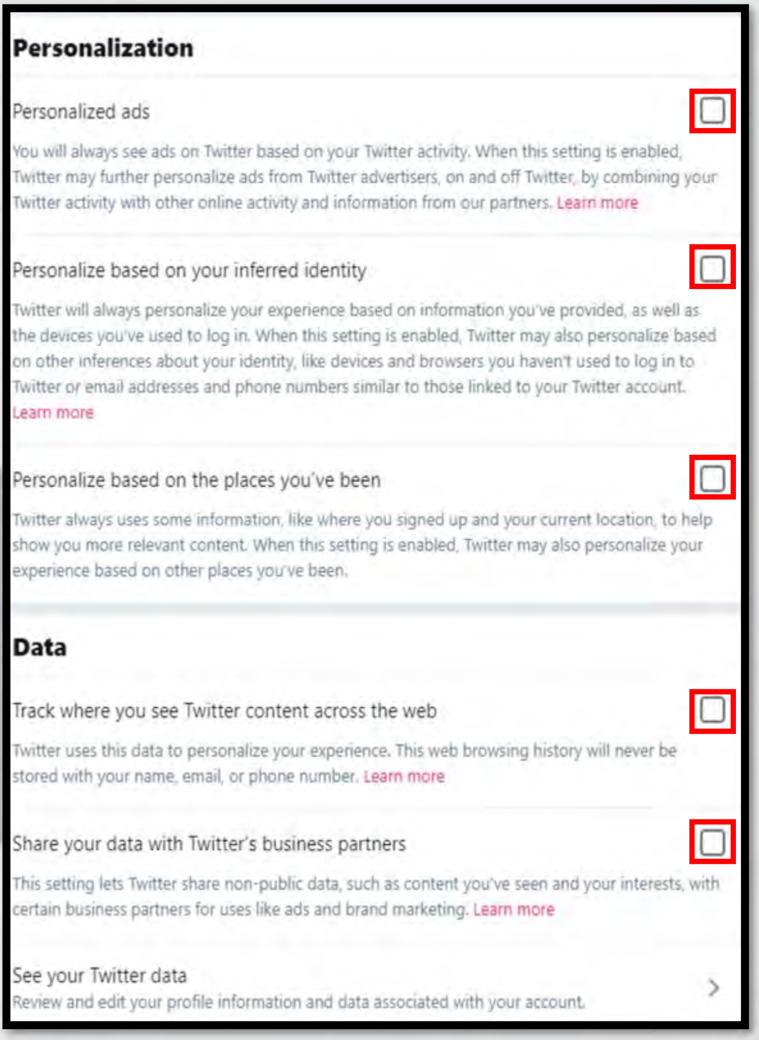
Blocked accounts ›

Notifications ›

Search filters ›

Please see the section under "Privacy and Safety," entitled "safety," (framed in green to the left). This section is really at your discretion, but if your children have a Twitter account, you may want to review these settings to help keep them from seeing unwanted or objectionable content.

Quickly, lets go back and select the arrow right next to the "Personalization and Data" section closer to the bottom of the page. As always it is highly recommended that you limit what Twitter ads have access to and this is the section to help. Once you "Disable All" items make sure to save your changes and you have completed this section.



Personalization

Personalized ads ☐

You will always see ads on Twitter based on your Twitter activity. When this setting is enabled, Twitter may further personalize ads from Twitter advertisers, on and off Twitter, by combining your Twitter activity with other online activity and information from our partners. 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

Personalize based on the 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.

Data

Track where you see Twitter content across the web ☐

Twitter uses this data to personalize your experience. This web browsing history will never be stored with your name, email, or phone number. Learn more

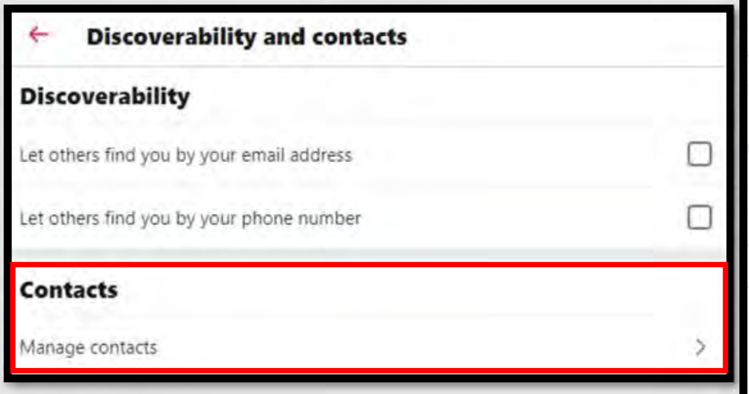
Share your data with Twitter's business partners ☐

This setting lets Twitter share non-public data, such as content you've seen and your interests, with certain business partners for uses like ads and brand marketing. Learn more

See your Twitter data ›

Review and edit your profile information and data associated with your account.

Now, let's go back to the "Privacy and Safety" menu and select "Discoverability and contacts. Here you will be able to manage any uploaded contacts from any of your devices and remove them if present by the following procedures detailed below. Here you will also be able to see if more than one email is linked to your twitter account and limit how other individuals can discover you on Twitter..



← **Discoverability and contacts**

Discoverability

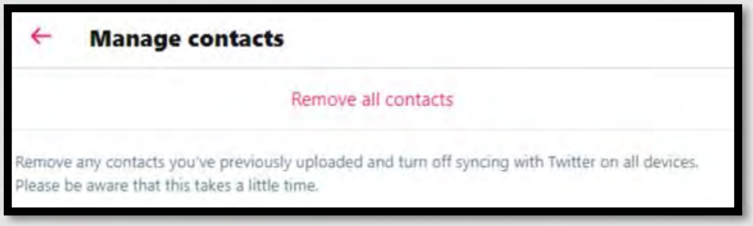
Let others find you by your email address ☐

Let others find you by your phone number ☐

Contacts

Manage contacts ›

From here, click on the "Contacts" link, shown above in red. Here you can review and remove any contacts Twitter has collected. It is highly recommended that you not synchronize any of your accounts together, to include any email accounts with contact information on them. Synchronizing your email accounts allows Twitter to do more than just upload your contacts; they also use the information to find out more about you and your contacts.



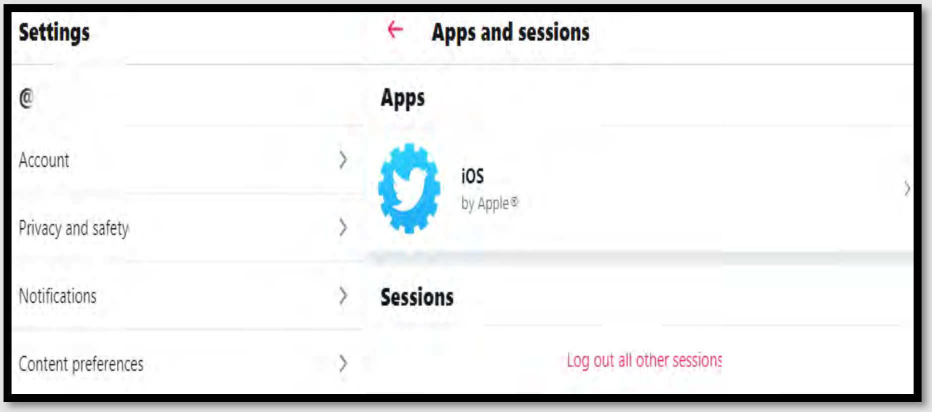
← **Manage contacts**

Remove all contacts

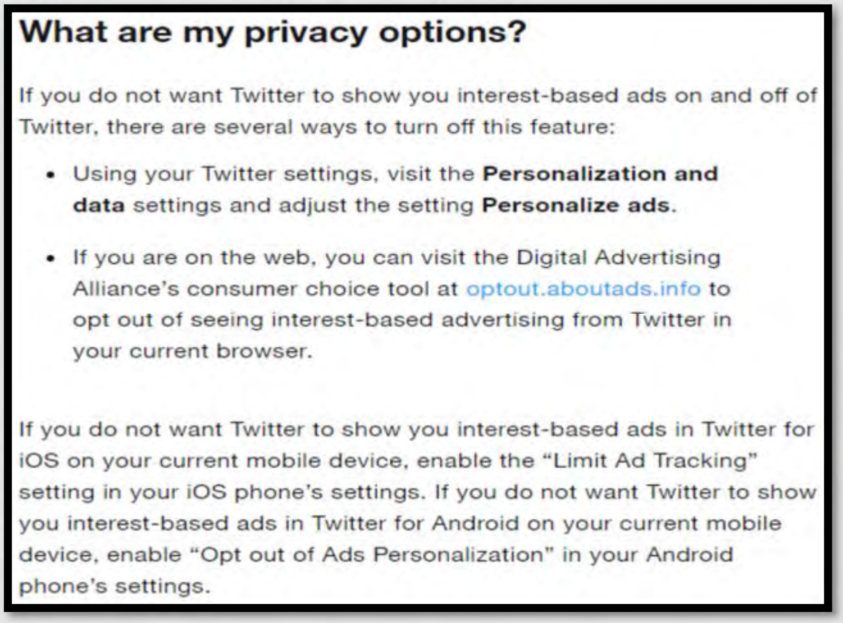
Remove any contacts you've previously uploaded and turn off syncing with Twitter on all devices. Please be aware that this takes a little time.

If your account is locked down, you're doing GREAT! If you reach out and post on a public account your comment will be visible. #privacymatters

TWITTER SMART CARD



In order to manage your Apps and/or sessions go to "Account" and on the right hand column select "Apps and Sessions". Here you can go through any apps you may have granted access to your Twitter account and revoke access. It is highly recommended that you significantly limit which apps have access to your account and your personal information.



What are my privacy options?

If you do not want Twitter to show you interest-based ads on and off of Twitter, there are several ways to turn off this feature:

- Using your Twitter settings, visit the **Personalization and data** settings and adjust the setting **Personalize ads.**
- If you are on the web, you can visit the Digital Advertising Alliance's consumer choice tool at optout.aboutads.info to opt out of seeing interest-based advertising from Twitter in your current browser.

If you do not want Twitter to show you interest-based ads in Twitter for iOS on your current mobile device, enable the "Limit Ad Tracking" setting in your iOS phone's settings. If you do not want Twitter to show you interest-based ads in Twitter for Android on your current mobile device, enable "Opt out of Ads Personalization" in your Android phone's settings.

Now, if you are adamant that Twitter not show you any Interest-based ads, there is only one place you can go to in order to turn them off. In the address bar type in **optout.aboutads.info** which will then take you outside of Twitter to the Digital Advertising Alliance page where you can not only opt out of Ads from Twitter but other Ads that might be using your "cookies" to track you. You do need to be logged into Twitter in order to remove the interest-based ads from your account. Additionally, if you are blocking your cookies, you may have to allow access to them prior to beginning the removal process.

#DataSecurity #TheMoreYouKnow #dataprivacy

#identitytheft #cyberresilience #ThinkHappyThoughts

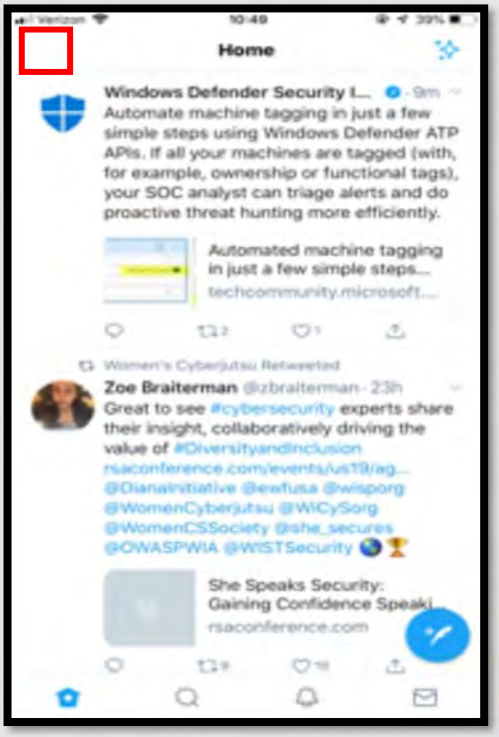
Hashtags # are used to index key words and topics on Twitter, think of them as the topic of your "tweet" or "post". **Please note that if your account is public and you use a hashtag on a tweet, anyone who does a search on that hashtag may find your tweet. Many people use a "Hashtag" as a way to improve crowdsourcing requests. When you add a hashtag to a tweet, Twitter adds the message to the hashtag group so that more Twitter users see your "tweet". Even if your Twitter account is private and your tweets are protected, be cautious of what you post online. Accounts can be compromised and settings can mistakenly be disabled.

Even if your Tweets are private, your followers are still able to screenshot them and post as they see fit. #thinkbeforeyoupost

UPDATED DEC 2019

TWITTER SMART CARD

Always check to make sure your location settings are locked down on Twitter. This means on your smart device in the "Settings" section and via the App.



Windows Defender Security I... · 9m
Automate machine tagging in just a few simple steps using Windows Defender ATP APIs. If all your machines are tagged (with, for example, ownership or functional tags), your SOC analyst can triage alerts and do proactive threat hunting more efficiently.

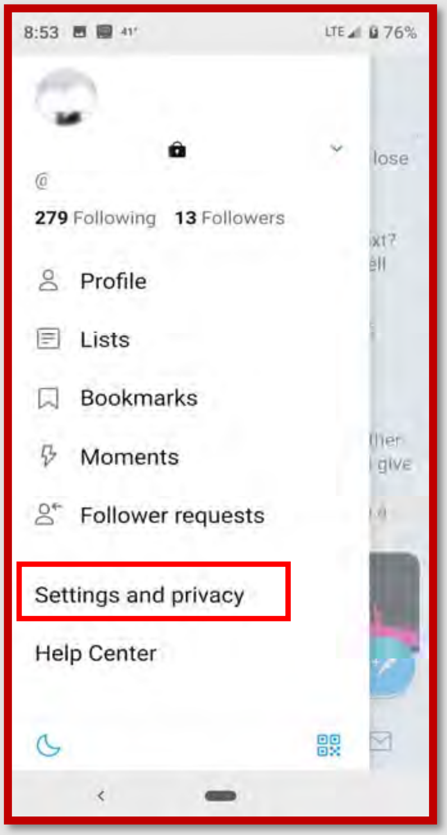
Automated machine tagging in just a few simple steps...
techcommunity.microsoft...

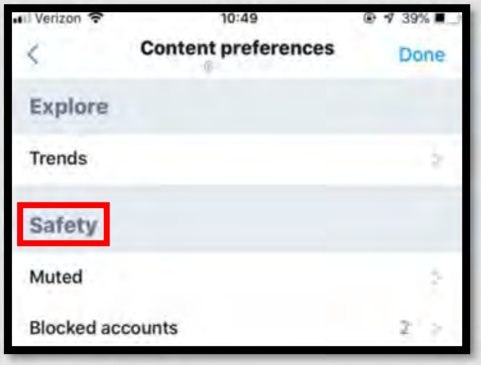
Women's Cyberjutsu Retweeted
Zoe Braiterman @zbraiterman · 23h
Great to see #cybersecurity experts share their insight, collaboratively driving the value of #Diversityandinclusion rsaconference.com/events/us19/ag... @DianaInitiative @ewfusa @wisporg @WomenCyberjutsu @WiCySorg @WomenCSSociety @she_secures @OWASPWIA @WISTSecurity 🌏🏆

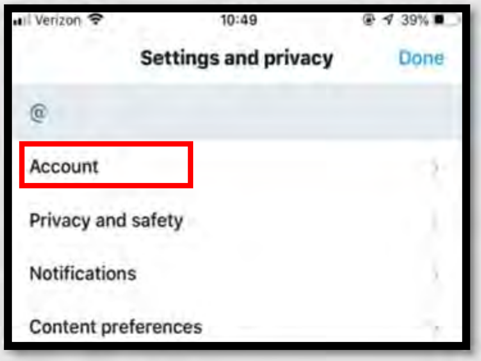
She Speaks Security: Gaining Confidence Speaki...
rsaconference.com

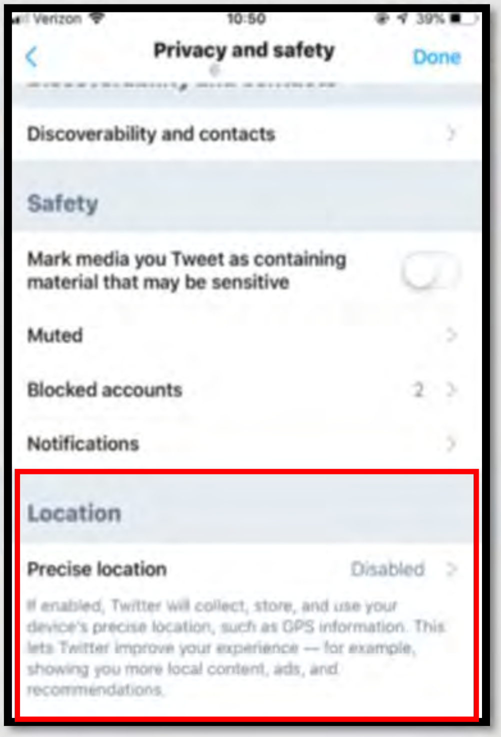
If you are planning to lock down your Twitter account from a smart phone the process is fairly similar. Getting to the "settings" section on your smart phone is one of the biggest differences between the computer based and phone based accounts and is shown in the screenshots displayed on this page. The most important lock down feature you will need to make sure you turn off and that can only be turned off on your smart device is the "Precise Location" feature which is separate from the location in any other place on Twitter. First, head to the top left of your screen and select the icon to make the pop– up menu appear (shown highlighted in red all the way to the top left).

Now for IPhone users ONLY; Finding the "Settings" section can be done as described above or by the following: Select "View Content Preferences" and once there select the "back arrow" at the top left of your screen, this will take you to your "Settings and Privacy" page. For 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." It is recommended that you turn this function to "disable" and then select "done."









If enabled, Twitter will collect, store, and use your device's precise location, such as GPS information. This lets Twitter improve your experience — for example, showing you more local content, ads, and recommendations.

UPDATED DEC 2019

TWITTER SMART CARD

Indicators of Possible Account Compromise:

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

- Unexpected Tweets posted by your account
- Any Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Twitter stating that your account may be compromised
- A notification from Twitter stating that 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 that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , Twitter advises you take the following actions:

- Delete any unwanted Tweets 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 that you and only you can access your Twitter account
- Be sure to check that your email is secure. It may be worth changing the password to both your Twitter account and the email associated with your Twitter account.

If you need to report **Spam/Fake Accounts/Harassment**: Go to https://help.twitter.com/en/contact-us

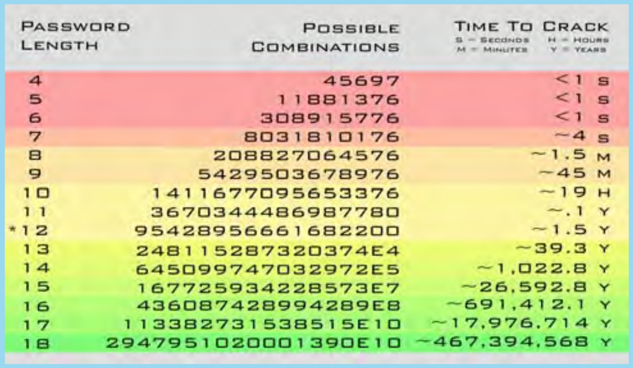
If your account was hacked: https://help.twitter.com/en/safety-and-security/twitter-account-hacked

Also, if you find that your account has in fact been hacked, it is best to let Twitter know by filling out the "Hacked Account" form located on the forms site at: https://help.twitter.com/forms

If you cannot log in to your email account, Twitter has provided links to each email accounts "having trouble signing in" page for your convenience. https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address

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

A six character password can be cracked in one second



Password Length	Possible Combinations	Time To Crack
		S = Seconds H = Hours
		M = Minutes Y = Years

4	45697	<1 S
5	11881376	<1 S
6	308915776	<1 S
7	8031810176	~4 S
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	1411677095653376	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	248115287320374E4	~39.3 Y
14	645099747032972E5	~1,022.8 Y
15	167725934228573E7	~26,592.8 Y
16	436087428994289E8	~691,412.1 Y
17	113382731538515E10	~17,976.714 Y
18	2947951020001390E10	~467,394,568 Y

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.

If you frequently receive password reset messages that you did not request, you can require that your email address and/or phone number must be entered in order to initiate a password reset. Find instructions and information about resetting your password.

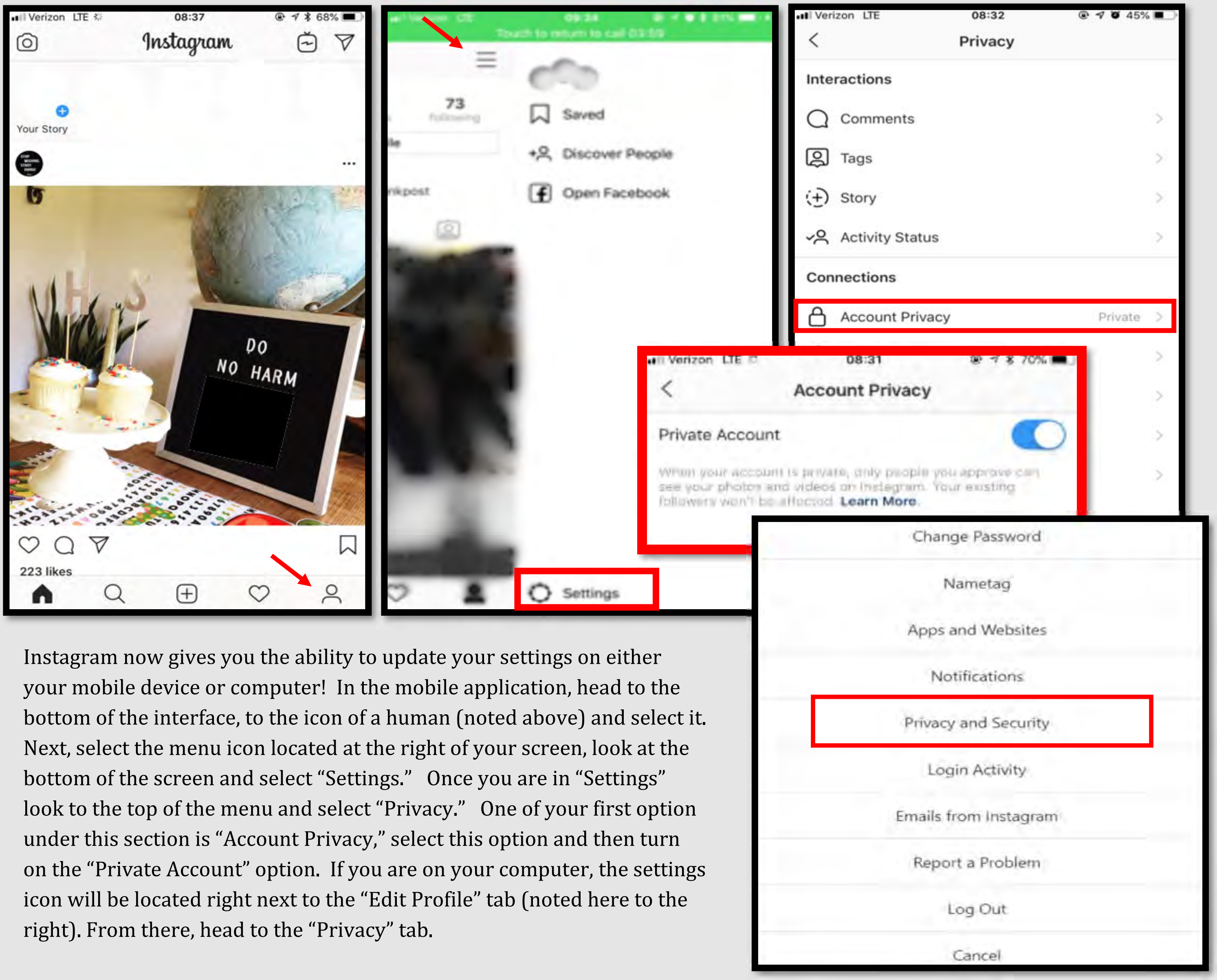
INSTAGRAM SMART CARD

(Mobile Application)

Do's and Don'ts

- Don't use geo-location tags to prevent others from seeing your location. Instagram deletes metadata from a photo the moment of uploading; however, geo-tags that spell out your location pose a personal security risk.
- Don't establish connections with people you do not know. Understand that not everyone is who he or she says 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.

- 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.



When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected. Learn More

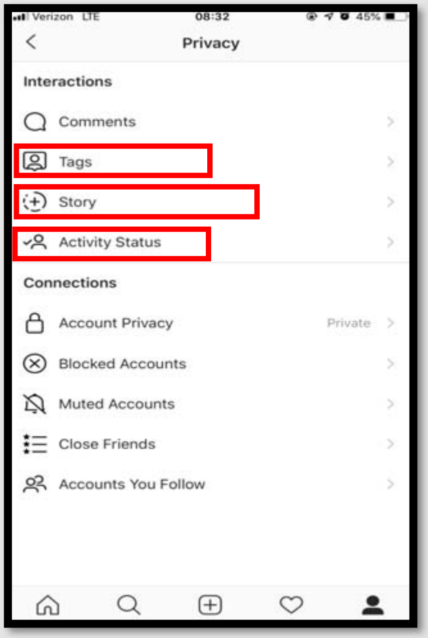
Instagram now gives you the ability to update your settings on either your mobile device or computer! In the mobile application, head to the bottom of the interface, to the icon of a human (noted above) and select it. Next, select the menu icon located at the right of your screen, look at the bottom of the screen and select "Settings." Once you are in "Settings" look to the top of the menu and select "Privacy." One of your first option under this section is "Account Privacy," select this option and then turn on the "Private Account" option. If you are on your computer, the settings icon will be located right next to the "Edit Profile" tab (noted here to the right). From there, head to the "Privacy" tab.

Do not allow your Teens and Preteens to accept followers that they do not know personally. Instagram has a plethora of fake accounts. #stophumantrafficking

UPDATED DEC 2019

INSTAGRAM SMART CARD

(Mobile Application)


Verizon LTE 08:32 45%

Privacy

Interactions

- Comments
- Tags
- Story
- Activity Status

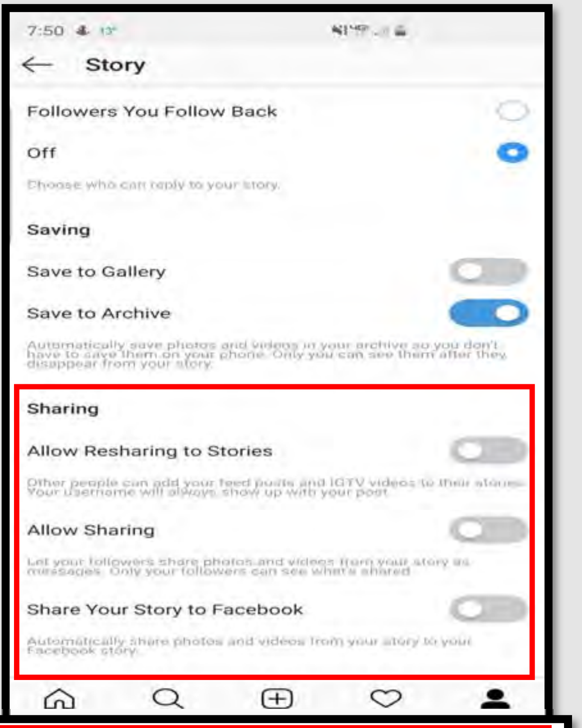
Connections

- Account Privacy — Private
- Blocked Accounts
- Muted Accounts
- Close Friends
- Accounts You Follow

In order to control what photos and videos do and do not go onto your profile, it is important to ensure you lock down your settings. Let's go back to the side menu (shown to the left of this text in the first **red** box) and select "Tags." Next, there will be an option to turn off having photos and/or videos added automatically. It is recommended that you opt to turn off the "Add Automatically" function.

Next, head to "Story" listed under "Privacy" and shown here in **red.** Here you will be able to turn off the "Allow Sharing" function, which allows others to share stories that you have posted. It is also recommended that you take a second to ensure you have not allowed Instagram to "Share Your Story to Facebook." You can turn this function off at the bottom of the "Story Controls" sections.

To the left you will also see "Activity Status" this allows users to see when and possibly where you are while Active on Instagram. If you do not want users to know when you are active you can select "Activity Status" and then toggle "On" to "Off."


7:50

Story

Followers You Follow Back ○

Off ●

Choose who can reply to your story.

Saving

Save to Gallery — off

Save to Archive — on

Automatically save photos and videos in your archive so you don't have to save them on your phone. Only you can see them after they disappear from your story.

Sharing

Allow Resharing to Stories — off

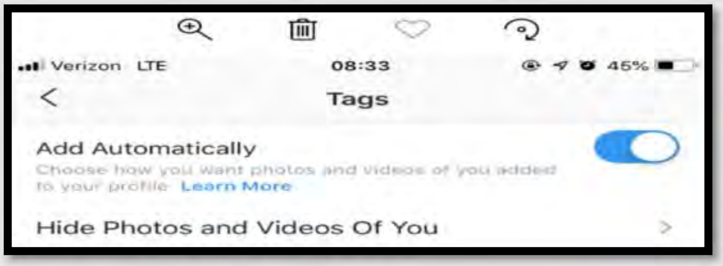
Other people can add your feed posts and IGTV videos to their stories. Your username will always show up with your post.

Allow Sharing — off

Let your followers share photos and videos from your story as messages. Only your followers can see what's shared.

Share Your Story to Facebook — off

Automatically share photos and videos from your story to your Facebook story.


Verizon LTE 08:33 45%

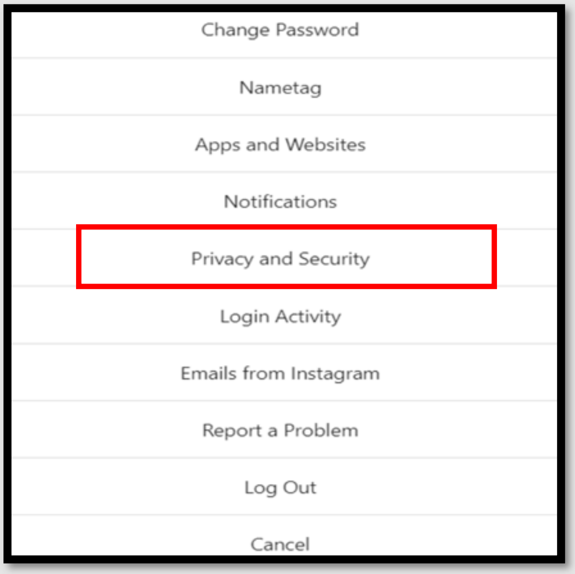
Tags

Add Automatically — on

Choose how you want photos and videos of you added to your profile. Learn More

Hide Photos and Videos Of You >

Once you have gone over the "Tags" and the "Story Controls" from your mobile device, it is a good idea to check these settings from your computer (as shown below) to ensure any changes you made have been updated.


Change Password

Nametag

Apps and Websites

Notifications

Privacy and Security

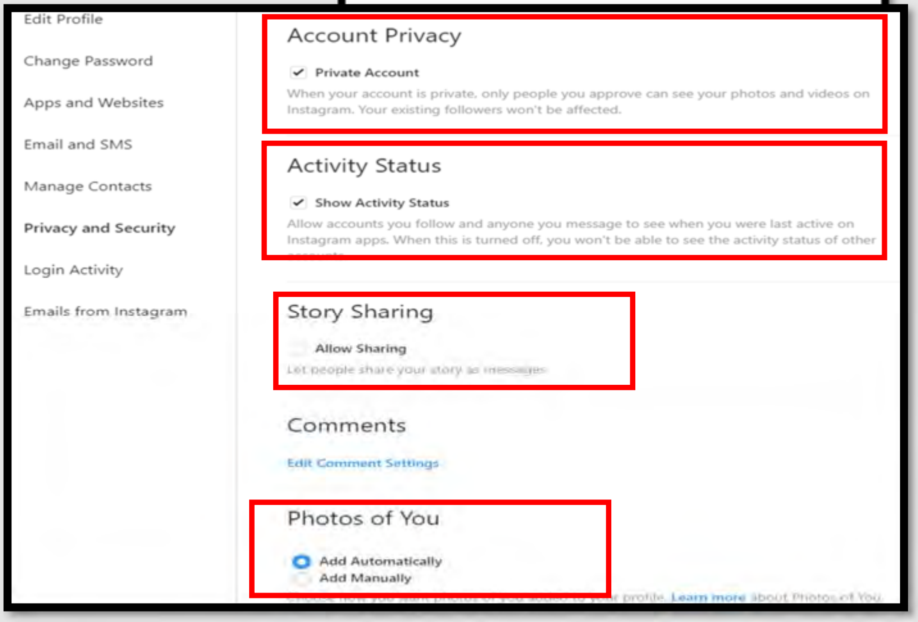
Login Activity

Emails from Instagram

Report a Problem

Log Out

Cancel


Edit Profile

Change Password

Apps and Websites

Email and SMS

Manage Contacts

Privacy and Security

Login Activity

Emails from Instagram

Account Privacy

☑ Private Account

When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected.

Activity Status

☑ Show Activity Status

Allow accounts you follow and anyone you message to see when you were last active on Instagram apps. When this is turned off, you won't be able to see the activity status of other accounts.

Story Sharing

☐ Allow Sharing

Let people share your story as messages

Comments

Edit Comment Settings

Photos of You

● Add Automatically

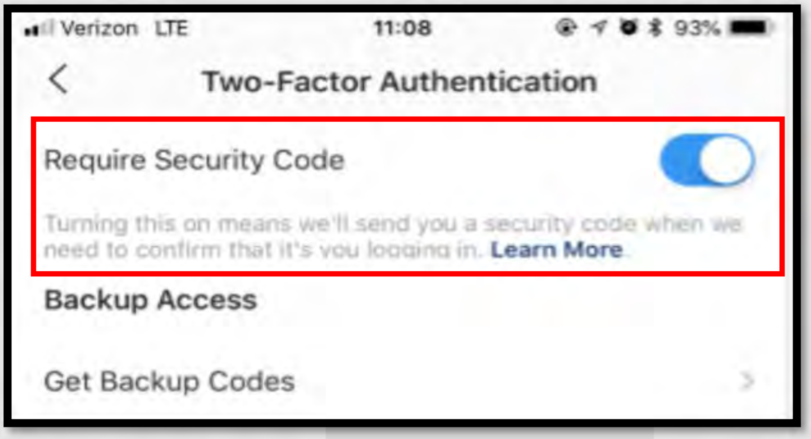
○ Add Manually

Choose how you want photos of you added to your profile. Learn more about Photos of You.

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. #trustbutverify

INSTAGRAM SMART CARD

(Mobile Application)



Verizon LTE 11:08 93%

Two-Factor Authentication

Require Security Code ●

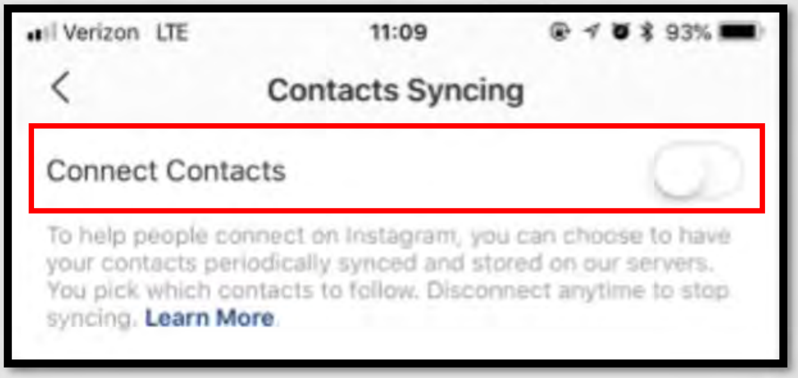
Turning this on means we'll send you a security code when we need to confirm that it's you logging in. Learn More

Backup Access

Get Backup Codes

Now, let's head to the "Security" menu and select "Two-Factor Authentication." It is very highly recommended that you turn on the Two- Factor Authentication function in order to better protect your account.

Next, head back to the "Settings" menu and select "Account" then "Contacts Syncing" It is recommended that you do not allow Instagram to upload your contacts by turning off the "Connect Contacts" option.

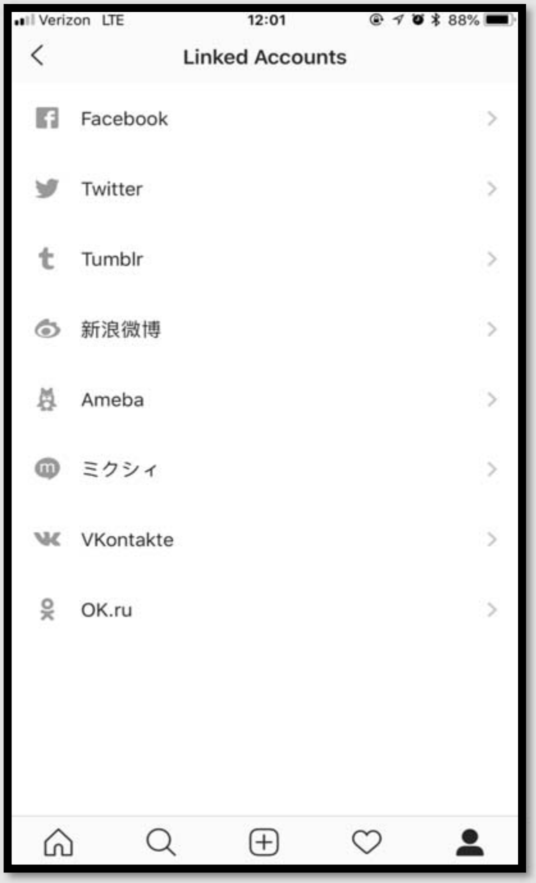


Verizon LTE 11:09 93%

Contacts Syncing

Connect Contacts ○

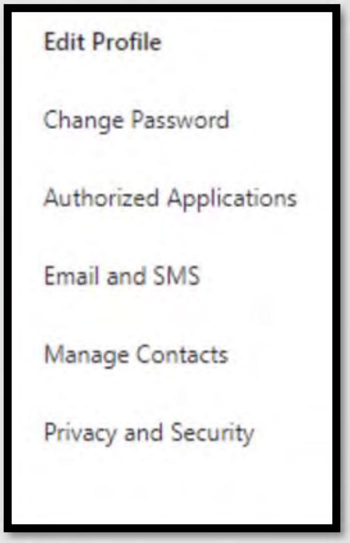
To help people connect on Instagram, you can choose to have your contacts periodically synced and stored on our servers. You pick which contacts to follow. Disconnect anytime to stop syncing. Learn More

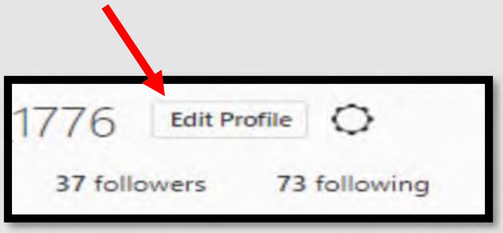


Verizon LTE 12:01 88%

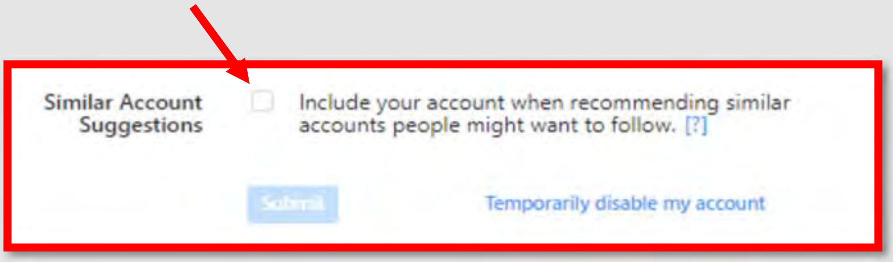
Linked Accounts

Let's go back to the "Account" menu and scroll down to the "Linked Accounts" tab. Here you want to make sure that you have not linked any of your social media accounts to Instagram. If you have, simply select the arrow next to the social media app and delink that account.





Next, lets go back to your profile (icon of the human), and select "Edit Profile." Once there, scroll to the bottom of the page and find the "Similar Account Suggestions" and deselect the box if checked. Once deselected, Instagram will no longer be allowed to push your profile to other users as "suggested users to follow." *This feature may not show on all Android devices.



Similar Account Suggestions □ Include your account when recommending similar accounts people might want to follow. [?]

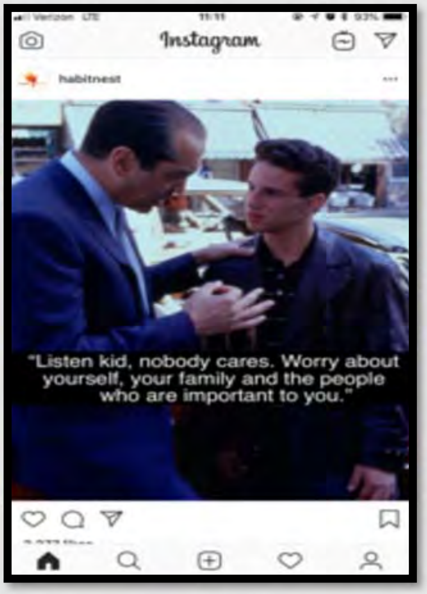
Teenagers use Instagram more so than any other social networking site. It is important to know who they know and what they are talking about. #keepthemsafe

UPDATED DEC 2019

INSTAGRAM SMART CARD

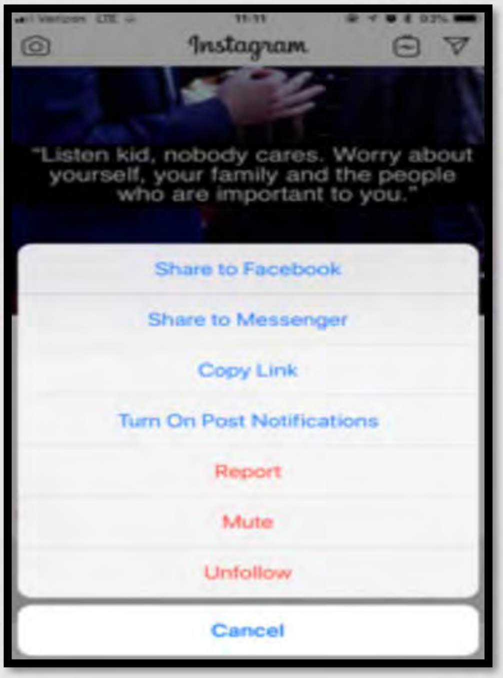
(Mobile Application)

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. #protectourkids



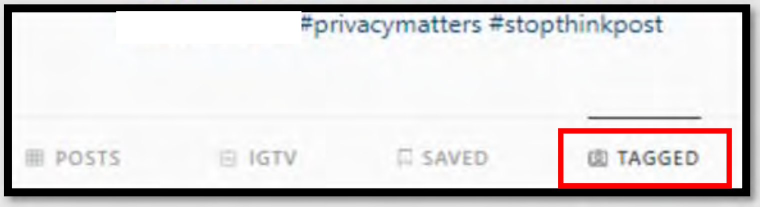
"Listen kid, nobody cares. Worry about yourself, your family and the people who are important to you."

Instagram allows you to report, or remove from your feed, any offensive post you come across. Simply select the menu button at the top left of the post and select which option best applies to that particular post from the drop-down menu.

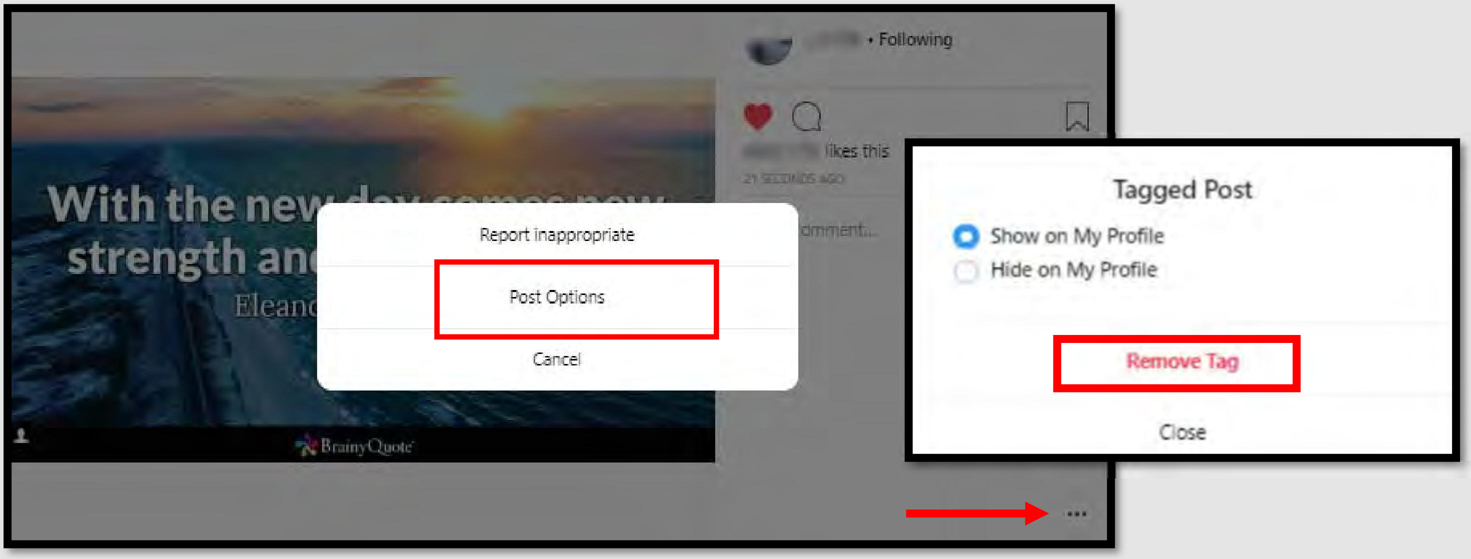


"Listen kid, nobody cares. Worry about yourself, your family and the people who are important to you."

Removing unwanted tagged photos/posts is important. If you have a profile that is "Private," you are on the right track to staying safe online. It is important for you to know that even if your profile is locked, a comment or tag on a post whose user profile is public will make your "tag" or comment visible to everyone.



In order to remove a tag of yourself from someone else's post you can follow these simple steps. First, go back to your profile (human icon) and select the "Tagged" icon (shown on the left). Next, select the post you are tagged in that you wish to un-tag yourself from, this can be from your phone or computer. Find and select the menu at the bottom of the post (shown at the bottom of the page by a **red** arrow), then select "Post Options." Now you can decide whether you would like to allow the post to show on your profile. Next, if you would like, you can "Remove Tag" simply by selecting the link highlighted here in red.



UPDATED DEC 2019

INSTAGRAM SMART CARD

(Mobile Application)

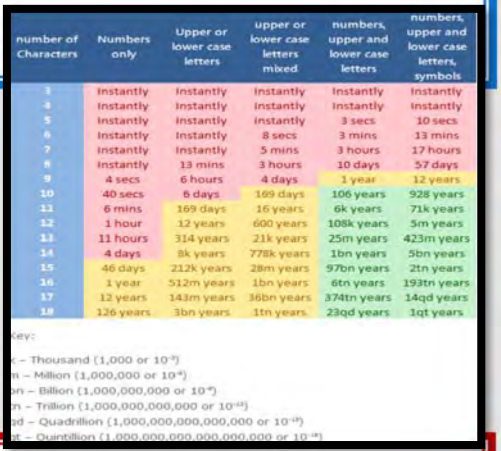
Indicators of Possible Account Compromise:

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

- Unexpected posts posted by your account
- Any Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Instagram stating that your account may be compromised
- A notification from Instagram stating that 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 that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- Delete any unwanted posts 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 that you and only you can access your Instagram account
- Be sure to check that your email is secure. It may be worth changing the password to both your Instagram account and the email associated with your Instagram account. *If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.



number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{3})
m – Million (1,000,000 or 10^{6})
bn – Billion (1,000,000,000 or 10^{9})
tn – Trillion (1,000,000,000,000 or 10^{12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{18})

If you need to report **Spam/Harassment**: Go to https://help.instagram.com/contact/383679321740945?helpref=page_content

If your account was hacked: https://help.instagram.com/, then go to "Privacy and Safety Center," "Report Something," and finally select "Hacked."

Also, 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."

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

If you received an email from Instagram letting you know that your email address was changed, you may be able to undo this by using the revert this change option in that message. If additional information was also changed (example: your password), and you're unable to change back your email address, then you should report the account to Instagram.

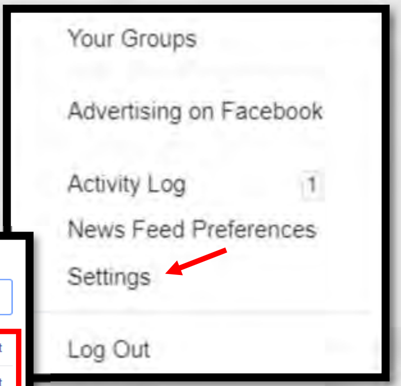
UPDATED DEC 2019

FACEBOOK SMART CARD

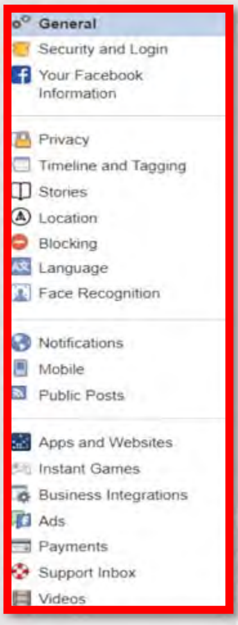
Do's and Don'ts

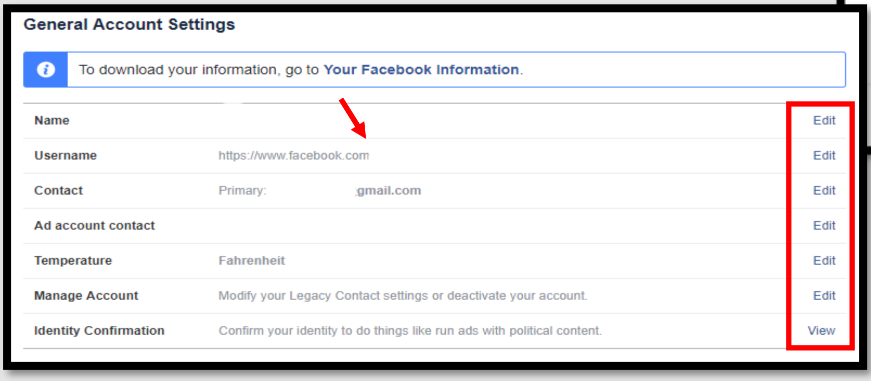
- Do use pictures of something other than yourself for your cover and profile photos. Cover and profile photos are viewable to the public. Remember if you change your profile picture you must change the privacy setting on it from "Public" to perhaps "Friends", Facebook will not do it for you.
- Do use 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. Their privacy and share settings can expose your personal data.
- Don't add your birthdate, location, phone number, or other personal details to your profile. If you do add this information make sure you set it so that it is not public.
- Don't link your Facebook account to any third party applications such as Twitter, LinkedIn, or any gaming apps. #protectyourusername
- Don't establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.
- Don't discuss specific details online, try to stay broad or wave top in your discussions. Also, when posting pictures try to stay more generic. For instance, if you are posting a picture of your car you will want to make sure the license plate is not showing.

Facebook has recently worked to enhance its privacy efforts and better protect user's data. As a result, many settings have changed and more have been added. Now, lets get started. Click the down arrow at the top right of the Facebook screen. From the drop down, select "Settings". From here it is good idea to review each different section listed on the left-hand side of your screen.



Starting, in the "General" section, go through and review your information. Remember your Username (which is located in the URL) will be public just as your "Name" is on Facebook. In this section you also have the option to deactivate your account should you want to.



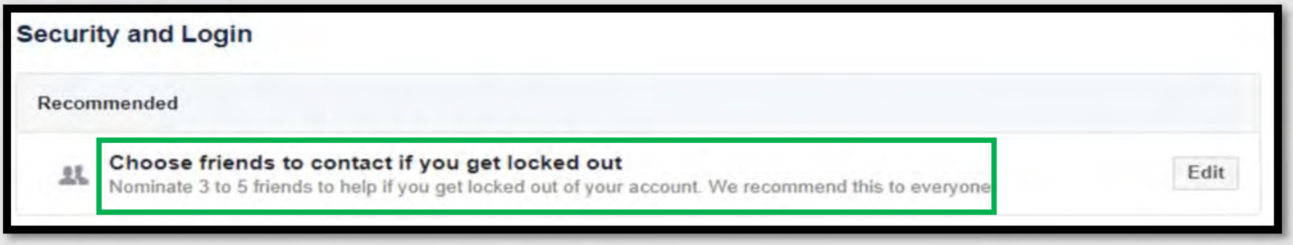


General Account Settings

To download your information, go to Your Facebook Information.

Name		Edit
Username	https://www.facebook.com	Edit
Contact	Primary: gmail.com	Edit
Ad account contact		Edit
Temperature	Fahrenheit	Edit
Manage Account	Modify your Legacy Contact settings or deactivate your account.	Edit
Identity Confirmation	Confirm your identity to do things like run ads with political content.	View

Next, head back to the left hand column and select "Security and Login". Here you can check and update your security settings and see all the places that Facebook thinks you are logged in at. First look at the Recommended section shown below. It is highly recommended that you choose friends that can help you to log in to Facebook should you ever become locked out.



Security and Login

Recommended

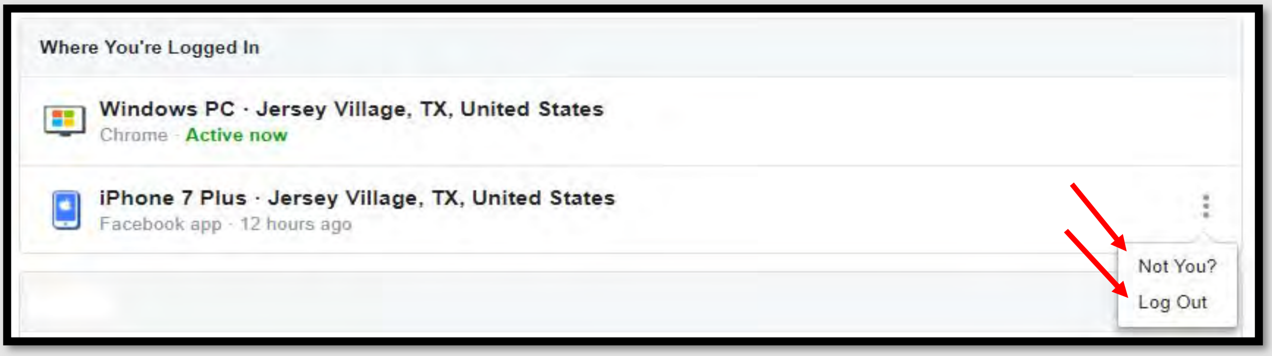
Choose friends to contact if you get locked out

Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone

Facebook quizzes could be taking more from you than you realize, it's time to think twice about finding out which Star Wars character you are. #keepyouridentitysafe

FACEBOOK SMART CARD

Once you have selected your friends as an additional security measure, scroll to the "Where You're Logged in at" box and look to ensure you recognize each location Facebook says you are logged in from. Some of these locations can be repetitive based on how many times you log in or for each different session.

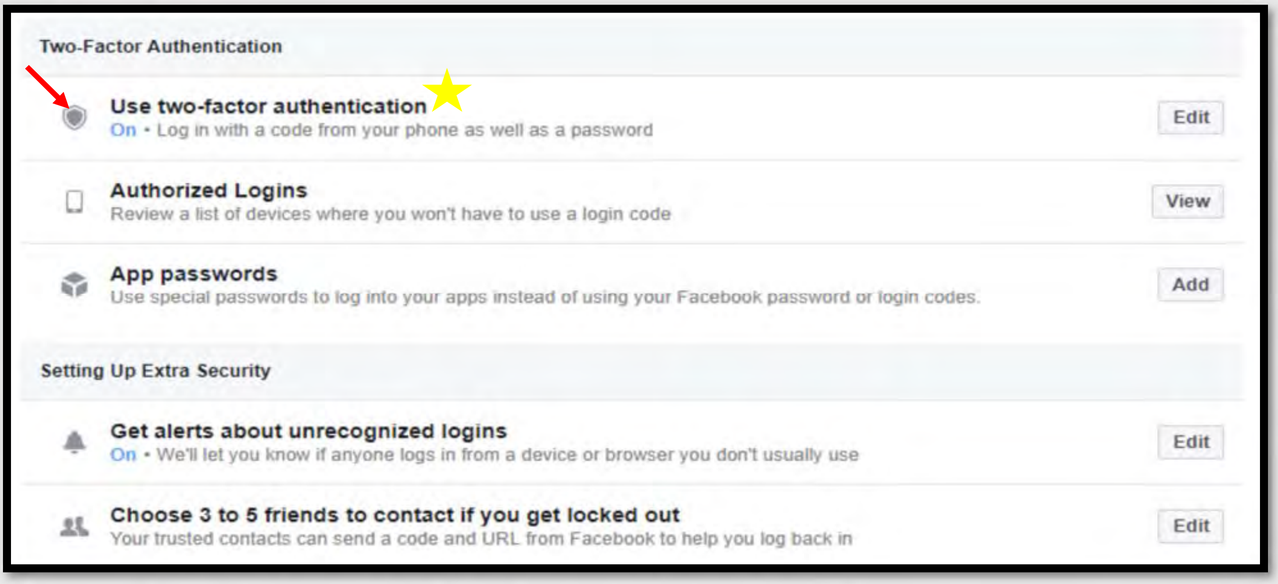


Where You're Logged In

Windows PC · Jersey Village, TX, United States
Chrome · Active now

iPhone 7 Plus · Jersey Village, TX, United States
Facebook app · 12 hours ago

If you do not recognize a location you can select the "Not You Tab" and log out of that session, (perhaps consider changing your password).



Two-Factor Authentication

Use two-factor authentication
On • Log in with a code from your phone as well as a password

Authorized Logins
Review a list of devices where you won't have to use a login code

App passwords
Use special passwords to log into your apps instead of using your Facebook password or login codes.

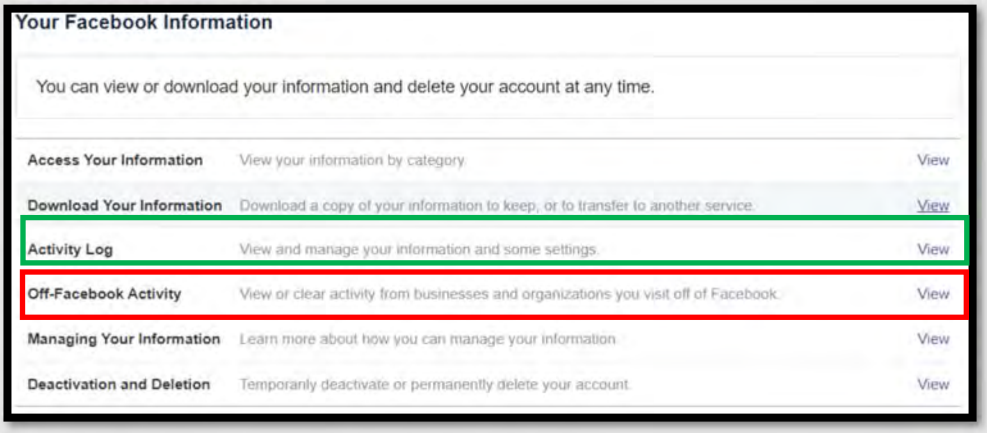
Setting Up Extra Security

Get alerts about unrecognized logins
On • We'll let you know if anyone logs in from a device or browser you don't usually use

Choose 3 to 5 friends to contact if you get locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in

Lastly in this section it is very highly recommended that you turn on "**Two Factor Authentication"** as an additional security measure . It is also a good idea to allow Facebook to notify you if a login is unrecognized.

Next, go back to the column on the left hand side and select "Your Facebook information". Here you can easily manage the information you have allowed onto Facebook or delete your account entirely. * Time Saver...both the "Access Your Information" and "Activity Log" sections take you to the same "Activity Log" page allow you to manage your information. Next select "Off-Facebook Activity" to clear your history. It is recommended that you not allow Facebook to track your offline activity.



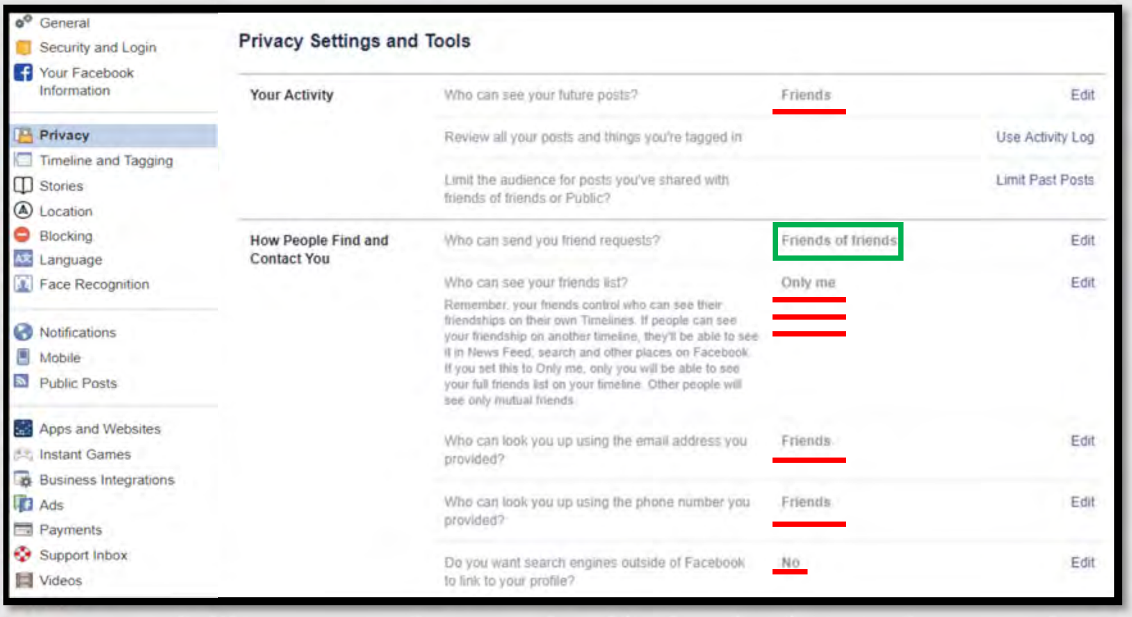
Your Facebook Information

You can view or download your information and delete your account at any time.

Access Your Information	View your information by category	View
Download Your Information	Download a copy of your information to keep, or to transfer to another service.	View
Activity Log	View and manage your information and some settings.	View
Off-Facebook Activity	View or clear activity from businesses and organizations you visit off of Facebook.	View
Managing Your Information	Learn more about how you can manage your information.	View
Deactivation and Deletion	Temporarily deactivate or permanently delete your account.	View

It is not possible to lock down someone else's' account so it is important to note the privacy setting on a post before you comment or "react" to each post. #privacymatters

FACEBOOK SMART CARD



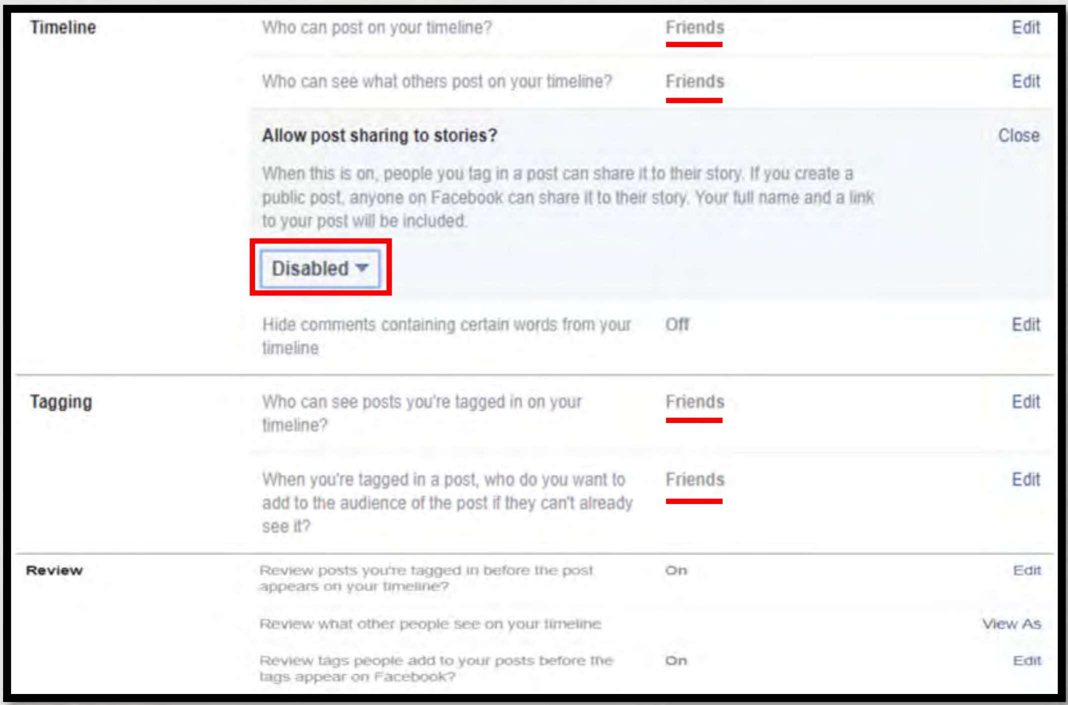
General
Security and Login
Your Facebook Information
Privacy
Timeline and Tagging
Stories
Location
Blocking
Language
Face Recognition
Notifications
Mobile
Public Posts
Apps and Websites
Instant Games
Business Integrations
Ads
Payments
Support Inbox
Videos

Privacy Settings and Tools

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
How People Find and Contact You	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list? Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.	Only me	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

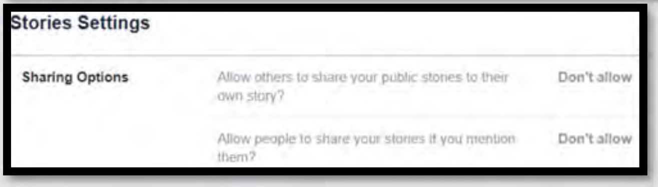
Now look at the tabs on the left and find the "Privacy" section. Completing this section is one of the most important aspects to keeping your information safeguarded on Facebook. This section puts you, the user, in the drivers seat to make decisions about where your data goes and who can see it. Take some time here to ensure each section is set to your specification.

It is recommended that no category be open to the public, the safest choice is, of course to select "Only Me". This does take away from the social aspect of the Facebook and therefore selecting "Friends" is the next best option. It is highly recommended that your Friend's List be locked down however to "Only me". Finally, it is recommended that you not allow Facebook to link other search engines to your profile.



Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
	Allow post sharing to stories? When this is on, people you tag in a post can share it to their story. If you create a public post, anyone on Facebook can share it to their story. Your full name and a link to your post will be included. Disabled ▾		Close
	Hide comments containing certain words from your timeline	Off	Edit
Tagging	Who can see posts you're tagged in on your timeline?	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
Review	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review what other people see on your timeline		View As
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

Next up, "Timeline and Tagging". This section is yet another section that puts the control of your data in your hands. Take a few moments again here to make sure you agree with all the settings. Some recommendations for this section are the following: Ensure nothing is allowed for Public dissemination, make sure to turn on each section under "Review" so that no one can tag you in anything without your permission. *Under Review you can also view your profile from the perspective of the Public, simply select "View As". While reviewing your profile from the publics' perspective take note of anything you see that you might want to lock down later such as old profile pictures. Since the "Stories" function has become more and more popular amongst all users it is important to remember it too needs to be locked down. Facebook has created a lock down feature in order to prohibit other individuals from sharing your "Stories" as shown above. It is recommended that you turn this function to "Disabled."



Stories Settings

Sharing Options	Allow others to share your public stories to their own story?	Don't allow
	Allow people to share your stories if you mention them?	Don't allow

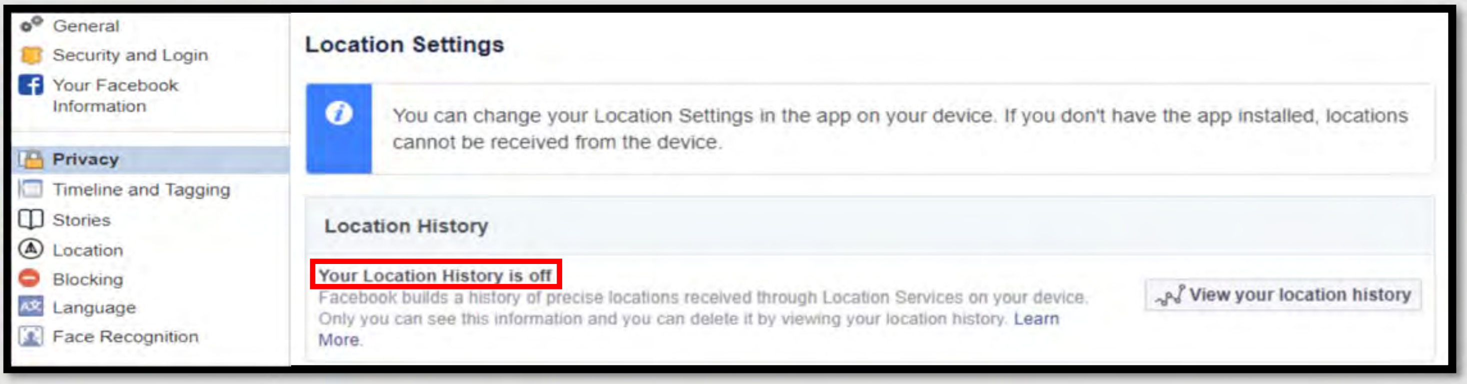
Now, along with noting in the "Timeline and Tagging" section, you will also need to lock down your stories in the "Stories" section shown directly above.

Never become complacent with your Privacy settings. Checking your settings once a quarter could help to keep your information safe online. #updatethoseprivacysettings

UPDATED DEC 2019

FACEBOOK SMART CARD

In the “Location” section make sure Facebook shows your location is “Off”. You must also turn your location settings to “Off” on each of your mobile devices to ensure the pictures/data you post do not contain geolocation information.



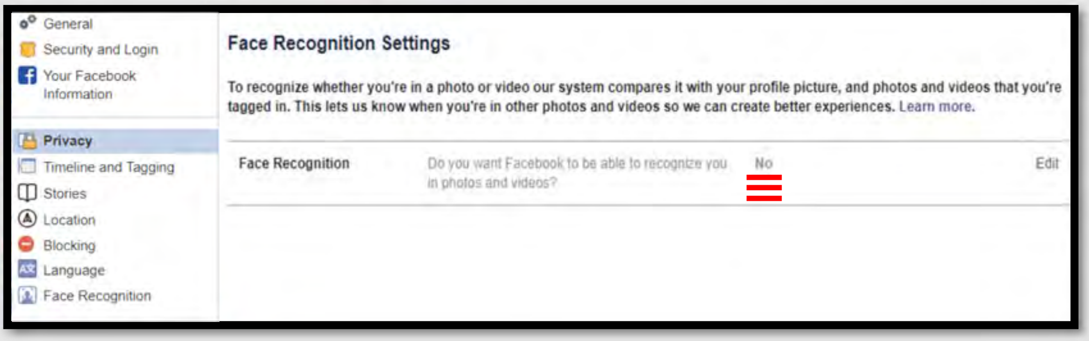
Location Settings

You can change your Location Settings in the app on your device. If you don't have the app installed, locations cannot be received from the device.

Location History

Your Location History is off

Facebook builds a history of precise locations received through Location Services on your device. Only you can see this information and you can delete it by viewing your location history. Learn More.

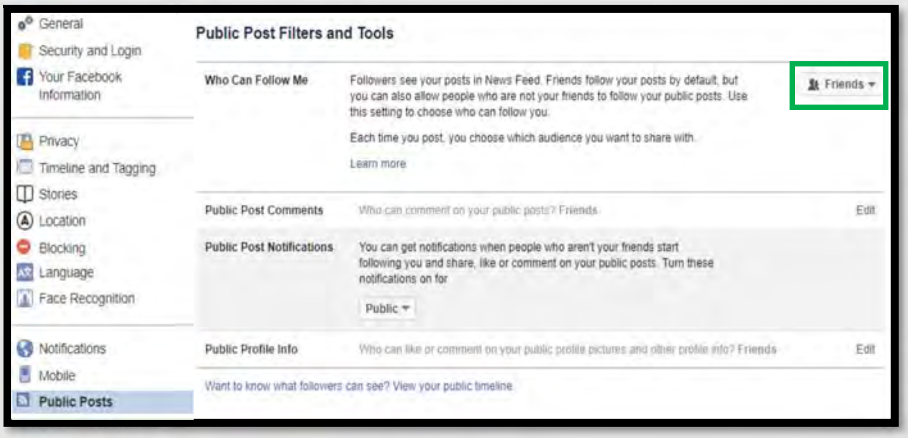


Face Recognition Settings

To recognize whether you're in a photo or video our system compares it with your profile picture, and photos and videos that you're tagged in. This lets us know when you're in other photos and videos so we can create better experiences. Learn more.

Face Recognition	Do you want Facebook to be able to recognize you in photos and videos?	No	Edit

Do you want Facebook to be able to recognize your face in pictures? Neither do we! Recommended setting for this section is a easy No.



Public Post Filters and Tools

Who Can Follow Me	Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Each time you post, you choose which audience you want to share with. Learn more	Friends ▾
Public Post Comments	Who can comment on your public posts? Friends	Edit
Public Post Notifications	You can get notifications when people who aren't your friends start following you and share, like or comment on your public posts. Turn these notifications on for Public ▾	
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? Friends	Edit

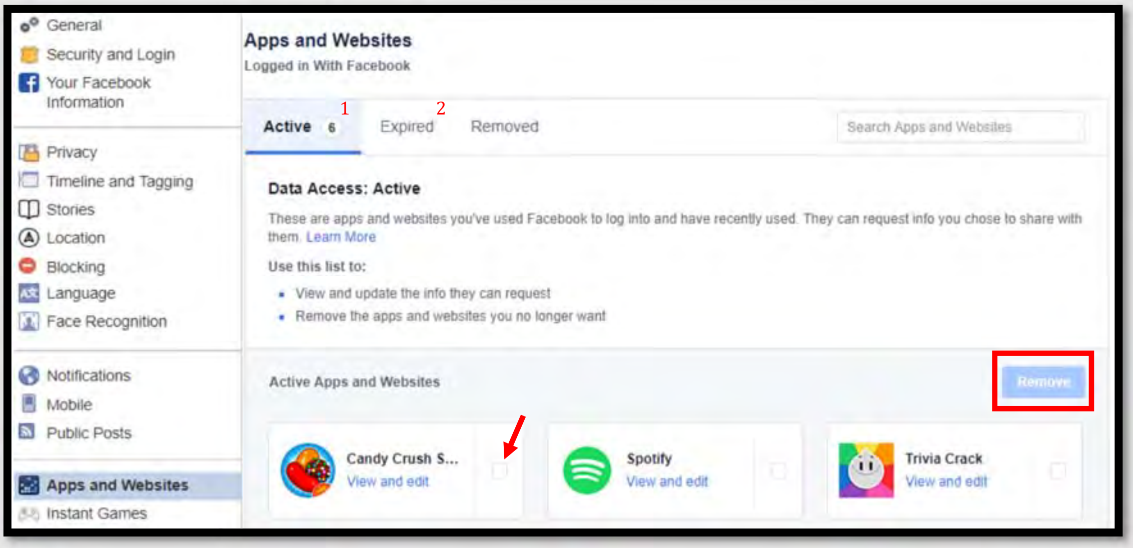
Want to know what followers can see? View your public timeline

Next, in the “Public Post Filters and Tools” section lets review public filtering. It is recommended that you do not let the public follow you. Remember, allowing the “Public” to follow you means anyone with a Facebook profile, and possibly even without one, can see what you are posting.

Letting people know where you are at the exact moment you are there can be an extremely dangerous act. #thinkbeforeyoupost #staysafeonline

FACEBOOK SMART CARD

Next, lets clean up all the "Apps and Websites" that have been allowed to use your information. Here you can review all the applications you may have allowed access to your Facebook account.



Apps and Websites

Logged in With Facebook

Data Access: Active

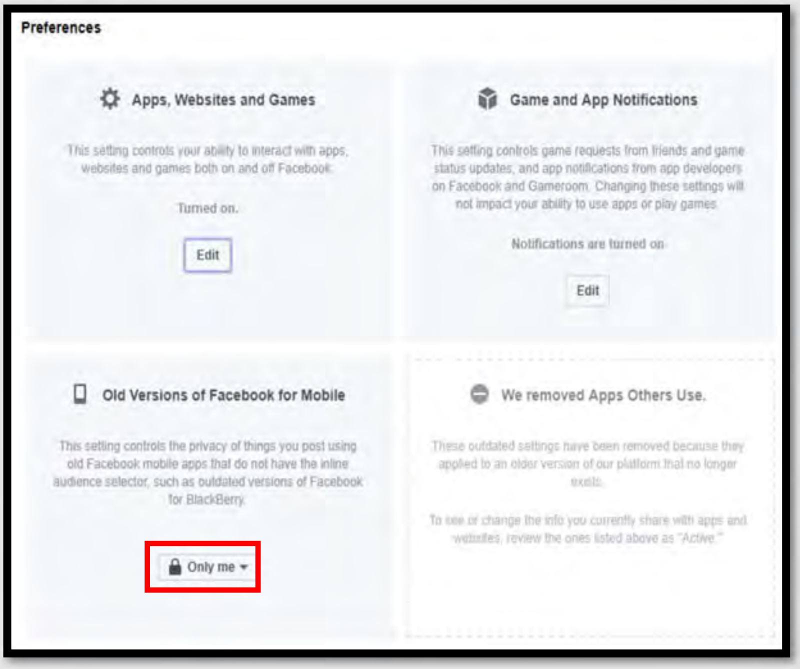
These are apps and websites you've used Facebook to log into and have recently used. They can request info you chose to share with them. Learn More

Use this list to:

- View and update the info they can request
- Remove the apps and websites you no longer want

Active Apps and Websites

If you find apps that you no longer wish to have access, simply check the box and then select "Remove". Make sure to do this for the "Active" and "Expired" sections tabs at the top of this box.



Preferences

Apps, Websites and Games

This setting controls your ability to interact with apps, websites and games both on and off Facebook.

Turned on.

Game and App Notifications

This setting controls game requests from friends and game status updates, and app notifications from app developers on Facebook and Gameroom. Changing these settings will not impact your ability to use apps or play games.

Notifications are turned on

Old Versions of Facebook for Mobile

This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.

Only me

We removed Apps Others Use.

These outdated settings have been removed because they applied to an older version of our platform that no longer exists.

To see or change the info you currently share with apps and websites, review the ones listed above as "Active."

Next scroll down to the "Preferences" section on the same page. Here you can control how Apps, Websites, and Games are able to interact with your Facebook account.

It is recommended that you keep the Old Version of Facebook for Mobile in a setting set to "Only Me". So that it is not viewable to any one else.

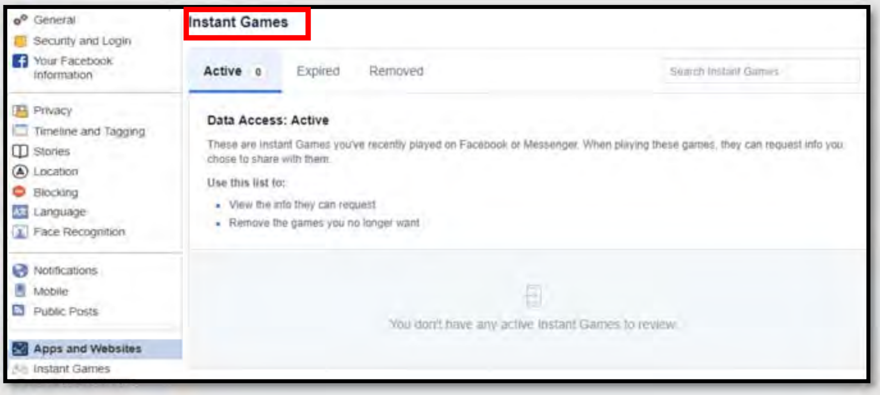
> *Some users are so overwhelmed by the curiosity that they tend to ignore some of the risks involved, and inadvertently give the app access to sensitive data.*[1]

Managing your Facebook Profile is important. Equally as important, is knowing what other users are saying about you. #ownyourprofile #fbtagging

References:

1. https://www.thequint.com/tech-and-auto/tech-news/sharing-data-with-facebook-apps-and-games-can-have-serious-consequences

FACEBOOK SMART CARD



Instant Games

Active 0 Expired Removed

Search Instant Games

Data Access: Active

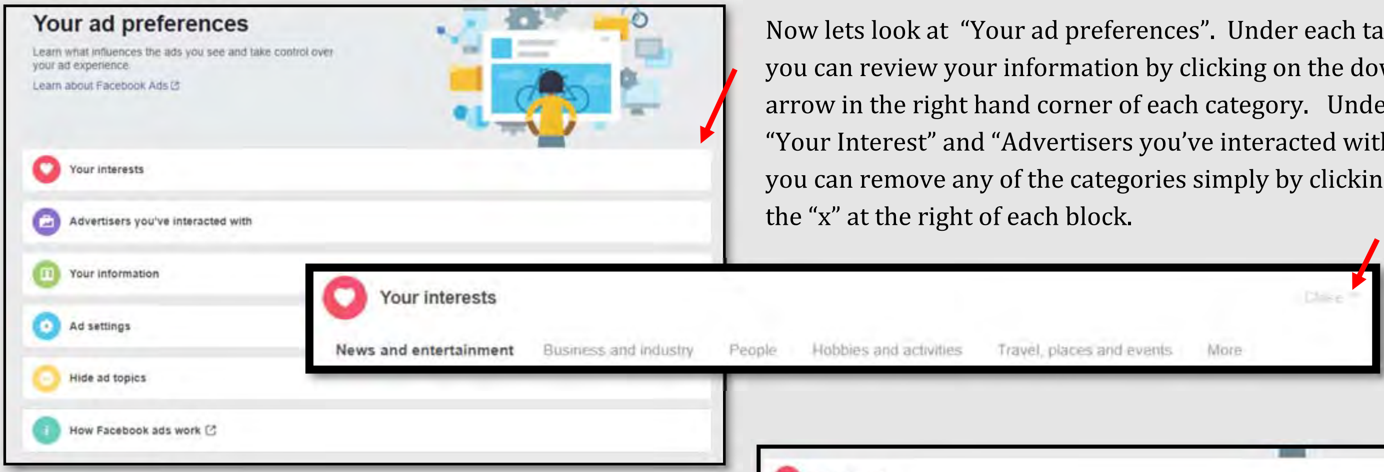
These are instant Games you've recently played on Facebook or Messenger. When playing these games, they can request info you chose to share with them.

Use this list to:

- View the info they can request
- Remove the games you no longer want

You don't have any active Instant Games to review.

Now click on the "Instant Games" tab on the left hand side. Review any games you may have allowed access to your account, the type of data they are collecting, and whether or not you want them to remain on your Facebook account. If you choose to, you can delete any of the games much like you just did in the "Apps and Websites" section.



Your ad preferences

Learn what influences the ads you see and take control over your ad experience.

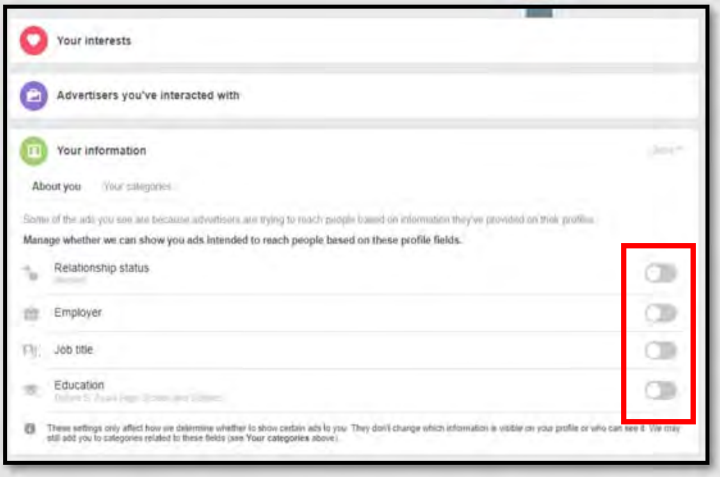
Learn about Facebook Ads

Your interests

Close

News and entertainment Business and industry People Hobbies and activities Travel, places and events More

Now lets look at "Your ad preferences". Under each tab you can review your information by clicking on the down arrow in the right hand corner of each category. Under "Your Interest" and "Advertisers you've interacted with" you can remove any of the categories simply by clicking the "x" at the right of each block.



About you Your categories

Some of the ads you see are because advertisers are trying to reach people based on information they've provided on their profiles.

Manage whether we can show you ads intended to reach people based on these profile fields.

Relationship status

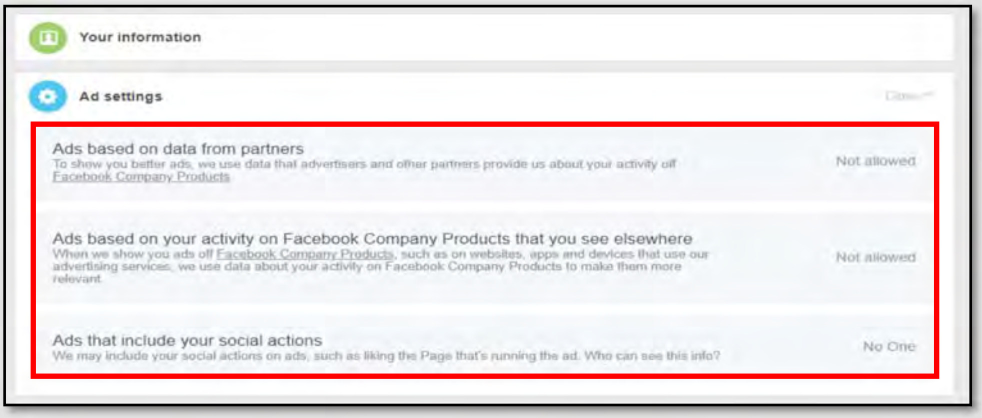
Employer

Job title

Education

These settings only affect how we determine whether to show certain ads to you. They don't change which information is visible on your profile or who can see it. We may still add you to categories related to these fields (see Your categories above).

Under the "Your Information" tab, ensure all the sliders are off (greyed out) so that none of your information is provided by Facebook to advertisers." It is important to limit the information advertisers have access to about you. This will help to ensure your information doesn't show up on advertisements and will limit unwanted Ads on your **Timeline**.



Ads based on data from partners
To show you better ads, we use data that advertisers and other partners provide us about your activity off Facebook Company Products — Not allowed

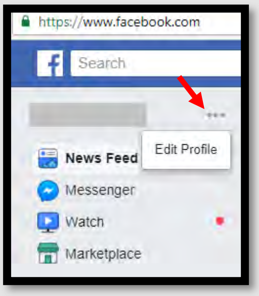
Ads based on your activity on Facebook Company Products that you see elsewhere
When we show you ads off Facebook Company Products, such as on websites, apps and devices that use our advertising services, we use data about your activity on Facebook Company Products to make them more relevant — Not allowed

Ads that include your social actions
We may include your social actions on ads, such as liking the Page that's running the ad. Who can see this info? — No One

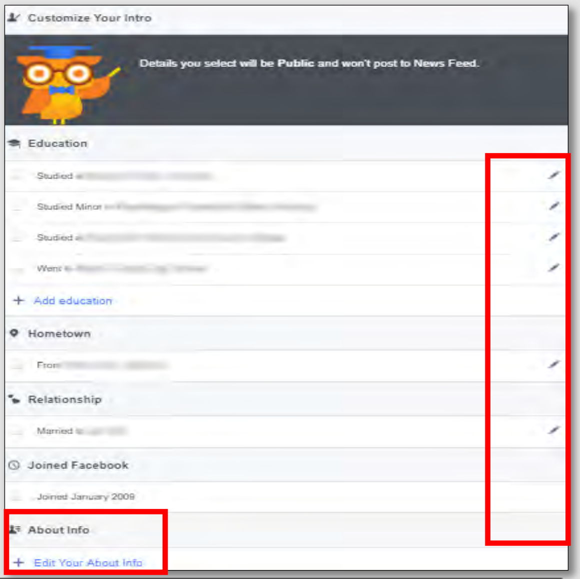
Under the "Ad Settings" it is recommended that you select "Not Allowed" or "No One" for each category.

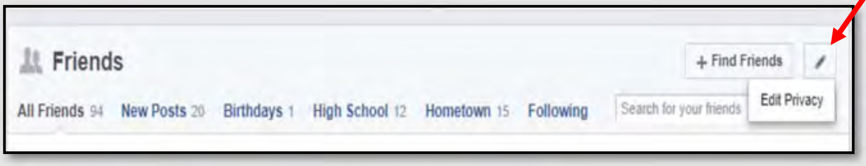
Never give up too much information, drawing out your family members on Facebook could help an Identity Thief answer security questions about you. #themoreyouknow

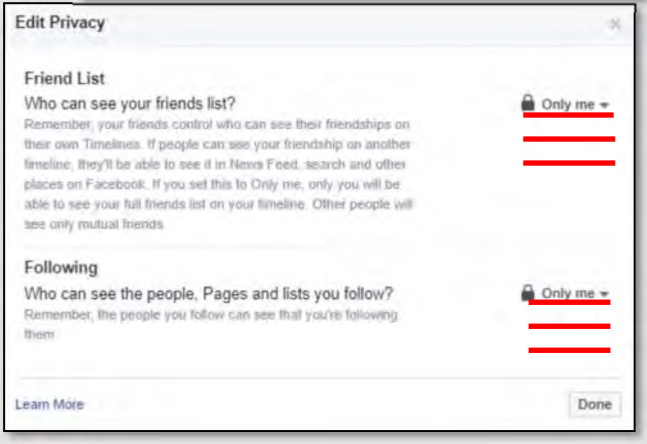
FACEBOOK SMART CARD



Now that you have completed the Settings sections lets move on. From the Home screen, select the three dots on the left hand side of the screen near your profile picture. A drop down menu will appear that allows you to edit your profile and change the privacy settings on your personal information. Once you review the privacy settings in this section scroll to the bottom of the page and select " Edit Your About Info".






Edit Privacy

Friend List

Who can see your friends list? 🔒 Only me ▾

Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends

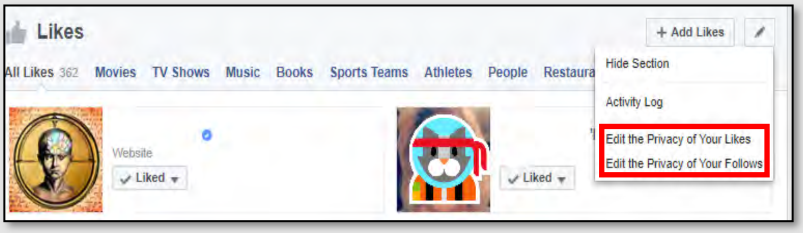
Following

Who can see the people, Pages and lists you follow? 🔒 Only me ▾

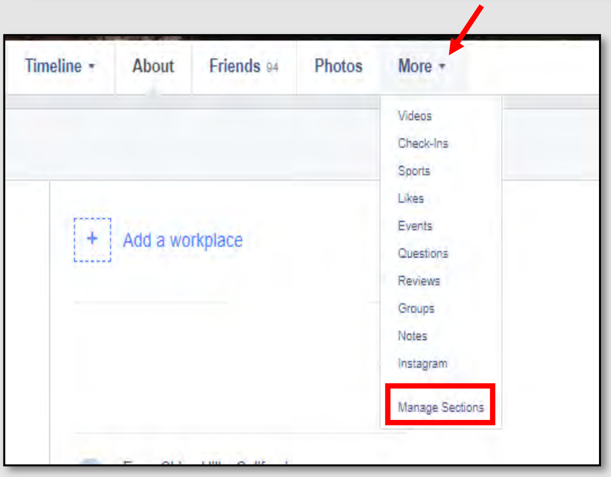
Remember, the people you follow can see that you're following them

Learn More Done

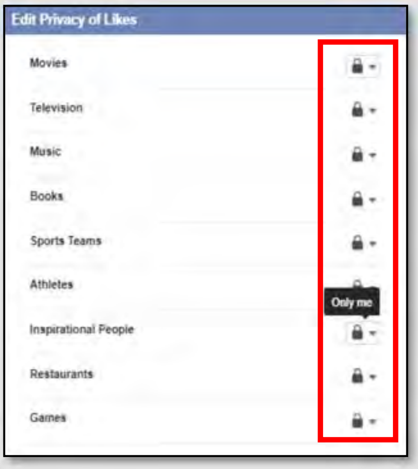
Now you can scroll through each tab in the "About You" section to ensure the privacy settings there are not set to "Public" view. Next up is your Friends List. Click on the pencil icon to display the Edit Privacy box. From here you can change the settings to "Only Me" or "Friends" so that only you and your friends can see the information. It is highly recommended you set your "Friends List" to "Only Me".



Now, there are two different spots on your **profile** where you need to lock down your "likes". The first is simply by scrolling down in the section you are already in and selecting the pencil icon to edit the privacy setting. The second, shown below, can be found in the "More" tab at the top of the page.



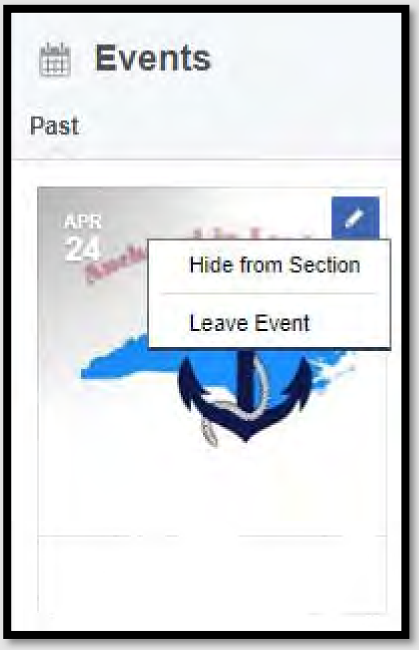
Locking down your "likes" will help to limit what criminals can figure out about you and your family. In this day and age you never want to give away even the slightest clue as to who you are, which includes, any of your hobbies/interests or perhaps the fact that you "like" your child's school or youth sports team. Recommended setting here "Only Me".


Edit Privacy of Likes

Movies	🔒 ▾
Television	🔒 ▾
Music	🔒 ▾
Books	🔒 ▾
Sports Teams	🔒 ▾
Athletes	Only me 🔒 ▾
Inspirational People	🔒 ▾
Restaurants	🔒 ▾
Games	🔒 ▾

How much information does a criminal have to have to make you think you know them and can therefore trust them? #lockitdown

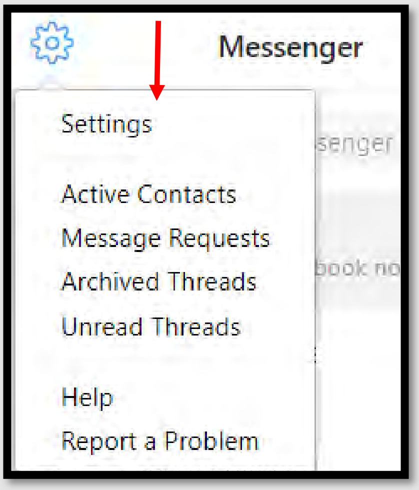
FACEBOOK SMART CARD

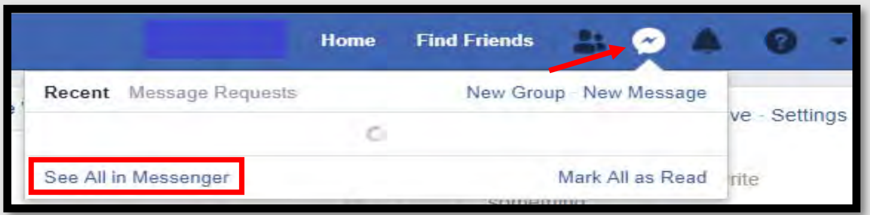


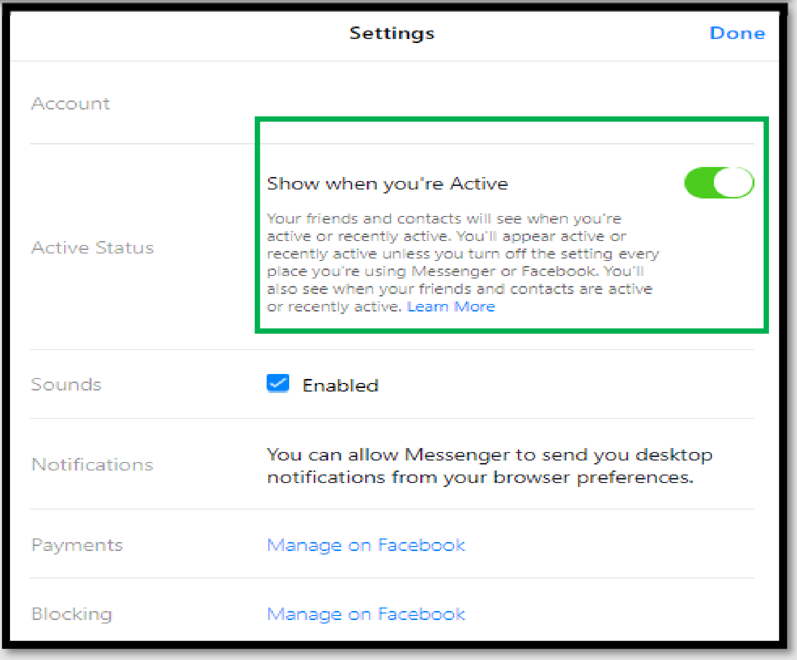
Next, as you continue to scroll down the page, you may want to go through all your "Events" to see if there are any you can delete and to make sure all your events are "Private" (which can only be done through the Event Creator). If you have an up-coming "Event" or an "Event" that you are "interested in" that is not set to "Private", be aware that anyone will be able to see that you will be attending that event. You also have the option of hiding the 'Events" section by unselecting it from the "Manage Selection" discussed on page 31.

*Social Engineers or Human Hackers are more likely to convince you that they know you if they have access to personal information about you. This information can be in the form of your likes/hobbies, friends, events you will or have been to or what schools you have previously attended. They can even review past posts you may have open to the public for some additional insight. Once they have convinced you that you are, "old friends" there is no limit to the dangers. They could convince you to meet in person, lend them money, steal your identity or worse get close to your children. The best option is to limit who can see such critical information about you to your "friends" people that you trust and already know.

You may want to go back to the top of the page to the conversation Icon. This Icon will take you to your Messenger page. Here you will be able to turn on and off your "status" on messenger.







Settings Done

Account

Active Status — Show when you're Active

Your friends and contacts will see when you're active or recently active. You'll appear active or recently active unless you turn off the setting every place you're using Messenger or Facebook. You'll also see when your friends and contacts are active or recently active. Learn More

Sounds ☑ Enabled

Notifications — You can allow Messenger to send you desktop notifications from your browser preferences.

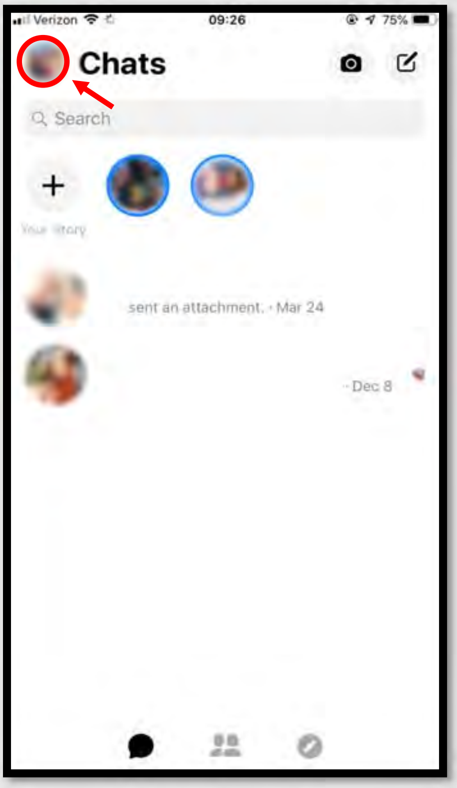
Payments — Manage on Facebook

Blocking — Manage on Facebook

Here you can manage some of the settings associated with your Messenger account, most notably the "Active" status button. If you do not want to allow people to know whether or not you are on Facebook Messenger you can turn off the "Active" status. #keepthemguessing

How many "friends" do you have on Facebook? Would you recognize them if they were standing right in front of you? #FBpurge #whoareyourfbfriends

FACEBOOK SMART CARD



Verizon 09:26 75%

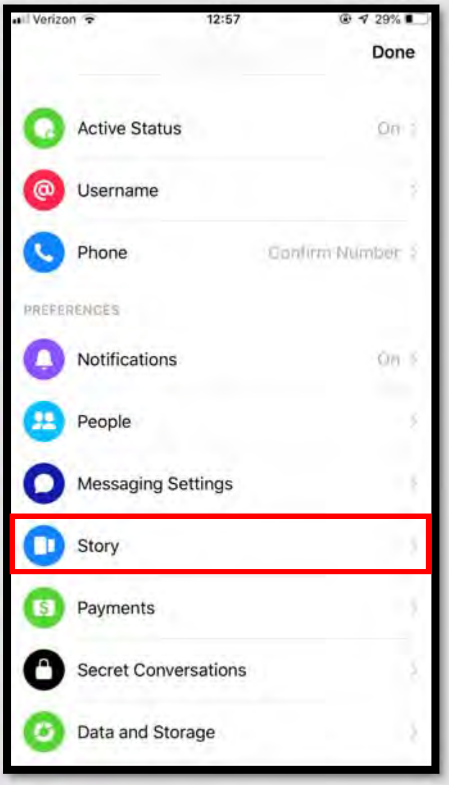
Chats

Search

Your Story

sent an attachment. · Mar 24

· Dec 8



Verizon 12:57 29%

Done

Active Status On

Username

Phone Confirm Number

PREFERENCES

Notifications On

People

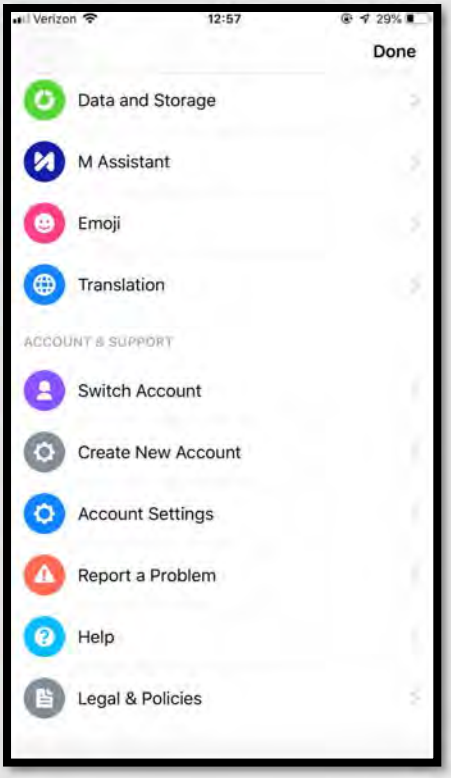
Messaging Settings

Story

Payments

Secret Conversations

Data and Storage



Verizon 12:57 29%

Done

Data and Storage

M Assistant

Emoji

Translation

ACCOUNT & SUPPORT

Switch Account

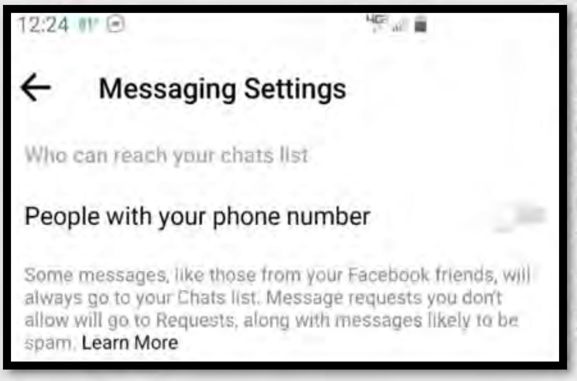
Create New Account

Account Settings

Report a Problem

Help

Legal & Policies



12:24

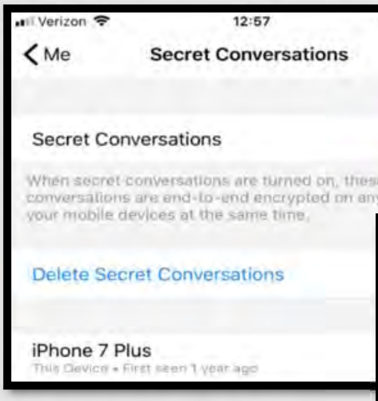
Messaging Settings

Who can reach your chats list

People with your phone number

Some messages, like those from your Facebook friends, will always go to your Chats list. Message requests you don't allow will go to Requests, along with messages likely to be spam. Learn More

In order to accurately lock down your Facebook, you will need to also review your Messenger App. Once logged in, head to the top left of the screen select the picture icon (highlighted here in red). Here you can review all of the additional settings Messenger has to offer. You can chose whether or not you want people to know when you are "Active" on Messenger by selecting the "Active Status" and turning it "off." Next scroll down to the "Messaging Settings" where you can select who can and cannot reach you via Facebook Messenger. It is recommended that you not allow "others you're not connected to" contact you via Messenger.



Verizon 12:57 29%

Me Secret Conversations

Secret Conversations

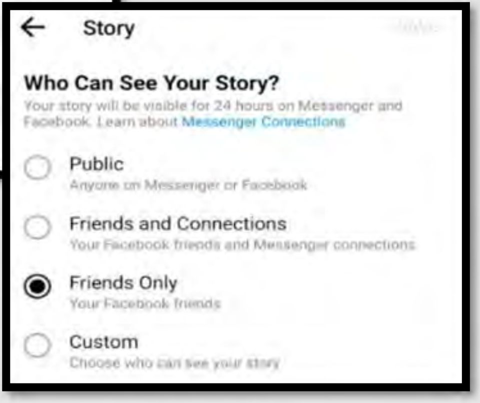
When secret conversations are turned on, these conversations are end-to-end encrypted on any or all of your mobile devices at the same time.

Delete Secret Conversations

iPhone 7 Plus

This Device • First seen 1 year ago

Facebook Messenger has a new feature called "Secret Conversations" where you conversations are encrypted end-to-end. To turn this feature on Go back to your settings and select "Secret Conversations" where you will then be able to turn the feature on. If you have children that use Facebook Messenger it is important to know about this feature so you can monitor it as you see fit.



Story

Who Can See Your Story?

Your story will be visible for 24 hours on Messenger and Facebook. Learn about Messenger Connections

○ Public
Anyone on Messenger or Facebook

○ Friends and Connections
Your Facebook friends and Messenger connections

● Friends Only
Your Facebook friends

○ Custom
Choose who can see your story

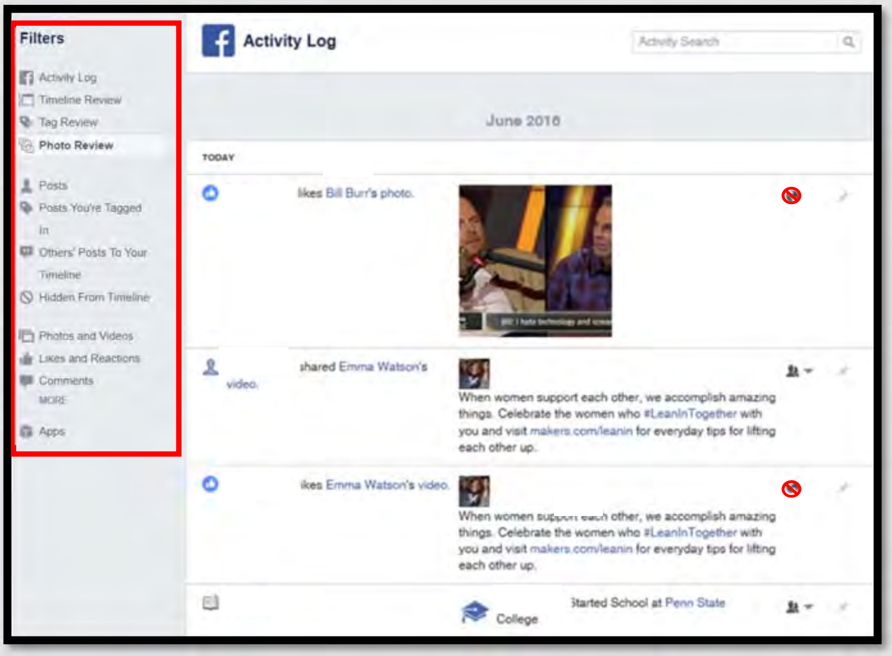
Also, located in the "Settings" section of your Facebook Messenger select "Story" (shown above highlighted in red). This is another location where you can set the settings for your Stories on Facebook. It is recommended that you only allow your friends to see your "Story".

Remember, it is important to lock down your Facebook Messenger the same way you lock down the rest of your Facebook.

UPDATED DEC 2019

FACEBOOK SMART CARD

Finally, lets go back to Facebook's **Activity Log**, accessed from the upper panel of your **Timeline.** The **Activity Log** allows users' to review any click of the button (photos, comments, Likes, posts, etc.) or tag that has ever occurred and been associated with that users profile. It's essentially your one stop shop for cleaning up your entire Facebook profile.



likes Bill Burr's photo.

shared Emma Watson's video.

When women support each other, we accomplish amazing things. Celebrate the women who #LeanInTogether with you and visit makers.com/leanin for everyday tips for lifting each other up.

likes Emma Watson's video.

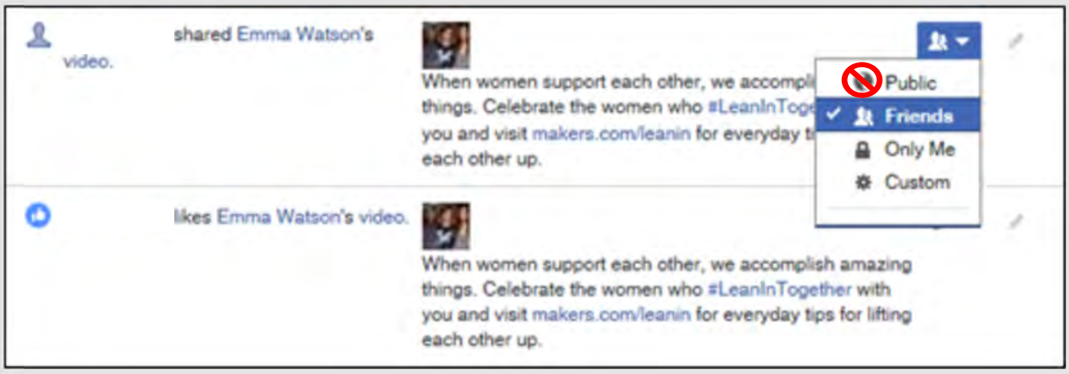
When women support each other, we accomplish amazing things. Celebrate the women who #LeanInTogether with you and visit makers.com/leanin for everyday tips for lifting each other up.

Started School at Penn State

College

More specifically, from the **Activity Log**, users are able review information by date, all the way from the creation of the profile to the present. Users can also see if a post is viewable to the public or just to friends, as well as review any and all posts they have been tagged in. Finally, the **Activity Log** also allows users to remove any actions they have taken on Facebook and decide whether or not to remove a tag of themselves that someone else may have posted.

You can limit each post's visibility by setting every one to **Only Me** or **Friends.** Remember if you **Like** or **Comment** on someone's post whose privacy settings are set to **Public** your comment will also be **Public.** You can only set your own privacy settings for your profile and once you reach outside of your profile, you have no control over privacy (yours or anyone else's), so be aware of how others treat their privacy as well.



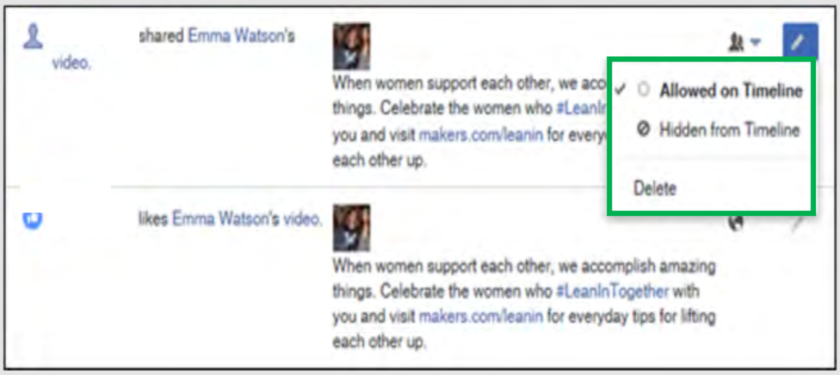
shared Emma Watson's video.

When women support each other, we accompli... things. Celebrate the women who #LeanInTog... you and visit makers.com/leanin for everyday ti... each other up.

likes Emma Watson's video.

When women support each other, we accomplish amazing things. Celebrate the women who #LeanInTogether with you and visit makers.com/leanin for everyday tips for lifting each other up.

You can also choose to **Delete** or **Hide** each post from your Timeline. For other users' posts you have Liked, you can also choose to Unlike them. This will remove the post from your Activity Log and profile.



shared Emma Watson's video.

When women support each other, we acc... things. Celebrate the women who #Leanl... you and visit makers.com/leanin for every... each other up.

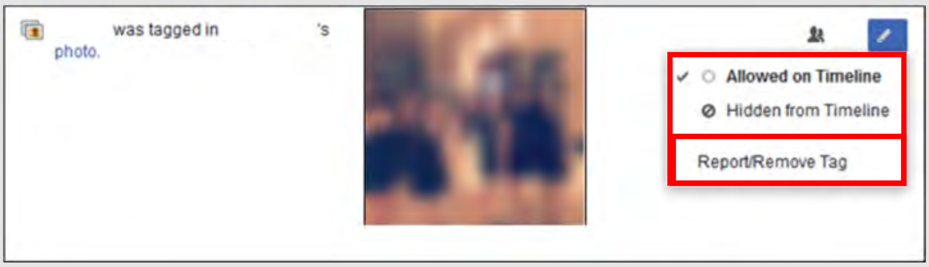
likes Emma Watson's video.

When women support each other, we accomplish amazing things. Celebrate the women who #LeanInTogether with you and visit makers.com/leanin for everyday tips for lifting each other up.

Correcting posts might be tempting, but think about what correcting that post says about you and the information you have access to. #staysafeonfb

FACEBOOK SMART CARD

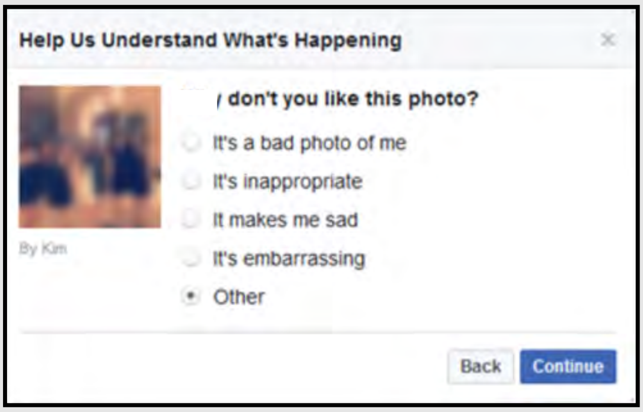
To "**Untag** a photo, click the **Pencil** icon at the top right of the post and select **Report/ Remove Tag**.



was tagged in 's photo.

✓ ○ Allowed on Timeline
⊘ Hidden from Timeline
Report/Remove Tag

Facebook will then ask why you want to Report/Remove the picture or tag. **Note**: If you remove a Tag of yourself, it will NOT notify the individual who owns the post/picture that you have removed the tag.



Help Us Understand What's Happening ×

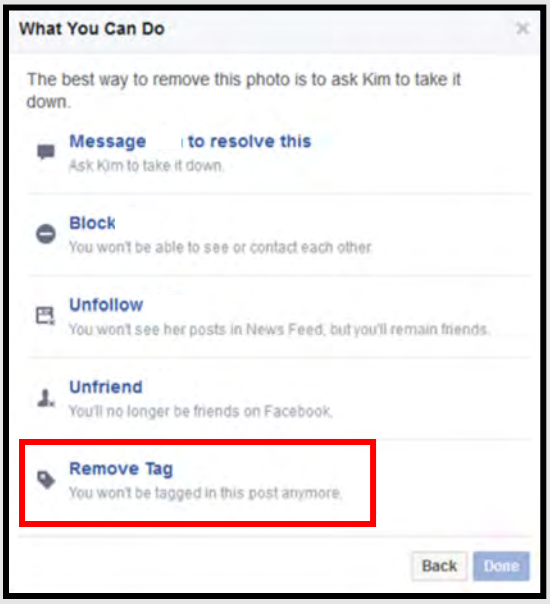
/ don't you like this photo?

○ It's a bad photo of me
○ It's inappropriate
○ It makes me sad
○ It's embarrassing
● Other

By Kim

Back | Continue

You will then be given several options on what you would like to do with the picture/post, including **Remove Tag**. Once you have selected the **Remove Tag** option and are **untagged** from the post/photo, it will no longer appear on your profile.



What You Can Do ×

The best way to remove this photo is to ask Kim to take it down.

Message to resolve this
Ask Kim to take it down.

Block
You won't be able to see or contact each other

Unfollow
You won't see her posts in News Feed, but you'll remain friends.

Unfriend
You'll no longer be friends on Facebook.

Remove Tag
You won't be tagged in this post anymore.

Back | Done

Remember: Although the photo is untagged and no longer on your profile, the photo has ***not*** been deleted from Facebook. It will remain on the profile of the individual who originally posted the photo. *Backdoor avenues* used in finding your profile may still exist (e.g. via a tagged photo of you on your spouse's profile or simply finding your name in the comments of the picture/post).

If you'd like for the photo to be removed, the best way is to ask the individual to **delete** the photo/post.

I think it is important to fortify ourselves online the same way we would fortify our homes if we knew we were under attack.

-II MEF Commanding General LtGen Hedelund's response when asked for his take on social media and force protection.

Don't think you can hide your FB profile by using a different name. Better to assume people can find you and set your privacy/security settings accordingly. #bettersafethansorry

FACEBOOK SMART CARD

Indicators of Possible Account Compromise:

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

- Unexpected posts posted by your account
- Any Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Facebook stating that your account may be compromised
- A notification from Facebook stating that 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 that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- Delete any unwanted posts 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 that you and only you can access your Facebook account
- Be sure to check that your email is secure. It may be worth changing the password to both your Facebook account and the email associated with your Facebook account. *If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

If you need to report **Spam/Harassment**: Go to https://www.facebook.com/help/968185709965912/?helpref=hc_fnav

If your account was hacked: https://www.facebook.com/help/hacked

Also, if you find that someone is impersonating you Facebook: https://www.facebook.com/help/hacked then scroll down to the "Impersonation Accounts" section and follow the directions. If you do not have a Facebook account and want to report an impersonating account go to: https://www.facebook.com/help/contact/295309487309948

To find additional "Security Features and Tips go to: https://www.facebook.com/help/379220725465972?helpref=faq_content

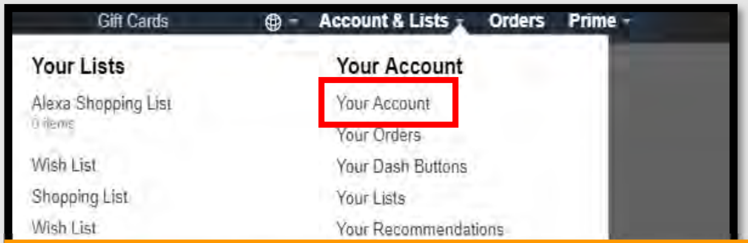
If you still need help or have questions, you can always contact Facebook by: https://www.facebook.com/facebookapp where you can message a Bot Facebook created to help answer questions while they work on building a live customer support capability.

If someone is threatening to share information (ex: messages or photos) on Facebook of your child that they do not want shared you should report it to the local law enforcement. Facebook also says you can do the following: Report the incident to Facebook https://www.facebook.com/help/contact/567360146613371, then make sure that this person is blocked so they no longer have access to your child. It is important to talk to your children about this possibility before they begin to use social media so that they know what to do should this happen to them.

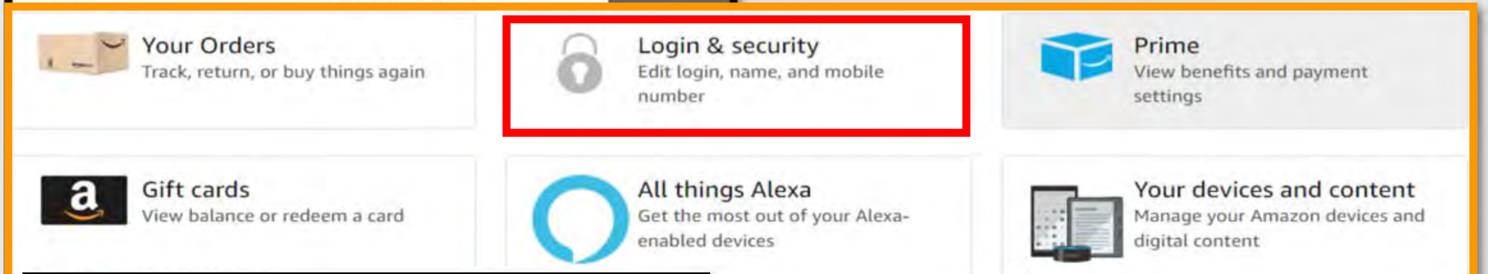
LOCKING DOWN amazon

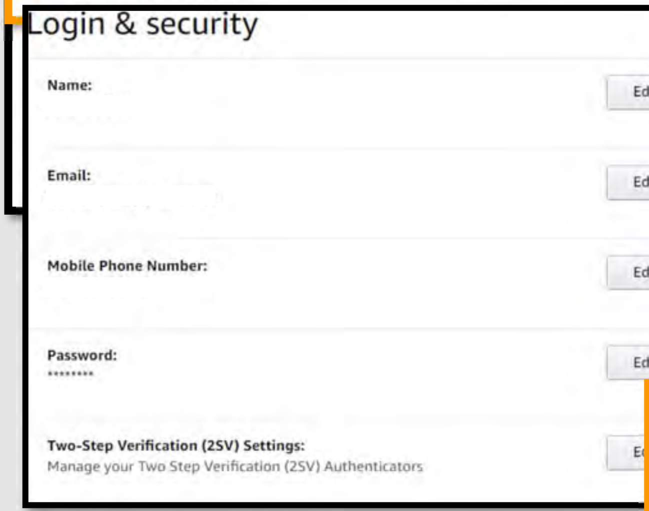
Do's and Don'ts

- 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 vitally important to make sure it is protected by every means available.
- Do frequently update your password for Amazon.
- Do not link any other accounts to your Amazon account to limit what outsiders can find out about you, to include your pattern of life and hobbies.
- Do not fall for scams on Amazon or from emails that appear to be from Amazon.
- Do not buy from international sellers wherever possible to protect yourself from Identity theft and scams.



In order to lock down your Amazon account you will need to access "Your Account," located on the upper right side of your screen. From the "Account & Lists" icon, select the down arrow to expand the menu. From this list, select "Your Account." Let's look at the "Login & Security" settings first.


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 or redeem a card
All things Alexa
Get the most out of your Alexa-enabled devices
Your devices and content
Manage your Amazon devices and digital content



Login & security

Name: Edit

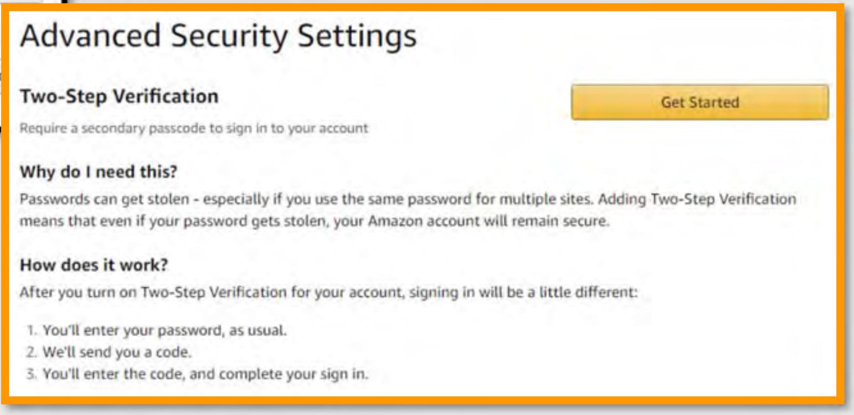
Email: Edit

Mobile Phone Number: Edit

Password: ******** Edit

Two-Step Verification (2SV) Settings:
Manage your Two Step Verification (2SV) Authenticators Ed

The "Login & Security" settings are located at the top of the "Your Account" page (shown above highlighted in red). First, review the general login information provided to ensure its accuracy. Next, head down to the "Two-Step Verification (25V) Settings" section and select "Edit." Here, you can set up "Two-Step Verification" for your Account. It is highly recommended that you enable this to help prevent hacking of your account.



Advanced Security Settings

Two-Step Verification

Get Started

Require a secondary passcode to sign in to your account

Why do I need this?

Passwords can get stolen - especially if you use the same password for multiple sites. Adding Two-Step Verification means that even if your password gets stolen, your Amazon account will remain secure.

How does it work?

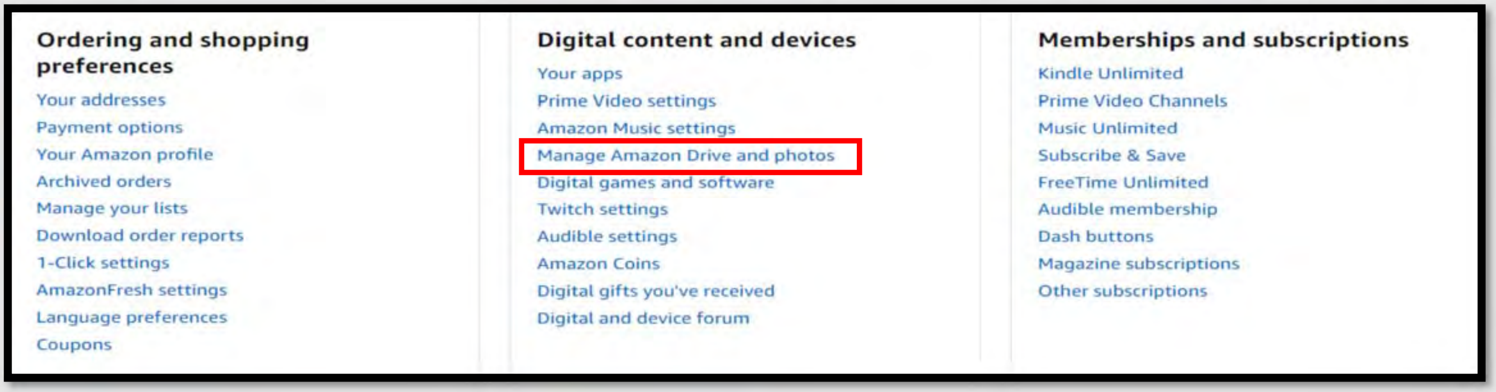
After you turn on Two-Step Verification for your account, signing in will be a little different:

1. You'll enter your password, as usual.
2. We'll send you a code.
3. You'll enter the code, and complete your sign in.

To set-up "Two-Step Authentication" simply select "Get Started" (highlighted in Red to the right) and follow the steps provided. This process is an important feature to help secure your account given the credit card, addresses, and other personal information maintained by Amazon.

Con artists are more sophisticated than ever, targeting unsuspecting consumers with fake online listings, and money-payment scams make sure to protect your information #privacymatters

LOCKING DOWN amazon



Ordering and shopping preferences

Your addresses
Payment options
Your Amazon profile
Archived orders
Manage your lists
Download order reports
1-Click settings
AmazonFresh settings
Language preferences
Coupons

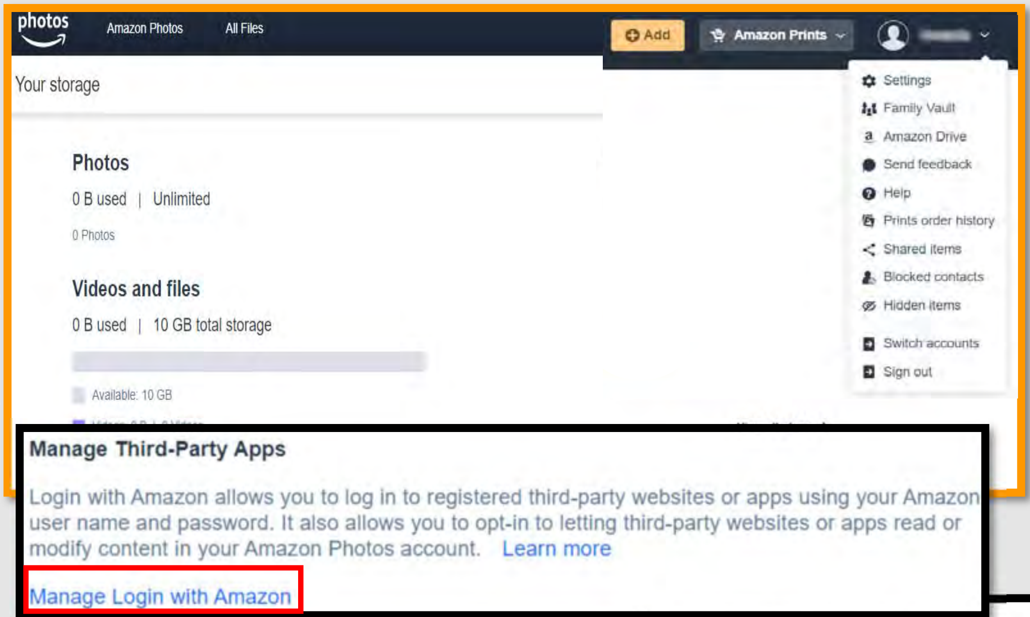
Digital content and devices

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
FreeTime Unlimited
Audible membership
Dash buttons
Magazine subscriptions
Other subscriptions

With each Amazon account comes an "Amazon Drive". In order to lock down your "Amazon Drive," go back to the "Your Account" section (shown on page one), and select " Manage Amazon Drive and Photos." On the left of the screen, select the down arrow to open the "Drive" menu. Next, select "Account Settings" and scroll down to the "Manage Third-Party Apps" section. Once there, select "Manage Login with Amazon." Here you can review any apps you may have logged on to through your Amazon account and if need be, remove accounts you no longer use.



Your storage

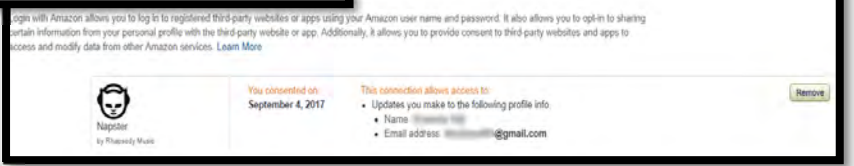
Photos
0 B used | Unlimited
0 Photos

Videos and files
0 B used | 10 GB total storage
Available: 10 GB

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

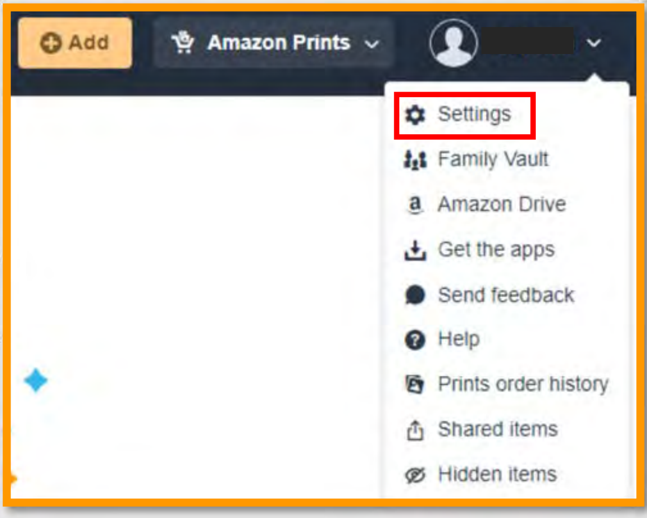


Login with Amazon allows you to log in to registered third-party websites or apps using your Amazon user name and password. It also allows you to opt-in to sharing certain information from your personal profile with the third-party website or app. Additionally, it allows you to provide consent to third-party websites and apps to access and modify data from other Amazon services. Learn More

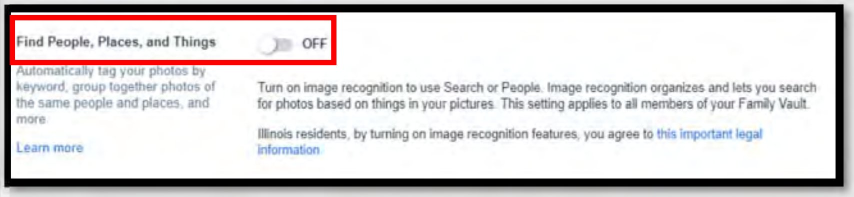
You consented on: September 4, 2017

This connection allows access to:
- Updates you make to the following profile info
  - Name [redacted]
  - Email address [redacted]@gmail.com

Next, go back to the "Amazon Drive" link and from the left hand corner select "Amazon Photos." Once there head to the right side of the window and select the drop down menu.



From the drop down menu select "Settings" and scroll to the middle of the page where you will find the "Find People, Places, and Things" section. This function, when left on allows Amazon image recognition to identify images in your pictures so you can search for them later. It is recommended that you turn this function off to prevent Amazon from collecting additional data on you.



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.

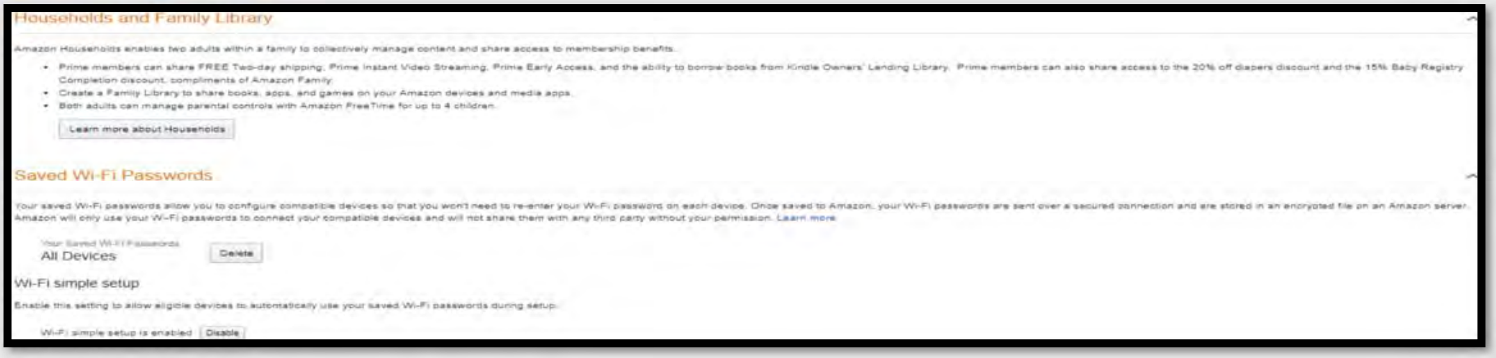
Illinois residents, by turning on image recognition features, you agree to this important legal information.

Don't assume every email you receive is trustworthy, messages may appear to be coming from a legitimate retailer and could include a request for account information. #BeatIdentitytheft

LOCKING DOWN amazon

You can call the customer service department and ask about suspicious emails to see if it's authentic. Whatever you do, don't try to get to Amazon through the suspicious email. #trustbutverify

Now, let's go back to "Your Account" and select "Your devices and content", then select "Change your digital and device settings" section you may want to review the settings below to make sure the content comports with your needs. It is recommended that you review the "Saved Wi-Fi Passwords" to make sure there are no passwords saved that you do not wish Amazon to retain.



Households and Family Library

Amazon Households enables two adults within a family to collectively manage content and share access to membership benefits.

- Prime members can share FREE Two-day shipping, Prime Instant Video Streaming, Prime Early Access, and the ability to borrow books from Kindle Owners' Lending Library. Prime members can also share access to the 20% off diapers discount and the 15% Baby Registry Completion discount, compliments of Amazon Family.
- Create a Family Library to share books, apps, and games on your Amazon devices and media apps.
- Both adults can manage parental controls with Amazon FreeTime for up to 4 children.

Learn more about Households

Saved Wi-Fi Passwords

Your saved Wi-Fi passwords allow you to configure compatible devices so that you won't need to re-enter your Wi-Fi password on each device. Once saved to Amazon, your Wi-Fi passwords are sent over a secured connection and are stored in an encrypted file on an Amazon server. Amazon will only use your Wi-Fi passwords to connect your compatible devices and will not share them with any third party without your permission. Learn more

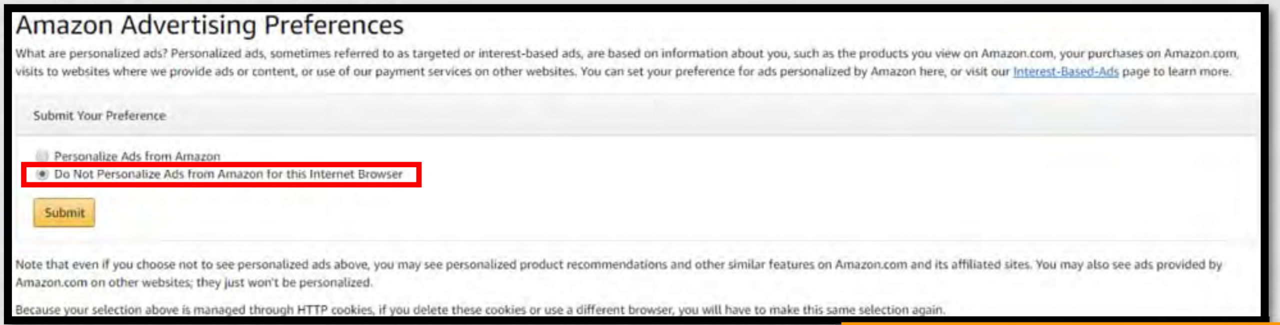
Your Saved Wi-Fi Passwords
All Devices Delete

Wi-Fi simple setup

Enable this setting to allow eligible devices to automatically use your saved Wi-Fi passwords during setup.

Wi-Fi simple setup is enabled Disable

Now let's head 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 based on information about you, such as the products you view or purchases you make on Amazon, or websites you visit where Amazon might provide ads or content.



Amazon Advertising Preferences

What are personalized ads? Personalized ads, sometimes referred to as targeted or interest-based ads, are based on information about you, such as the products you view on Amazon.com, your purchases on Amazon.com, visits to websites where we provide ads or content, or use of our payment services on other websites. You can set your preference for ads personalized by Amazon here, or visit our Interest-Based-Ads page to learn more.

Submit Your Preference

○ Personalize Ads from Amazon
● Do Not Personalize Ads from Amazon for this Internet Browser

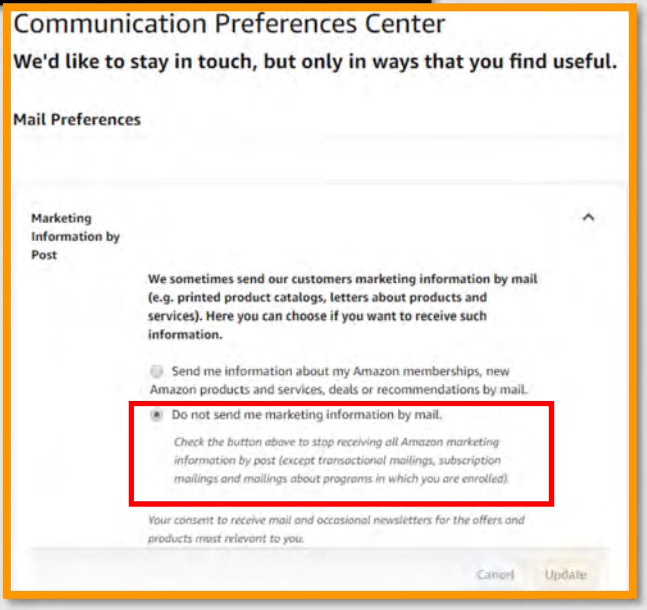
Submit

Note that even if you choose not to see personalized ads above, you may see personalized product recommendations and other similar features on Amazon.com and its affiliated sites. You may also see ads provided by Amazon.com on other websites; they just won't be personalized.

Because your selection above is managed through HTTP cookies, if you delete these cookies or use a different browser, you will have to make this same selection again.

It is recommended you select "Do Not Personalize Ads from Amazon for this Internet Browser." What this does is exactly what it says in the title, but for the current browser only. Amazon has been known to reset your privacy and other settings if it is opened from a browser different from the one used to lock it down originally. It will also reset your settings if you clear your cookies and delete your internet history. This means that you will need to go back into Amazon and make sure your settings are still intact any time you delete cookies and / or clear your browser history.

Now, let's go back to "Your Account" and select "Communication Preferences." From there it is recommended you select "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

We sometimes send our customers marketing information by mail (e.g. printed product catalogs, letters about products and services). Here you can choose if you want to receive such information.

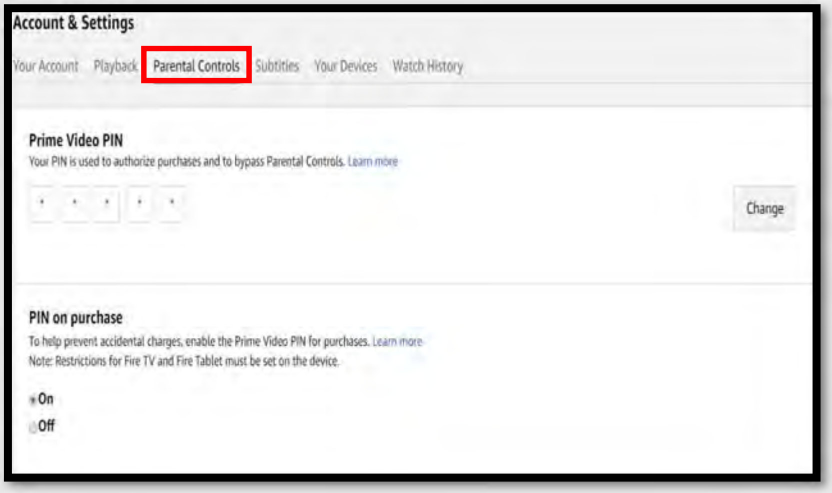
○ Send me information about my Amazon memberships, new Amazon products and services, deals or recommendations by mail.
● Do not send me marketing information by mail.

Check the button above to stop receiving all Amazon marketing information by post (except transactional mailings, subscription mailings and mailings about programs in which you are enrolled).

Your consent to receive mail and occasional newsletters for the offers and products most relevant to you.

Cancel Update

LOCKING DOWN amazon



Account & Settings

Your Account | Playback | Parental Controls | Subtitles | Your Devices | Watch History

Prime Video PIN

Your PIN is used to authorize purchases and to bypass Parental Controls. Learn more

• • • • •   Change

PIN on purchase

To help prevent accidental charges, enable the Prime Video PIN for purchases. Learn more

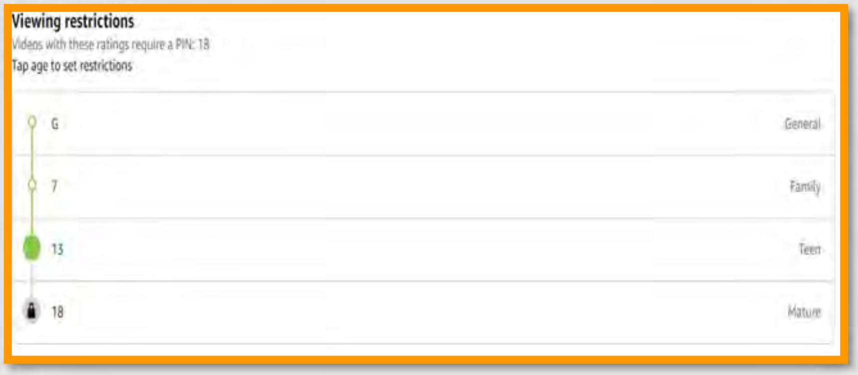
Note: Restrictions for Fire TV and Fire Tablet must be set on the device.

● On

○ Off

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 simply select "Video Settings." Now at the top of the page find and select "Parental Controls" and let's begin. For parents, it is always important to monitor and protect our children from non-age appropriate material on the internet and television screen. Amazon allows parents to set Prime Video PINs and viewing restriction. Settings the restrictions means that any time someone attempts to play a video or other content (depending on the device i.e. The Amazon Fire Stick) they will be required to put in a PIN, which will be designated here by you.

If you scroll down on the "Video Settings" page, you will find the "Viewing restrictions" section. Here you can select at what age rating you would like a PIN to be required. If you scroll even further down, Amazon lists other Amazon devices (as shown below) that require parental controls be set separately. These settings are inherent to and accessed from the devices themselves.

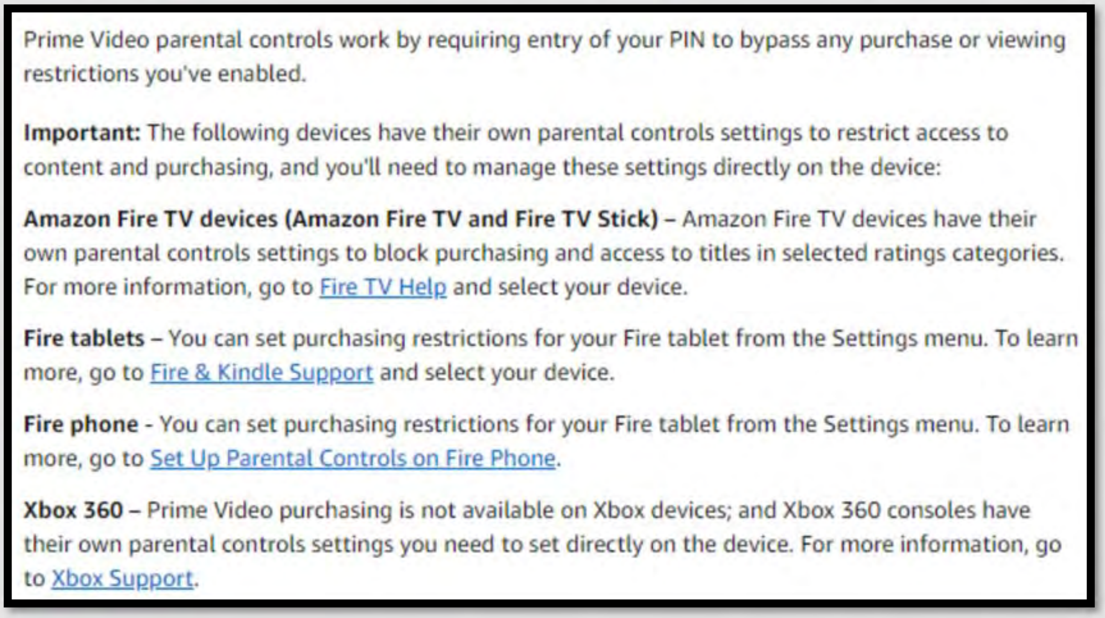


Viewing restrictions

Videos with these ratings require a PIN: 18

Tap age to set restrictions

G	General
7	Family
13	Teen
18	Mature



Prime Video parental controls work by requiring entry of your PIN to bypass any purchase or viewing restrictions you've enabled.

Important: The following devices have their own parental controls settings to restrict access to content and purchasing, and you'll need to manage these settings directly on the device:

Amazon Fire TV devices (Amazon Fire TV and Fire TV Stick) – Amazon Fire TV devices have their own parental controls settings to block purchasing and access to titles in selected ratings categories. For more information, go to Fire TV Help and select your device.

Fire tablets – You can set purchasing restrictions for your Fire tablet from the Settings menu. To learn more, go to Fire & Kindle Support and select your device.

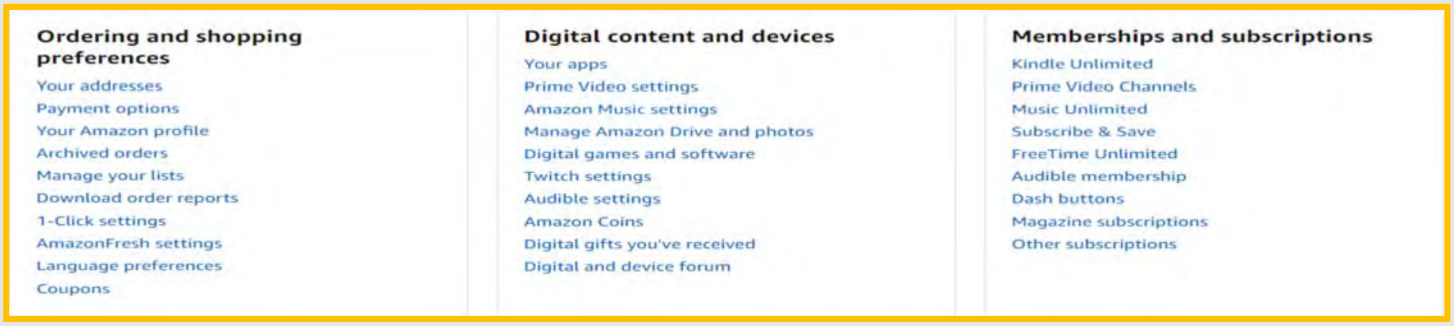
Fire phone - You can set purchasing restrictions for your Fire tablet from the Settings menu. To learn more, go to Set Up Parental Controls on Fire Phone.

Xbox 360 – Prime Video purchasing is not available on Xbox devices; and Xbox 360 consoles have their own parental controls settings you need to set directly on the device. For more information, go to Xbox Support.

It is highly recommended that you take time to review each device you may own and set the parental controls according to your preferences. This is even more important for the Xbox and other gaming devices. These types of devices, if parental controls are not set, allow users to interact with others and purchase items utilizing the credit card on file.

If you need to contact Amazon's customer service make sure to find the number from the Official Amazon site. Searching for it online could lead to you providing information to a fake call center.

LOCKING DOWN amazon

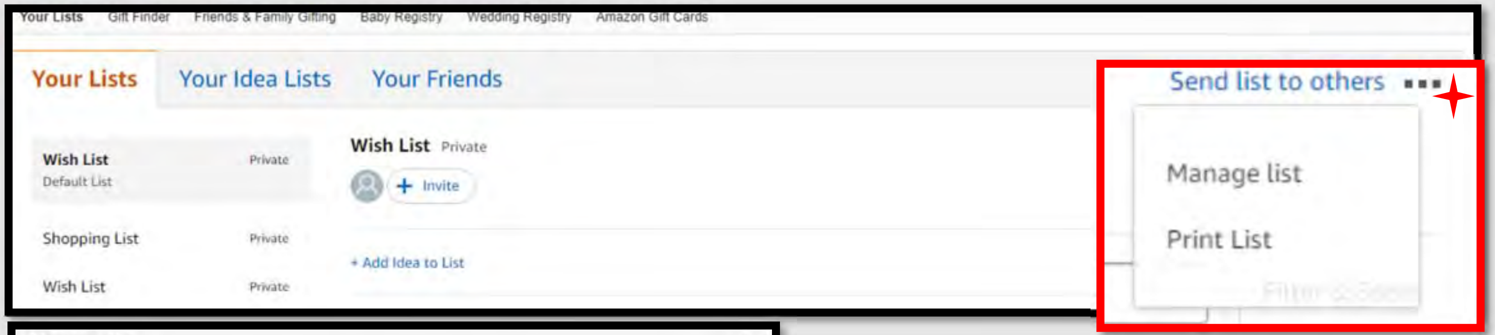


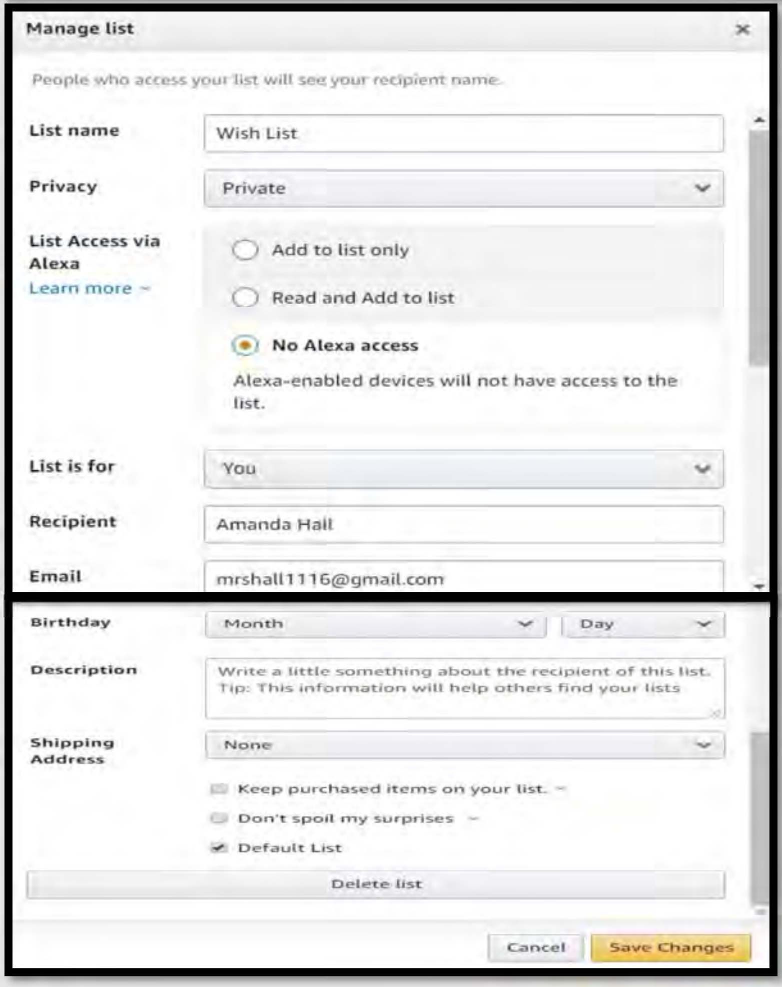
Ordering and shopping preferences
Your addresses
Payment options
Your Amazon profile
Archived orders
Manage your lists
Download order reports
1-Click settings
AmazonFresh settings
Language preferences
Coupons

Digital 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
FreeTime Unlimited
Audible membership
Dash buttons
Magazine subscriptions
Other subscriptions

Moving on, go back to "Your Account" and review the following sections: "Ordering and shopping preferences;" "Other accounts;" and "Shopping programs and rentals."





Manage list ×

People who access your list will see your recipient name.

List name	Wish List
Privacy	Private
List Access via Alexa Learn more	○ Add to list only ○ Read and Add to list ● No Alexa access Alexa-enabled devices will not have access to the list.
List is for	You
Recipient	Amanda Hall
Email	mrshall1116@gmail.com
Birthday	Month / Day
Description	Write a little something about the recipient of this list. Tip: This information will help others find your lists
Shipping Address	None

□ Keep purchased items on your list.
□ Don't spoil my surprises
☑ Default List

Delete list

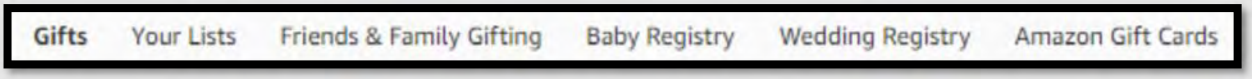
Cancel | Save Changes

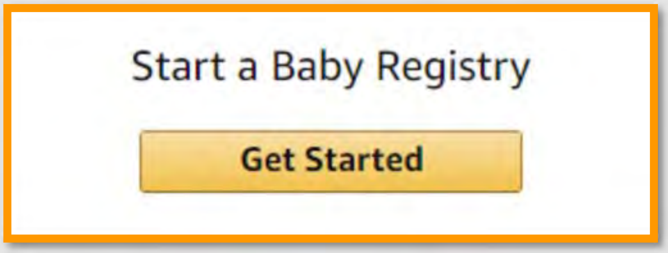
One of the most public sections of Amazon are the "Wish Lists." If not made private, anyone can view your list(s) and gain or infer information about who you are or who the people in your family are (How many, gender, age, etc.). Many times, you may find yourself making Christmas lists, birthday lists, or even grocery lists. The titles of these lists are usually specific (i.e. a child's name for a birthday or Christmas list). These small tid bits of information could be extremely useful to a Social Engineer or identity thief when combined with other bits of data on you. It is important to note that Amazon has changed their privacy for "Wish Lists," a User now needs 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 or not, Alexa with access to your "Lists," it is not recommended that you provide such access but instead continue to lock down and privatize each list.

Select "Manage your list" from "Ordering and Shopping Preferences" in order to begin the process of locking down any of these lists you may have. 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 ellipse (as shown above in Red), and select "Manage List." From there, select "Privacy" and select "Private" from the list. Be sure to select "Save Changes."

If you see a product that is listed way below market value, don't hand over your credit card info right away. If it's too good to be true it very like is. #themoreyouknow

LOCKING DOWN amazon



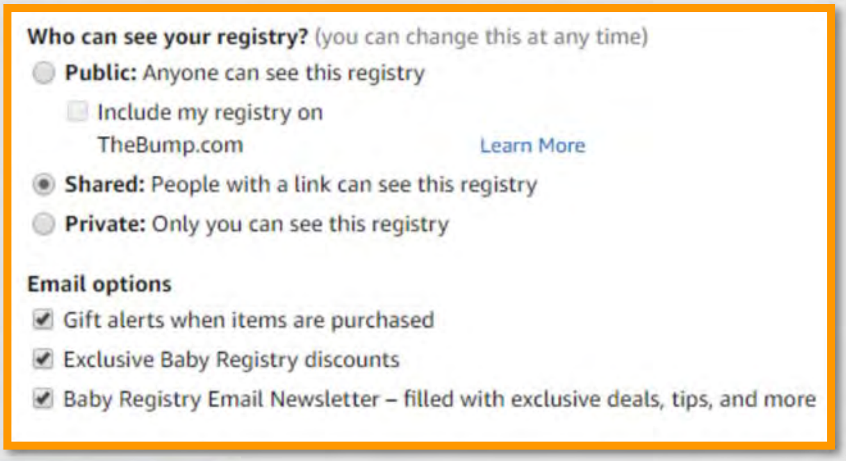


Start a Baby Registry

Much like a "Wish List", your registries can also be displayed publically unless you say otherwise. While still in your "Wish List", go to the top menu and select "Baby Registry." To create your Registry select "Get Started" from the center of your page. Scroll down to the "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 also be included on a third party website, TheBump unless you unselect that option.

If you have already created a Baby Registry, you simply need to go to the "Registry Settings" and change the Privacy from there. It is also important to remember to delete any Registries you use when they are no longer needed.

Your "Wedding Registry" is equally important to lock down. Think about every-thing that goes into a Wedding Registry, what it might say about a couple, and how beneficial that information could prove to an identity thief.



Who can see your registry? (you can change this at any time)

○ **Public:** Anyone can see this registry

□ Include my registry on TheBump.com Learn More

● **Shared:** People with a link can see this registry

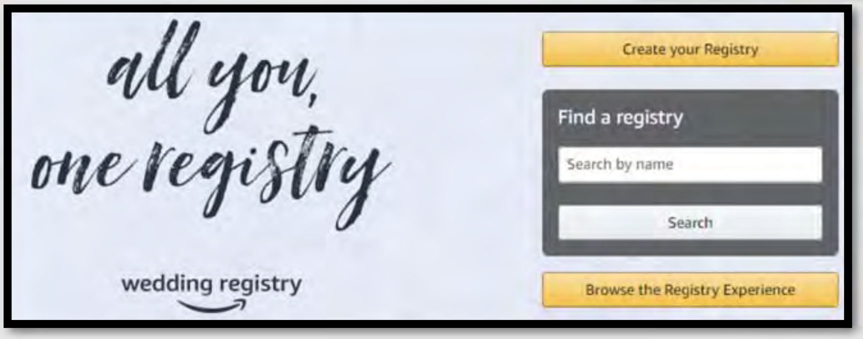
○ **Private:** Only you can see this registry

Email options

☑ Gift alerts when items are purchased

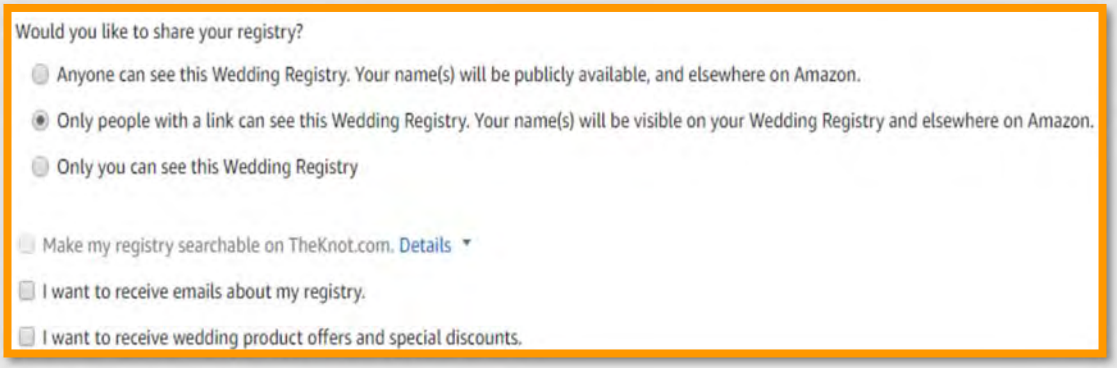
☑ Exclusive Baby Registry discounts

☑ Baby Registry Email Newsletter – filled with exclusive deals, tips, and more



In order to lock down your Wedding Registry, go back to the "Wish List" menu and select "Wedding Registry." From there, scroll to the middle and select the appropriate privacy settings for your Registry. It is recommended that you not make your Registry "Public" and remember that once you no longer need the registry, be sure to delete it.

Like the "Baby Registry," the "Wedding Registry" may also be listed on a third party vendor, TheKnott.com. It is recommended that you not make your registry searchable on The-Knott.com



Would you like to share your registry?

○ Anyone can see this Wedding Registry. Your name(s) will be publicly available, and elsewhere on Amazon.

● Only people with a link can see this Wedding Registry. Your name(s) will be visible on your Wedding Registry and elsewhere on Amazon.

○ Only you can see this Wedding Registry

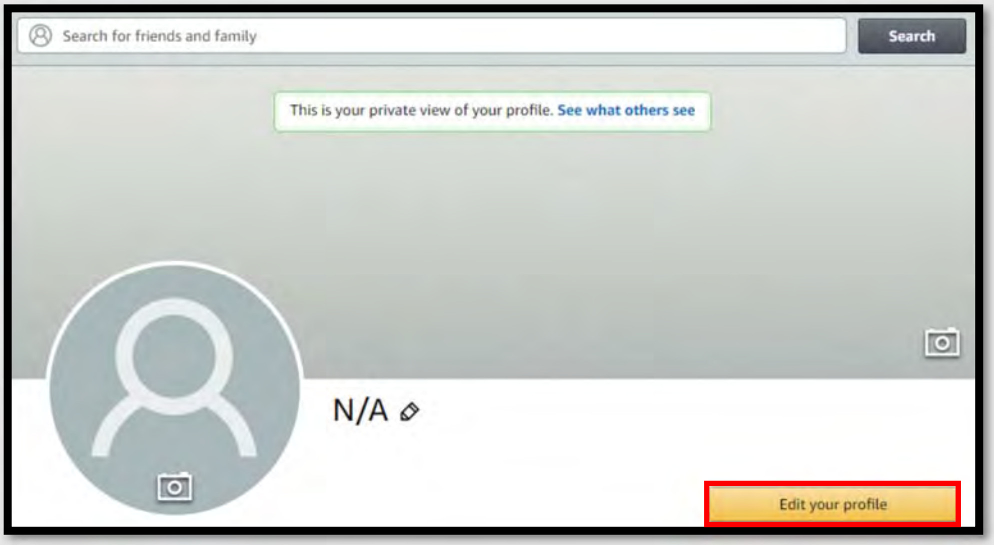
□ Make my registry searchable on TheKnot.com. Details ▾

□ I want to receive emails about my registry.

□ I want to receive wedding product offers and special discounts.

Keep all communication and transactions on Amazon, that way if you do happen to be scammed, Amazon can track the scam and all correspondences. #cyberfraud

LOCKING DOWN amazon

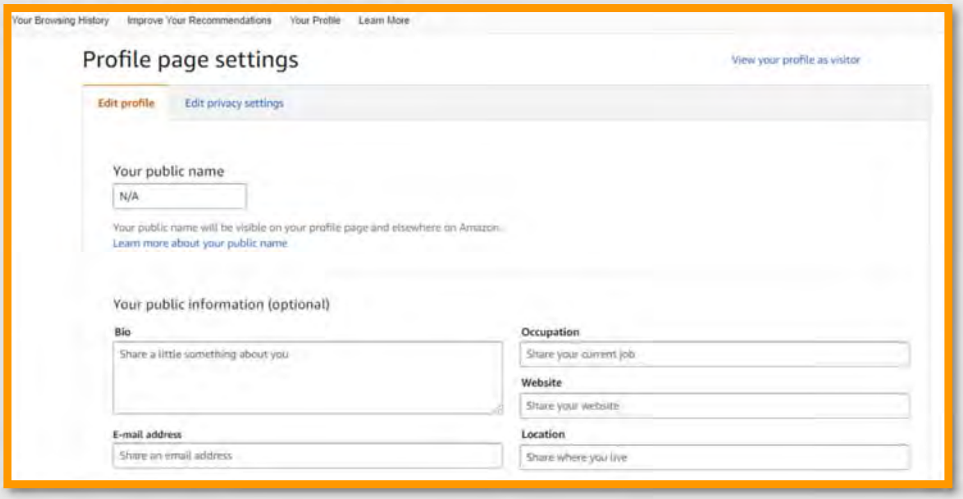


This is your private view of your profile. See what others see

What most people do not realize about Amazon is that it comes with your own public profile. This profile and your entire Amazon account can be linked to any of your social media accounts. It is therefore 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.

In order to lock down your Amazon account, go back to "Your Account" and select "Your Amazon Profile." From there, follow the steps below and on the remaining pages to best secure your profile.

Now let's begin the process of making sure your "Profile" is locked down. Select "Edit your profile" as shown above in **red**. In the "Profile page settings" review, all of your information to make sure, only information you want on public profile is filled in. It is recommended that you not display your full name in the "Your public name" section.



Profile page settings

Your public name

N/A

Your public name will be visible on your profile page and elsewhere on Amazon.
Learn more about your public name

Your public information (optional)

Bio: Share a little something about you

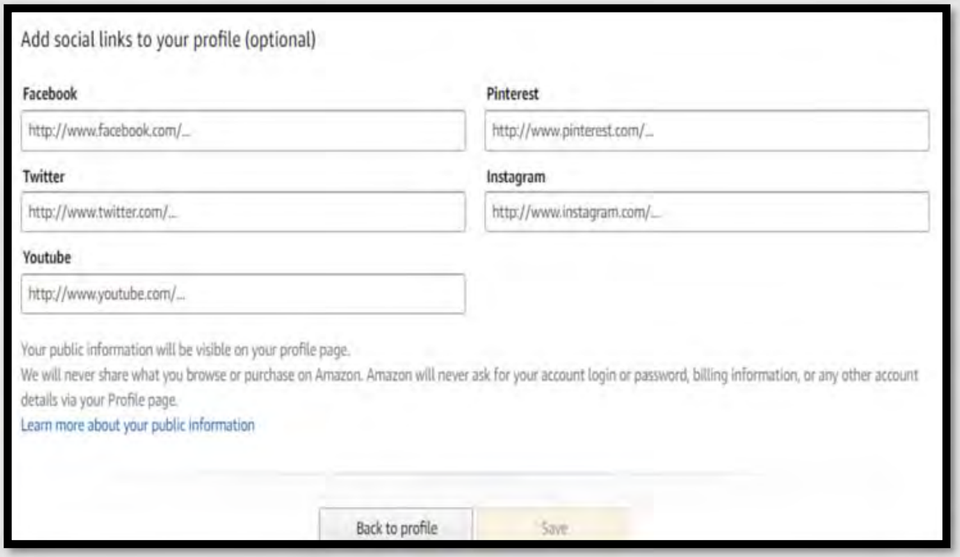
Occupation: Share your current job

Website: Share your website

E-mail address: Share an email address

Location: Share where you live

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. Amazon is a great place to shop for just about anything, and as such it becomes a picture of who you are and who your family might be. This includes any product reviews you may post on Amazon. It is recommended that if you do review products that you try not to put any personal in-formation inside your review.



Add social links to your profile (optional)

Facebook: http://www.facebook.com/...

Pinterest: http://www.pinterest.com/...

Twitter: http://www.twitter.com/...

Instagram: http://www.instagram.com/...

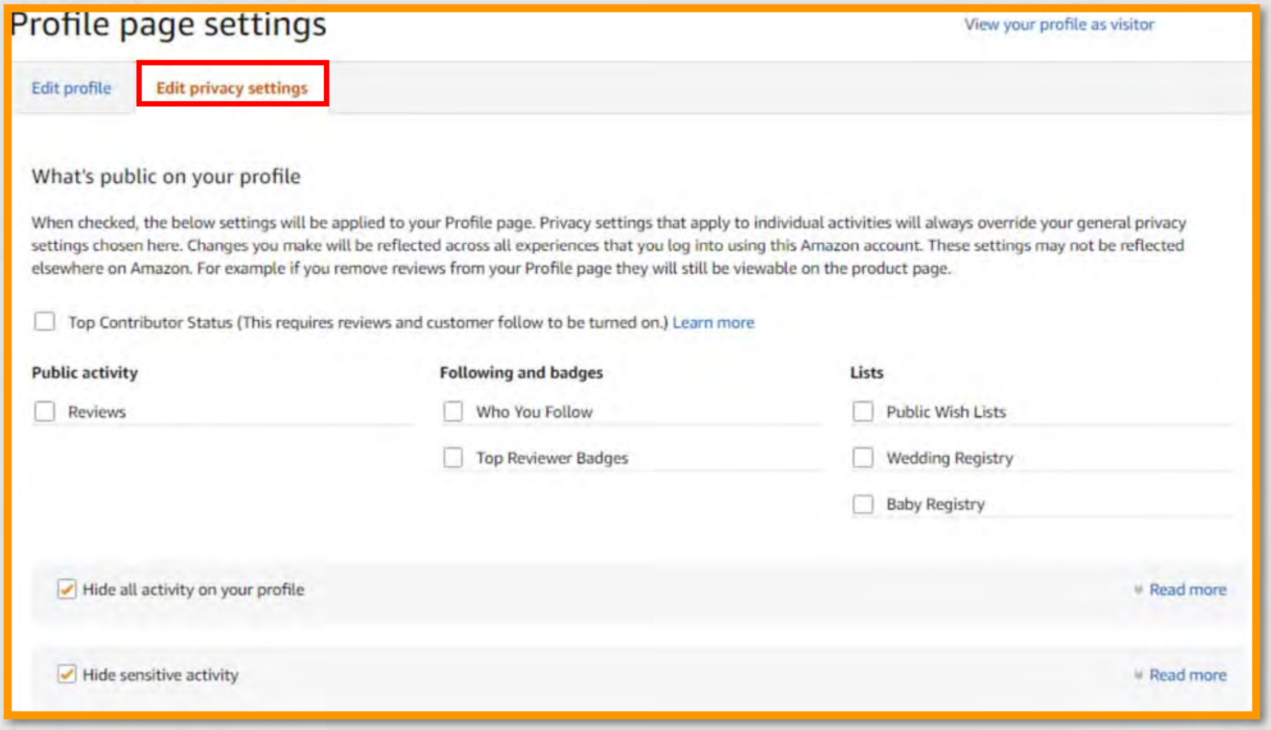
Youtube: http://www.youtube.com/...

Your public information will be visible on your 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 Profile page.
Learn more about your public information

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. #themoreyouknow

LOCKING DOWN amazon

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



Profile page settings

View your profile as visitor

Edit profile | Edit privacy settings

What's public on your profile

When checked, the below settings will be applied to your 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 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

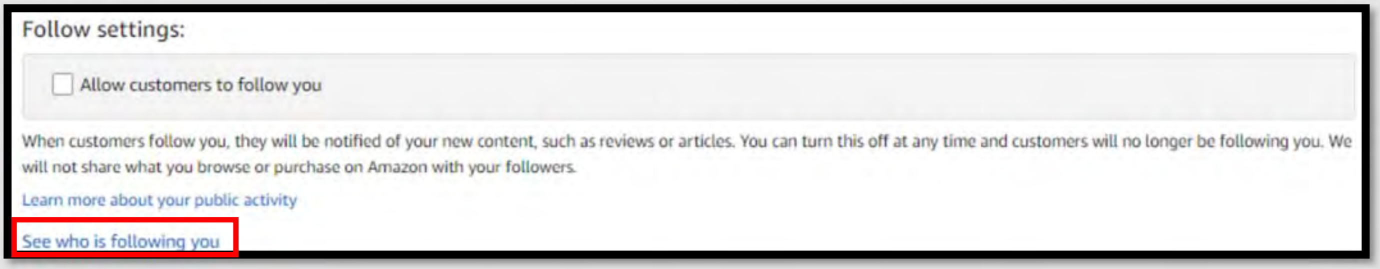
Public activity	Following and badges	Lists
☐ Reviews	☐ Who You Follow	☐ Public Wish Lists
	☐ Top Reviewer Badges	☐ Wedding Registry
		☐ Baby Registry

☑ Hide all activity on your profile — Read more

☑ Hide sensitive activity — Read more

Let's now go to the "Edit privacy settings" to review and make sure they are set. Select "Edit privacy settings" (see above) to review how they are presently configured. It is recommended that you select the box "Hide all activity on your profile" as well as "Hide sensitive activity."

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.



Follow settings:

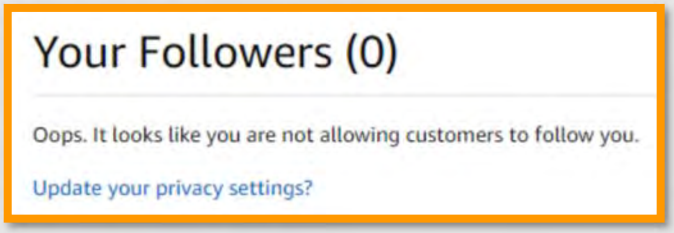
☐ Allow customers to follow you

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.

Learn more about your public activity

See who is following you

If you have any followers, you can delete / remove them from this link and then update your privacy settings as shown above to preclude any other followers. It is not recommended that you allow people to follow you on Amazon, but especially if you do not know them.



Your Followers (0)

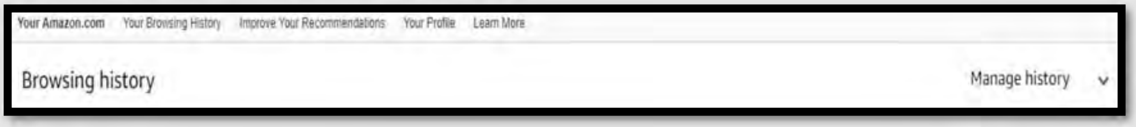
Oops. It looks like you are not allowing customers to follow you.

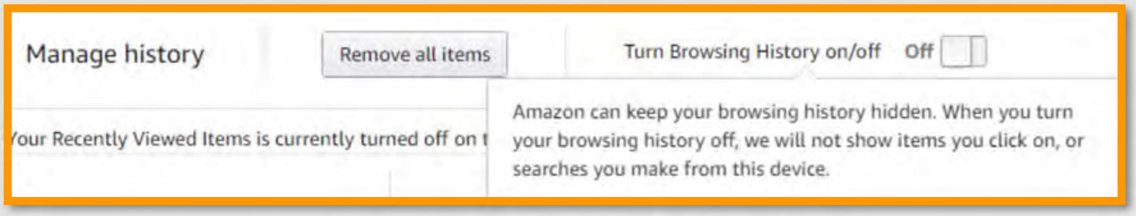
Update your privacy settings?

LOCKING DOWN

amazon

Now let's take a look at your Browsing history. Simply go to the top menu bar, from either the "Your Profile" section or 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 recommend you remove all items and "Turn Browsing History" to "off."

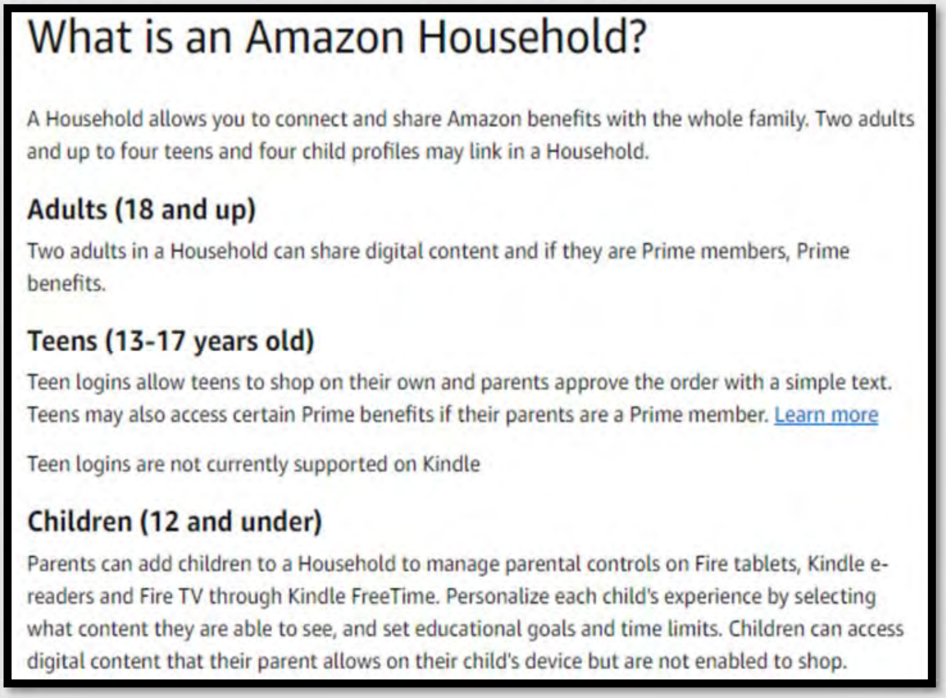




Your Recently Viewed Items is currently turned off on t

Amazon can keep your browsing history hidden. When you turn your browsing history off, we will not show items you click on, or searches you make from this device.

Amazon has many 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, but the parents maintain control over any 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.



What is an Amazon Household?

A Household allows you to connect and share Amazon benefits with the whole family. Two adults and up to four teens and four child profiles may link in a Household.

Adults (18 and up)

Two adults in a Household can share digital content and if they are Prime members, Prime benefits.

Teens (13-17 years old)

Teen logins allow teens to shop on their own and parents approve the order with a simple text. Teens may also access certain Prime benefits if their parents are a Prime member. Learn more

Teen logins are not currently supported on Kindle

Children (12 and under)

Parents can add children to a Household to manage parental controls on Fire tablets, Kindle e-readers and Fire TV through Kindle FreeTime. Personalize each child's experience by selecting what content they are able to see, and set educational goals and time limits. Children can access digital content that their parent allows on their child's device but are not enabled to shop.

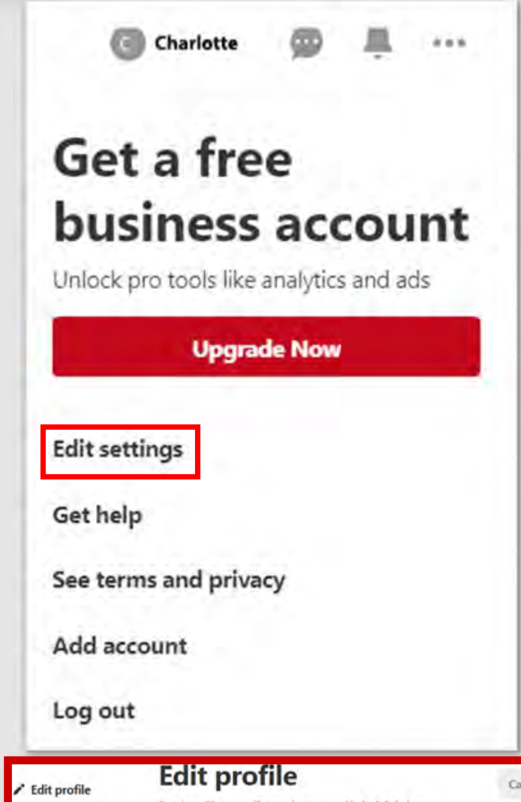
Ships from and sold by Amazon.com: This is the real deal and almost certainly not a scam of any kind. #themoreyouknow #beatidentitytheft

LOCKING DOWN

Pinterest

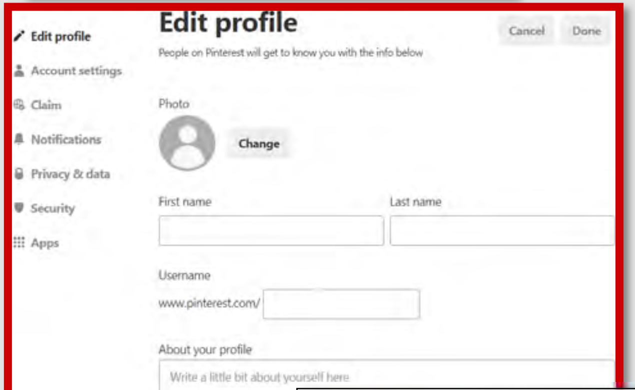
Do's and Don'ts

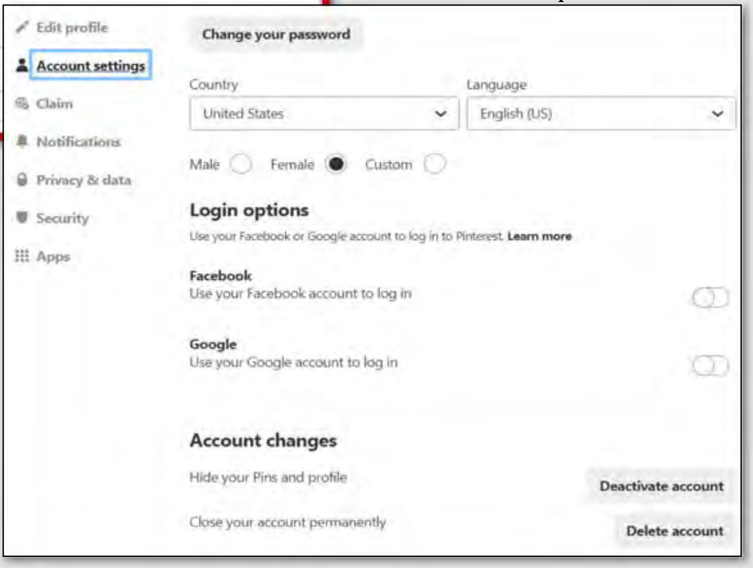
- Do use Two-Factor Authentication to protect all your information. Like all other social media accounts, it is important to make sure your Pinterest is as secured as possible. Two-Factor Authentication is one of the best ways to control your information.
- Do make sure your email is up to date! If Pinterest 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 not 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.).
- Do not forget it is highly recommended that you 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 not forget to make your boards private once you create them so that they are not searchable by any and all Pinners.



While there aren't many privacy settings to manage on Pinterest, it is no less important to ensure those settings are locked down. In order to change your Pinterest settings look to the top right of your screen and select the horizontal ellipsis to expand the menu. It is recommended you make your account private by selecting "Search privacy" (highlighted below). Once you are in the "Edit Settings" page you will be able to go through each of the settings provided by Pinterest. The first settings to review are the "Edit settings," which provides your basic information on Pinterest. It is recommended that you do not include your "location" when building your Pinterest Profile.

Under "Account settings" you will find the options to delete or deactivate your account in case you decide you no longer want to use your Pinterest. Here you can also chose (or not) the option to login from other social networking accounts. This step is highly discouraged, it is instead recommended that you login to your Pinterest with only your Pinterest username and password.





Country: United States

Language: English (US)

Male ○ Female ● Custom ○

Login options

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

Facebook
Use your Facebook account to log in

Google
Use your Google account to log in

Account changes

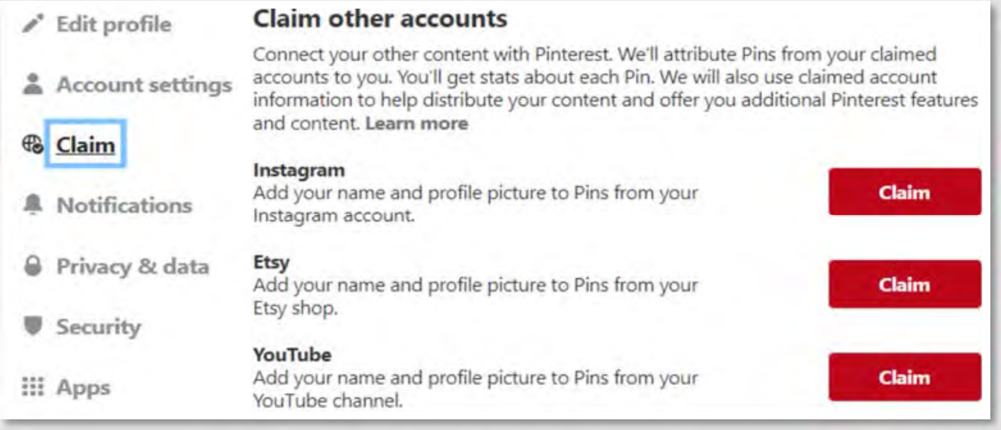
Hide your Pins and profile — Deactivate account

Close your account permanently — Delete account

Check your credit report at least once a year. You may also want to check your credit report if you feel any of your social media accounts have been compromised. #beatidentitytheft

LOCKING DOWN

Pinterest



Claim other accounts

Connect your other content with Pinterest. We'll attribute Pins from your claimed accounts to you. You'll get stats about each Pin. We will also use claimed account information to help distribute your content and offer you additional Pinterest features and content. **Learn more**

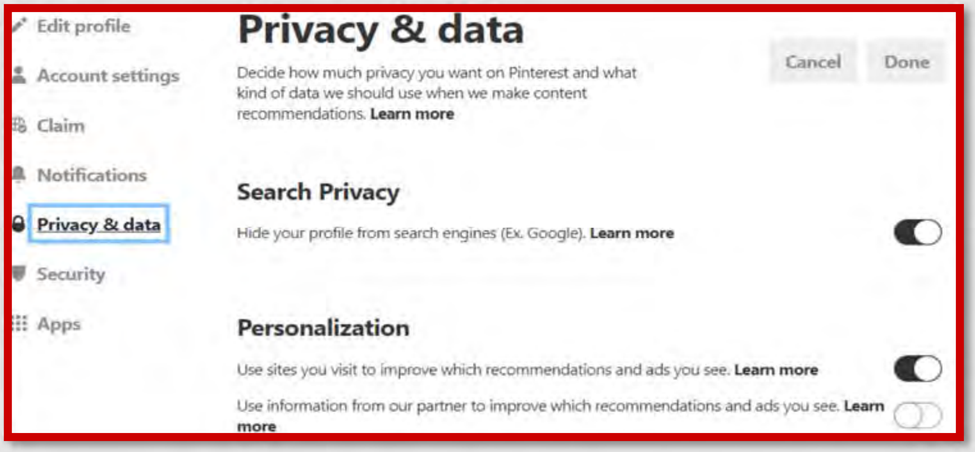
Instagram
Add your name and profile picture to Pins from your Instagram account.

Etsy
Add your name and profile picture to Pins from your Etsy shop.

YouTube
Add your name and profile picture to Pins from your YouTube channel.

The next few settings have to do with linking (or not) your other social media accounts to Pinterest. **As always, it is highly recommended that you do not link any other social media accounts to each other.** If by some possibility someone was able to access, one of your social media accounts, not linking your accounts together prevents an intruder from accessing all your other accounts.

Next, continue down the screen to find "Privacy & data" and review the settings. These settings will help to limit what Pinterest Ads gather about you. It is recommended here that you do not enable these settings and allow Pinterest to push ads based on other internet habits of yours.



Privacy & data

Decide how much privacy you want on Pinterest and what kind of data we should use when we make content recommendations. **Learn more**

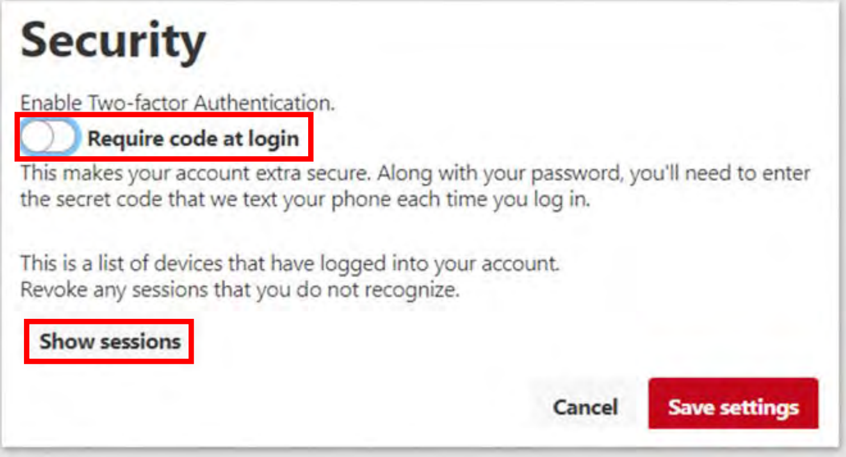
Search Privacy

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 partner to improve which recommendations and ads you see. **Learn more**



Security

Enable Two-factor Authentication.

○ **Require code at login**

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.

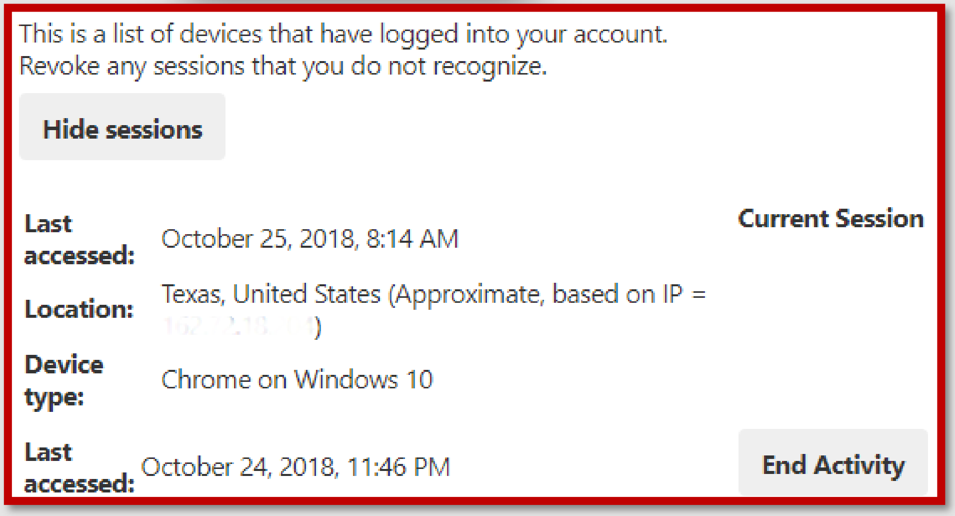
This is a list of devices that have logged into your account. Revoke any sessions that you do not recognize.

Now, let's ensure that you enable Two-Factor Authentication. As recommended for all your accounts, it is highly recommended that you enable Two-Factor Authentication. This will help to ensure you have taken all steps to secure your account and keep it safe.

Below, highlighted in **red**, you will see a smaller section labeled "Show Sessions" which will be discussed on the next page.

Make sure your antivirus and antimalware software stays up to date. Keeping software up to date helps to prevent advanced malware and viruses from affecting your computer.

LOCKING DOWN Pinterest



This is a list of devices that have logged into your account. Revoke any sessions that you do not recognize.

Hide sessions

Current Session

Last accessed: October 25, 2018, 8:14 AM

Location: Texas, United States (Approximate, based on IP = [redacted])

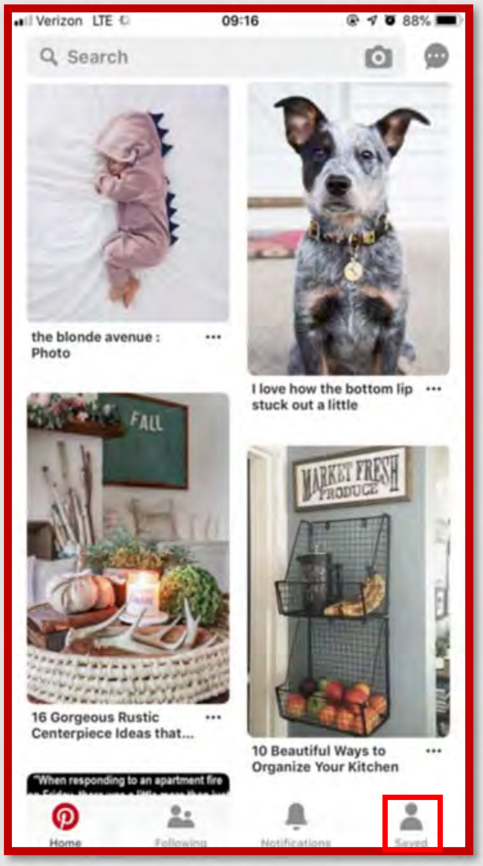
Device type: Chrome on Windows 10

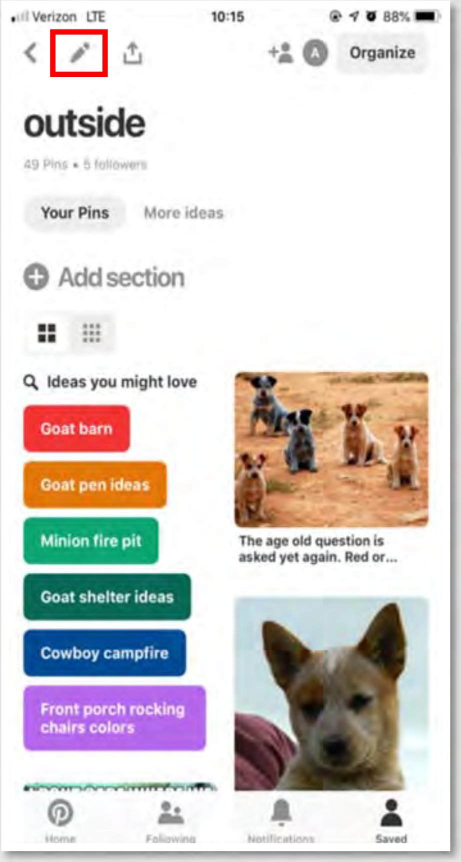
Last accessed: October 24, 2018, 11:46 PM

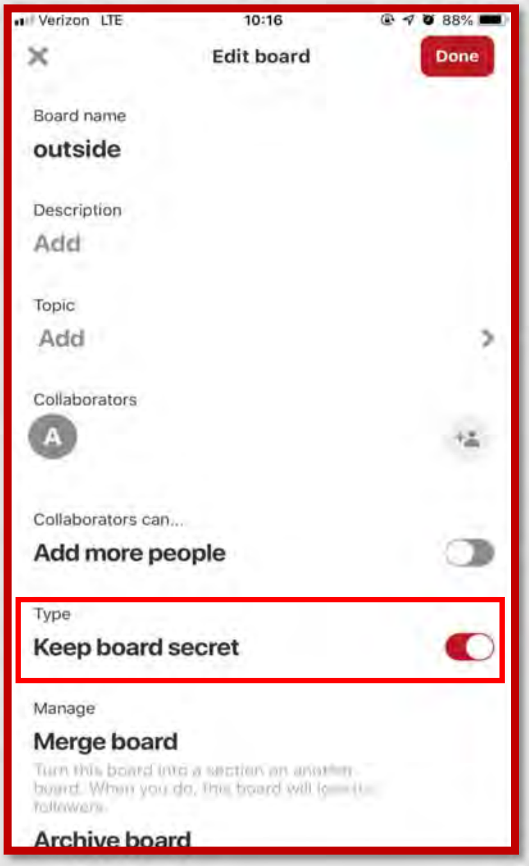
End Activity

After selecting "Show Sessions" directly under the "Two-Factor Authentication" section, you will be provided the opportunity to "End Activity" for all sessions that may seem suspicious or that you do not see a need to be active any longer. If you suspect that your Pinterest account may have been compromised, the "Show Sessions" section may help you to identify the account and "End Activity" so that you can then secure your account and change your password. It is a good idea periodically, to go through the "Show Sessions" section to make sure nothing looks suspicious and end older activity.

Lastly, let's look at your boards and make sure that there isn't too much, if any, information available for others to see. In order to review or to lock down your boards via your smart device, head to the bottom of your screen, select "saved," and then select a board to review and edit. Once you are inside the board, look to the top and find the "pencil" icon, and select it to edit your board. If you are not going to make your board private, then the title of your board becomes important. Try to make sure the title of your board doesn't provide too much information about you or your family; for instance naming the board after a child or stating their birthday. Finally, it is recommended that you enable "Keep board secret" so that your boards are not viewable to the public. Boards often times provide likes and dislikes of a person as well as other hobbies and interests that may make it easier for an Identity Thief to steal your identity.


Verizon LTE
09:16
88%
Search
the blonde avenue : Photo
I love how the bottom lip stuck out a little
FALL
MARKET FRESH PRODUCE
16 Gorgeous Rustic Centerpiece Ideas that...
10 Beautiful Ways to Organize Your Kitchen
Home
Following
Notifications
Saved





Edit board

Done

Board name
outside

Description
Add

Topic
Add

Collaborators
A

Collaborators can...
Add more people

Type
Keep board secret

Manage
Merge board
Turn this board into a section on another board. When you do, this board will lose its followers.

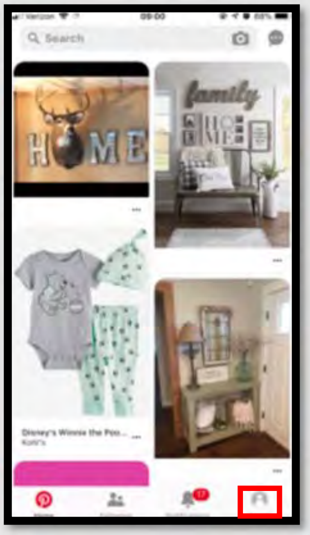
Archive board

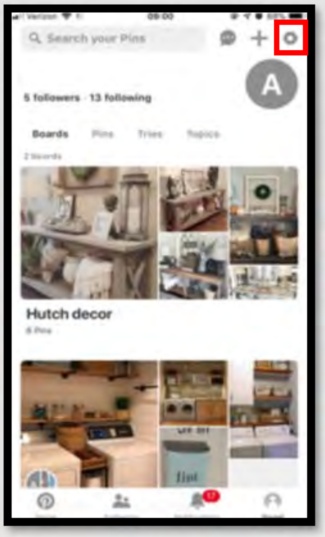
Remember if a "Pin" seems too good to be true it very likely is. Pinterest has many spam "pins" where a single click can lead to a third party site. #staysafeonline

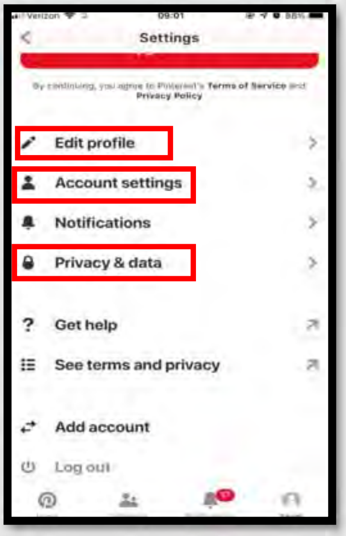
LOCKING DOWN

Pinterest

Using your smart device to lock down your Pinterest account might just make the entire process even easier. As shown below, in just a few simple clicks you can be in your "Edit Profile" section, "Account Settings" and most importantly your "Privacy & data" setting. You will still want to lock down each section as previously discussed in the beginning of this Smartcard most of which is now in the same format as it is on your computer, however the "Privacy & data" section is a bit different and therefore renders some extra looking into. One important section to note in the "Privacy & data" section is the "Store your contacts" section, it is recommended that you do not link your phone contacts to your Pinterest account. It is a good idea to check your Pinterest App settings on your smart device even if you have changed or updated the settings on your computer to make sure they also transferred to the app. As a reminder, the recommended settings that you should set are highlighted by the **red** box.







Settings

By continuing, you agree to Pinterest's Terms of Service and Privacy Policy

Edit profile

Account settings

Notifications

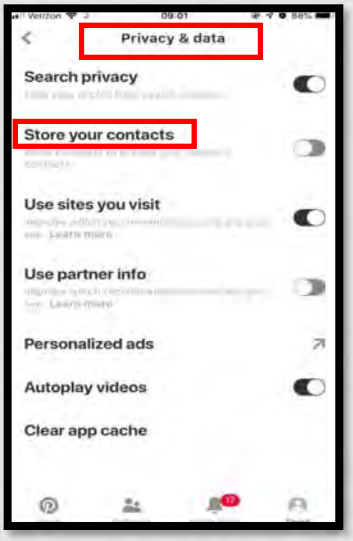
Privacy & data

Get help

See terms and privacy

Add account

Log out



Privacy & data

Search privacy ●

Store your contacts ○

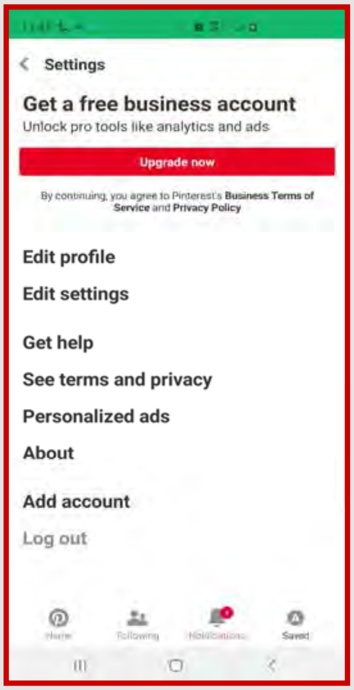
Use sites you visit ●

Use partner info ○

Personalized ads

Autoplay videos ●

Clear app cache



Settings

Get a free business account

Unlock pro tools like analytics and ads

Upgrade now

By continuing, you agree to Pinterest's Business Terms of Service and Privacy Policy

Edit profile

Edit settings

Get help

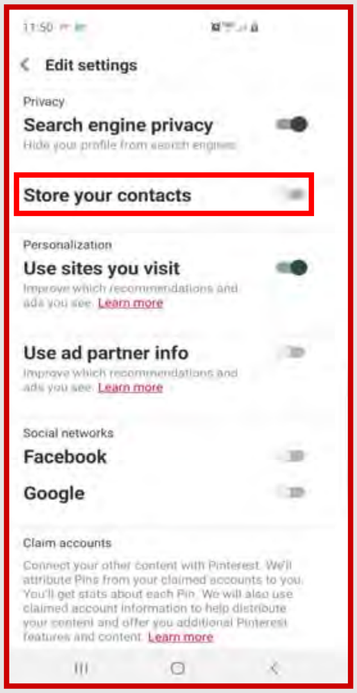
See terms and privacy

Personalized ads

About

Add account

Log out



11:50

Edit settings

Privacy

Search engine privacy ●

Hide your profile from search engines

Store your contacts ○

Personalization

Use sites you visit ●

Improve which recommendations and ads you see. Learn more

Use ad partner info ○

Improve which recommendations and ads you see. Learn more

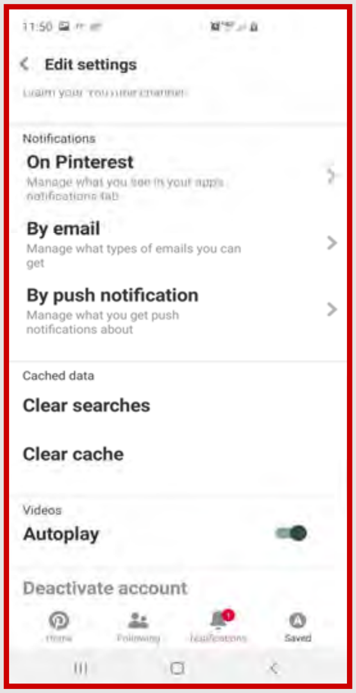
Social networks

Facebook ○

Google ○

Claim accounts

Connect your other content with Pinterest. We'll attribute Pins from your claimed accounts to you. You'll get stats about each Pin. We will also use claimed account information to help distribute your content and offer you additional Pinterest features and content. Learn more



11:50

Edit settings

Claim your YouTube channel

Notifications

On Pinterest

Manage what you see in your app's notifications tab

By email

Manage what types of emails you can get

By push notification

Manage what you get push notifications about

Cached data

Clear searches

Clear cache

Videos

Autoplay ●

Deactivate account

If you have an Android Smartphone, the "Edit Settings" functions may be a bit different (as shown to the left). All the necessary settings for the Android phone will be located all under the "Edit Settings" section. Simply scroll down the list of options in order to decide what best suits your security needs. As noted earlier it is recommended that you do not allow Pinterest to store your contacts (highlighted to the left in red).

While Pinterest is full of entertaining content, remember it is for all ages and as such its content can be "for Adults Only" and not what you want your children to see.

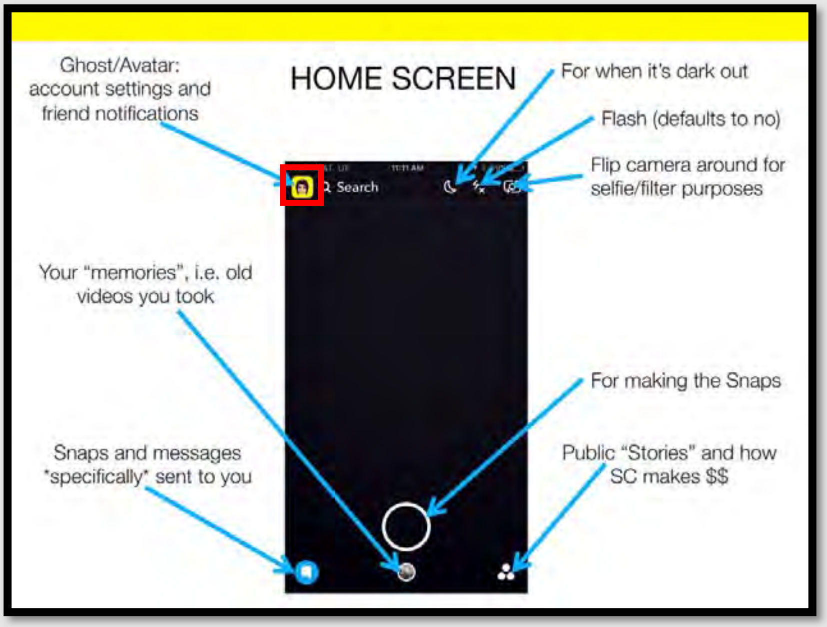
LOCKING DOWN YOUR SNAPCHAT

There are an estimated 82 million users, the majority of which are 13 to 25 years old. Make sure you know who your children are talking too. #keepourkidssafe

Do's and Don'ts

- Do set up privacy and security settings on your Snapchat and help your Teenager to do the same.
- Assume ALL information and images you share are publicly viewable, regardless of your settings.
- Do talk to your Teenager(s) about the dangers Snapchat might pose. Make sure they know to come and tell you if someone should talk to them that they do not know or provides them pictures that are inappropriate.
- Do ***not*** add your birthdate, location, or other personal details to online profiles.
- Do not allow users you do not know personally to contact you via Snapchat.
- Do not think that all pictures and videos are automatically deleted, assume if you send it that someone can keep it or that it could be shared.

Shown to the right is an overview of the chat features of Snapchat. Here you can see if someone has sent you a message, posted a story, or review posts you've already read. You can also start a chat or again select the icon at the top left and head to your Snapchat statics and "Settings" section.



HOME SCREEN

Ghost/Avatar: account settings and friend notifications

For when it's dark out

Flash (defaults to no)

Flip camera around for selfie/filter purposes

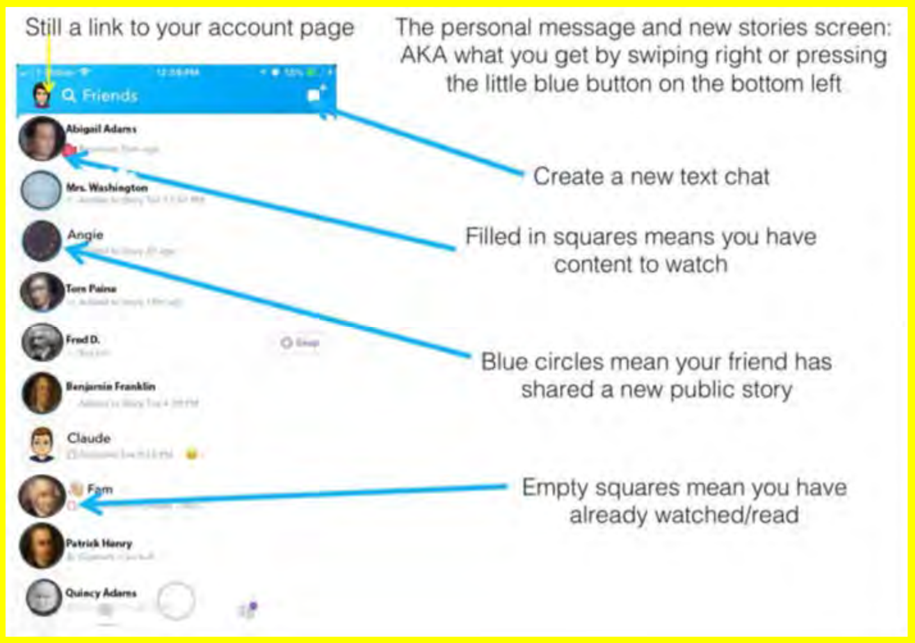
Your "memories", i.e. old videos you took

For making the Snaps

Snaps and messages *specifically* sent to you

Public "Stories" and how SC makes $$

The best way to begin understanding and locking down Snapchat's capabilities is to familiarize yourself with Snapchat basics. In the box above you can look over the main icons and functions located in Snapchat. The most important icon to note is the Ghost or Avatar picture at the left of the box (highlighted in **red**), this icon will take you to your Snapchat statistics and lead you to the "Settings" icon . The icons may differentiate slightly depending on the device that you are using but the location of each function should remain the same.



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

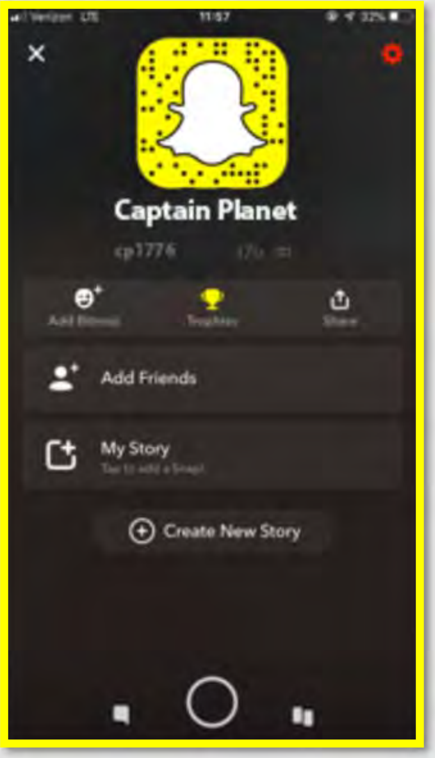
Filled in squares means you have content to watch

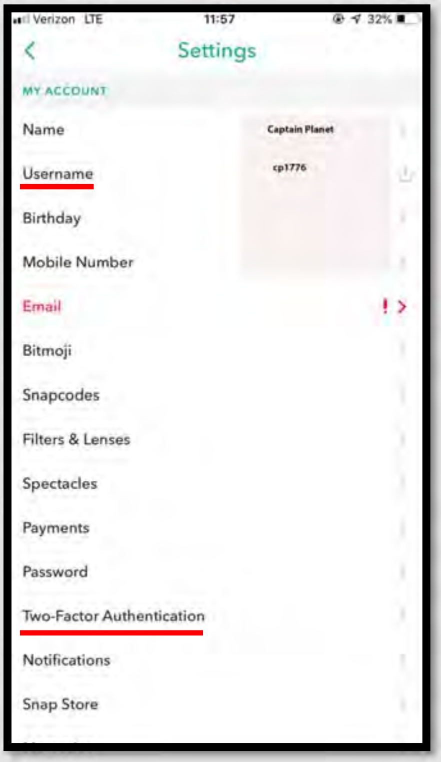
Blue circles mean your friend has shared a new public story

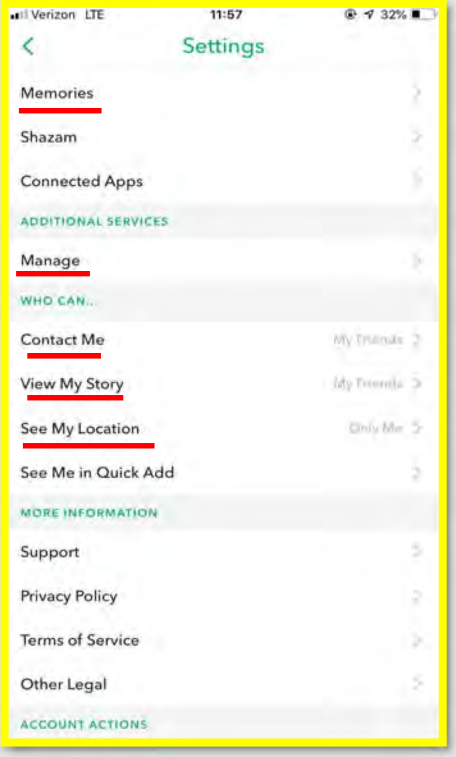
Empty squares mean you have already watched/read

LOCKING DOWN YOUR SNAPCHAT

The Pew Internet and American Life Project found that 15 percent of teenagers between the ages of 12 and 17 acknowledge they received a “sext” from someone they know.







Contact Me My Friends

View My Story My Friends

See My Location Only Me

See Me in Quick Add

After reviewing the different sections on page one of the Snapchat Card let us begin locking down our actual account.

Let’s begin by selecting your Profile picture “Account Settings” for the top of the screen on your “home page” as shown on page one.

Now, select the “Settings” Icon from the top right corner of the screen (shown above in **Red**).

From here, we can review all of the settings offered by Snapchat

Please note that the Android Snapchat App may have slightly different wording for each section, but the process is the same.

While you are reviewing and familiarizing yourself with all of Snapchats settings, one item to make sure you review is your “Username”. It is recommended that you create a username that does not give too much away about you or any personal information i.e. birthday, full name etc.

If not properly locked down any individual will be able to look you up as well as certain pieces of information, therefore, it is important to review each section here periodically to make sure everything remains locked down to your comfort level.

We will be reviewing settings from each of the **Red** underlined.

Snapchat Lingo:

Geo-filters: These are location-specific elements that can only be unlocked by visiting a specific place. Businesses use geo-filters as a way for customers to check in and advertise them. A teenager could create a special geo-filter for their sweet-16 party for attendees to add to their photos.

Snapcash: Like PayPal or Venmo, Snapcash lets users transfer money to each other.

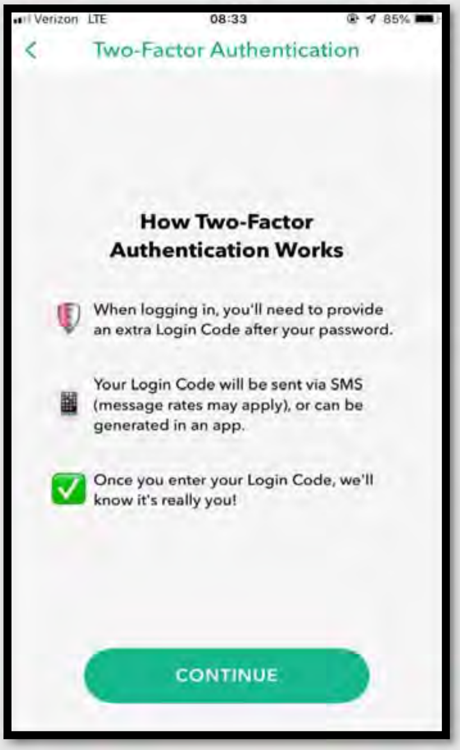
Memories: If you don't want your snaps to disappear, you can store them to send later.

Snapstore: This is exactly what it sounds like: a place to buy Snapchat-related items.

Shazam: A feature that helps you identify a song.

LOCKING DOWN YOUR SNAPCHAT

Hackers have been known to publish thousands of snaps mainly of 13 to 17 year old's. Talk to your teenagers periodically about who they are connecting with.



Verizon LTE 08:33 85%

Two-Factor Authentication

How Two-Factor Authentication Works

When logging in, you'll need to provide an extra Login Code after your password.

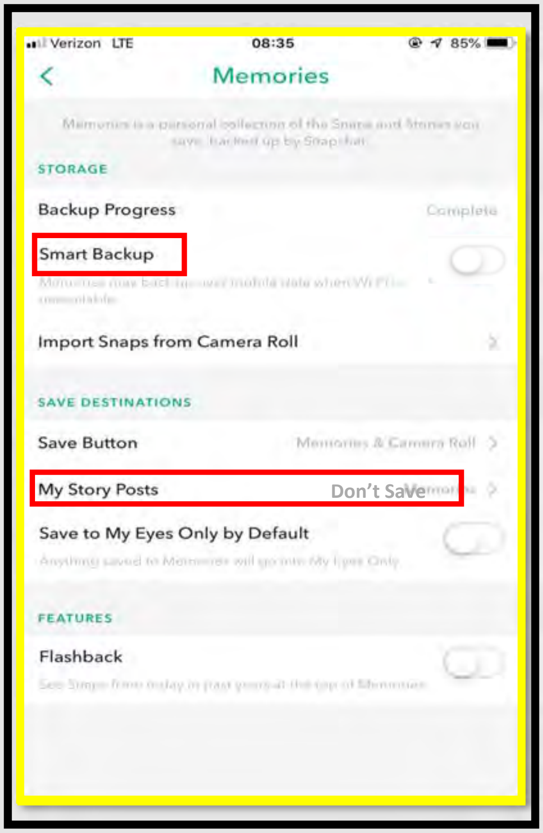
Your Login Code will be sent via SMS (message rates may apply), or can be generated in an app.

Once you enter your Login Code, we'll know it's really you!

CONTINUE

As always, it is important to and highly recommended that you enable Two-Factor Authentication for your Snapchat, to help minimize other individuals from accessing it. Simply select the "Two-Factor Authentication" from the settings menu (shown on page 2 of this card) and follow the few steps to complete the process.

Next, go back to the "setting" section and select "Memories." From here, it is recommended that you not enable to "Smart Backup" or "My Story Posts" to prevent Snapchat from storing your photos and videos.



Verizon LTE 08:35 85%

Memories

Memories is a personal collection of the Snaps and Stories you save, backed up by Snapchat.

STORAGE

Backup Progress — Complete

Smart Backup ○

Memories may back up over mobile data when Wi-Fi is unavailable.

Import Snaps from Camera Roll >

SAVE DESTINATIONS

Save Button — Memories & Camera Roll >

My Story Posts — Don't Save >

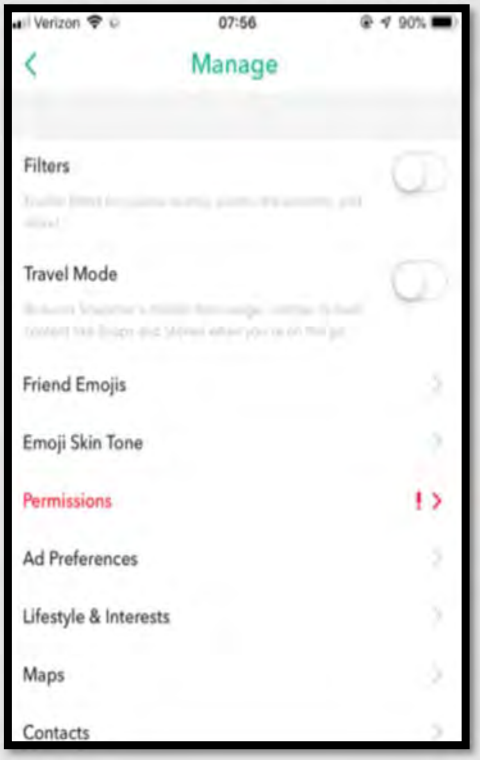
Save to My Eyes Only by Default ○

Anything saved to Memories will go into My Eyes Only

FEATURES

Flashback ○

See Snaps from today in past years at the top of Memories.



Verizon 07:56 90%

Manage

Filters ○

[illegible]

Travel Mode ○

[illegible]

Friend Emojis >

Emoji Skin Tone >

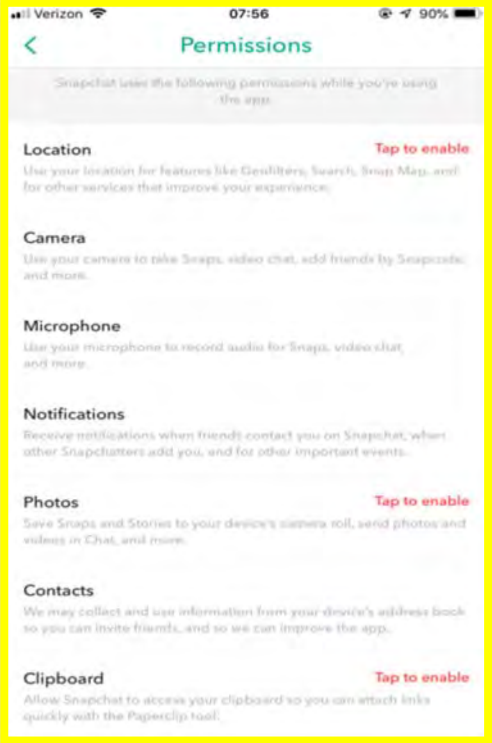
Permissions ! >

Ad Preferences >

Lifestyle & Interests >

Maps >

Contacts >



Verizon 07:56 90%

Permissions

Snapchat uses the following permissions while you're using the app.

Location — Tap to enable

Use your location for features like Geofilters, Search, Snap Map, and for other services that improve your experience.

Camera

Use your camera to take Snaps, video chat, add friends by Snapcode and more.

Microphone

Use your microphone to record audio for Snaps, video chat, and more.

Notifications

Receive notifications when friends contact you on Snapchat, when other Snapchatters add you, and for other important events.

Photos — Tap to enable

Save Snaps and Stories to your device's camera roll, send photos and videos in Chat, and more.

Contacts

We may collect and use information from your device's address book so you can invite friends, and so we can improve the app.

Clipboard — Tap to enable

Allow Snapchat to access your clipboard so you can attach links quickly with the Paperclip tool.

Let's head back to the "Settings" section and scroll down to select "Manage" once there scroll to select "Permissions." Note: If you have an Android this settings is listed under the "Settings" section. From here, there are a few important section to "disable" or to ensure you do not "enable," such as "Location." It is highly recommended that you not enable the "Location," "Photos" or the "Clipboard" from this section. Each of these functions allows Snapchat to have access to your phone that you limits your privacy and allows Snapchat to access and store photos/information from your device onto their cloud.

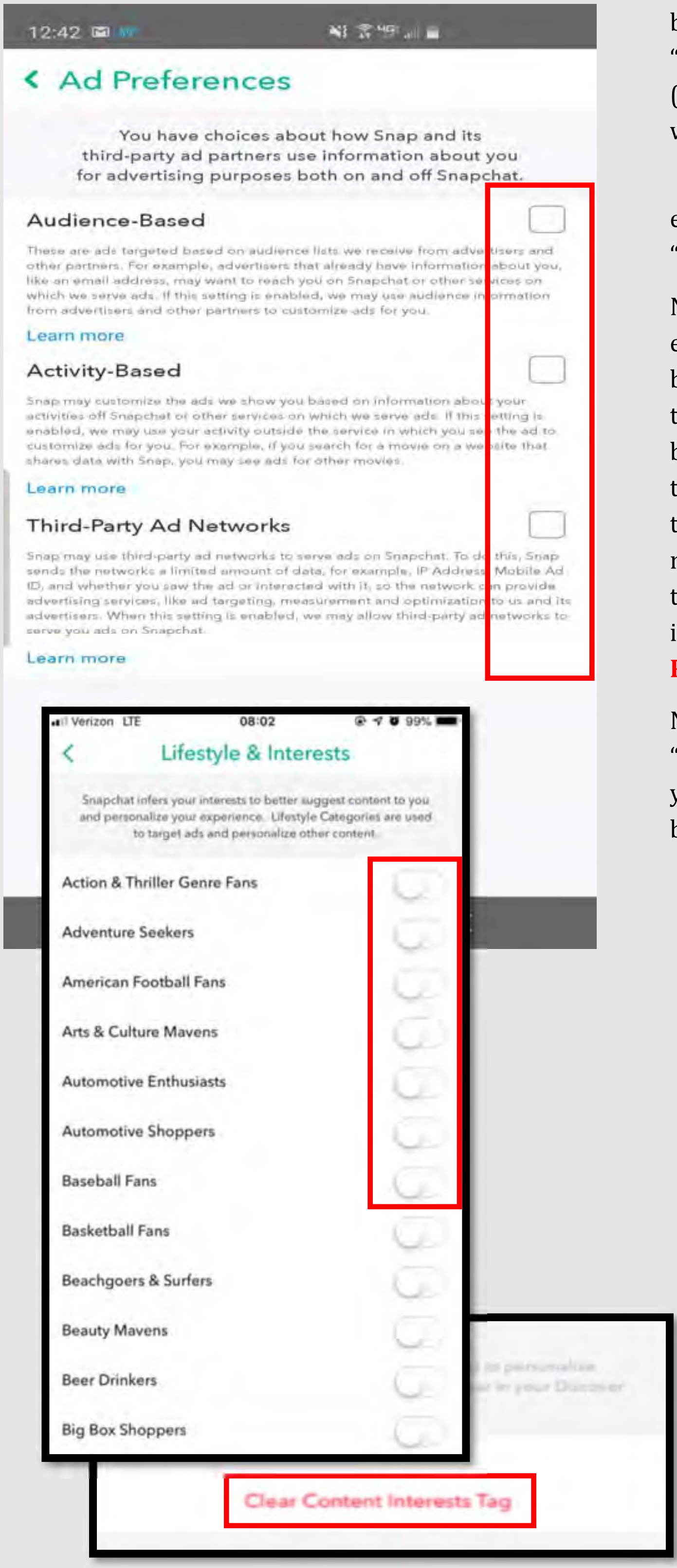
LOCKING DOWN YOUR SNAPCHAT

After you have finished locking down the “Permissions” section, go back to the “Manage” section (as shown on page four) and select “Ad Preferences.” Here it is recommended that neither selections (“Audience-Based” or “Activity Based”) be enabled to decrease what Snapchat learns about you.

Note: If you have an Android Based Smart phone “Ad Preferences” will be located on the “Settings” page. You will also find “Lifestyle & Interests” under “Ad Settings.”

Next, go back to the “Manage” section and select “Lifestyle & Interests,” its recommended that you unselect any section that is enabled. You can also clear any tags that may have specified your interests by selecting “Clear Content Interests Tag” (shown at the bottom left in **red**) periodically from this section. Next, go back to “Manage” and select “Contacts” (If you have an Android this function is in the “Settings” section) there it is recommended that you make sure you have not enabled Snapchat to view your device contacts. If you had enabled “Sync Contacts” but have now disabled it, it is important to also “Delete All Contacts Data” as shown below in **Red**.

Now, let’s go back to “Manage”, select “Maps”, and make sure that “Share Usage Data” is not enabled. It is always recommended that you hide your location or ensure it is not enabled wherever possible.



12:42

‹ Ad Preferences

You have choices about how Snap and its third-party ad partners use information about you for advertising purposes both on and off Snapchat.

Audience-Based □

These are ads targeted based on audience lists we receive from advertisers and other partners. For example, advertisers that already have information about you, like an email address, may want to reach you on Snapchat or other services on which we serve ads. If this setting is enabled, we may use audience information from advertisers and other partners to customize ads for you.

Learn more

Activity-Based □

Snap may customize the ads we show you based on information about your activities off Snapchat or other services on which we serve ads. If this setting is enabled, we may use your activity outside the service in which you see the ad to customize ads for you. For example, if you search for a movie on a website that shares data with Snap, you may see ads for other movies.

Learn more

Third-Party Ad Networks □

Snap may use third-party ad networks to serve ads on Snapchat. To do this, Snap sends the networks a limited amount of data, for example, IP Address, Mobile Ad ID, and whether you saw the ad or interacted with it, so the network can provide advertising services, like ad targeting, measurement and optimization to us and its advertisers. When this setting is enabled, we may allow third-party ad networks to serve you ads on Snapchat.

Learn more

Verizon LTE 08:02 99%

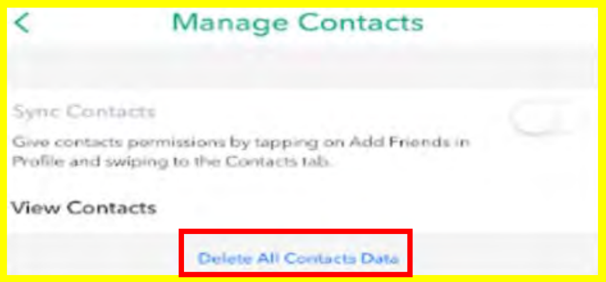
‹ Lifestyle & Interests

Snapchat infers your interests to better suggest content to you and personalize your experience. Lifestyle Categories are used to target ads and personalize other content.

- Action & Thriller Genre Fans ○
- Adventure Seekers ○
- American Football Fans ○
- Arts & Culture Mavens ○
- Automotive Enthusiasts ○
- Automotive Shoppers ○
- Baseball Fans ○
- Basketball Fans ○
- Beachgoers & Surfers ○
- Beauty Mavens ○
- Beer Drinkers ○
- Big Box Shoppers ○

to personalize
in your Discover

Clear Content Interests Tag



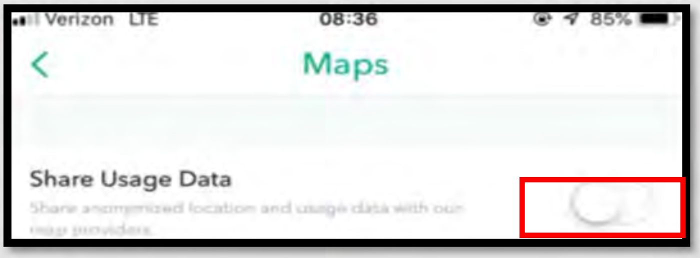
‹ Manage Contacts

Sync Contacts ○

Give contacts permissions by tapping on Add Friends in Profile and swiping to the Contacts tab.

View Contacts

Delete All Contacts Data



Verizon LTE 08:36 85%

‹ Maps

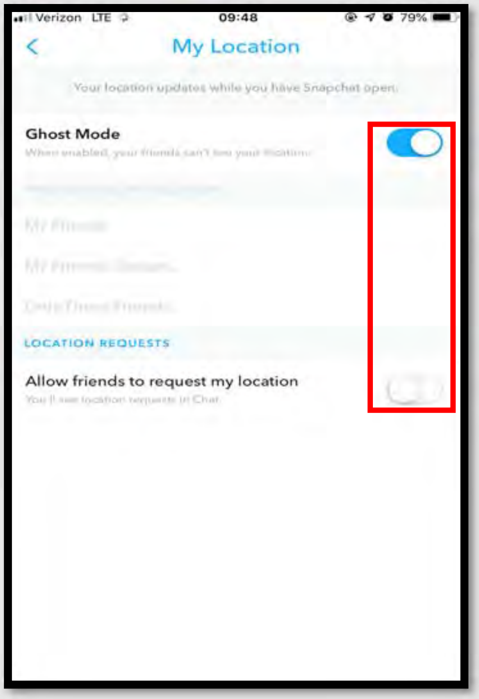
Share Usage Data ○

Share anonymized location and usage data with our map providers.

According to TeenSafe.com 47 percent of users admit to using screenshots and 52 percent note that others have used screenshots of their messages. #Staysafeonline

LOCKING DOWN YOUR SNAPCHAT

The FBI warns parents that pedophiles are using Snapchat to solicit images from young teens. These images are used for personal use or are sold to others in the underground.


Verizon LTE 09:48 79%

My Location

Your location updates while you have Snapchat open.

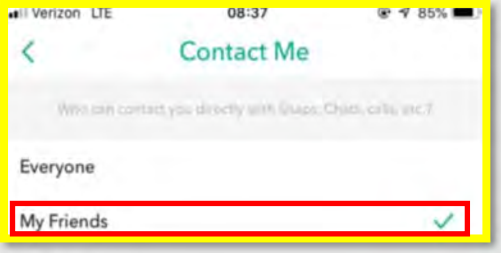
Ghost Mode

LOCATION REQUESTS

Allow friends to request my location

You'll see location requests in Chat.

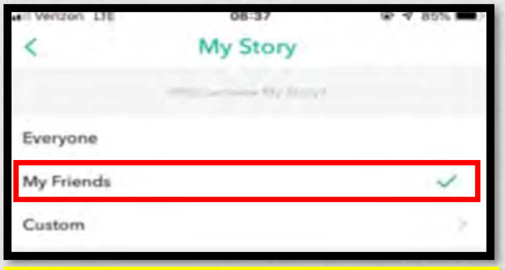
Let's go back to "Settings" and select "Contact Me" under the "Who Can..." section. It is recommended here that only "My Friends" are able to contact you, in order to help keep you and your children safer while using this App. Under the same "Who Can..." section select "View My Story" where it is also recommended that "My Friends" be enabled to ensure that your videos and pictures are not available to the public. Now, depending on your level of involvement (or your child's) with this App, you may also want to lock down the "See Me in Quick Add" section (shown to the right). Making sure this is NOT enabled will prevent your profile from showing up in profiles as a suggested contact.


Verizon LTE 08:37 85%

Contact Me

Everyone

My Friends ✓

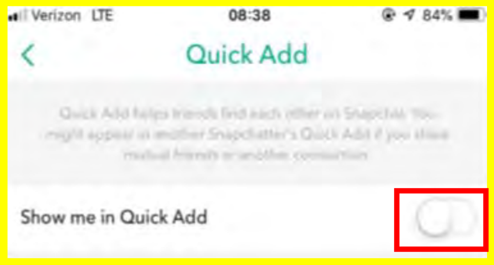

Verizon LTE 08:37 85%

My Story

Everyone

My Friends ✓

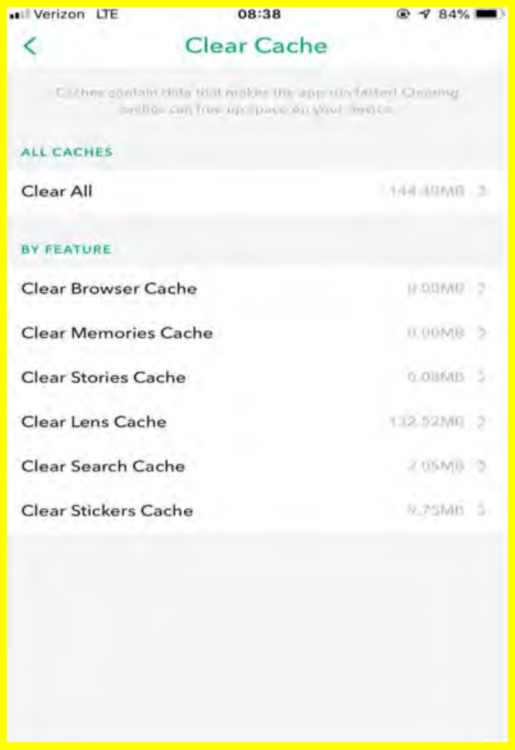
Custom


Verizon LTE 08:38 84%

Quick Add

Show me in Quick Add

Heading back to the "Settings" section, lets review the "See My Location." Snapchat allows users to be in "Ghost Mode" to prevent even their friends from viewing their location. It is highly recommended that you enable "Ghost Mode" while using Snapchat in order to prevent individuals from viewing your precise location on the Snapchat Map. It is also recommended that you not enable "Allow friends to request my location."


Verizon LTE 08:38 84%

Clear Cache

ALL CACHES

Clear All

BY FEATURE

Clear Browser Cache

Clear Memories Cache

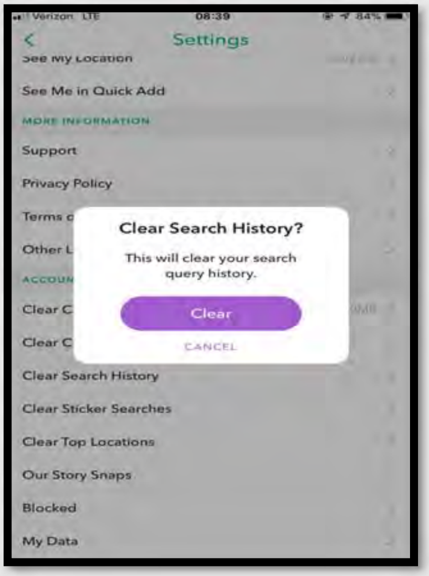
Clear Stories Cache

Clear Lens Cache

Clear Search Cache

Clear Stickers Cache

Snapchat also provides you the opportunity to Clear your Cache, conversations, search history, and top locations (as shown below). It is recommended that you periodically go through and clear these much like you would your Internet Browser.


Settings

See My Location

See Me in Quick Add

MORE INFORMATION

Support

Privacy Policy

Clear Search History?

This will clear your search query history.

Clear

CANCEL

Clear Search History

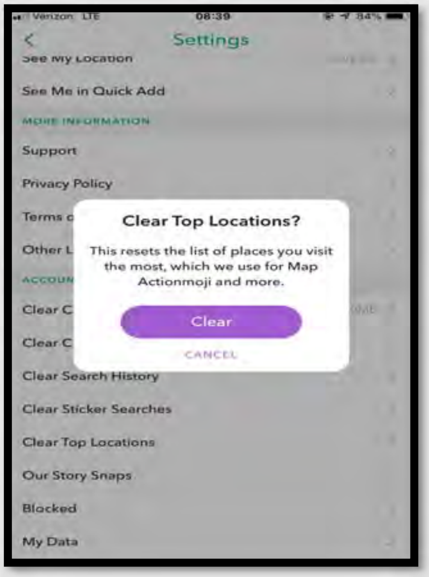
Clear Sticker Searches

Clear Top Locations

Our Story Snaps

Blocked

My Data


Settings

See My Location

See Me in Quick Add

MORE INFORMATION

Support

Privacy Policy

Clear Top Locations?

This resets the list of places you visit the most, which we use for Map Actionmoji and more.

Clear

CANCEL

Clear Search History

Clear Sticker Searches

Clear Top Locations

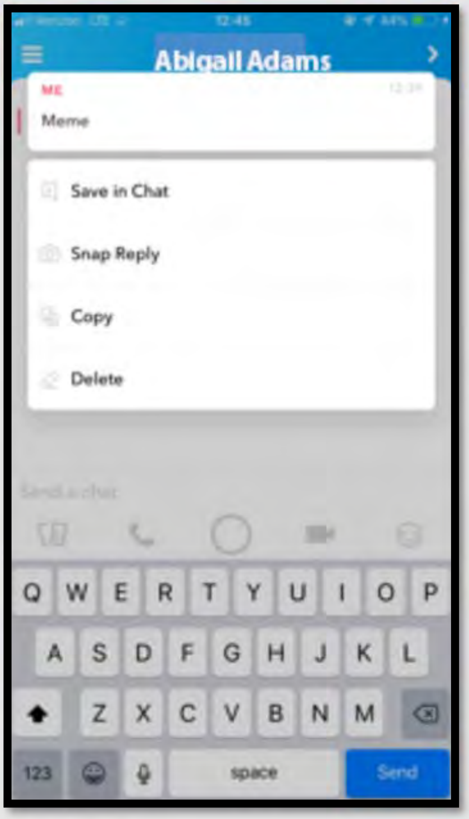
Our Story Snaps

Blocked

My Data

LOCKING DOWN YOUR SNAPCHAT

Snapchat created a new feature to Snapchat that lets you unsend a sent message regardless of whether recipient(s) saw it. This feature is different from the already available "Clear Conversation" option, which only deletes the content from your end. "Clear Chats" works in-group chats or in one-on-one conversations, and applies to text, stickers, audio, or pictures and videos sent from your "Memories" section — not content you just took though. Important to note that the person(s) in the conversation will be alerted that a message was deleted; the function's purpose is to clean up a typo or prevent unintentional messaging.

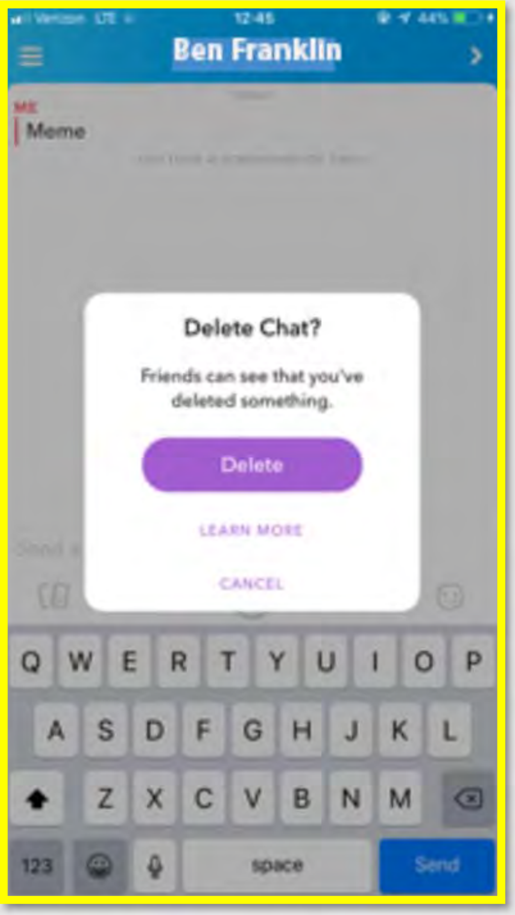


Abigail Adams

ME

Meme

In order to delete a chat that you may have already sent simply hold down the chat (shown here to the left as "Meme") and then 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 even though the message will be deleted, your friends will still be able to see that something was deleted, just not the deleted content itself.



Ben Franklin

ME

Meme

Delete Chat?

Friends can see that you've deleted something.

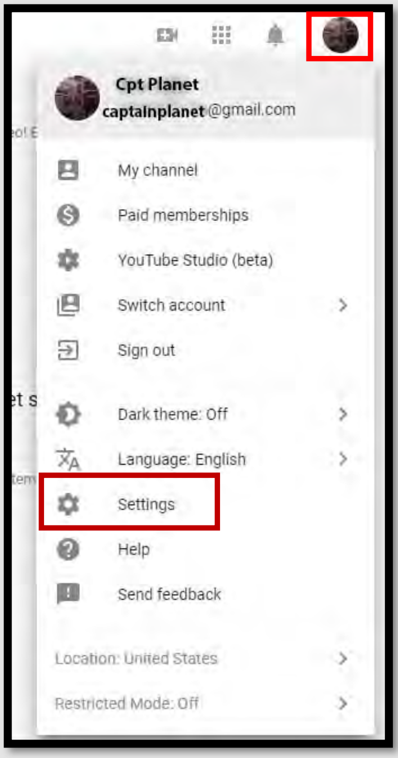
Depending on the State, parents can be held liable for a child's cyberbullying or sexting if they fail to take appropriate action. #themoreyouknow

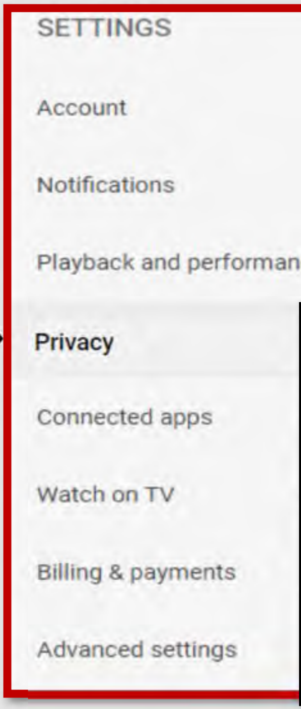
UPDATED DEC 2019

LOCKING DOWN YouTube

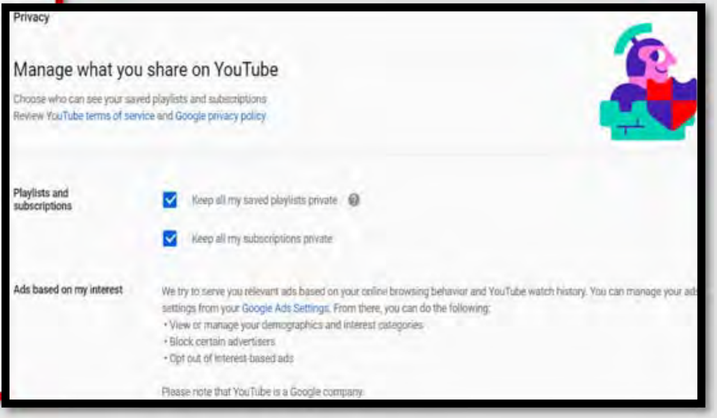
Do's and Don'ts

- Do monitor the videos that your children are watching, even if they are on "Restricted Mode."
- Do use Two-Factor Authentication to protect all your information. If you have a YouTube account that likely means you also own a "Google" account which is where you can turn on Two-Factor Authentication.
- Do lock down your videos so that they are not public for everyone to view.
- Do not allow your children to post public videos to their YouTube account. Posting public videos will allow "subscribers" to follow your children on YouTube.
- Do not ignore the comments and feedback from your published videos. They may contain personal information about you or your video that you would otherwise not want put out.





In order to ensure the privacy on your YouTube account lets being with our Settings. Head to the top right of your screen and select your Google Profile picture (shown to the left in **red**). Once the drop down menu appears, look towards the bottom and select "Settings." To the right of your screen are a list of functions in YouTube, select "Privacy" to manage your YouTube privacy.



Privacy

Manage what you share on YouTube

Choose who can see your saved playlists and subscriptions
Review YouTube terms of service and Google privacy policy

Playlists and subscriptions

☑ Keep all my saved playlists private

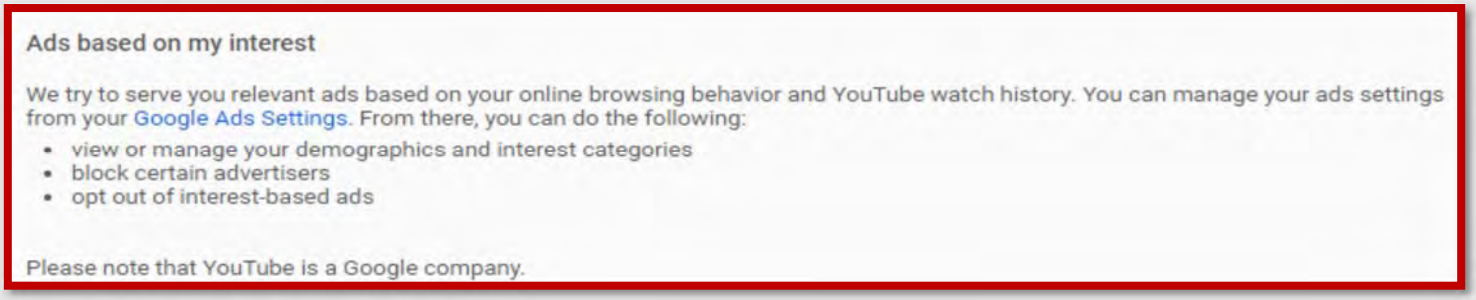
☑ Keep all my subscriptions private

Ads based on my interest

We try to serve you relevant ads based on your online browsing behavior and YouTube watch history. You can manage your ads settings from your Google Ads Settings. From there, you can do the following:
- View or manage your demographics and interest categories
- Block certain advertisers
- Opt out of interest-based ads

Please note that YouTube is a Google company.

Now that you are in the "Privacy" section scroll through each of the settings to make sure they are locked down to your satisfaction. It is recommended that your keep all sections in "Manage what you share on YouTube" private. Finally, in order to turn off the "Ads based on my interest" select the link "Google Ads Settings," then select "turn off." It is recommended that this feature be turned off for all social media sites.



Ads based on my interest

We try to serve you relevant ads based on your online browsing behavior and YouTube watch history. You can manage your ads settings from your Google Ads Settings. From there, you can do the following:

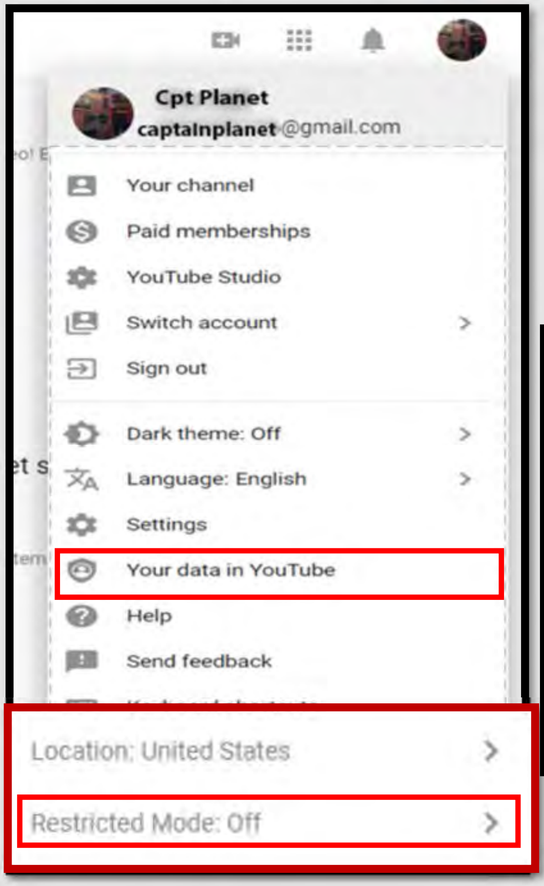
- view or manage your demographics and interest categories
- block certain advertisers
- opt out of interest-based ads

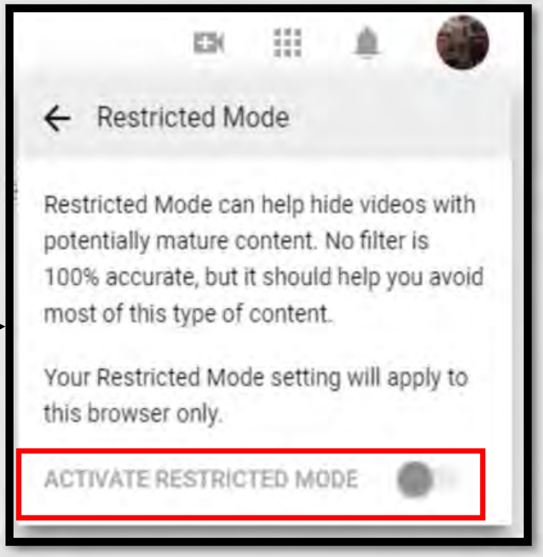
Please note that YouTube is a Google company.

YouTube looks like it refreshes after that last step, but you'll still see the same content as you did before if you don't refresh your screen. #themoreyouknow

LOCKING DOWN YouTube

Unlike any other social networks, YouTube doesn't require you to create an account before you or your child can search for content or view videos.





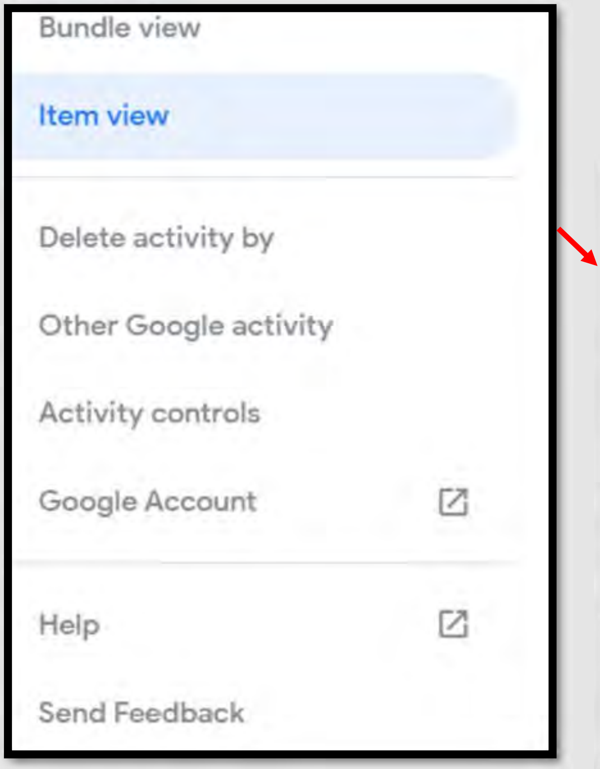
Restricted Mode can help hide videos with potentially mature content. No filter is 100% accurate, but it should help you avoid most of this type of content.

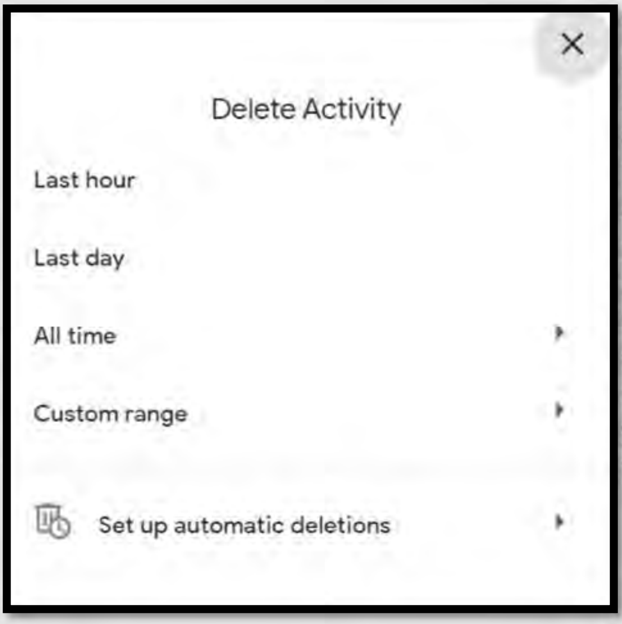
Your Restricted Mode setting will apply to this browser only.

Parents do you worry about what your child is watching on YouTube? Now you are able to put them in what YouTube is calling the "Restricted Mode" to help protect what your children are watching. There are a few ways to turn on this function, first by going back to your profile settings picture at the top of the screen and selecting the drop down menu.

Once the drop down menu appears, look towards the bottom of the menu and select "Restricted Mode" (as shown to the left in **red**). Selecting the "Restricted Mode" function will bring up an additional pop-up box to confirm that you in fact, want to "Activate Restricted Mode" (as shown above in **red**).

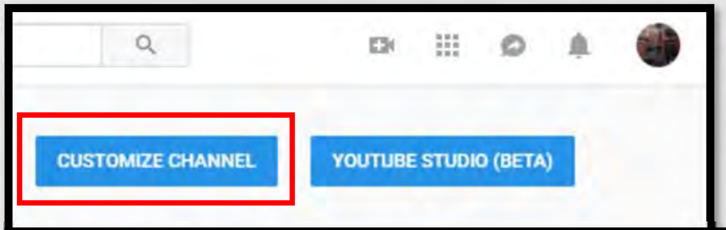
There is one other important feature located at the bottom of your YouTube Main Menu (shown here in the upper left) and that is the "Your data in YouTube" tab. Just as it is important to clear your browser history on your Search Engines, it is important to manage and clear your history on your YouTube account. Scroll down and select the "Manage your YouTube Search History." From here, look to the left of your screen to see a menu of available options to manage and delete your history. It is recommended that you "Clear All Watch History" periodically from your YouTube account. After having selected "Clear All Watch History" a pop up box will appear on your screen to confirm that you would in fact like to clear your history. Simply select "Clear Watch History."

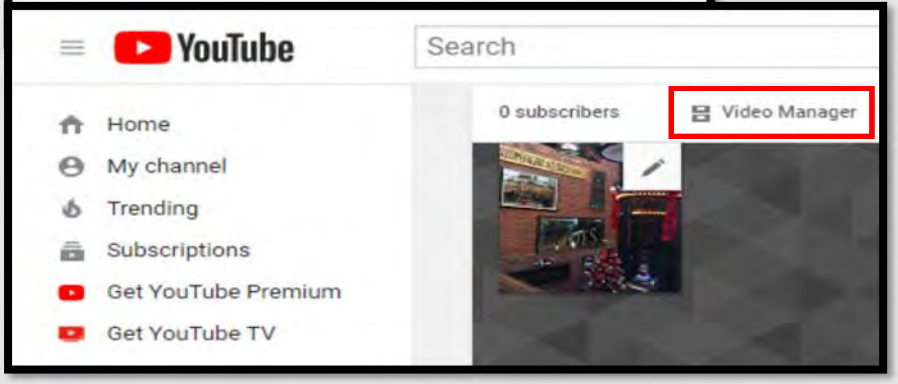




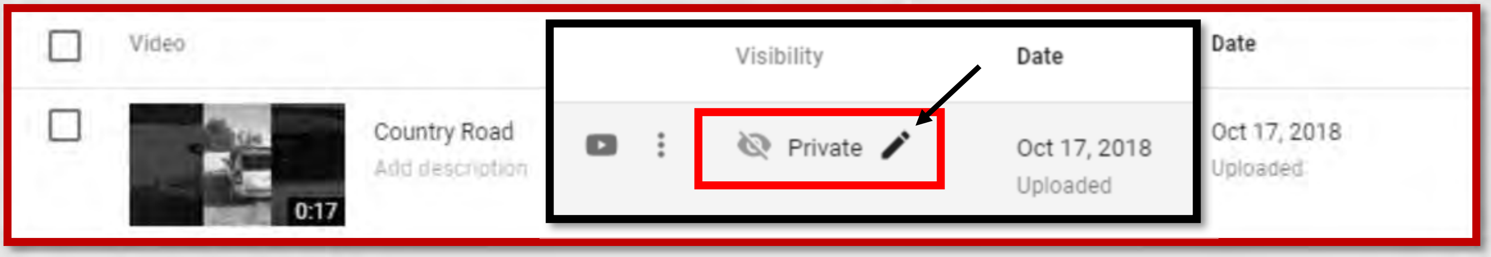
Restricted Mode doesn't catch everything, and it's easy to disable which is why it's important to check on your children and even teenagers, while they are using YouTube.

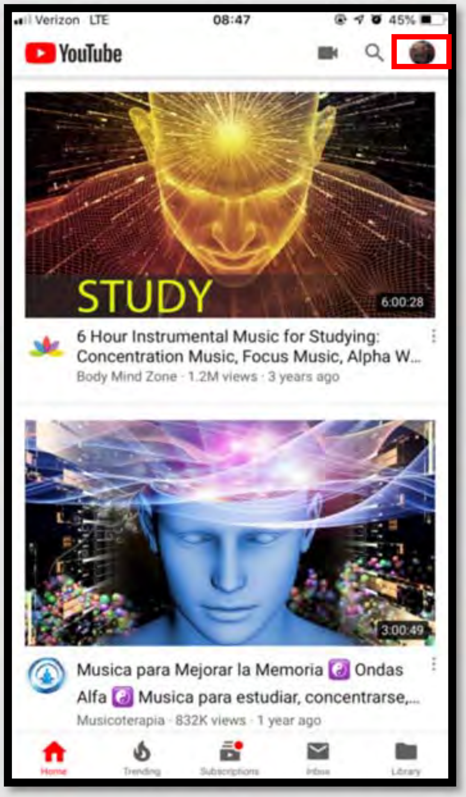
LOCKING DOWN YouTube

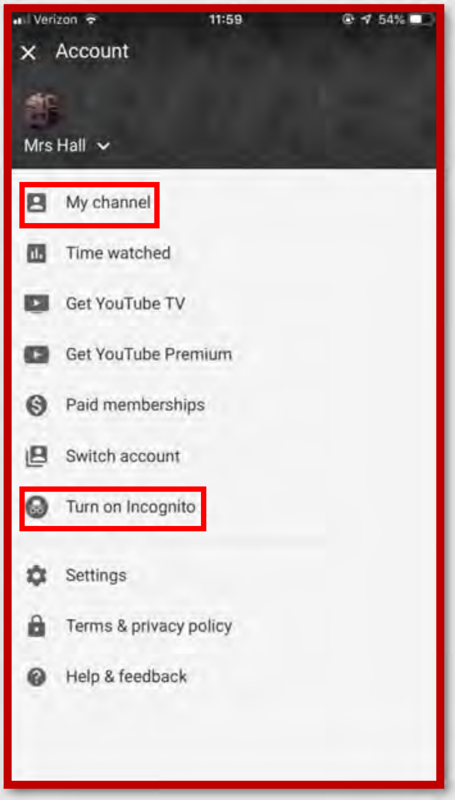


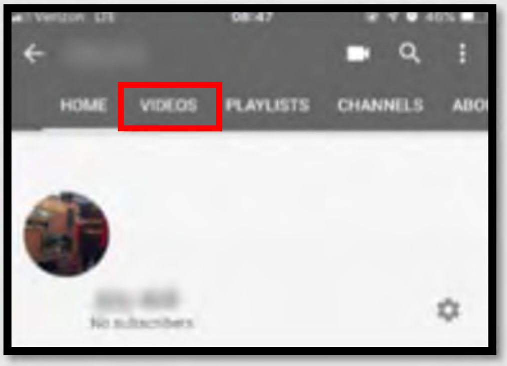


One of the main uses for YouTube is of course uploading and watching videos. In order to upload your videos and create privacy settings you must first locate your "Video Manager." Select the "Profile" drop down menu and select "My Channel." Then select "Customize Channel" in the blue box (highlighted here in **red**). Next, select "Video Manager" from the middle of the page. Here you will be able to upload videos and edit any videos you have already uploaded. In order to edit the "Visibility" of a video simply hover over the current visibility of the video and select the "pencil" icon. From the drop down menu that will appear simply select the desired privacy setting. It is recommended that your videos remain "Private."




Verizon LTE
08:47
45%
YouTube
STUDY
6:00:28
6 Hour Instrumental Music for Studying: Concentration Music, Focus Music, Alpha W...
Body Mind Zone · 1.2M views · 3 years ago
3:00:49
Musica para Mejorar la Memoria Ondas Alfa Musica para estudiar, concentrarse,...
Musicoterapia · 832K views · 1 year ago
Home
Trending
Subscriptions
Inbox
Library

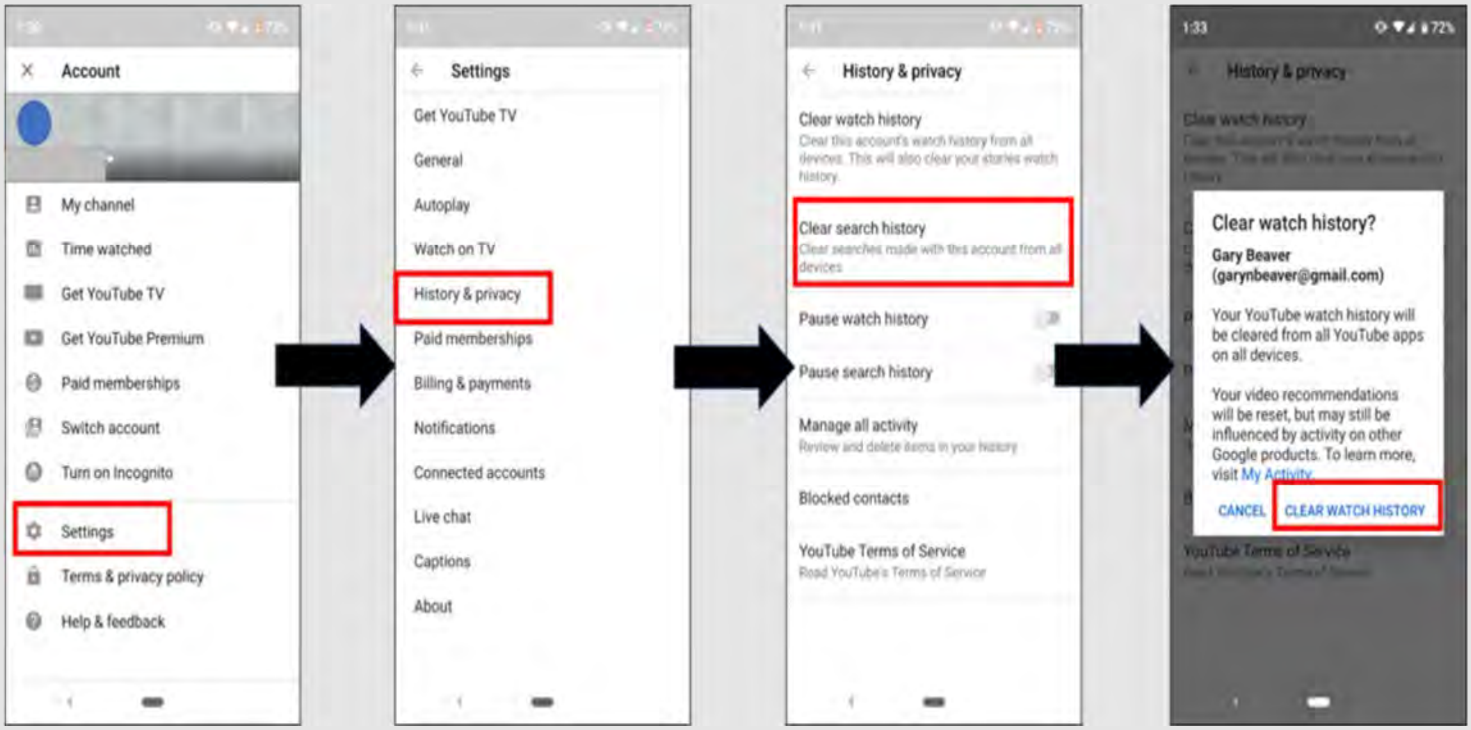




In order to access uploaded videos and change their privacy settings via your smart devices the process is a bit different. From the App and like the Browser version, select your profile settings, then select "My Channel." Next head to the top menu and select "Videos" to take you to the video upload and settings section.

YouTube now allows its users to be in Incognito mode. Simply select the "Turn on Incognito."

LOCKING DOWN YouTube



Clear watch history: Clear this account's watch history from all devices. This will also clear your stories watch history.

Clear search history: Clear searches made with this account from all devices

Manage all activity: Review and delete items in your history

YouTube Terms of Service: Read YouTube's Terms of Service

Clear watch history?

Gary Beaver (garynbeaver@gmail.com)

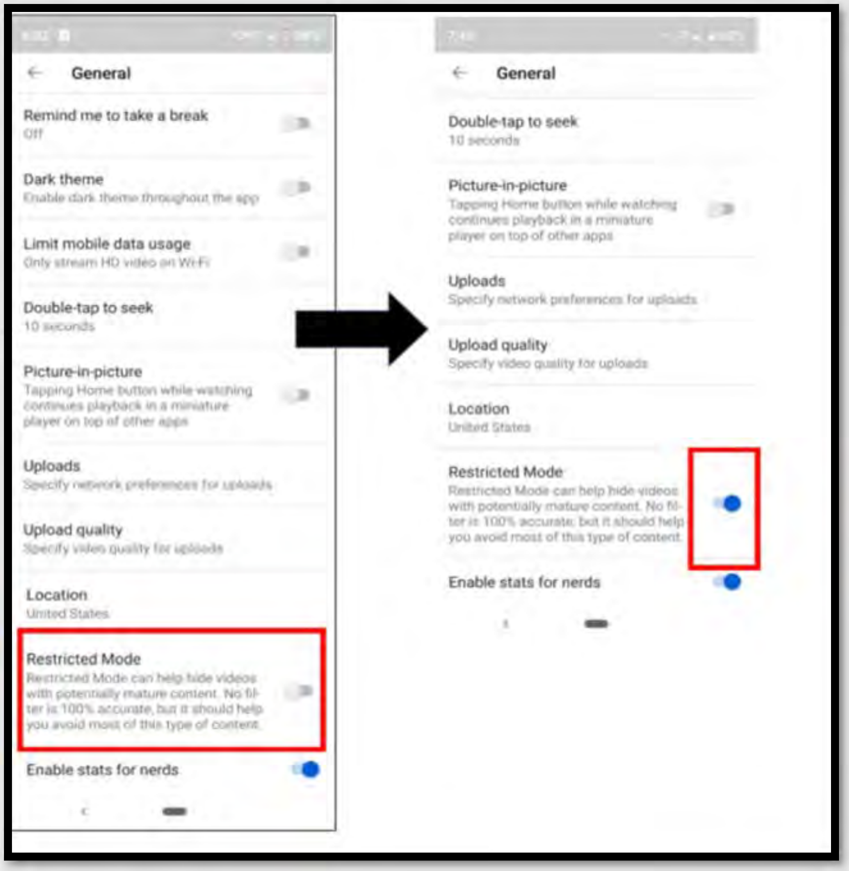
Your YouTube watch history will be cleared from all YouTube apps on all devices.

Your video recommendations will be reset, but may still be influenced by activity on other Google products. To learn more, visit My Activity.

If you are an iPhone user, most of these settings will be found directly under the "Settings" section, instead of having to go into multiple different tabs. Above are the steps necessary to get to the "History & Privacy" section as well as to clear your History on YouTube.

If you are sharing your device or just wanting to protect your privacy, it is a good idea to make sure you clear your history at any time by accessing the YouTube app's settings and following these steps.

In order to turn on "Restricted Mode" from your Android simply follow the steps to the right. Remember this is a good idea if you have children that use your YouTube account.



Remind me to take a break: Off

Dark theme: Enable dark theme throughout the app

Limit mobile data usage: Only stream HD video on Wi-Fi

Double-tap to seek: 10 seconds

Picture-in-picture: Tapping Home button while watching continues playback in a miniature player on top of other apps

Uploads: Specify network preferences for uploads

Upload quality: Specify video quality for uploads

Location: United States

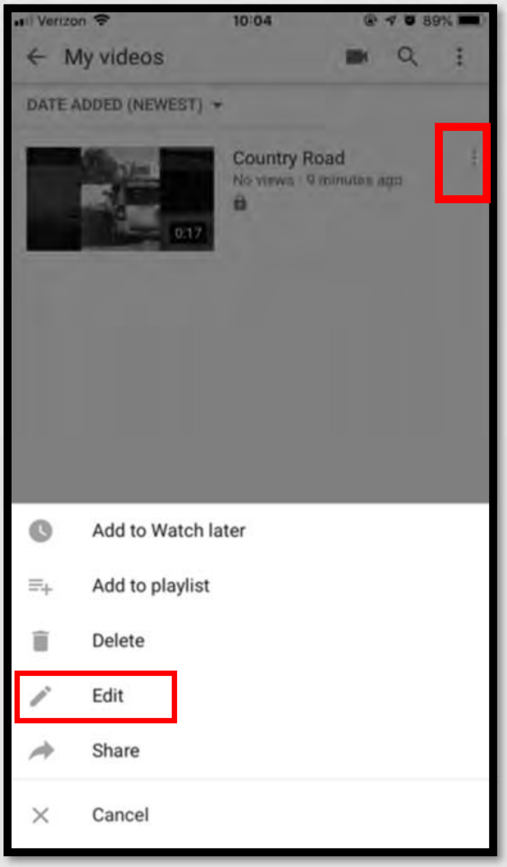
Restricted Mode: Restricted Mode can help hide videos with potentially mature content. No filter is 100% accurate, but it should help you avoid most of this type of content.

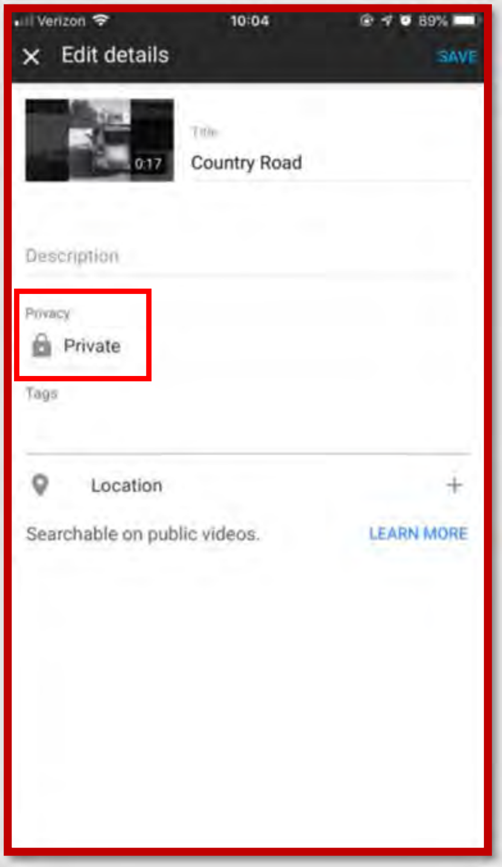
Enable stats for nerds

Your phone is your ultimate endpoint. You likely carry it everywhere and it typically holds your most sensitive information. Make sure to check for updates quarterly. #Staysafeonline

LOCKING DOWN YouTube

Social media sites can cover people in anonymity, allowing them to attempt to exploit children without the fear of being caught. Monitor your child's Internet usage to help keep them safe.





Title: Country Road

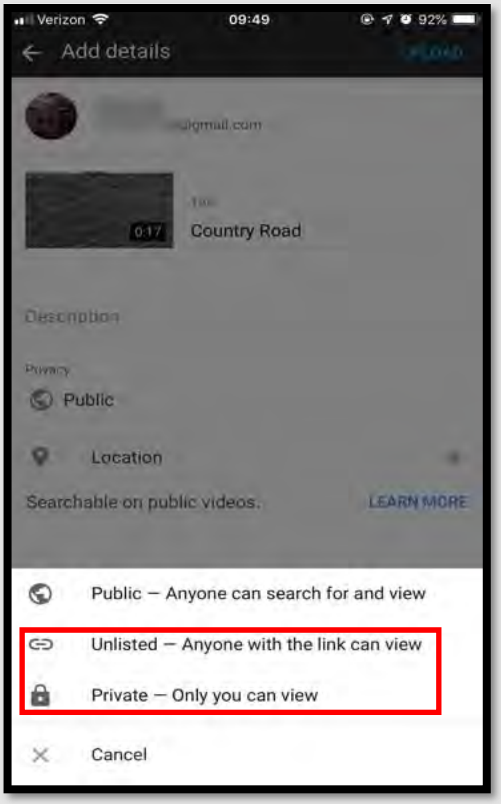
Description

Privacy: Private

Tags

In order to edit the privacy settings of your video from your smart device, now locate the vertical ellipsis (three vertical dots to the right) and select it to show a pop up menu appearing from the bottom of the screen.

Next, select "Edit" from the pop up menu where you will then be able to select "Privacy", set or turn off the "Location" of a particular video, or provide a description of the video for viewers, if you allow any.



Title: Country Road

Description

Privacy: Public

Public – Anyone can search for and view

Unlisted – Anyone with the link can view

Private – Only you can view

Now you will be able to select how private you would like to keep you videos. The purpose of YouTube is to upload and watch videos; therefore, with that in mind, it is recommended that you select "Unlisted" as your privacy setting for all videos. An "Unlisted" privacy setting on YouTube means that your video is only public to individuals that have a link directly to the video. If you make your video "Public" or your child makes his or her video "Public" then anyone will be able to view it. Once a video is uploaded to YouTube and made "Public" there is no real way to pull back the video, it can be shared, liked, and commented on very quickly at which time you lose any ability to pull it back from the public eye.

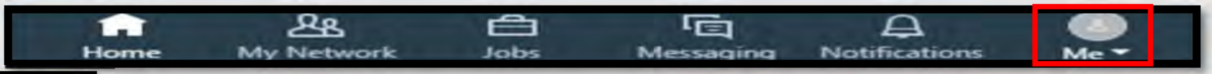
SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

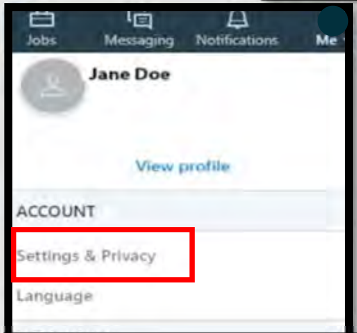
UPDATED DEC 2019

LINKEDIN SMART CARD

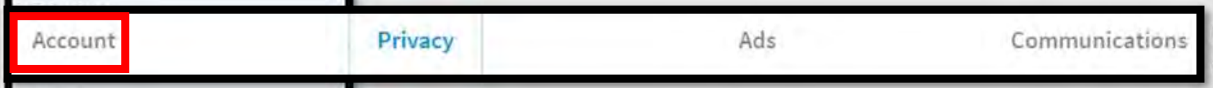
Do's and Don'ts

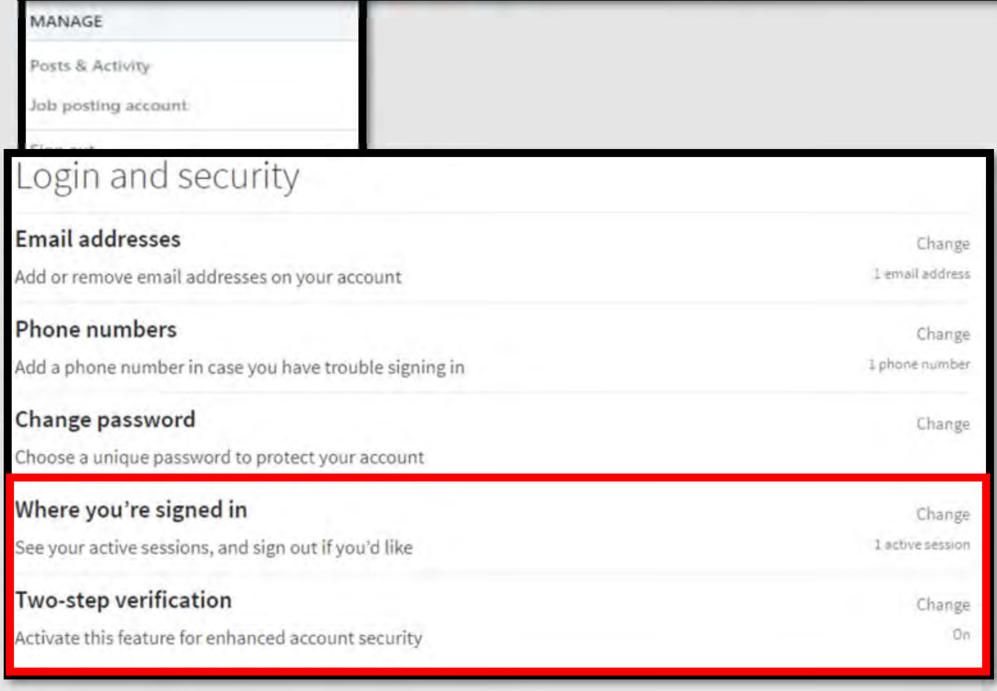
- Do not use an email account that is associated with banking, finances, or other important contacts. Instead, consider creating an email account specific to this site.
- Do not establish connections with people you do not know and trust. Understand that not everyone is who they say they are.
- Do not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





The privacy settings for LinkedIn can be found in the "Me" section on the top right corner of the website (shown above). From the drop down menu, select "Settings & Privacy" (highlighted in **red** to the left). A new screen will appear with a header like the one shown below. The first section we are going to review will be the "Account" settings (highlight in **red** below).





Login and security

Email addresses — Add or remove email addresses on your account — Change — 1 email address

Phone numbers — Add a phone number in case you have trouble signing in — Change — 1 phone number

Change password — Choose a unique password to protect your account — Change

Where you're signed in — See your active sessions, and sign out if you'd like — Change — 1 active session

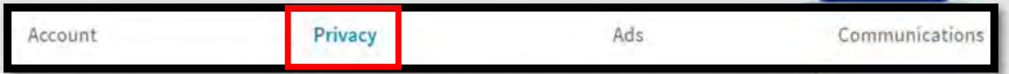
Two-step verification — Activate this feature for enhanced account security — Change — On

One item in the "Login and Security" menu that is important to highlight is the "Where you're signed in" section (shown on the right). In this section you can review any "Active" session you have on your account and where those sessions are located If you see an active session or location that does not look familiar, it is recommended to close all unfamiliar sessions and change your password. Next, at the bottom of the "Login and Security" section, the "Two-step verification" setting allows a user to add a phone number so that a code will be sent as a text acting as a second password. It is recommended you enable this process to add an additional layer of security to your LinkedIn account. This will prevent access to your account in the case your password has been exposed in a security breach.

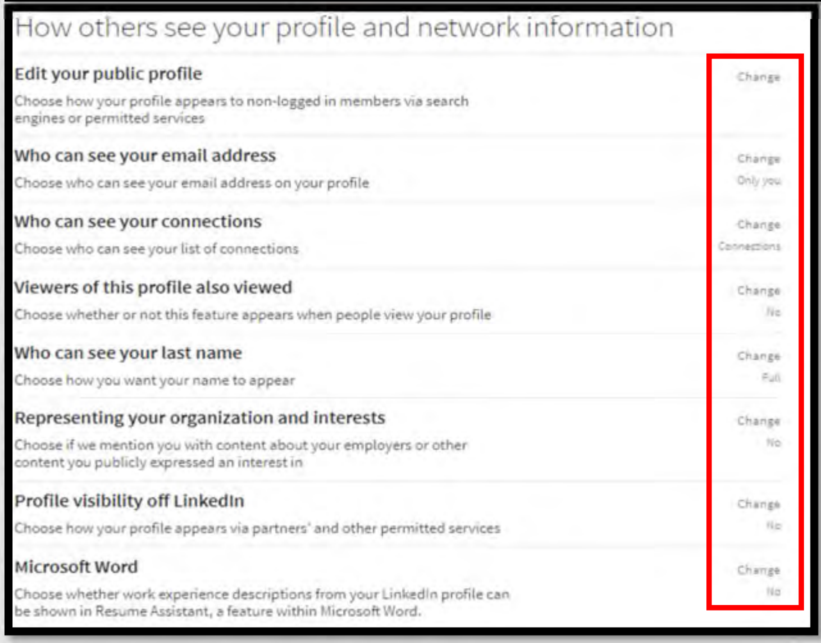
Sign out of your accounts after you use a publicly shared computer or your home computer. #stophackers #keepyouraccountsafe

LINKEDIN SMART CARD

Manage your account information and privacy settings from your Settings & Privacy page. Remember to update update update! #privacymatters.



Account | Privacy | Ads | Communications



How others see your profile and network information

Edit your public profile
Choose how your profile appears to non-logged in members via search engines or permitted services
Change

Who can see your email address
Choose who can see your email address on your profile
Change
Only you

Who can see your connections
Choose who can see your list of connections
Change
Connections

Viewers of this profile also viewed
Choose whether or not this feature appears when people view your profile
Change
No

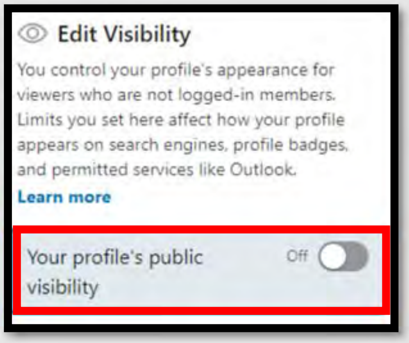
Who can see your last name
Choose how you want your name to appear
Change
Full

Representing your organization and interests
Choose if we mention you with content about your employers or other content you publicly expressed an interest in
Change
No

Profile visibility off LinkedIn
Choose how your profile appears via partners' and other permitted services
Change
No

Microsoft Word
Choose whether work experience descriptions from your LinkedIn profile can be shown in Resume Assistant, a feature within Microsoft Word.
Change
No

Next, go to the menu at the top of the “Settings & Privacy” section and select “Privacy” (shown here in **red**). Choose the “Edit your public profile” link in order to change the visibility of the LinkedIn profile so that search engines will not display the profile when the account name is searched. Purpose is to ensure you do NOT have a public profile.

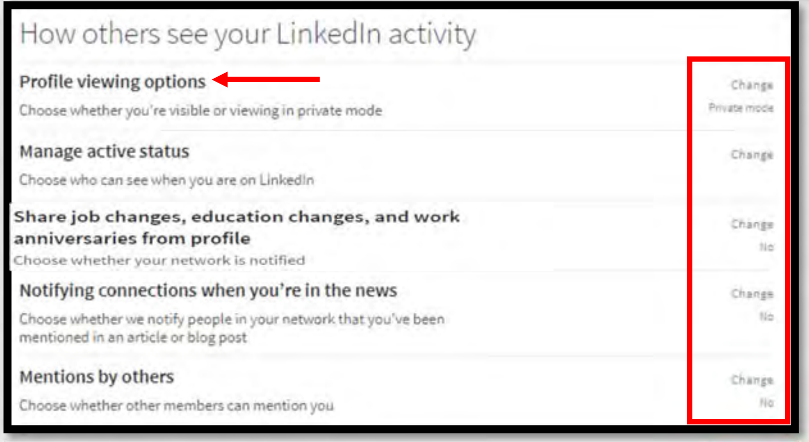


Edit Visibility

You control your profile's appearance for viewers who are not logged-in members. Limits you set here affect how your profile appears on search engines, profile badges, and permitted services like Outlook.

Learn more

Your profile's public visibility — Off



How others see your LinkedIn activity

Profile viewing options
Choose whether you're visible or viewing in private mode
Change
Private mode

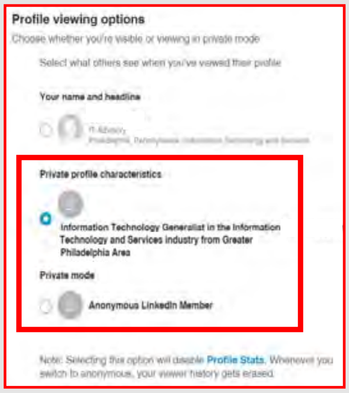
Manage active status
Choose who can see when you are on LinkedIn
Change

Share job changes, education changes, and work anniversaries from profile
Choose whether your network is notified
Change
No

Notifying connections when you're in the news
Choose whether we notify people in your network that you've been mentioned in an article or blog post
Change
No

Mentions by others
Choose whether other members can mention you
Change
No

The “How others see your LinkedIn activity” settings can been seen on the left of the page. In this section, you can change the “Profile viewing options,” which informs other LinkedIn users if you have reviewed their profile (as seen to the right). To remain anonymous when viewing other profiles select the “Private Mode”, button.



Profile viewing options
Choose whether you're visible or viewing in private mode

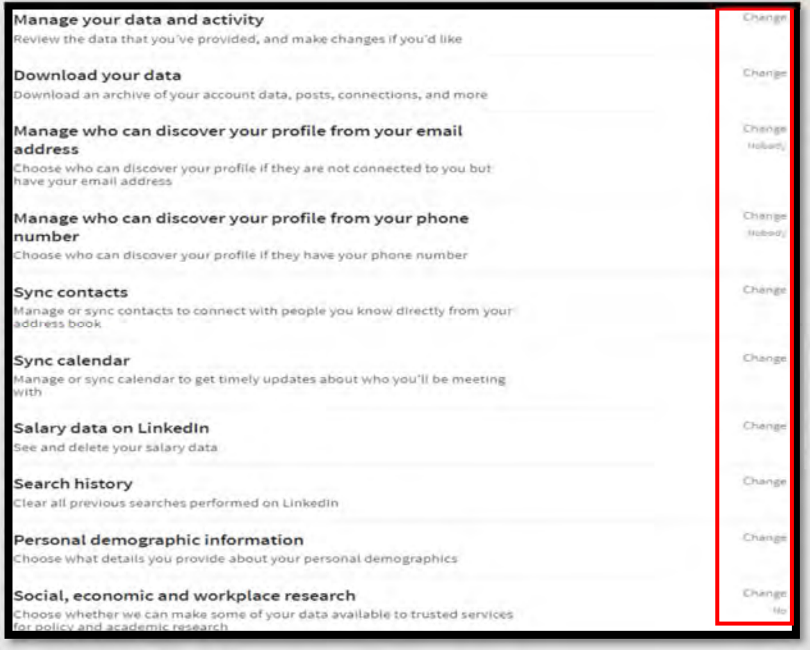
Select what others see when you've viewed their profile

Your name and headline
○ IT Advisory
Philadelphia, Pennsylvania Information Technology and Services

Private profile characteristics
● Information Technology Generalist in the Information Technology and Services industry from Greater Philadelphia Area

Private mode
○ Anonymous LinkedIn Member

Note: Selecting this option will disable Profile Stats. Whenever you switch to anonymous, your viewer history gets erased.



Manage your data and activity
Review the data that you've provided, and make changes if you'd like
Change

Download your data
Download an archive of your account data, posts, connections, and more
Change

Manage who can discover your profile from your email address
Choose who can discover your profile if they are not connected to you but have your email address
Change
Nobody

Manage who can discover your profile from your phone number
Choose who can discover your profile if they have your phone number
Change
Nobody

Sync contacts
Manage or sync contacts to connect with people you know directly from your address book
Change

Sync calendar
Manage or sync calendar to get timely updates about who you'll be meeting with
Change

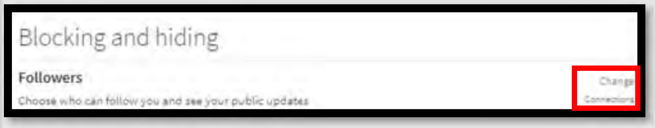
Salary data on LinkedIn
See and delete your salary data
Change

Search history
Clear all previous searches performed on LinkedIn
Change

Personal demographic information
Choose what details you provide about your personal demographics
Change

Social, economic and workplace research
Choose whether we can make some of your data available to trusted services for policy and academic research
Change
No

As you scroll down in the “Privacy” section, notice a section called “Mentions by others”. This function controls whether or not other members can tag you in a post or photo. It is recommended that you turn this function off by toggling the switch to “no”. If working with an already established profile, page four of the LinkedIn card will explain how to find and remove older “mentions”.

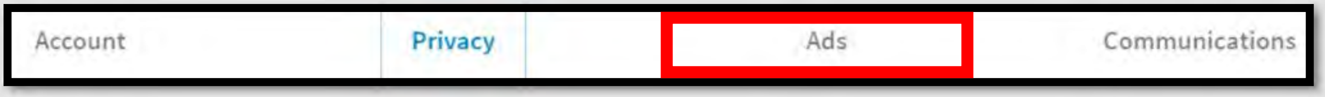


Blocking and hiding

Followers
Choose who can follow you and see your public updates
Change
Connections

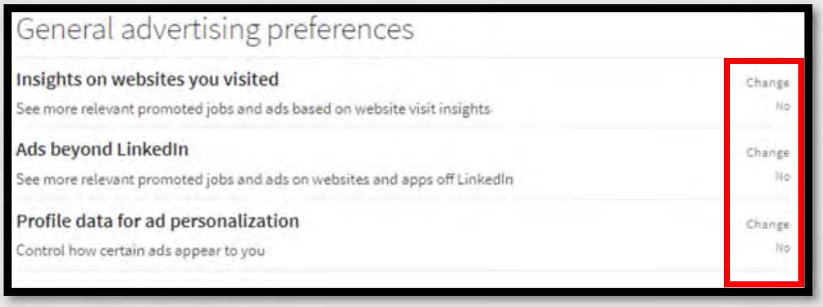
Finally, at the bottom of the “Privacy” section under “Blocking and hiding,” you can turn off the ability of others to “follow” you, especially those not in your “Connections.” From the drop down menu, change “Everyone on LinkedIn” to “Your Connections”.

LINKEDIN SMART CARD



Now let's tackle Advertisements by selecting "Ads" from the top of the "Settings and Privacy" menu. It is recommended you limit the amount of information that LinkedIn is allowed to share with other third party apps / ads as much as possible.

Recommended setting are highlighted in **red** (to the right).

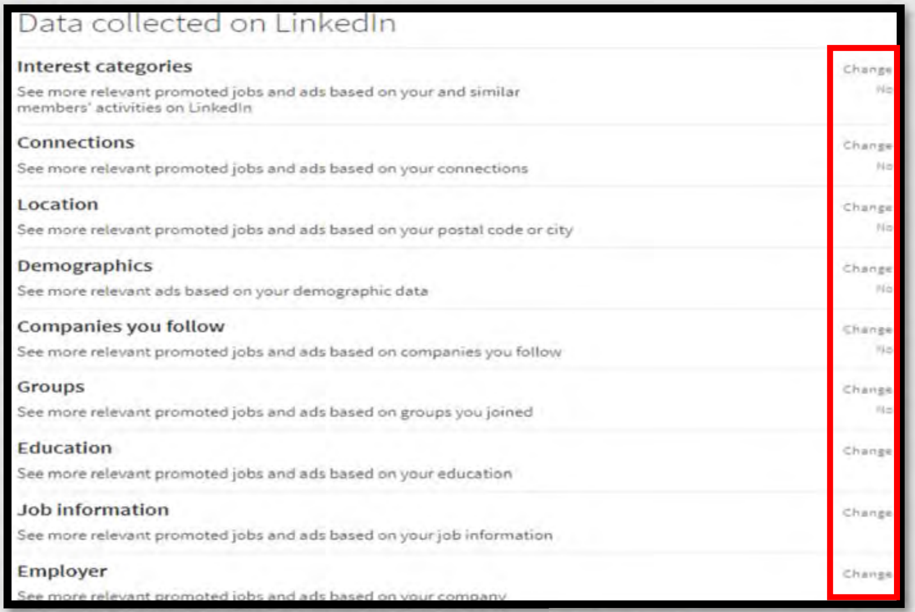


General advertising preferences

Insights on websites you visited
See more relevant promoted jobs and ads based on website visit insights
Change
No

Ads beyond LinkedIn
See more relevant promoted jobs and ads on websites and apps off LinkedIn
Change
No

Profile data for ad personalization
Control how certain ads appear to you
Change
No



Data collected on LinkedIn

Interest categories
See more relevant promoted jobs and ads based on your and similar members' activities on LinkedIn
Change
No

Connections
See more relevant promoted jobs and ads based on your connections
Change
No

Location
See more relevant promoted jobs and ads based on your postal code or city
Change
No

Demographics
See more relevant ads based on your demographic data
Change
No

Companies you follow
See more relevant promoted jobs and ads based on companies you follow
Change
No

Groups
See more relevant promoted jobs and ads based on groups you joined
Change
No

Education
See more relevant promoted jobs and ads based on your education
Change

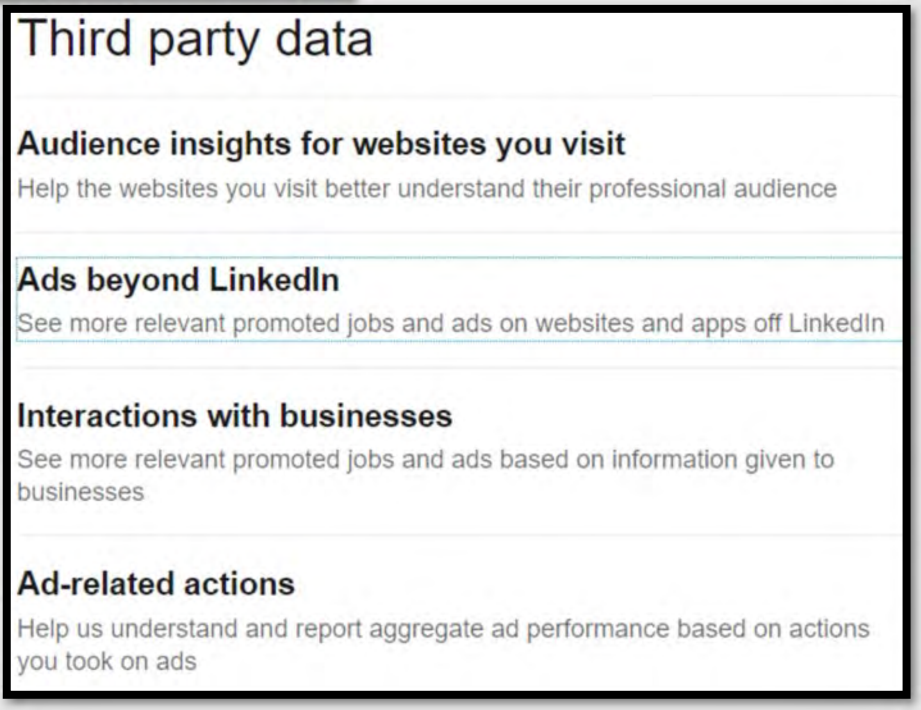
Job information
See more relevant promoted jobs and ads based on your job information
Change

Employer
See more relevant promoted jobs and ads based on your company
Change

Under the "Data collected on LinkedIn" settings, you will find the breakdown pictured to the left. Sharing this information with LinkedIn will leave it, and you vulnerable even if your account is otherwise locked down. It is important to know into exactly how your information is shared should you enable any of these categories. It is recommended that, regardless of your intent in using LinkedIn that you choose NOT to share your data with LinkedIn to avoid it being shared with and used by third party aps.

To the right you will find "Third party data" options that will help to eliminate unwanted ads, marketers collecting your information, and perhaps even spam in your emails! Simply review each section and begin controlling your data today.

Remember, if you are a LinkedIn member but logged out of your account on a browser, LinkedIn may still continue to log your interaction with (their) services on that browser for up to 30 days in order to generate usage analytics for our services, which analytics (they) may share in aggregate form with (their) advertising customers.[1] #manageyourdata



Third party data

Audience insights for websites you visit
Help the websites you visit better understand their professional audience

Ads beyond LinkedIn
See more relevant promoted jobs and ads on websites and apps off LinkedIn

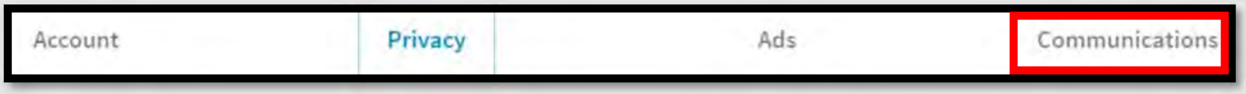
Interactions with businesses
See more relevant promoted jobs and ads based on information given to businesses

Ad-related actions
Help us understand and report aggregate ad performance based on actions you took on ads

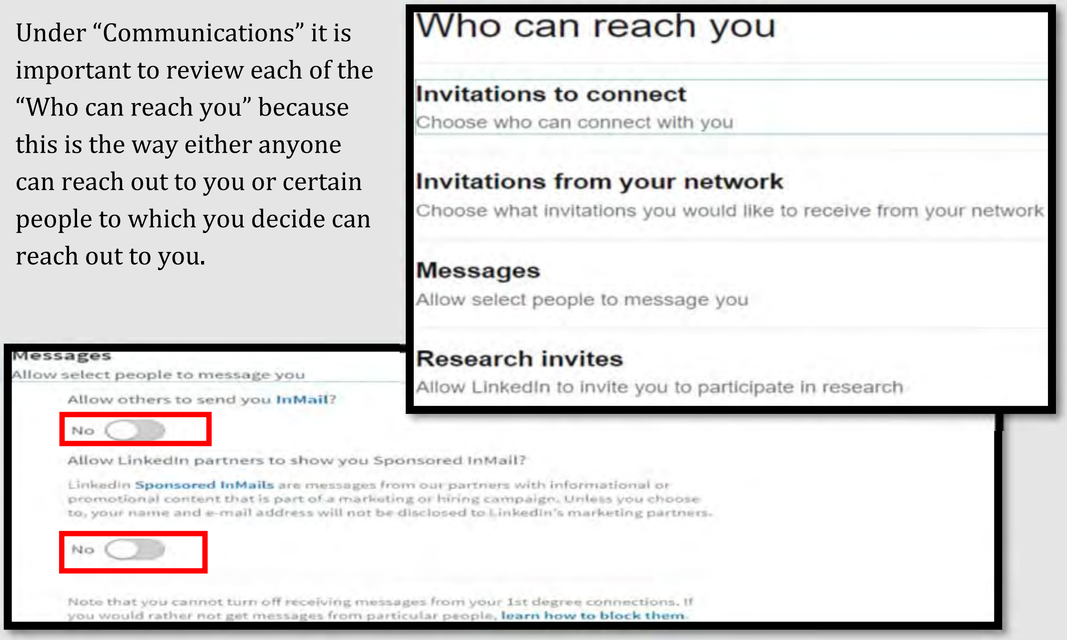
Reference: 1. https://www.linkedin.com/legal/cookie-

Even LinkedIn recommends not putting your email address, home address, or phone number in your profile's Summary. #staysafeonline

LINKEDIN SMART CARD



Under "Communications" it is important to review each of the "Who can reach you" because this is the way either anyone can reach out to you or certain people to which you decide can reach out to you.



Who can reach you

Invitations to connect
Choose who can connect with you

Invitations from your network
Choose what invitations you would like to receive from your network

Messages
Allow select people to message you

Research invites
Allow LinkedIn to invite you to participate in research

Messages
Allow select people to message you

Allow others to send you InMail?

No

Allow LinkedIn partners to show you Sponsored InMail?

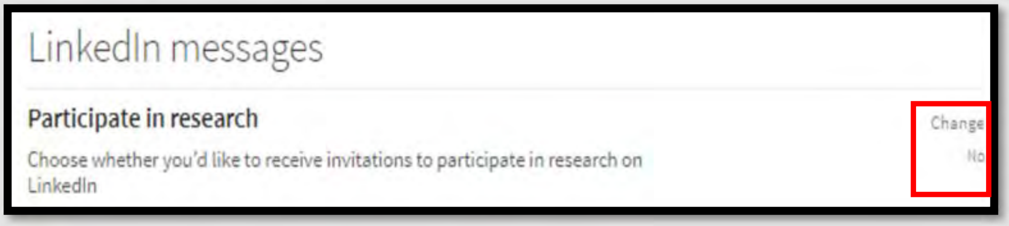
LinkedIn Sponsored InMails are messages from our partners with informational or promotional content that is part of a marketing or hiring campaign. Unless you choose to, your name and e-mail address will not be disclosed to LinkedIn's marketing partners.

No

Note that you cannot turn off receiving messages from your 1st degree connections. If you would rather not get messages from particular people, learn how to block them.

When reviewing your "Communications" on LinkedIn, it is important to consider why you are using LinkedIn…what benefit(s) you hope to gain. Do you desire a job? Are you simply trying to connect with specific people? Depending on your intent, following the recommendations herein will restrict available information on you, therefore limiting LinkedIn's benefits. What is important is to go back and lock these settings down once you have attained your desired goals.

To review (and, when ready, lock down) these settings, select the "Communications" tab at the top of the "Settings and Privacy" section. Review each setting to determine what best suits your desired purpose for using LinkedIn. Recommended settings are highlighted in **red** above.

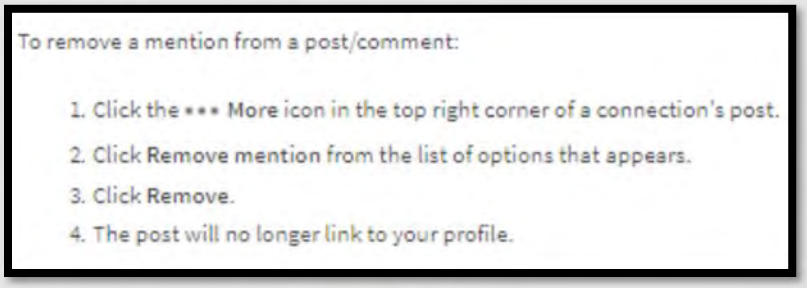


LinkedIn messages

Participate in research
Choose whether you'd like to receive invitations to participate in research on LinkedIn

Change
No

Under the "LinkedIn message" section of the "Communications" tab – it is highly recommended that you choose to not "Participate in research" that LinkedIn conducts. Participating in research events could mean giving up information about yourself that you wouldn't otherwise give up to third parties.



To remove a mention from a post/comment:

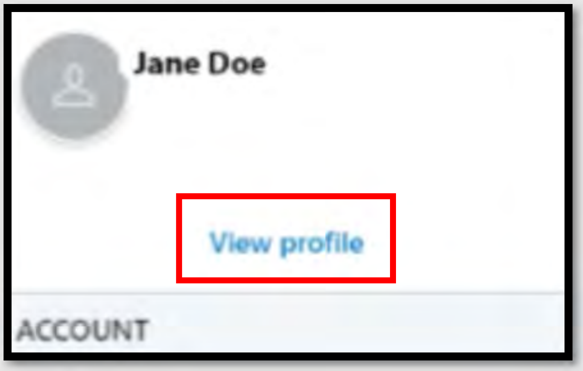
1. Click the ••• More icon in the top right corner of a connection's post.
2. Click Remove mention from the list of options that appears.
3. Click Remove.
4. The post will no longer link to your profile.

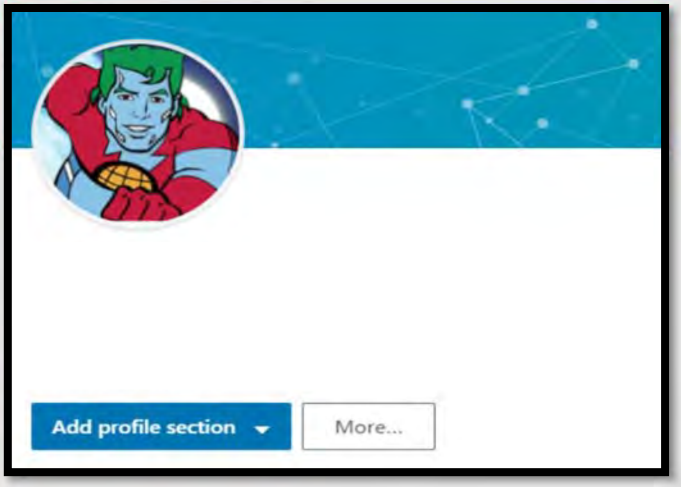
If you happen to be "mentioned" in a post on LinkedIn, you can easily remove yourself from the tag following a few steps as noted above. It is important to manage what these "mentions" link you to or imply about you.

DON'T STOP BECAUSE YOU'RE TIRED. KEEP GOING BECAUSE YOU'RE ALMOST THERE.

#PHISHINGALERT: Messages containing bad spelling, grammar, and that aren't addressed to you personally, or asking you to act immediately are major red flags.

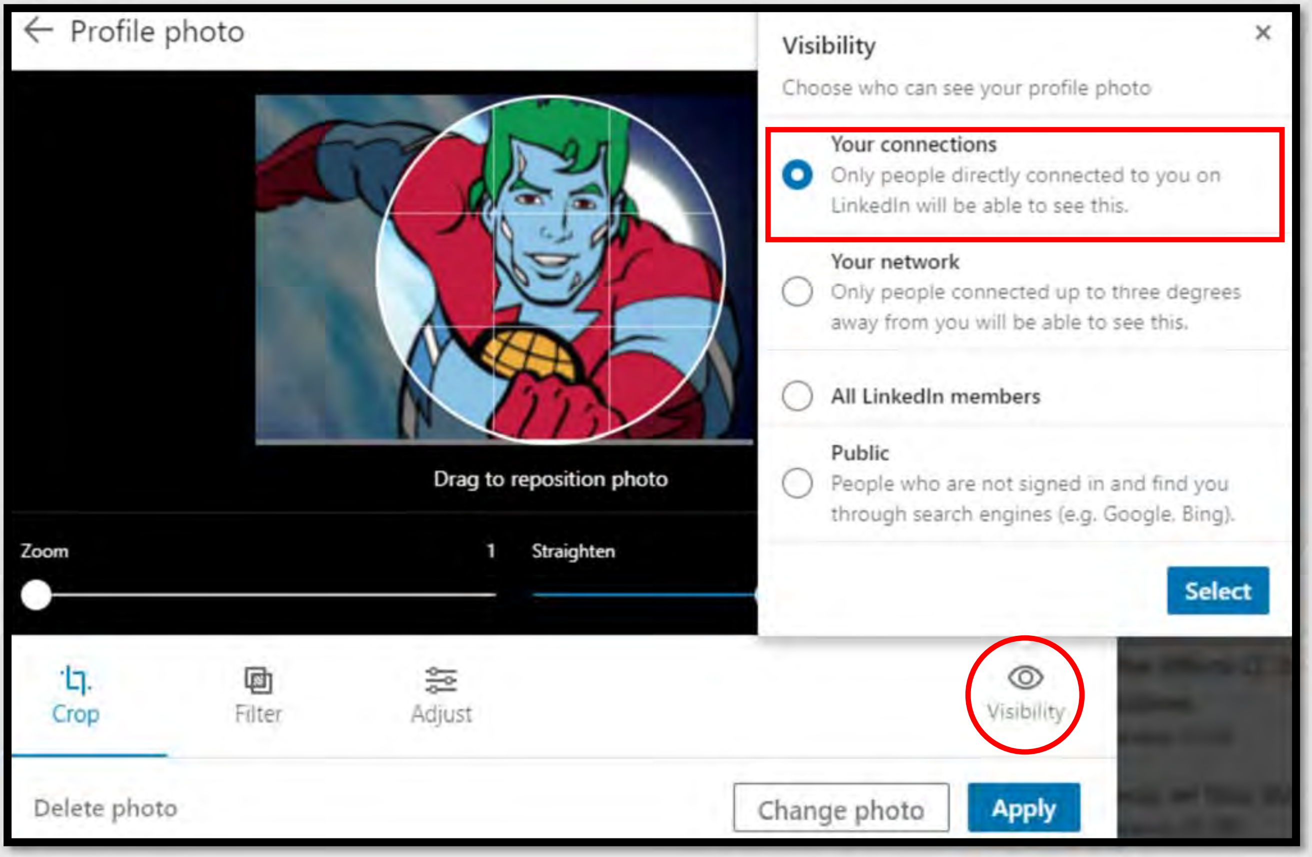
LINKEDIN SMART CARD





It is highly recommended that you do ***not*** use photos of yourself for your profile or header photo. These are viewable to the public and therefore presents an unnecessary vulnerability. If you decide to upload a profile picture, ensure that it is visible only to your connections. Try to hide any obvious identifying marks that could make you more easily identified on any other site or even in person.

To add a picture to your profile, simply select the "View Profile" link in the Menu drop down on the top of your screen. Once there, select the "Picture" icon and navigate to and upload your preferred picture. When complete, look down at the bottom of the window (shown below in the red circle) and select "Visibility. Here you can decide who on LinkedIn is able to view your profile photo: we recommend "Your connections."



Visibility

Choose who can see your profile photo

● Your connections
Only people directly connected to you on LinkedIn will be able to see this.

○ Your network
Only people connected up to three degrees away from you will be able to see this.

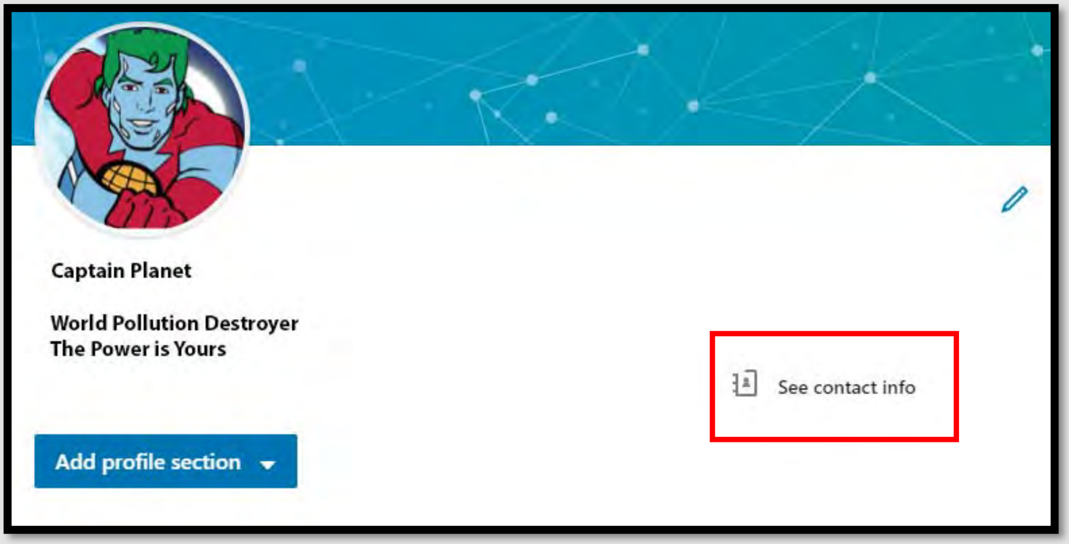
○ All LinkedIn members

○ Public
People who are not signed in and find you through search engines (e.g. Google, Bing).

Stop.Think.Act—if anyone (a connection or not) sends you a message with an attachment, would you open it? Does your action depend on whether or not you think you know, and therefore trust the sender? Even if someone you know sends you an attachment, it is always a good idea to verify with that person (over the phone or face to face) they are the sender before opening it. Remember, people don't always know immediately when they've been hacked. By the time you find out, it could be too late.

Private mode with a Basic LinkedIn account will not allow you to see other users who have viewed your profile. #knowwhatyoudon'tknow

LINKEDIN SMART CARD



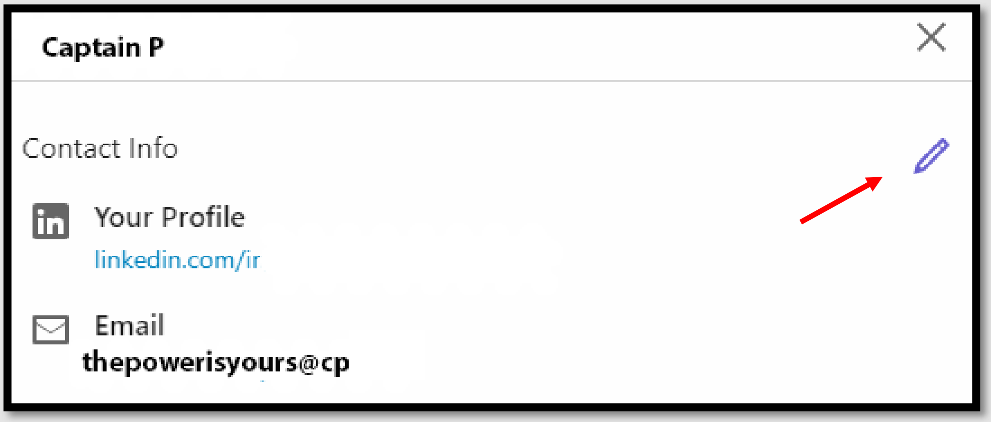
Captain Planet

World Pollution Destroyer
The Power is Yours

See contact info

To further protect your information you will need to check whether your Date of Birth (DoB) is displayed on your profile page. In order to do this, click the "Me" tab at the top right of the page (usually with your picture in it), then select the "view profile" link. This will take you to your profile-viewing page.

On the "view profile" page, locate the "See contact Info" icon as shown above. Find and click on the "Pencil" icon, located to the upper right of the window (see the red arrow to the right). From there review the information shown and edit as necessary. Keep in mind; this is what others can view on your profile.

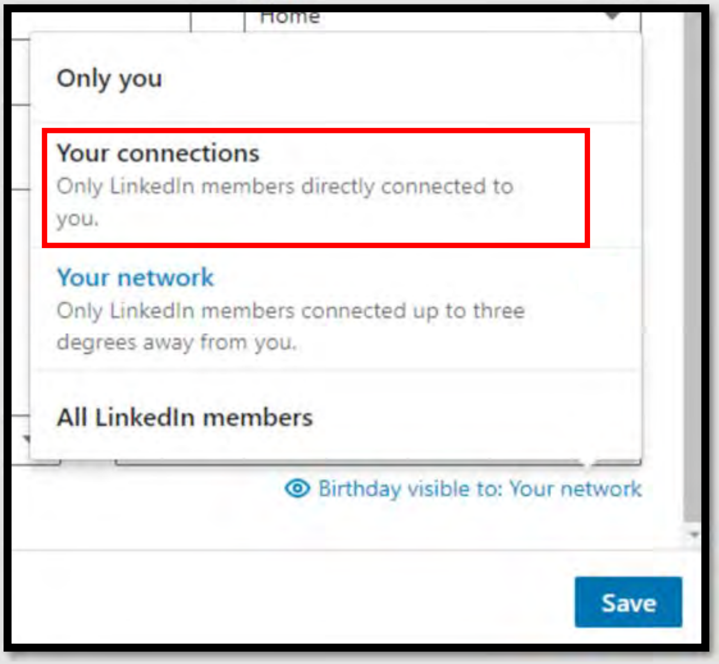


Captain P

Contact Info

Your Profile
linkedin.com/ir

Email
thepowerisyours@cp



Home

Only you

Your connections
Only LinkedIn members directly connected to you.

Your network
Only LinkedIn members connected up to three degrees away from you.

All LinkedIn members

Birthday visible to: Your network

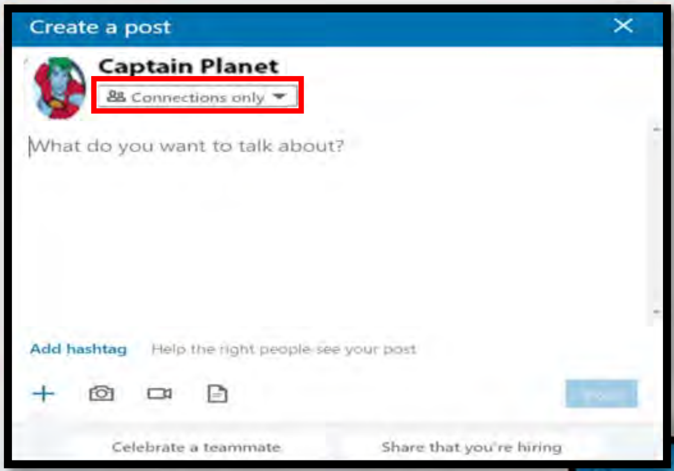
Ensure the information listed in the "view profile" section is not displaying identifiable information to the public. It is recommended to not add a phone number, birthdate, or address to this section, as they are not required.

If it is important to display the birthdate, ensure that it is only visible to Your Connections. This is done by selecting the "Birthday visible to:" link at the bottom of the screen (shown here to the left highlighted in red). Ensure that "Only you" or "Your Connections" are selected to not expose your private information the public.

Select "Save" before you exit out of this screen to keep selected settings.

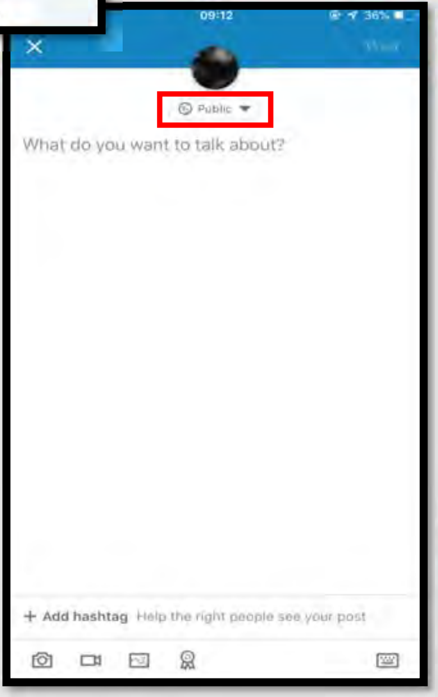
https://www.linkedin.com/help/linkedin will provide you with additional and continuously up to date information on how LinkedIn is changing.

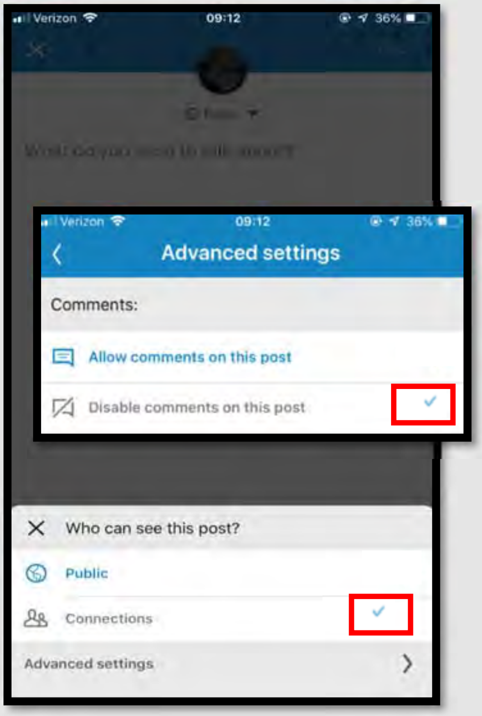
LINKEDIN SMART CARD



When and if you decide to post on LinkedIn, be sure to set the privacy settings of the posts containing personal information so those posts not appear to the public. As shown in the box to the left, posts made public on LinkedIn can be viewed by anyone.

In order to change your privacy settings for your post simply locate the "Post Settings" drop down menu located on the post itself (shown here to the left highlighted in red). From there select the appropriate audience for your post likely "Connections."


09:12
36%
Post
Public
What do you want to talk about?
Add hashtag
Help the right people see your post



Shown to the right and below are the steps necessary to lock down your posts via your mobile device.

In order to change privacy settings for individual posts: simply locate the "Who Can See This Post" (If using an Android smartphone it will be the "visibility settings") drop down menu from the top of the post under your picture (shown here to the right, highlighted in red). From the drop-down, select the appropriate audience for your post. It is recommended to choose "Connections". You can also select "Advanced Settings" to disable comments on the post.

Try Substituting numbers for letters that look similar (for example, substitute "0" for "o" or "3" for "E") for your password to help its strength #updateyourpasssword

Helpful Extra Hints

iOS/Android

To access your "**Privacy Settings**" page from your mobile device simply follow these steps:

1. Tap your profile picture.
2. Tap the Settings icon in the upper right corner.
3. Navigate through the four tabs to adjust settings for "Account", "Privacy"," Ads", or "Communications".

In order to **delete a post from your feed** from your browser:

1. Locate the post you want to delete in your LinkedIn homepage feed.
2. Click the "More" icon in the top right corner of the post. ···
3. Click Delete post from the dropdown.
4. Click Delete to confirm.

iOS/Android

To delete a post from your feed:

1. Locate the post you want to delete in your LinkedIn homepage feed.
2. Tap the More icon in the top right corner of the post.
3. Tap Delete post.
4. Tap Delete to confirm.

Hidden Phone Apps

Hidden Apps Defined

Hidden apps, Vault apps and Ghost apps, are apps that look innocuous, perhaps like a calculator, but are actually used to hide pictures, videos and messages on your smart device. Teens often use these apps because they want to hide their activity from their parents. Most 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	
	Gallery Vault—Hide Pictures & Videos
	Hide Photos, Videos– Hide it pro
	Hide Pictures and Videos
	Keepsafe Photo Vault
	Vault –Hide

iPhone Hidden Apps	
	Fake Calculator App
	Private Photo Vault
	Secret Calculator Fake Vault
	Secret Photo Vault
	Secret Vault Lock Photos

Do's and Don'ts

- Do periodically check your child's smart devices to make sure they have not downloaded anything you have not approved.
- Do think about using a monitoring service (as discussed in the Keeping Children Safe Online Smart card) for your child/teens smart devices, especially if you have given them the ability to download apps themselves.
- Do talk to you children and teens about the dangers of taking and sending nude photos or videos on their smart devices and what repercussions doing so could bring.
- Do not 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.
- Do not 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.
- Do not allow your child to make up his or her own password that they keep to themselves. Always ensure that you can access your child/teens phone at any time.

According to MediaSmarts research twenty-six per cent of students in eighth Grade said a sext they sent was forwarded to other people by the recipient. #protectourchildren

Hidden Phone Apps

Finding 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 devices- In the Google Play Store select the menu then select “My apps & games.” Now, select “Installed” in the middle of your screen. Here you can review all Apps that have been downloaded to this particular device. Additionally, from your “Account” you can review the “Order History” which will also provide you an overview of all purchased apps.
    - iPhone devices- In the App Store find and select the “Account” icon at the top right of your screen. Then select “Purchased” and the account (if you have an Apple Family Sharing Plan more than one account will appear) you wish to review purchases from.
- Another way to review purchased history on smart devices is to find their respective App store and search for “hidden Apps.” Once a list of available apps appears on the screen, you can scroll through the list and if any are downloaded on the device it will be noted to the left side of the screen. This method runs the risk of missing certain apps depending on their category.

Red Flag Indicators

I. 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 usually means one is a Hidden App.

II. If your child seems to try and hide his or her screen any time you enter the room, that may indicate that they are trying to hide their phone activity from you.

How to Prevent Your Child from Downloading Hidden Apps

- iOS has a “Apple Family Sharing Plan” that allows parents to turn on a feature called “Ask to Buy” and when turned on any time your child/teen tries to download something on their iPhone; they must first get it approved by their parents.
- 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.” 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 the password.
- Android Users can setup parental controls in Google Play Store by creating a pin and choosing the maturity levels you want to allow. It is 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 Google Play Store purchases.

Making sure children put up their smart device before bed, in the kitchen or living room, helps to limit the amount of unsupervised time your child has on their device.

UPDATED DEC 2019

Pay Apps

G Pay Pay

Do's and Don'ts

- ♦ 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 Pay stores.

DEFINED

Mobile wallets utilize technology you already own— your smartphone, for example — to allow you to make in-store payments quickly and securely without having to use your credit or debit card. The term digital wallet may refer to both 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 your phone essentially becomes that equivalent of losing your wallet. Whoever finds your phone holds the keys to your identity.

Using pay apps via your smart device means having to be on the alert for cyber criminals.

Using mobile pay apps means you may run the risk of malware infecting your phone and gaining access to payment and identity information.

Gains

Unlike your wallet, if your cell phone is stolen or even misplaced, there are levels of security that will limit or even prevent anyone from accessing the contents of your smartphone. Additionally, the user usually has the ability to "wipe" (delete all personal information) their phone if they feel it has been compromised or simply cannot be found, unlike a physical wallet which becomes immediately compromised.

Using physical debit or credit cards means you run the risk of having your card copied upon scanning it if the machine being used has been tampered with.

The Privacy Policy for each Pay App states what a User consents to when signing up for the Application. Be aware that 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 as well as other possible information. Also be ware that the company may be able to keep the information, for as long as they deem necessary, depending on what the privacy policy states.

Even if you rely solely on Mobile Pay Apps, it is important to have some other form of payment handy in case you are unable to access your phone.

Use any available password protection for your smart device; two-factor authentication, phone log on password, and any other password protection available to ensure the safety of your data.

UPDATED DEC 2019

Pay Apps

App	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
Security	High	Low-Medium	Medium-High	Medium-High	High	Medium	High
International Pay Feature	No	No	Yes, limited	No	No	Yes	US/UK Only
Linked to Bank Account	Transfer to Bank account	Yes	No	Transfer to	Yes	Yes	Yes
Linked to Debit Card	Yes	Yes	Yes	Yes	No	Yes	Yes
Linked to Credit Card	Yes + Fee	Yes +Fee	No	Yes + Fee	No	Yes	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.	Payments can only go to other FB friends.	No	No	No	Yes if accepted
In Store Payments	Yes	Limited acceptance at retailers.	No	No	No	No	Yes

	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
Pros	Rated most secured payment app. Most widely accepted.	User friendly. owned by PayPal	Secure payment method. User friendly.	Easy to use and friends do not need the app to receive money. Can purchase and sell Bitcoin. You can cancel payments after you send them.	Works directly with your bank app.	Offers a money back guarantee, pay bills and reload mobile phones. Powered by PayPal.	Widely accepted, easy to use.
Cons	Transfers can only be made to other Apple device users.	Default privacy setting shares your payment history with the world. Requires recipients to install app. Customer Service	Limited use. No ability to stop a payment on your end once you send it (however, receiver can reject it).	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.	In order to use Pay to Pay (pay a friend etc.) you have to download the Google Pay Send App separately.

DATING SITE BEST PRACTICES

#DATESAFE

Do's and Don'ts

- 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 an individual for the first few times
- Do use more popular dating apps and stay away from less popular sites, which may have less security put in place.
- Do not use dating app sites on any public Wi-Fi. It is important to always make sure your connected through a secured internet connection.
- Do not synch your social media accounts with your dating accounts.
- Do not forget to trust your "gut". If something doesn't feel or seem right it very likely isn't.

Be Anonymous -Don't include your last name or any other identifying information such as your place of work, in your profile or initial communications. Likewise it is a good idea not to include your contact information such as your email address, home address, or phone number on your profile

Create a Different Username/email

Keep your financial information private!

Do not meet at your house or place of work

Do not ask or allow a lot of personal questions save that for the date, this will help to prevent you from giving away to much information.

It is a good idea to stay sober the first few or several encounters.

When possible you should do a search of the individual on the internet (see the Self Assessment Smart Card) before meeting up with the individual.

Online dating scams could run as long as six months before you notice anything suspicious so always be on the look out for unusual conversations such as needing money, or suddenly needing a ride somewhere.

Things to watch out for:

- An early request for photographs or videos
- Anytime anyone asks you for money or donations
- Minors using the platform!
- Users sending harassing or offensive messages
- Users behaving inappropriately after meeting in person
- Fraudulent profiles, if a profile looks incomplete or too good to be true it very well could be.

If someone immediately directs you to a different website from the one you are already on, you could be dealing with a scammer. #themoreyouknow

UPDATED DEC 2019

DATING SITE BEST PRACTICES

When you decide to give someone your phone number, use your cell, rather than your home or work phone. If things don't work out, cell phone numbers are easier to change

HOOKUP APPS: Tinder, Happn, HUD, Bumble

A hookup app is one that accepts and encourages casual sexual encounters or hookups, including one-night stands and other related activity, without necessarily including or requiring emotional bonding or long-term commitments. These types of sites pose a serious danger to Users because it often calls for meeting up someone you do not know and trusting that they are on the up and up.

With these types of apps it is extremely important to make sure that someone you trust knows where you are going and who you are going with before you meet up with someone you may have just met. It is important to note that these apps are not just used for hooking up and can be used to develop relationships however it is not its primary function.

CASUAL DATING SITES: Match, Zoosk, POF, OkCupid

Online dating services such as these allow users to become "members" by creating a profile and uploading personal information including (but not limited to) age, gender, sexual orientation, location, likes and dislikes. Most of thes services offer digital messaging, as well as online chat, telephone chat (VOIP), and message boards. Members can constrain their interactions to the online space, or they can arrange a date to meet in person. These type of dating sites usually mean a person is looking for something a bit more long term than a “hookup” and many times lead to a relationship, in fact many of these sites let you pick your level of interest in the dating world.
These sites target specific demographics based on features like shared interests, location, religion, or relationship type. Most of these sites are completely free and depend on advertising for revenue. Others offer a free registration and use, with optional, paid, premium services.

Larger Dating Apps: eHarmony, Christian Mingle, Farmers Only

Online dating services such as these tend to be more methodical in their matching of partners. They usually have a signature questionnaire (much like eHarmony) that helps to match with people who don’t just fit or share interests, but instead are compatible with each other in terms of emotional and relationship values. These sites go a bit deeper than any of the other It also helps you pace your communication with your matches, so that each of you remains comfortable and things don’t move too quickly.
These sites or this level of online dating usually requires a form of payment and a membership to the site for access to its full content. Mainly these are sites people use when they are serious about dating and looking for a partner that they can marry.

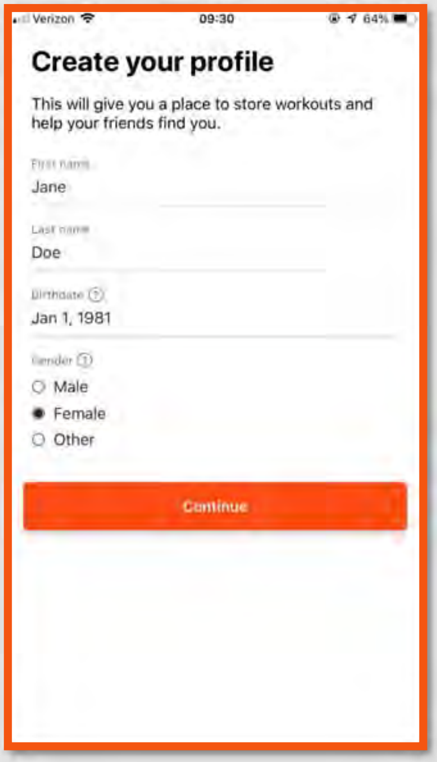
Millions of Americans use dating sites, social networking sites, and chat rooms to meet people. And many forge successful relationships. But scammers also use these sites to meet potential victims. They create fake profiles to build online relationships, and eventually convince people to send money in the name of love. Some even make wedding plans before disappearing with the money.

An online love interest who asks for money is almost certainly a scam artist
-Federal Trade Commission

Fitness Apps

Do's and Don'ts

- Do make sure that your profile is not Public. It is also recommended that you limit what information you put on your profile even if it is private.
- Do make sure you keep your fitness app activity 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 photo. Profile photos are viewable to the public.
- Do not link your fitness app to any of your social media accounts. Doing so could publish your routes and times you exercise on those accounts for others to see.
- Do not track exercises that begin at your own home, work place, or school.
- Do not chose 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

This will give you a place to store workouts and help your friends find you.

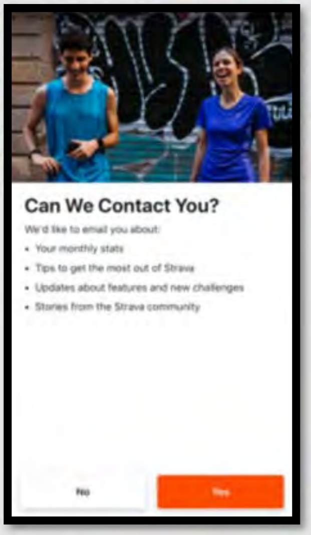
First name
Jane

Last name
Doe

Birthdate
Jan 1, 1981

Gender
○ Male
● Female
○ Other

Strava sells itself as an activity tracker with the ability to also social network: Users can view the most popular bike or running paths among other Strava users, follow their friends' running routes, even log group exercises. It's almost vital to the app that you share your location data in order to get the most out of it, and that comes with a big privacy trade-off. Late last year Strava's heat map came under fire for posting its users whereabouts publicly online. Allowing others to view your route location leaves users extremely vulnerable to potential attacks by stalkers or by criminals looking to know when you may or may not be home. The following describes the best way to create an account on Strava while maintaining the utmost privacy to ensure one's safety.



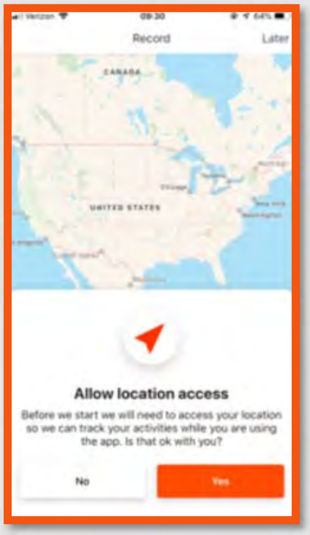
Can We Contact You?

We'd like to email you about:

- Your monthly stats
- Tips to get the most out of Strava
- Updates about features and new challenges
- Stories from the Strava community

First, start by creating your account, only putting in the minimum personal information required to create your log on (shown here to the left). Later you will have the option to build upon your "Profile" by adding additional information about yourself, but this is not recommended.

Next (shown on the top right), Strava will ask you if they can contact you to push you monthly reports etc. Though this seems benign, it is not recommended that you allow this function as there could be more information Strava shares with you or about you to others. The next screen will ask you if you want to allow Strava to utilize your location. Although this is a big part of the app, it is strongly recommended that you not allow your location to be accessed.

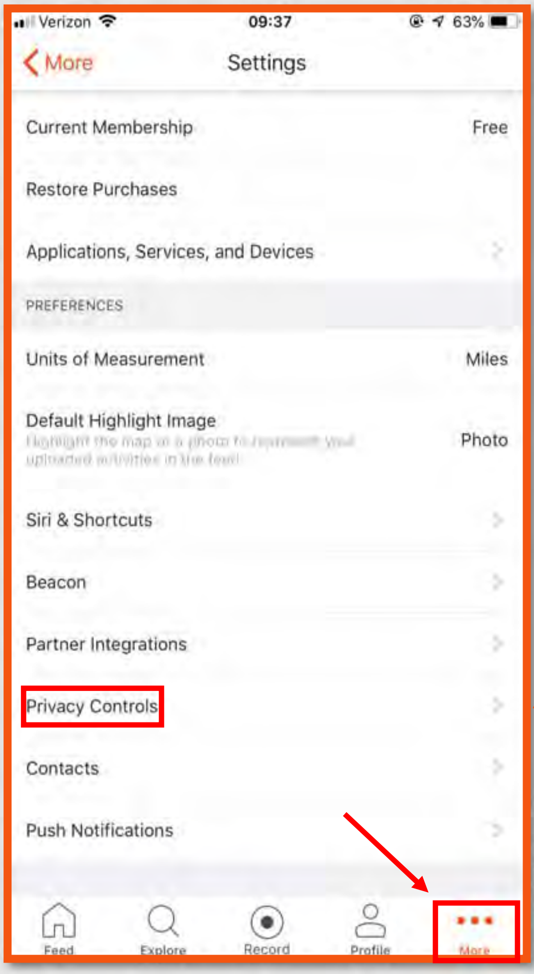


Allow location access

Before we start we will need to access your location so we can track your activities while you are using the app. Is that ok with you?

Always go back and check the privacy settings in your fitness app after an update has taken place to ensure they remained intact.

Fitness Apps



Verizon 09:37 63%

More Settings

Current Membership Free

Restore Purchases

Applications, Services, and Devices

PREFERENCES

Units of Measurement Miles

Default Highlight Image Photo
Highlight the map or a photo to represent your uploaded activities in the feed

Siri & Shortcuts

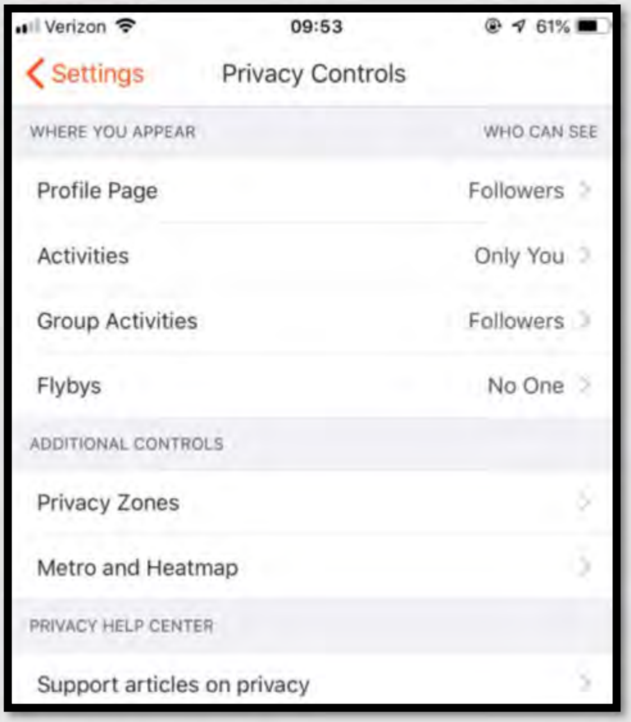
Beacon

Partner Integrations

Privacy Controls

Contacts

Push Notifications



Verizon 09:53 61%

Settings Privacy Controls

WHERE YOU APPEAR	WHO CAN SEE
Profile Page	Followers
Activities	Only You
Group Activities	Followers
Flybys	No One

ADDITIONAL CONTROLS

Privacy Zones

Metro and Heatmap

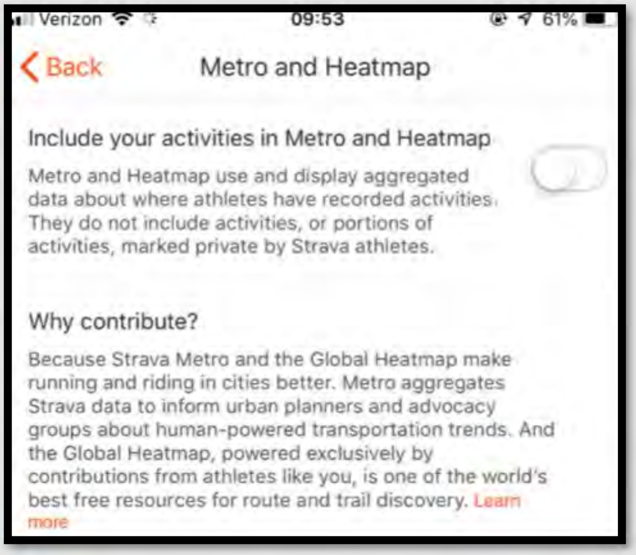
PRIVACY HELP CENTER

Support articles on privacy

Once you have completed the set-up process, there are still several settings that must be set in order to best protect your privacy. From the Home screen, look to the bottom of the page (top left if you are using an Android) and select the "More" tab (shown to the left highlighted in red). From there select the "Settings" tab and scroll to the bot-tom and select "Privacy Controls" (shown to the left).

Under “Privacy Controls” it is recommended that you change any of the tabs under “Where You Appear” from Public to either Followers or Only You to maximize your privacy.

The "Privacy Zones" function allows its Users to draw a privacy circle around a certain area such as their house or work. When the User runs in that circle it is automatically hidden from all other Users. The down side is that if the User steps outside of that designated circle, that data will become public automati-



Verizon 09:53 61%

Back Metro and Heatmap

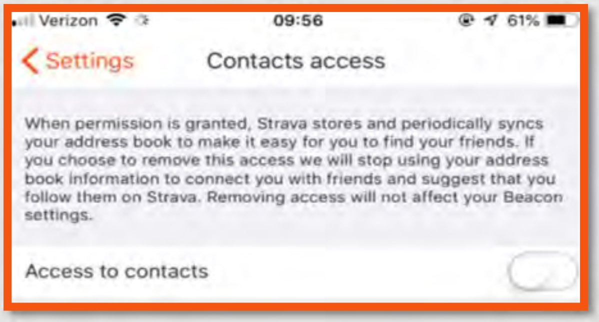
Include your activities in Metro and Heatmap

Metro and Heatmap use and display aggregated data about where athletes have recorded activities. They do not include activities, or portions of activities, marked private by Strava athletes.

Why contribute?

Because Strava Metro and the Global Heatmap make running and riding in cities better. Metro aggregates Strava data to inform urban planners and advocacy groups about human-powered transportation trends. And the Global Heatmap, powered exclusively by contributions from athletes like you, is one of the world's best free resources for route and trail discovery. Learn more

Strava now has a function that allows you to turn on or off whether or not a us-ers activities show up on their “Metro and Heatmap.” It is recommended that users leave this function “off”. Next, go back to the “Settings” section and scroll to the “Contacts” tab. Here it is recommended that users do not allow Strava to access your Contacts.



Verizon 09:56 61%

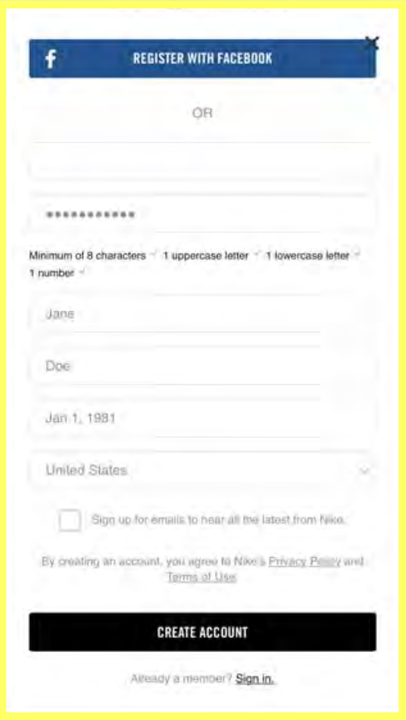
Settings Contacts access

When permission is granted, Strava stores and periodically syncs your address book to make it easy for you to find your friends. If you choose to remove this access we will stop using your address book information to connect you with friends and suggest that you follow them on Strava. Removing access will not affect your Beacon settings.

Access to contacts

Even with phone apps, it is important to make sure you keep a strong password to prevent anyone from accessing your account.

Fitness Apps



REGISTER WITH FACEBOOK

OR

••••••••••••

Minimum of 8 characters ✓ 1 uppercase letter ✓ 1 lowercase letter ✓ 1 number ✓

Jane

Doe

Jan 1, 1981

United States

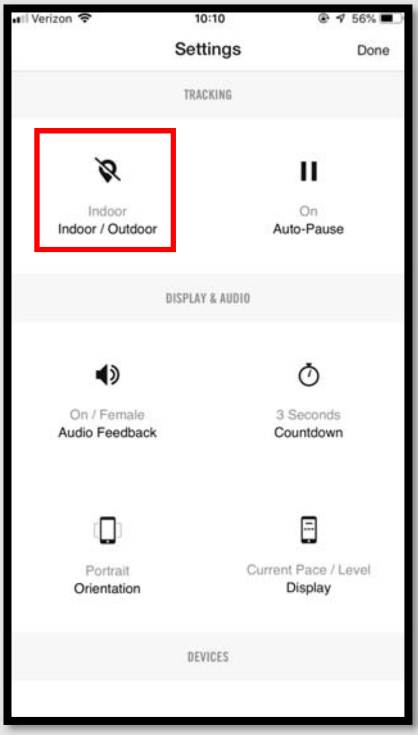
□ Sign up for emails to hear all the latest from Nike.

By creating an account, you agree to Nike's Privacy Policy and Terms of Use.

CREATE ACCOUNT

Already a member? Sign in.

→



Verizon 10:10 56%

Settings Done

TRACKING

Indoor / Outdoor: Indoor

Auto-Pause: On

DISPLAY & AUDIO

Audio Feedback: On / Female

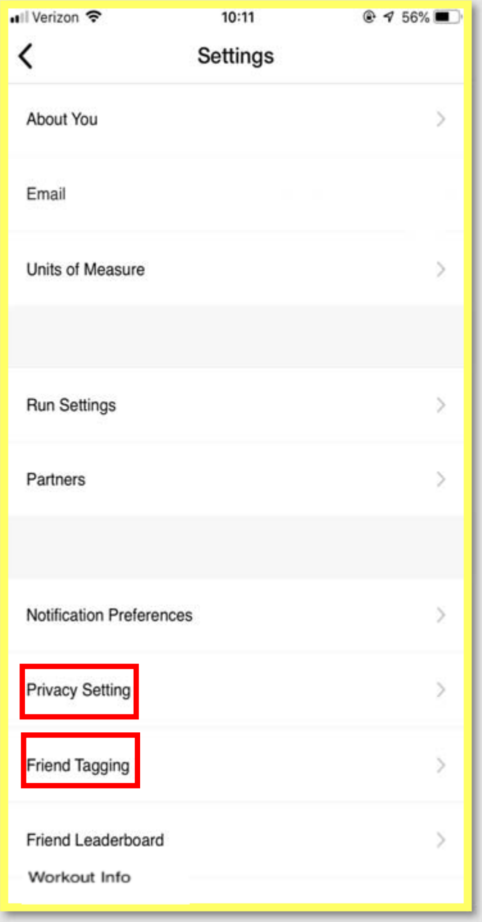
Countdown: 3 Seconds

Orientation: Portrait

Display: Current Pace / Level

DEVICES

→



Verizon 10:11 56%

Settings

About You

Email

Units of Measure

Run Settings

Partners

Notification Preferences

Privacy Setting

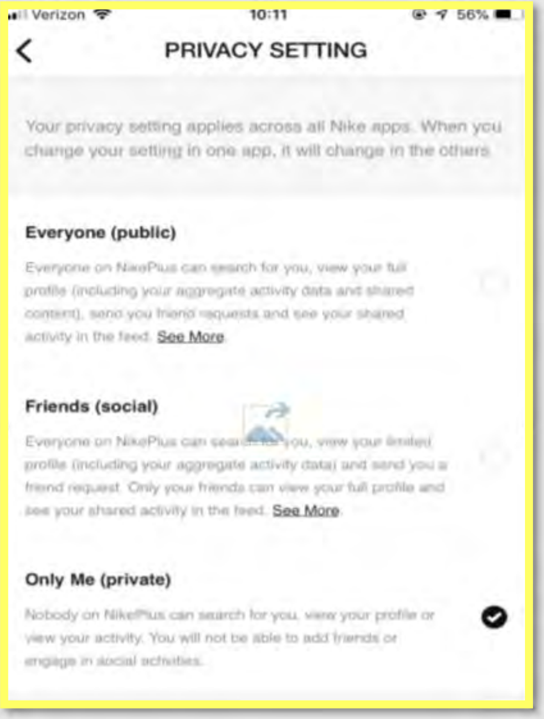
Friend Tagging

Friend Leaderboard

Workout Info

Nike's Run Club fitness app is widely popular and is known for being able to publish your run or other activities directly to your social media upon completion. Unfortunately, this also includes a user's run routes. When creating a User Account for this app it is important to limit the amount of information about one's self to only the minimum required. After putting in your basic information and creating your account, Nike will ask you a series of "Settings" questions, one of which (shown in the middle top screen in red) is whether or not the user wants to allow the App to track them (or use their location). It is recommended that

In order to get to the main “Settings” the User will need to select the “Picture” icon at the top left of their screen and then select the “Settings” icon in the middle of the page. Scroll to the “Privacy Setting” tab. It is recommended that Users set their privacy to “Only Me” or “Friends.” Next, head back to the “Settings” menu and select “Friend Tagging to turn off this function. Finally scroll to the Workout Info tab where it is recommended that Users turn this function off so as not to share unwanted information.



Verizon 10:11 56%

PRIVACY SETTING

Your privacy setting applies across all Nike apps. When you change your setting in one app, it will change in the others.

Everyone (public) ○

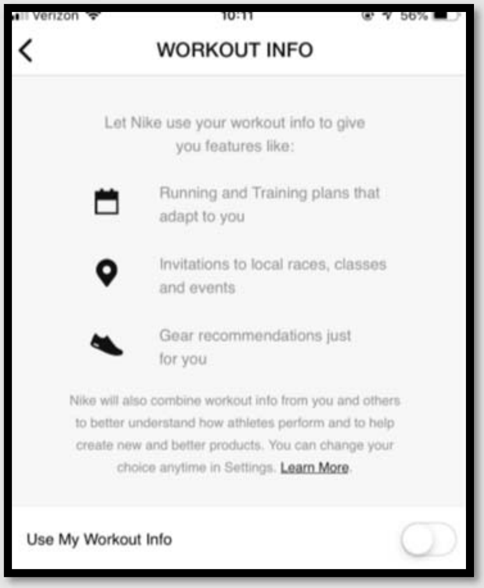
Everyone on NikePlus can search for you, view your full profile (including your aggregate activity data and shared content), send you friend requests and see your shared activity in the feed. See More.

Friends (social) ○

Everyone on NikePlus can search for you, view your limited profile (including your aggregate activity data) and send you a friend request. Only your friends can view your full profile and see your shared activity in the feed. See More.

Only Me (private) ✓

Nobody on NikePlus can search for you, view your profile or view your activity. You will not be able to add friends or engage in social activities.



Verizon 10:11 56%

WORKOUT INFO

Let Nike use your workout info to give you features like:

- Running and Training plans that adapt to you
- Invitations to local races, classes and events
- Gear recommendations just for you

Nike will also combine workout info from you and others to better understand how athletes perform and to help create new and better products. You can change your choice anytime in Settings. Learn More.

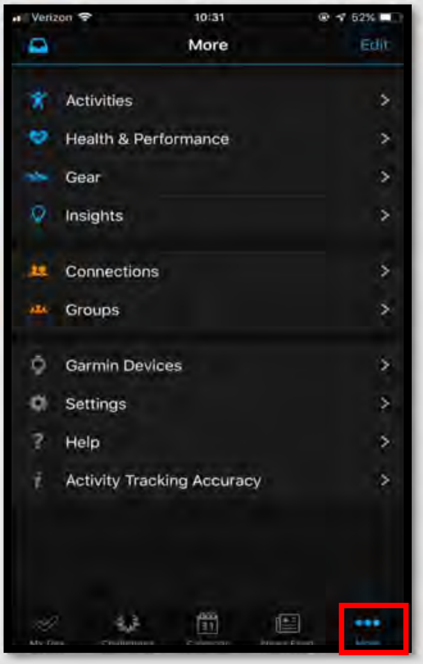
Use My Workout Info ○

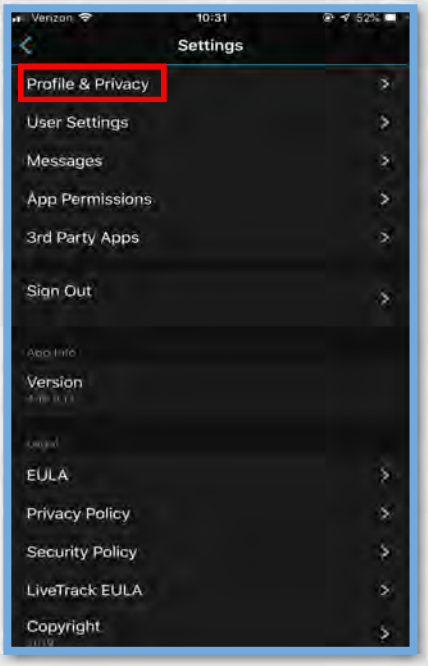
If you allow other third party apps to connect to your fitness app be sure to check both apps for up to date privacy settings.

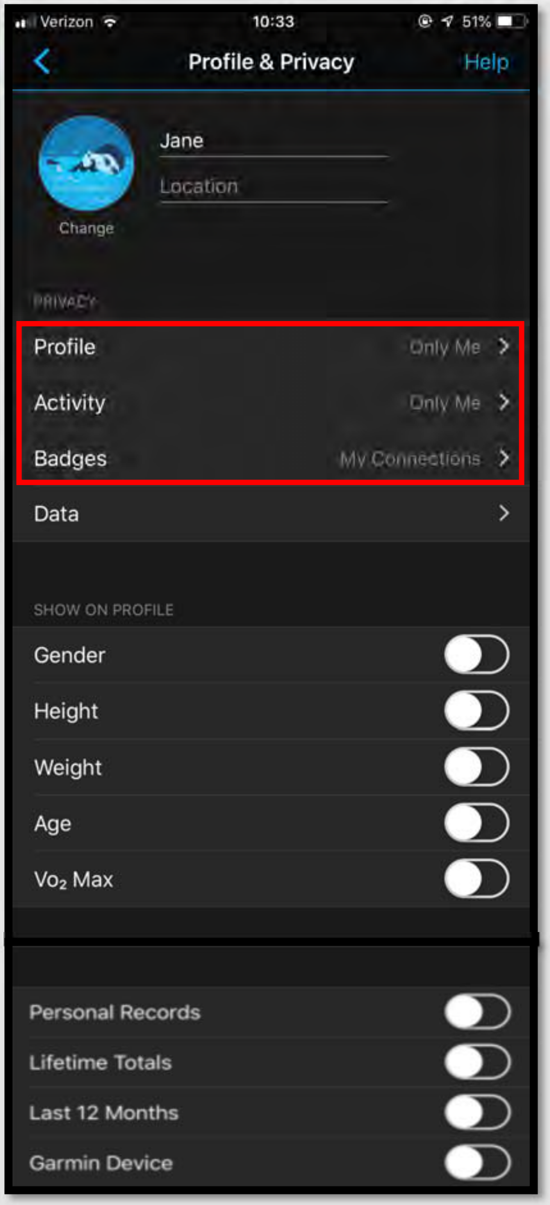
Fitness Apps

GARMIN fitbit STRAVA NTC

Connecting with friends on fitness apps means that you must be concerned with their privacy settings as well as yours.






Verizon 10:33 51%

Profile & Privacy — Help

Jane

Location

Change

PRIVACY

Profile: Only Me

Activity: Only Me

Badges: My Connections

Data

SHOW ON PROFILE

Gender ○

Height ○

Weight ○

Age ○

Vo_2 Max ○

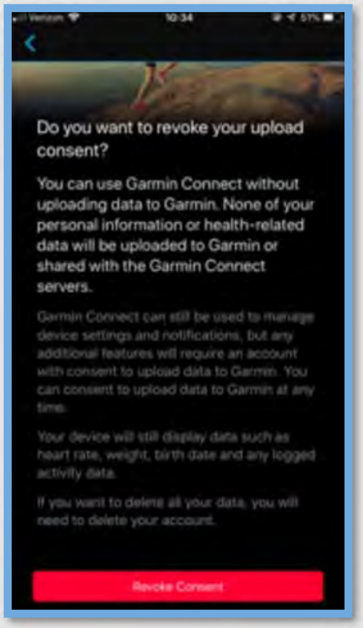
Personal Records ○

Lifetime Totals ○

Last 12 Months ○

Garmin Device ○

Many of the Garmin exercise apps offer a lot for the user to share with friends or the public. If these settings are not set correctly, they will automatically share your information with the Public. From the Home screen look to the bottom of the page (top left for Android users) for the "More" tab (shown above to the left in red), select this, then select the "Settings" tab to begin locking down your profile. Now select "Profile & Privacy" to look over the "privacy" section. It is recommended that the tabs in this section (highlighted to the right in red) be set to "only me" or "My Connections." Here you can also limit what details about yourself are shown on your profile.

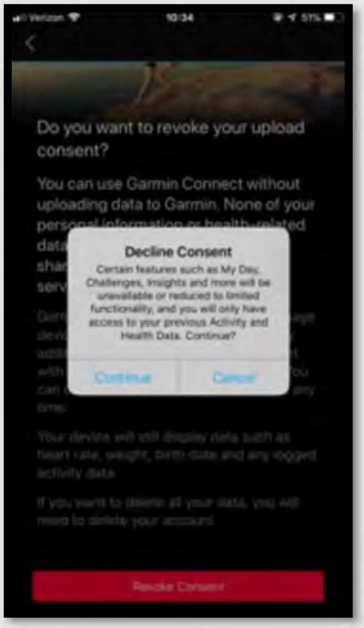

Do you want to revoke your upload consent?

You can use Garmin Connect without uploading data to Garmin. None of your personal information or health-related data will be uploaded to Garmin or shared with the Garmin Connect servers.

Garmin Connect can still be used to manage device settings and notifications, but any additional features will require an account with consent to upload data to Garmin. You can consent to upload data to Garmin at any time.

Your device will still display data such as heart rate, weight, birth date and any logged activity data.

If you want to delete all your data, you will need to delete your account.

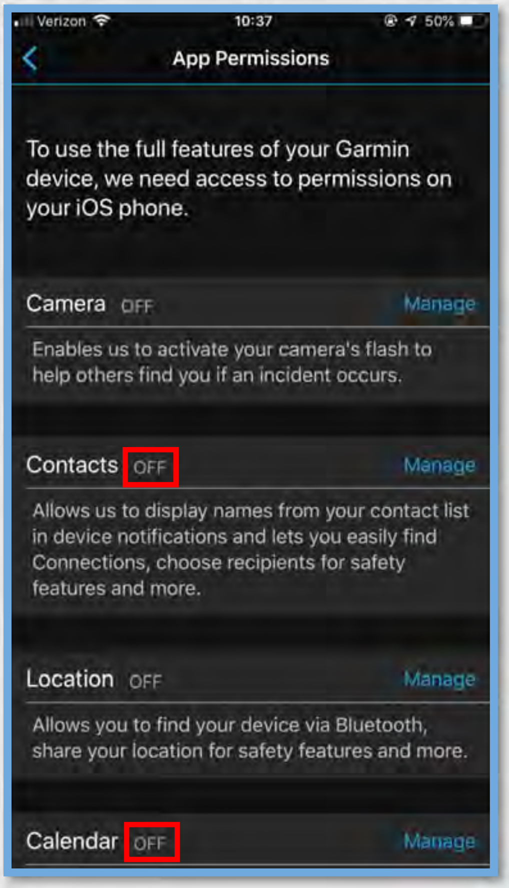

Decline Consent

Certain features such as My Day, Challenges, Insights and more will be unavailable or reduced to limited functionality, and you will only have access to your previous Activity and Health Data. Continue?

Now, select the “Data” tab under the “Privacy” section, here you will find three different tabs; “Data Upload,” “Insights,” and “Popularity Routing.” It is recommended that you select and turn off the “Popularity Routing” function. Next, Users may want to review the “Data Upload” section to review what information they have allowed Garmin access too and decide whether or not they want to continue to provide consent (shown here to the left). Users can do the same for the “Insights” tab after reviewing the consent policy.

Fitness Apps

Finally, head back to the "Settings" section and select the "App Permissions" tab to review what permissions you have allowed Garmin access to. Here it is recommended that you not allow Garmin access to your "Contacts" or "Calendar" and carefully consider whether or not you want to allow the app to have access to your "Camera" and "Location."


Verizon 10:37 50%

App Permissions

To use the full features of your Garmin device, we need access to permissions on your iOS phone.

Camera OFF Manage

Enables us to activate your camera's flash to help others find you if an incident occurs.

Contacts OFF Manage

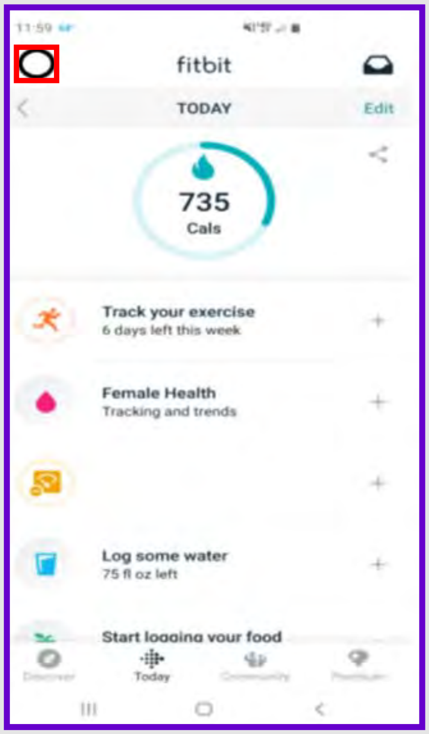
Allows us to display names from your contact list in device notifications and lets you easily find Connections, choose recipients for safety features and more.

Location OFF Manage

Allows you to find your device via Bluetooth, share your location for safety features and more.

Calendar OFF Manage

Fitbit


11:59

fitbit

TODAY Edit

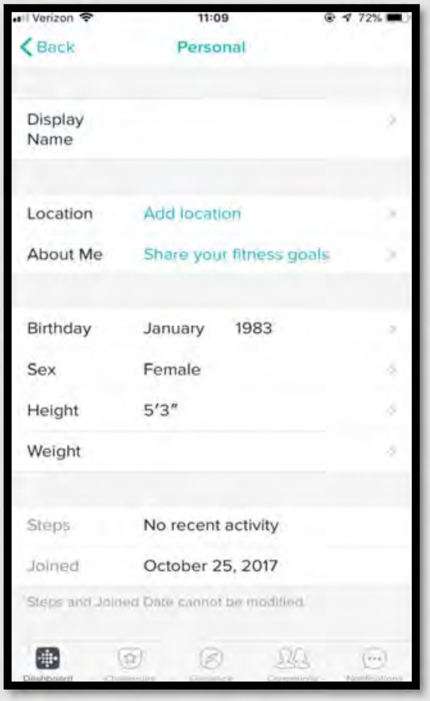
735 Cals

Track your exercise
6 days left this week

Female Health
Tracking and trends

Log some water
75 fl oz left

Start logging your food


Verizon 11:09 72%

Back Personal

Display Name

Location Add location

About Me Share your fitness goals

Birthday January 1983

Sex Female

Height 5'3"

Weight

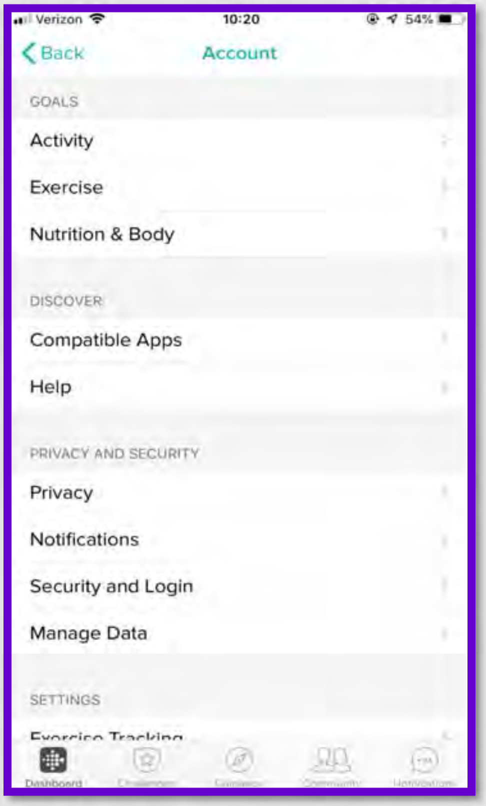
Steps No recent activity

Joined October 25, 2017

Steps and Joined Date cannot be modified.

FitBit is a physical activity tracker designed to help users become more active. By default, older versions of FitBit pushed user's workout information to the public. The company has since changed this setting in order to protect its Users. Now, user information is private until it is configured otherwise. Though it is presumed that your privacy settings are set in this app, it is a great idea to review those settings to make sure they are set to your personal standards.

In order to review your Fitbit account head to your Home Screen and select the "Picture Icon card" in the top Left corner (shown above in red). From here you can select your user account at the top of the page. Now, select "Personal" where you will then want to review whether or not you have allowed for your "location" to be turned on along with which personal data you have provided to Fitbit. Next, you will want to head back to the "Account" section. Here you can review each of your FitBit settings and then head to the "Privacy and Security" section where you will want to pay special attention to each setting.


Verizon 10:20 54%

Back Account

GOALS

Activity

Exercise

Nutrition & Body

DISCOVER

Compatible Apps

Help

PRIVACY AND SECURITY

Privacy

Notifications

Security and Login

Manage Data

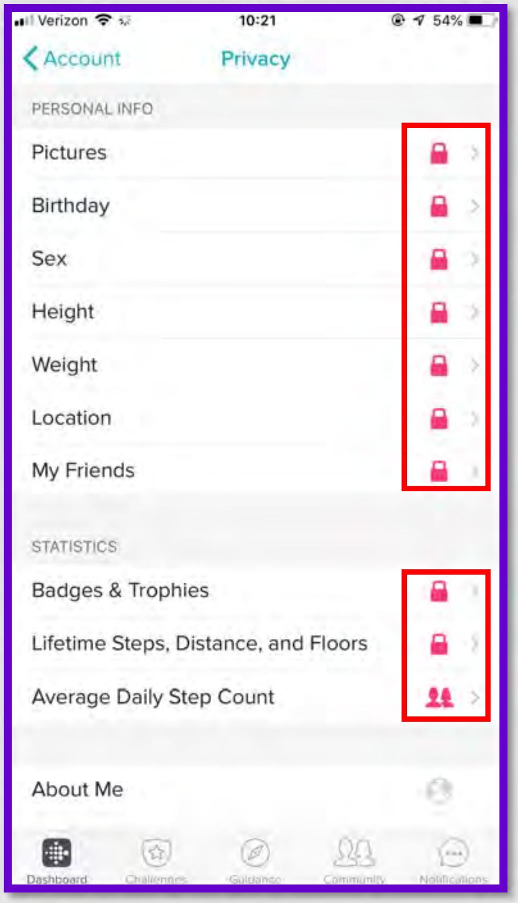
SETTINGS

Exercise Tracking

Anytime your Fitness app has an update it is a good idea to use this time to also update your password.

Fitness Apps

Don't just set the settings within the Fitness App, make sure you go into your phones settings and update what you do and do not allow for that app from your phone.



Verizon 10:21 54%

‹ Account Privacy

PERSONAL INFO

Pictures 🔒

Birthday 🔒

Sex 🔒

Height 🔒

Weight 🔒

Location 🔒

My Friends 🔒

STATISTICS

Badges & Trophies 🔒

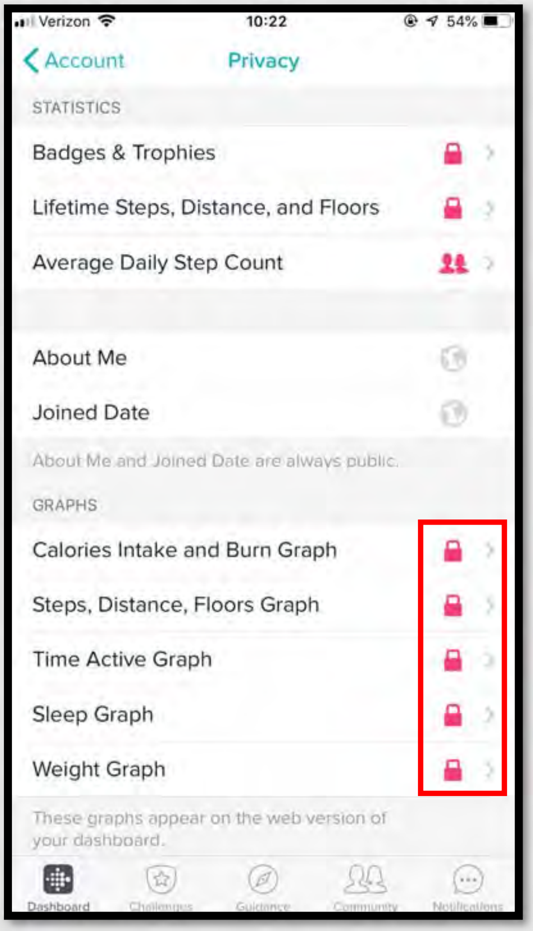
Lifetime Steps, Distance, and Floors 🔒

Average Daily Step Count 👥

About Me 🌐

Once you are in the "Privacy" section there are a lot of different tabs (highlighted in red to the left) that will need to be checked for privacy. It is recommended that you not share any information that might be considered PII or that you would not otherwise want available to the public. Remember the "About me" section is always going to be available to the public so it is important to note what information in available there.

Now that you have reviewed and updated all privacy settings you may want to go back to the "Account" section and review the "Manage Data" section where you can delete or limit what third party apps have access to your Fitbit and vice versa.



Verizon 10:22 54%

‹ Account Privacy

STATISTICS

Badges & Trophies 🔒

Lifetime Steps, Distance, and Floors 🔒

Average Daily Step Count 👥

About Me 🌐

Joined Date 🌐

About Me and Joined Date are always public.

GRAPHS

Calories Intake and Burn Graph 🔒

Steps, Distance, Floors Graph 🔒

Time Active Graph 🔒

Sleep Graph 🔒

Weight Graph 🔒

These graphs appear on the web version of your dashboard.

Polar is a company that produces fitness tracking watches and hardware, all of which connect to its popular app, Polar Flow. According to an investigation that began last June, the app's tracking map exposed the home addresses of thousands of users. This is in part because people often turn their fitness trackers on or off when they're close to home, unintentionally revealing where they live.

To keep your data private:

- Go to Settings and then Privacy to set the default for future runs to Private.
- Change the privacy of each of your past runs individually.
- Make sure to set your profile to Private as well.

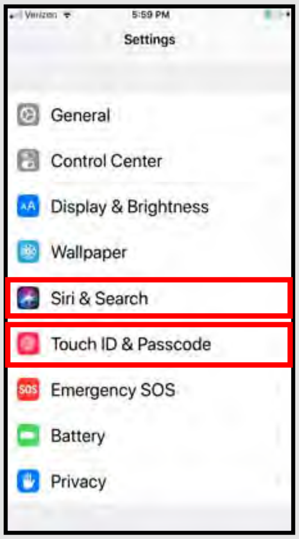
UPDATED DEC 2019

iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD

"Best Practices"

- 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 microphones 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 now require permission to access your camera, microphone, text messages, and contacts.
- Turn off location services until they are actually needed. Otherwise, your daily movements may be tracked by various apps or the vendor. Whether turned on or off, location services are always available to 911 and first responders.

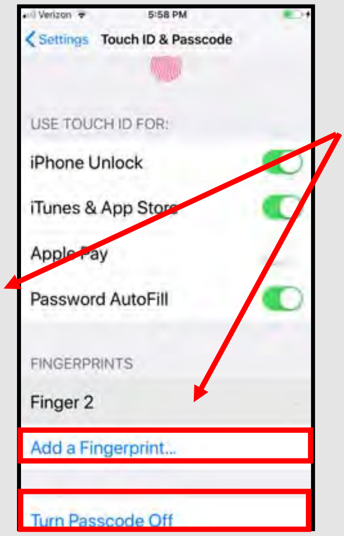
"Physical Security"



Verizon 5:59 PM

Settings

- General
- Control Center
- Display & Brightness
- Wallpaper
- Siri & Search
- Touch ID & Passcode
- Emergency SOS
- Battery
- Privacy



Verizon 5:58 PM

Settings Touch ID & Passcode

USE TOUCH ID FOR:

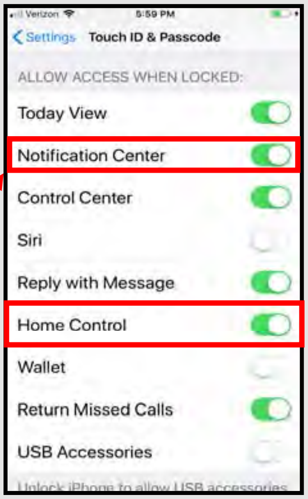
- iPhone Unlock: On
- iTunes & App Store: On
- Apple Pay
- Password AutoFill: On

FINGERPRINTS

- Finger 2
- Add a Fingerprint...
- Turn Passcode Off

Under "Settings" and "Touch ID & Passcode," select "Add a Fingerprint" and "Turn Passcode On". Be sure to use at least a 6 digit passcode. Alpha-numeric passcodes are even better options. Additionally, it is recommended that you turn off *Siri* due to the programs' listening capabilities and bugs associated with accessing your phone through Siri without a password.

Turn off the settings highlighted to the right in **red**. These settings allow others access to areas of your phone without a passcode.



Verizon 5:59 PM

Settings Touch ID & Passcode

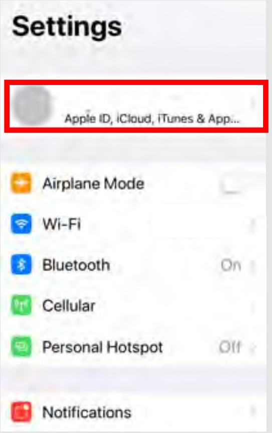
ALLOW ACCESS WHEN LOCKED:

- Today View: On
- Notification Center: On
- Control Center: On
- Siri: Off
- Reply with Message: On
- Home Control: On
- Wallet: Off
- Return Missed Calls: On
- USB Accessories: Off

Unlock iPhone to allow USB accessories

"Find My iPhone"

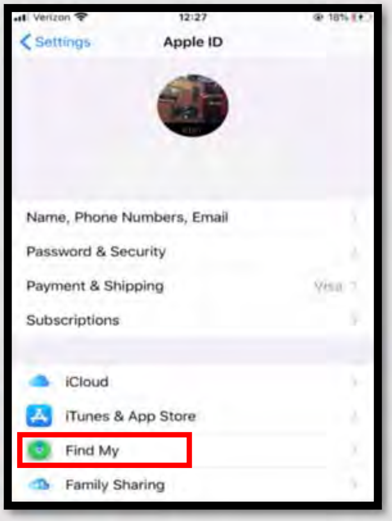
To start, go to "Settings" and select your account at the top (highlighted in **red** to the right). From there, select "Find My," then select "Find My iPhone" and ensure it is turned on. This way if you lose your phone you can access your account online and Geo-locate where it is.



Settings

Apple ID, iCloud, iTunes & App...

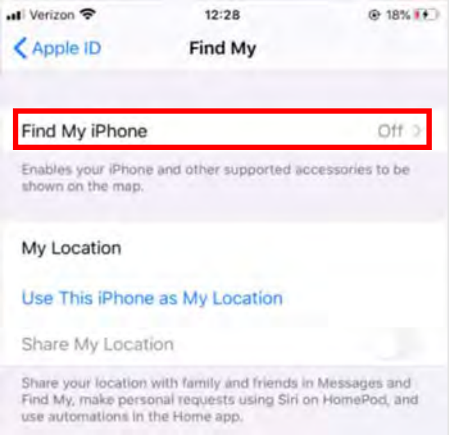
- Airplane Mode: Off
- Wi-Fi
- Bluetooth: On
- Cellular
- Personal Hotspot: Off
- Notifications



Verizon 12:27 18%

Settings Apple ID

- Name, Phone Numbers, Email
- Password & Security
- Payment & Shipping: Visa
- Subscriptions
- iCloud
- iTunes & App Store
- Find My
- Family Sharing



Verizon 12:28 18%

Apple ID Find My

Find My iPhone: Off

Enables your iPhone and other supported accessories to be shown on the map.

My Location

Use This iPhone as My Location

Share My Location: Off

Share your location with family and friends in Messages and Find My, make personal requests using Siri on HomePod, and use automations in the Home app.

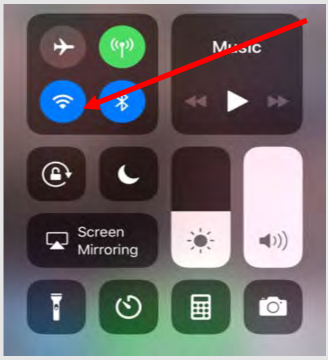
Smartphones contain extremely sensitive personal data and therefore should be treated with extra security precautions #protectyourdata

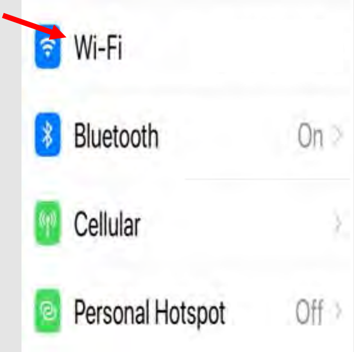
UPDATED DEC 2019

iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD

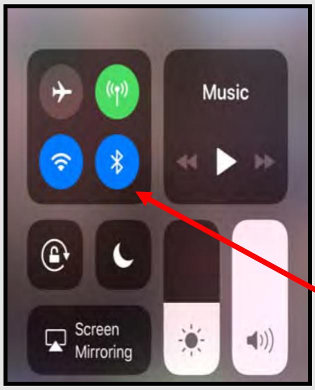
“Wireless Networks”

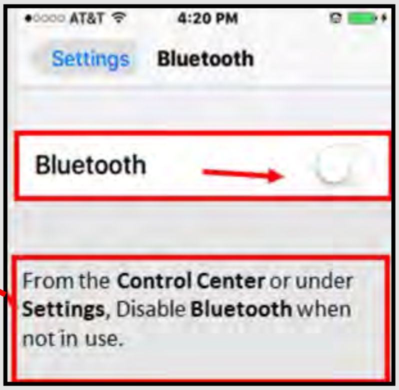
Where possible, public WIFI networks should be avoided due to the vulnerabilities they present to your personal data. If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt on-line transactions. There are two ways to turn off WIFI: 1) 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”





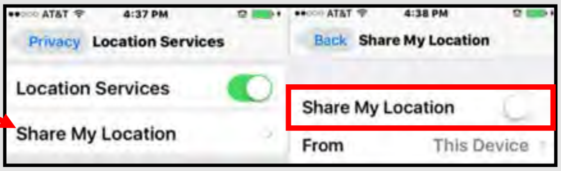
From the **Control Center** or under **Settings**, Disable **Bluetooth** when not in use.

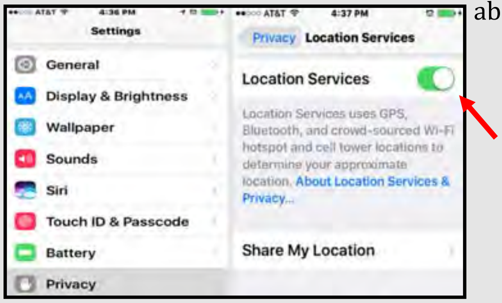
Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your iPhone or tablet, hackers can gain access to your device and obtain contacts, messages, calendars, photos, and notes without your knowledge. It is therefore 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.

“Location Services”

Whenever you take a photo, your phone records the location and saves that information inside the photo’s EXIF data. When you send that photo to someone else, they may be able to see where you took it, in some cases, down to a specific street. If you post a picture taken from your home, anyone who can view the EXIF data could figure out where you live and more. It is important to remove the EXIF data or, better yet prevent your devices from including it in pictures. Please refer to the “EXIF” Smartcard located in this book for information on how to do this.

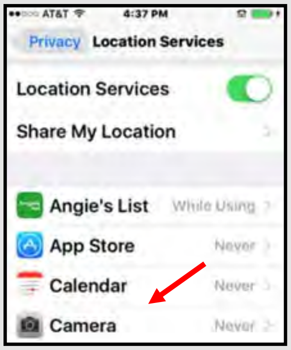
To disable your location from being shared in “Message “and “Find my Friends”, open the “Settings” app and navigate to “Privacy” > “Location Services.” Then navigate to “Share My Location“ and tap on the toggle to disable “Share My Location.”



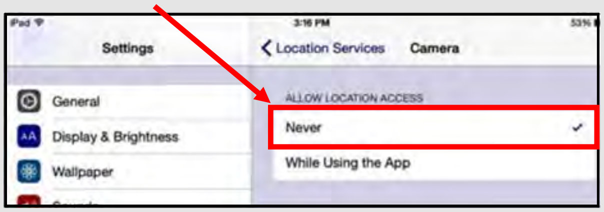


Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Note: If you turn off “Location Services” in the “Privacy Setting “menu, you cannot use location services for things such as navigation or locating your phone 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. “



Leaving location settings on can give someone a pattern of life for you and your family. #turnitoff

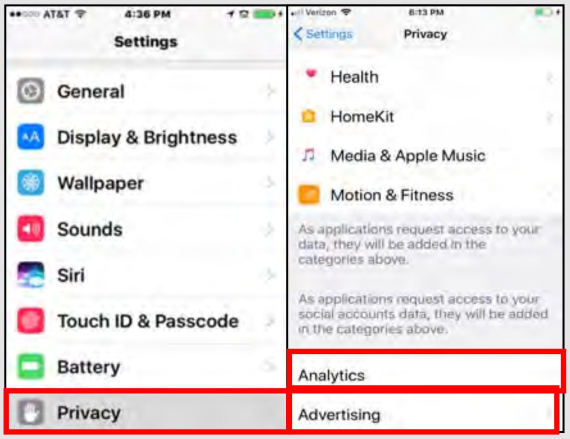
UPDATED DEC 2019

iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD

“Analytics Data and Ad Tracking”

“Analytics” enables a feature that gives Apple permission to track your activities. “Ad Tracking” allows vendors to send ads to you, targeted to your interests. Apple provides a setting to allow you to opt out of both of these features. It is recommended that you turn off “Ad Tracking.”

1) Open up the “Settings” app and navigate to “Privacy” then to “Analytics” and “Advertising”



AT&T 4:36 PM

Settings

- General
- Display & Brightness
- Wallpaper
- Sounds
- Siri
- Touch ID & Passcode
- Battery
- Privacy

Verizon 6:13 PM

Settings Privacy

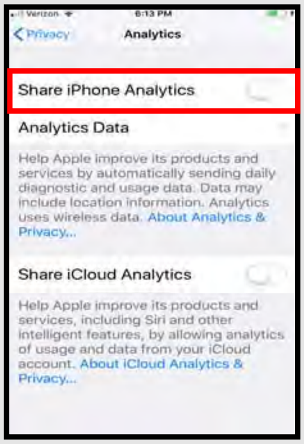
- Health
- HomeKit
- Media & Apple Music
- Motion & Fitness

As applications request access to your data, they will be added in the categories above.

As applications request access to your social accounts data, they will be added in the categories above.

- Analytics
- Advertising

2) Select “Analytics” and Then turn off “Share iPhone Analytics”



Verizon 6:13 PM

Privacy Analytics

Share iPhone Analytics

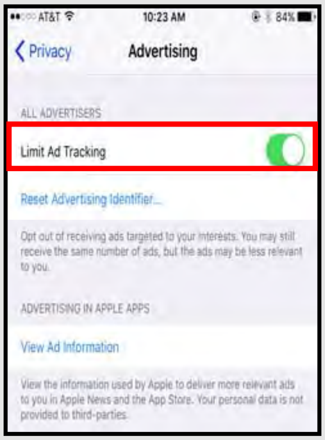
Analytics Data

Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data. About Analytics & Privacy...

Share iCloud Analytics

Help Apple improve its products and services, including Siri and other intelligent features, by allowing analytics of usage and data from your iCloud account. About iCloud Analytics & Privacy...

3) Then go back and select “Advertising” Turn ON “Limit Ad Tracking.”



AT&T 10:23 AM 84%

Privacy Advertising

ALL ADVERTISERS

Limit Ad Tracking

Reset Advertising Identifier...

Opt out of receiving ads targeted to your interests. You may still receive the same number of ads, but the ads may be less relevant to you.

ADVERTISING IN APPLE APPS

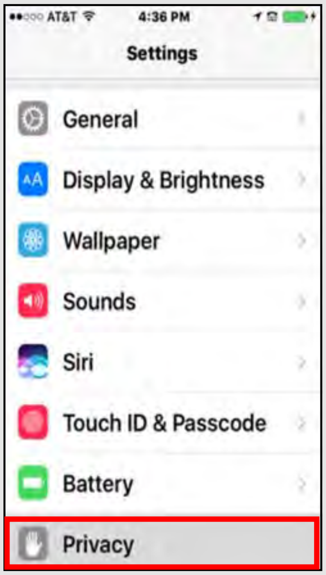
View Ad Information

View the information used by Apple to deliver more relevant ads to you in Apple News and the App Store. Your personal data is not provided to third-parties.

“Location Based Apple Ads”

“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. Here’s how to disable Apple Ads:

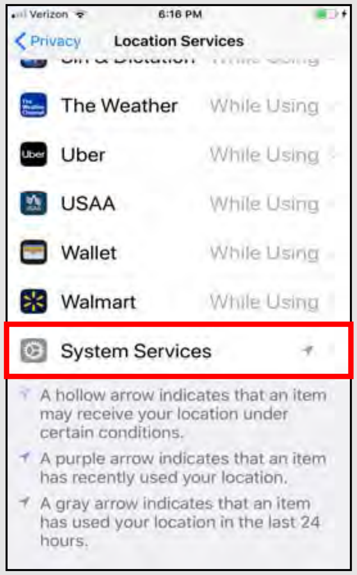
Open up “Settings” > “Privacy” > “Location Services” > “System Services.” You’ll see a list of Location Based selections that can be toggled off.



AT&T 4:36 PM

Settings

- General
- Display & Brightness
- Wallpaper
- Sounds
- Siri
- Touch ID & Passcode
- Battery
- Privacy



Verizon 6:16 PM

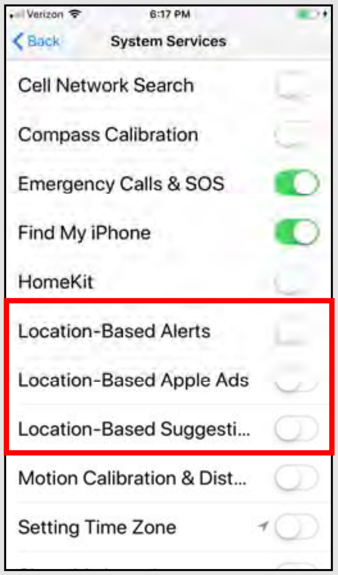
Privacy Location Services

The Weather	While Using
Uber	While Using
USAA	While Using
Wallet	While Using
Walmart	While Using
System Services	

A hollow arrow indicates that an item may receive your location under certain conditions.

A purple arrow indicates that an item has recently used your location.

A gray arrow indicates that an item has used your location in the last 24 hours.



Verizon 6:17 PM

Back System Services

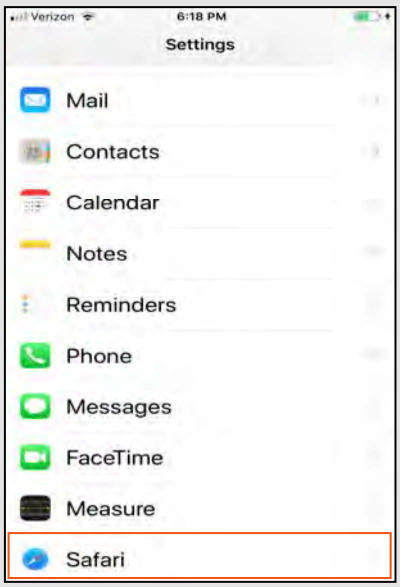
- Cell Network Search
- Compass Calibration
- Emergency Calls & SOS
- Find My iPhone
- HomeKit
- Location-Based Alerts
- Location-Based Apple Ads
- Location-Based Suggesti...
- Motion Calibration & Dist...
- Setting Time Zone

Marketing data is not just available to marketing companies anymore. #turnadsoff

iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD

Safari's "Do Not Track"

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 12.0 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, however, under "General" turn off "Frequently Visited Sites." This prevents Safari from tracking sites your regularly visit. Next, under "Privacy & Security" turn on prevent "Cross-Site Tracking", "Block All cookies", "Ask Websites Not to Track", and "Fraudulent Website Warning."


Verizon 6:18 PM

Settings

Mail

Contacts

Calendar

Notes

Reminders

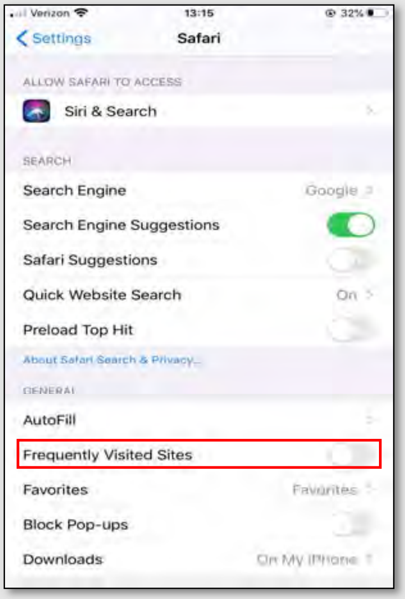
Phone

Messages

FaceTime

Measure

Safari


Verizon 13:15 32%

Settings Safari

ALLOW SAFARI TO ACCESS

Siri & Search

SEARCH

Search Engine Google

Search Engine Suggestions

Safari Suggestions

Quick Website Search On

Preload Top Hit

About Safari Search & Privacy...

GENERAL

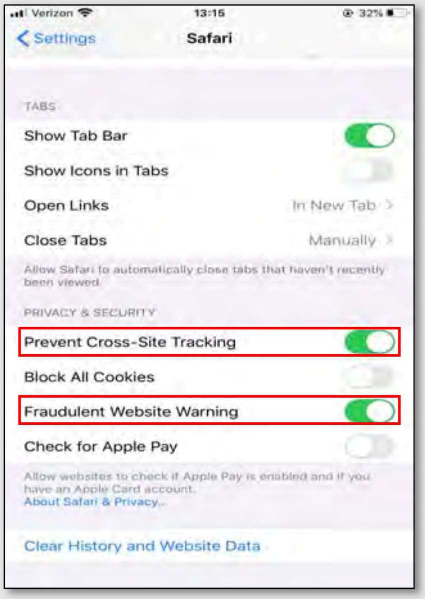
AutoFill

Frequently Visited Sites

Favorites Favorites

Block Pop-ups

Downloads On My iPhone


Verizon 13:15 32%

Settings Safari

TABS

Show Tab Bar

Show Icons in Tabs

Open Links In New Tab

Close Tabs Manually

Allow Safari to automatically close tabs that haven't recently been viewed.

PRIVACY & SECURITY

Prevent Cross-Site Tracking

Block All Cookies

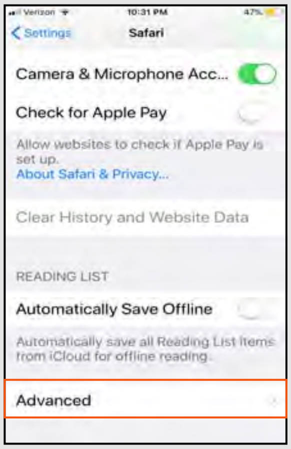
Fraudulent Website Warning

Check for Apple Pay

Allow websites to check if Apple Pay is enabled and if you have an Apple Card account.
About Safari & Privacy...

Clear History and Website Data

It is also 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" > "Website Data", then select "Remove All Website Data"


Verizon 10:31 PM 47%

Settings Safari

Camera & Microphone Acc...

Check for Apple Pay

Allow websites to check if Apple Pay is set up.
About Safari & Privacy...

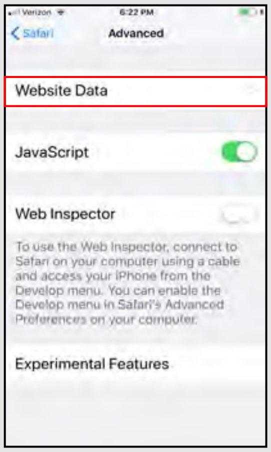
Clear History and Website Data

READING LIST

Automatically Save Offline

Automatically save all Reading List items from iCloud for offline reading.

Advanced


Verizon 6:22 PM

Safari Advanced

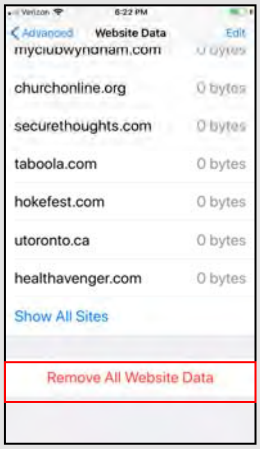
Website Data

JavaScript

Web Inspector

To use the Web Inspector, connect to Safari on your computer using a cable and access your iPhone from the Develop menu. You can enable the Develop menu in Safari's Advanced Preferences on your computer.

Experimental Features


Verizon 6:22 PM

Advanced Website Data Edit

myclubwyndham.com 0 bytes

churchonline.org 0 bytes

securethoughts.com 0 bytes

taboola.com 0 bytes

hokefest.com 0 bytes

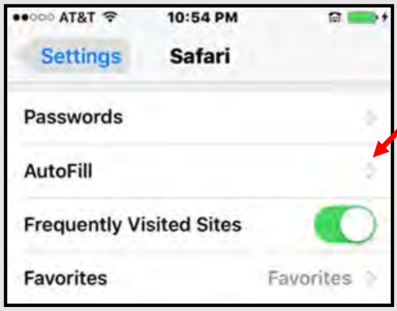
utoronto.ca 0 bytes

healthavenger.com 0 bytes

Show All Sites

Remove All Website Data

"Passwords and AutoFill"


AT&T 10:54 PM

Settings Safari

Passwords

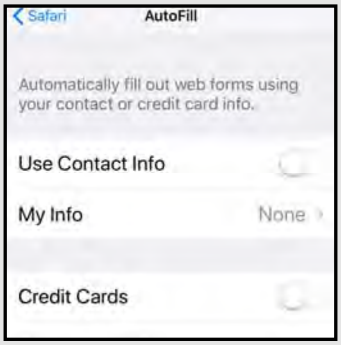
AutoFill

Frequently Visited Sites

Favorites Favorites

Clear the AutoFill to protect passwords and credit card information. To do so, open "Settings" > "Safari" and click on "AutoFill"

Next, select the following settings to disable "Use Contact Info", and "Credit Cards"


Safari AutoFill

Automatically fill out web forms using your contact or credit card info.

Use Contact Info

My Info None

Credit Cards

Google already tracks everything we do, so why let another search engine do it too? #saynototracking

UPDATED DEC 2019

ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Best Practices

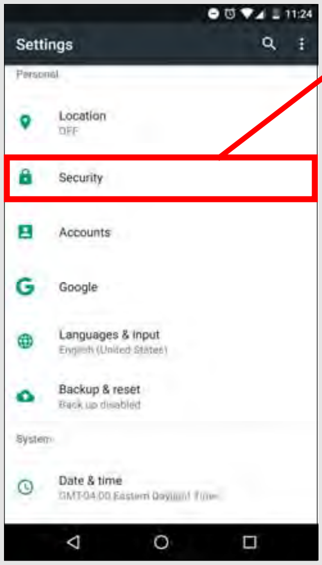
- Smartphones and tablets are not impenetrable. Secure your smartphone with a password or biometrics, and utilize apps such as **Find My Device** or **Prey Anti Theft** to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Caution should be used when your 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.
- Prior to downloading apps on your device, read the developers permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- Keep your locations services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked by various apps and/or the vendor. Location services are always available to 911 and first responders.
- If you have a google account, you can use your google credentials to login at maps.google.com/location history to see your device's 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.*

In order to make sure your Android is up to date with the latest Android Version follow these quick and simple steps. 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 .

Physical Security

The first line of defense in preventing unauthorized access to your device is to protect it with a passcode. Android 9.0 adds a slew of enhanced security features to accommodate this, including fingerprints, facial recognition, encryption, and setting of app-level permissions.



Settings

Personal

Location
OFF

Security

Accounts

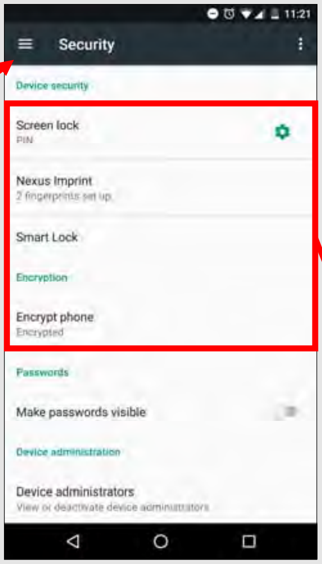
Google

Languages & input
English (United States)

Backup & reset
Back up disabled

System

Date & time
GMT-04:00 Eastern Daylight Time



Security

Device security

Screen lock
PIN

Nexus Imprint
2 fingerprints set up

Smart Lock

Encryption

Encrypt phone
Encrypted

Passwords

Make passwords visible

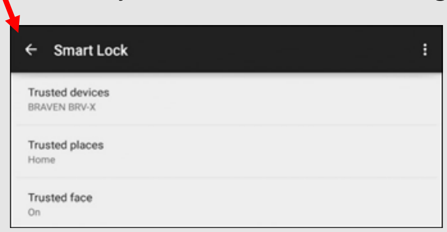
Device administration

Device administrators
View or deactivate device administrators

Tap the "Settings" icon and then tap "Biometrics & Security" or "Lock Screen".

Here you can configure your screen lock method. The options are Swipe, Pattern, PIN, Face, Iris, Fingerprints, and Password. The most secure way to protect your phone is to use the **biometric** options. A password is the strongest backup solution.

However, this can be cumbersome when unlocking your phone. So Smart Lock allows you to set trusted places (home, car, etc.) so when you are within a certain range, your phone will not lock. You can also set up trusted devices or trusted faces which will allow you to simply look at the device to unlock it. Set any Smart Lock option with caution.



Smart Lock

Trusted devices
BRAVEN BRV-X

Trusted places
Home

Trusted face
On

Biometrics: You can also add your fingerprint, face, or iris and set conditions for its use. This requires PIN entry and access.

Iris is the most secure of these Biometric options, but may not be a suitable option for those who wear glasses or contacts on a regular basis.

Selecting "Encrypt phone" allows you to initiate the encryption of all data on your device. According to the instructions, this could take up to an hour and requires your device to be plugged into its charger. This process must not be interrupted, so be sure to start it when you are sure you will not need to use your device for that amount of time. You will only need to perform this once. Locking your device encrypts the data on your phone. Unlocking your encrypted device decrypts your data.

Most Androids have a Secure Folder where you can save sensitive documents on your phone with additional password protection.

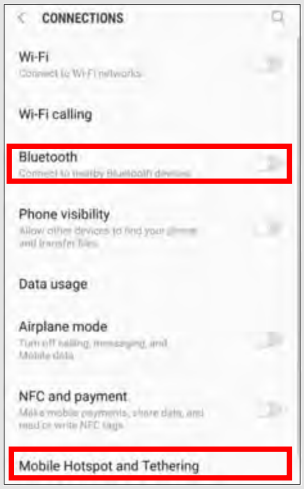
UPDATED DEC 2019

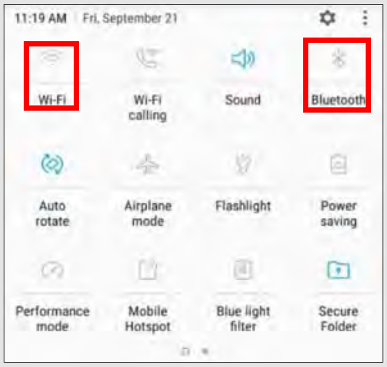
ANDROID PRIVACY SETTINGS (ANDROID 10.0)

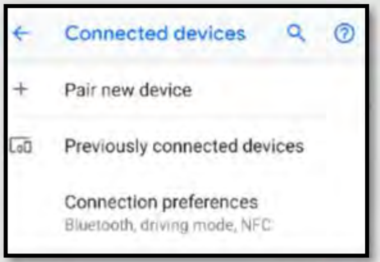
Mobile Hotspot and Bluetooth

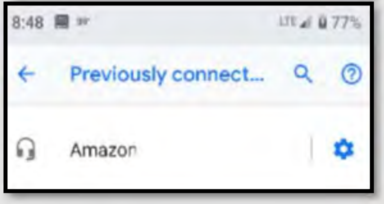
Rather than connecting to public Wi-Fi, most mobile carriers have an option to use the mobile device as a mobile hotspot. You can turn this option on and off under “Settings” > “Wireless & Networks” or “Connections” > “Mobile Hotpot and Tethering”. Bluetooth is a wireless technology standard for exchanging 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” > “Wireless & Networks” or “Connections”.

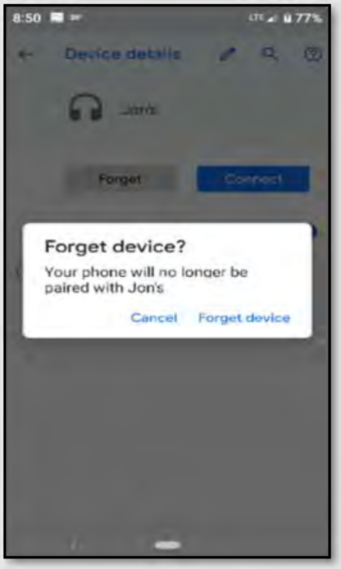
Wireless Networks


CONNECTIONS
Wi-Fi
Connect to Wi-Fi networks
Wi-Fi calling
Bluetooth
Connect to nearby Bluetooth devices
Phone visibility
Allow other devices to find your phone and transfer files
Data usage
Airplane mode
Turn off calling, messaging, and Mobile data
NFC and payment
Make mobile payments, share data, and read or write NFC tags
Mobile Hotspot and Tethering









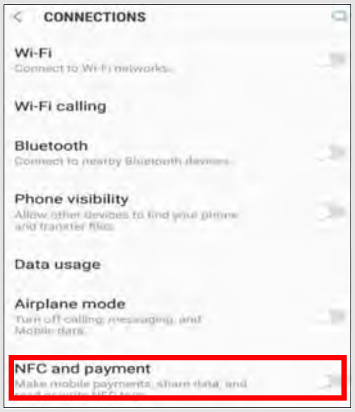
If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt online transactions.

If you would like to delete old Bluetooth devices with a few additional steps. While in the Bluetooth section select “Previously Connected Devices” then select the settings icon and hit “Forget.”

From the “Quick Settings” drag-down tray, tap and hold “Wi-Fi” to see available networks. Tap the “Wi-Fi” icon to turn Wi-Fi off when not in use.

Near Field Communication (NFC)

NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. The technology allows you to “bump” your smartphone with other NFC devices to exchange information or pay for items using a Pay app. Although extremely close range, a malicious user can tamper with the data being transmitted between two NFC devices if they are within range. NFC risks include: data tampering, data interception, and mobile malware.

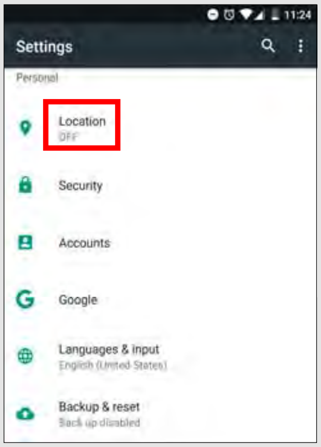

CONNECTIONS
Wi-Fi
Connect to Wi-Fi networks
Wi-Fi calling
Bluetooth
Connect to nearby Bluetooth devices
Phone visibility
Allow other devices to find your phone and transfer files
Data usage
Airplane mode
Turn off calling, messaging, and Mobile data
NFC and payment
Make mobile payments, share data, and

Turn off NFC when not in use by tapping “Settings” > “Wireless & Networks” or “Connections”.

Then tap the toggle switch for “NFC and payment” so that it is in the “off” position.

Location Services

Whenever you take a photo, data on your location is saved inside of the photo’s 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 “Biometrics and security.” Disable your location services by switching the toggle to “off”.

Google Maps will use your location history and travel times to notify you of traffic before you typically travel. #GoogleIsWatching

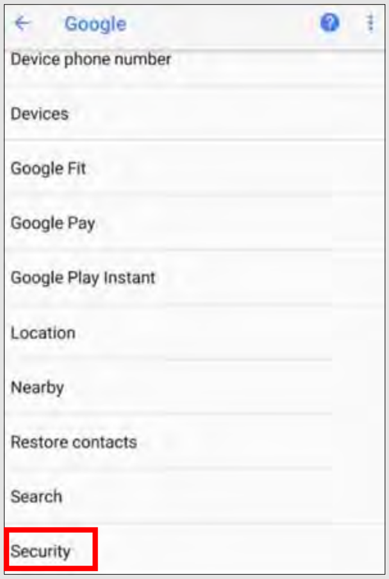
ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Lost/Stolen Phone

In the U.S. it has been reported that over 100 cell phones are stolen or lost every minute. This fact alone proves it is necessary to keep your device secure and locked with biometrics or a passcode. Since all Android phones work by syncing your phone to a google account, "android.com/find" is the native "Find my Device" tool for Android phones. Though this feature is automatically enabled, you may download the "Find my Device" app from the Google Play store to verify it's function, or to find a different device.

- 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.



Device phone number
Devices
Google Fit
Google Pay
Google Play Instant
Location
Nearby
Restore contacts
Search
Security

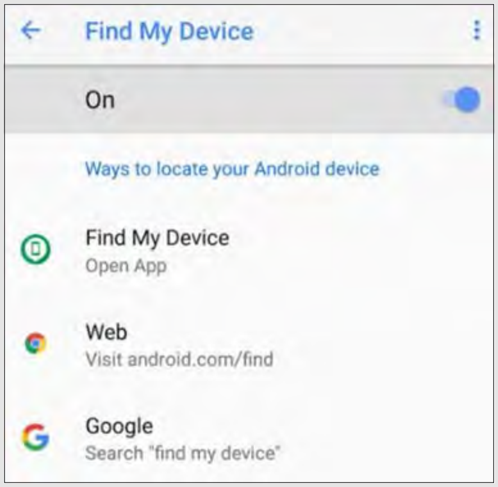
If your device is lost or stolen, you can go to Google's device management page and access your device's current or last reported location. You can make the device ring at full volume to help you find it or remotely lock or erase the device.

To enable:

Tap "Settings" > "Google" > "Security" > "Find My Device".

Ensure Location services are turned ON (follow instructions on previous page).

Go here: android.com/find and check that your device can be located.



On

Ways to locate your Android device

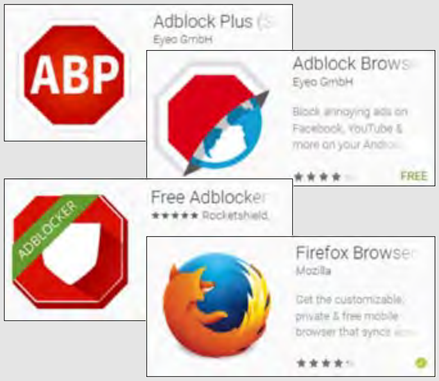
Find My Device
Open App

Web
Visit android.com/find

Google
Search "find my device"

Ad Tracking

Ads can track everything you do. Not all Android devices and OS versions have settings to turn Ad tracking off. For those that don't have this setting, you can download and use any number of ad blocking / privacy-oriented browsers or browser add-ons. These are just a few examples.



Adblock Plus (S
Eyeo GmbH
ABP
Adblock Brows
Eyeo GmbH
Block annoying ads on Facebook, YouTube & more on your Andro
FREE
Free Adblocker
Rocketshield
ADBLOCKER
Firefox Browser
Mozilla
Get the customizable, private & free mobile browser that syncs

For those devices with the option:

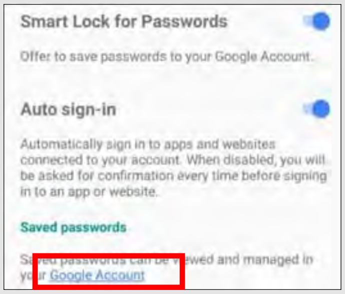
Go to "Settings" > "Google" > "Ads".

Tap the toggle switch to the "on" position for "Opt out of Ads Personalization".

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.



Smart Lock for Passwords

Offer to save passwords to your Google Account.

Auto sign-in

Automatically sign in to apps and websites connected to your account. When disabled, you will be asked for confirmation every time before signing in to an app or website.

Saved passwords

Saved passwords can be viewed and managed in your Google Account

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.

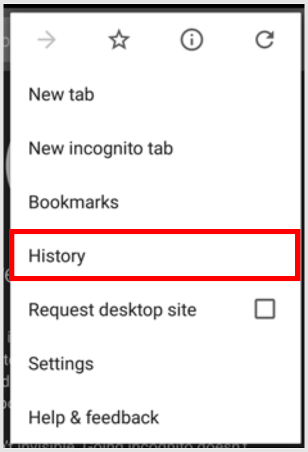
Although saving your passwords is convenient, it also poses a threat to your security should your device be stolen.

UPDATED DEC 2019

ANDROID PRIVACY SETTINGS (ANDROID 10.0)

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 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.



New tab

New incognito tab

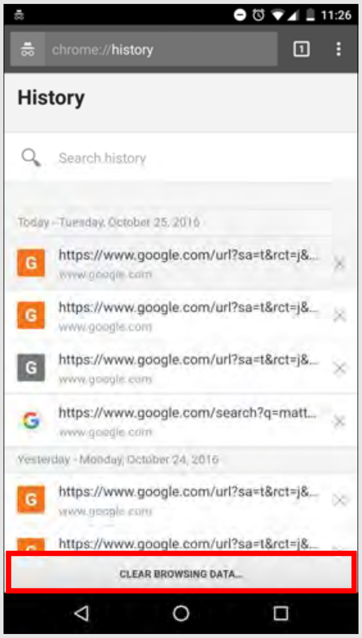
Bookmarks

History

Request desktop site □

Settings

Help & feedback



chrome://history

History

Search history

Today - Tuesday, October 25, 2016

https://www.google.com/url?sa=t&rct=j&...
www.google.com

https://www.google.com/url?sa=t&rct=j&...
www.google.com

https://www.google.com/url?sa=t&rct=j&...
www.google.com

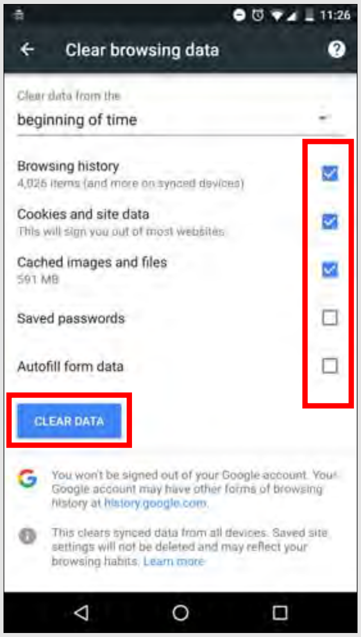
https://www.google.com/search?q=matt...
www.google.com

Yesterday - Monday, October 24, 2016

https://www.google.com/url?sa=t&rct=j&...
www.google.com

https://www.google.com/url?sa=t&rct=j&...

CLEAR BROWSING DATA...



Clear browsing data

Clear data from the
beginning of time

Browsing history ☑
4,026 items (and more on synced devices)

Cookies and site data ☑
This will sign you out of most websites

Cached images and files ☑
591 MB

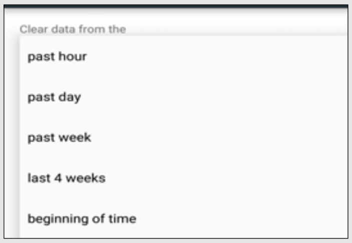
Saved passwords □

Autofill form data □

CLEAR DATA

You won't be signed out of your Google account. Your Google account may have other forms of browsing history at history.google.com.

This clears synced data from all devices. Saved site settings will not be deleted and may reflect your browsing habits. Learn more



Clear data from the

past hour

past day

past week

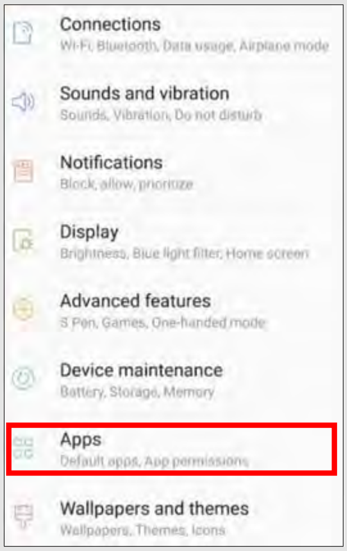
last 4 weeks

beginning of time

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.



Connections
Wi-Fi, Bluetooth, Data usage, Airplane mode

Sounds and vibration
Sounds, Vibration, Do not disturb

Notifications
Block, allow, prioritize

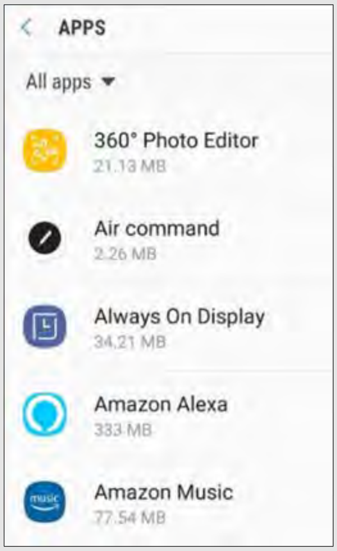
Display
Brightness, Blue light filter, Home screen

Advanced features
S Pen, Games, One-handed mode

Device maintenance
Battery, Storage, Memory

Apps
Default apps, App permissions

Wallpapers and themes
Wallpapers, Themes, Icons



APPS

All apps ▾

360° Photo Editor
21.13 MB

Air command
2.26 MB

Always On Display
34.21 MB

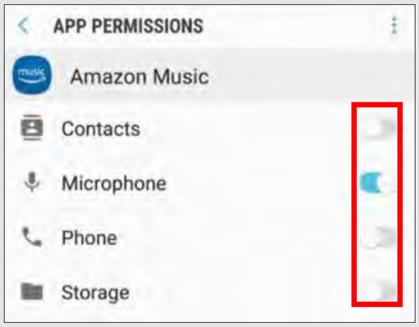
Amazon Alexa
333 MB

Amazon Music
77.54 MB

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.



APP PERMISSIONS

Amazon Music

Contacts

Microphone

Phone

Storage

This only works with apps designed for use specifically with Android. Permissions for older apps or those without full Android functionality can still be disabled, but this could make the app function unreliably.

Pay attention to user agreements when downloading new apps. This will tell you what the app is requesting access to on your device.

UPDATED DEC 2019

TRAVELING SAFELY WITH SMARTPHONES

Do's and Don'ts

- Enable password and fingerprint locks on your device. Also, protect "Settings" changes on your phone by requiring a password.
- Assume that all information on your device can be accessed remotely. Don't store passwords and sensitive information on your phone
- Always use complex passwords, the stronger and longer the password the more difficult it will be for someone to hack into.
- 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. Only use networks that the business provides the name, don't assume if its named appropriately it is safe. and WiFi off when you are not using them.

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.

Traveling internationally can present new problems, ensure you prepare yourself before you travel not once you are there.

UPDATED DEC 2019

IDENTITY THEFT SMART CARD

Identity Theft Scams On The Rise

Utility Bill Scam: As of September 2018, the Federal Trade Commission (FTC) reported an increase in local utility scams. The consumer receives a call from someone posing as a local utility company claiming the consumer has a past due bill. The caller is very convincing, even to a consumer who may have just paid their bill. Oftentimes the caller will threaten to cut off service, hoping this threat is enough to get the consumer to provide personal and financial information, thereby falling for the scam. If you feel a call from someone claiming to be a bill collector is suspicious in any way do NOT settle the bill at that time. You have the right to call the utility company yourself but remember do not use the phone number they provided you, look up the number yourself. Also, report this suspicious activity to the FTC.

"Do you know what an overdue bill could do to you credit?"

Imposter Scams: Reports of IRS impostors have surfaced during the 2018 tax season. Consumers receive a call from an individual claiming to be an "IRS Officer," who will then inform the consumer that they owe a large amount of money and if they don't pay an agreed upon amount immediately local law enforcement will issue a warrant for their arrest. They will often try to "negotiate" a smaller amount to make the consumer feel as if they are getting a deal. Instead of paying with a check or money order, these scammers instruct their victims to buy gift cards and read the numbers to the fake agent over the phone for verification. Remember, no legitimate organization will ever ask for payment in gift cards! Also, report all scams involving taxes or the IRS to the IRS fraud department.

"Just pay with Amazon gift cards or I will send the police to your house tonight!"

"Your Social Security Number was just used in a crime, we can help you"

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.

R**eport fraud & identity theft scams to the FTC at 1-877-FTC-HELP (1-877-382-4357) or online: ftc.gov/complaint**

12 Practices to Avoid Identity Theft

1. Do not disclose your full nine-digit Social Security number
2. Avoid paper billing by requesting secure electronic statements instead, or have them mailed to a Commercial Mail Receiving Agency (CMRA)
3. Lock your mailbox
4. Keep your information safe, both online and offline, by shredding documents containing personal information and passwords and protecting sensitive computer files
5. Use unique, hard-to-guess passwords that include a combination of letters, numbers, and symbols
6. Avoid using the same password across multiple accounts
7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, smartphones and operating systems
8. 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
9. Avoid making purchases, paying bills, or sending sensitive information over unsecured WiFi networks
10. Disable Bluetooth on devices when not in use
11. Watch out for "phishing" scams; do not trust unsolicited offers and ads
12. 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

Phone Scammers will say anything to get you to disclose personal information; always offer to call back on your own

IDENTITY THEFT SMART CARD

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.

According to the FTC, identity theft was the top complaint received for the past 15 years, increasing 47% from 2014 to 2015 as a result of a massive rise in tax-related identity theft (see "FTC Releases Annual Summary of Consumer Complaints," March 1, 2016).

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.

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:

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)

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

UPDATED DEC 2019

KEEPING YOUR CHILDREN SAFE ONLINE

- 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." Most of the teens also have used or use a smartphone. 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.

Do's and Don'ts

- Only connect with gamers and online profiles of people you know and trust. Review connections often.
- Assume ALL information and images you share are publicly viewable, regardless of your settings.
- Use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- Tell kids to let parents or responsible adults know if anything online makes them uncomfortable.
- Do ***not*** use location services.
- Do ***not*** add your birthdate, location, phone number, or other personal details to online profiles.
- Do ***not*** allow children to go to sleep with their smartphone or other device in their room. Pick a certain time that your tweens/teens have to bring you their device, roughly a hour before they go to bed.

YouTube

Now it is time to 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 coming soon to iOS. In the "Restricted mode", kids are not able to search for content on their own.

Open settings and scroll down to the bottom just past your child's (or your) profile. Select "approved content only" or "Restricted Mode On." Next, you may want to also Lock "Restricted Mode" on this browser. "Restricted Mode" lock prevents others from changing the "Restricted Mode" settings on this browser.

https://www.youtube.com/yt/kids/

CONTROL WHAT APPLICATIONS GET INSTALLED ON YOUR CHILD'S DEVICE

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 also be done on your Android devices as well.

Be a role model:

If you have privacy concerns on your social media, your child will too.

Your child's "right to privacy" doesn't supersede your right to protect them. Their smartphone is yours for the monitoring, after all who gets the bill? #keepourkidssafeonline

UPDATED DEC 2019

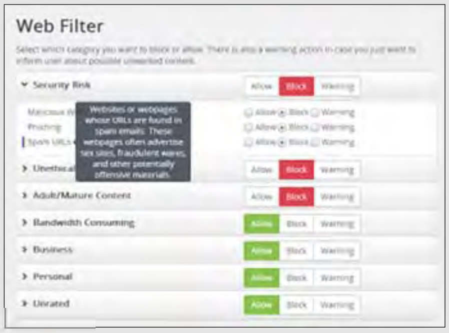
KEEPING YOUR CHILDREN SAFE ONLINE

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 certain online 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.



Web Filter

Select which category you want to block or allow. There is also a warning action in case you just want to inform user about possible unwanted content.

Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.

Security Risk	Allow	🟥 Block	Warning
Malicious W	○ Allow	● Block	○ Warning
Phishing	○ Allow	● Block	○ Warning
Spam URLs	○ Allow	● Block	○ Warning
Unethical	Allow	🟥 Block	Warning
Adult/Mature Content	Allow	🟥 Block	Warning
Bandwidth Consuming	🟩 Allow	Block	Warning
Business	🟩 Allow	Block	Warning
Personal	🟩 Allow	Block	Warning
Unrated	🟩 Allow	Block	Warning

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:

- Detects registered accounts any new accounts created
- Ability to identify cyberbullying, cyber-stalking, or grooming
- Access to view photos and videos child has published
- Alert Notifications
- Daily/Weekly Reports

My Mobile Watchdog

Monitor your child's cell phone use, including call logs, texting, photos (MMS), web history, web filtering, time restrictions, sync contacts and block applications. Receive real time alerts when a stranger contacts your child. Must be installed on your child's phone.

- Monitor your child's cell phone use
- Includes Web filtering, time restrictions, app blocking, and more
- Get real time alerts when a stranger calls the child's phone
- Location Tracking! Track up to 99 locations and know exactly where your child is at any time.
- DailyWatch Summaries! A daily breakdown of your child's activity conveniently packaged and sent to your email.

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, where you can also track kids' spending and add money to their Microsoft accounts.

Qustodio

Free 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
- Browser-independent content filter that handles HTTPS traffic

Norton by Symantec Family Premier

Includes support across Windows, Android and iOS devices (no MAC support):

- 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
- Location tracking to know where your child is at any time

Google has it's own Safety Center to help ensure your kids remain safe Online, stay up to date at www.google.com/safetycenter/families/start/ #themoreyouknow

PHOTO SHARING SERVICES CARD

Do's and Don't's:

- 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.

- Don't tag geolocations. The information in these tags can disclose location of where the photo was taken.
- Don't give apps permissions to access the cellphone location services.
- Don't 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 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. You can find more detailed information on how to set privacy settings for these Services on the following pages.

6 Popular Photo Sharing Services

Service	Primary Use	Image Privacy Options	Retains EXIF	Geo-Location Options (non-EXIF)	Allows Reposting	Populates in Google Searches (Indexed)
Instagram	Share photos and videos from camera enabled mobile devices	**Public;** Private (other users must request to follow you);	No	GPS-based device location and customizable location (both removable)	Yes, only with third party applications	Profiles are indexed, but not photos
snapchat	Share photos and videos that "disappear" after a certain number of views or a period of 24 hours.	**Public;** Private (other users must request to follow you)	No	Snapchat Geofilters use location services on your mobile device. Using Geofilters is optional.	No. Please note that viewers can still screenshot your Snaps.	No
facebook	Social network	**Public;** Only Me; Friends; Friends of Friends	No	Free-form text; location suggestions; map-based (removable)	Yes	Public profiles are indexed
Google Photos	Photo and video sharing and storage service	**Private**; Shared Albums allow anyone with the unique web link to view your photos	Yes	GPS-based from camera and Google's Estimated Location (both can be disabled in the phone settings)	Yes, photos can be downloaded from a Shared Album.	Shared photos may possibly be open to public search in the future
flickr	Photo and video hosting site used for sharing and embedding on blogs and social media	**Public;** Only You, Your Friends, Your Family	**Yes for original uploaded file (not for resized file)**; You can also hide EXIF data	Editable location; map-based (both removable)	Yes	Public albums are indexed; Offers opt-out for 3rd party searches
photobucket	Photo and video hosting site used for sharing and embedding on blogs and social media	**Public;** Private (optional password protection)	Yes for original uploaded file (not for resized file)	Location data is available unless you disable it	**Yes;** No	Public albums are indexed

*Default settings are in **bold**.

**Converting a photo to PNG file format will remove EXIF data.

Everything we post on the web creates a digital footprint. Protect yourself and your family by carefully choosing what you post.

UPDATED DEC 2019

PHOTO SHARING SERVICES CARD

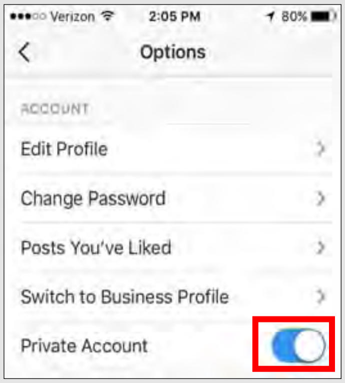
EXIF Removal Tools

- **EXIF Wizard**: https://itunes.apple.com/us/app/exif-wizard/id387652357?mt=8
- **TrashEXIF**: https://itunes.apple.com/us/app/trashexif-metadata-photo-remover/id585543219?mt=8
- **ACDSee Photo Software**: http://www.acdsee.com/
- **Paint Shop Pro Photo Software:** http://www.paintshoppro.com/en/

For more information, please see the EXIF Data Smartcard

Privacy Settings

Instagram



Private Account ●

Tap 👤 on the bottom right.

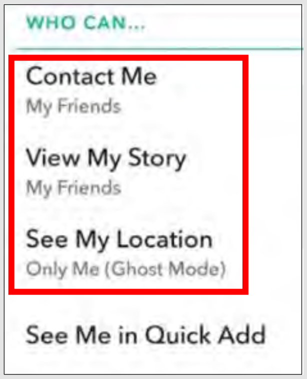
Then tap the menu icon at the top right ≡

Tap ⚙ at the bottom of the screen.

Scroll to find "Privacy" and then ""Account Privacy," make sure the toggle is on for "Private Account".

When your account is private, only people you approve can see your photos and videos.

snapchat


WHO CAN...

Contact Me: My Friends

View My Story: My Friends

See My Location: Only Me (Ghost Mode)

See Me in Quick Add

Tap 👤 at the top.

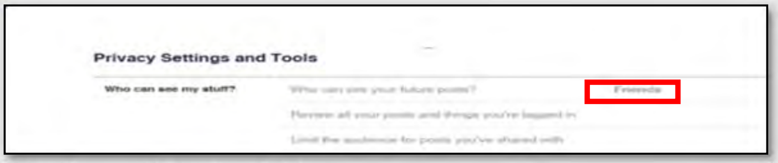
Tap ⚙ to access Settings.

Scroll down to the "Additional Services" section.

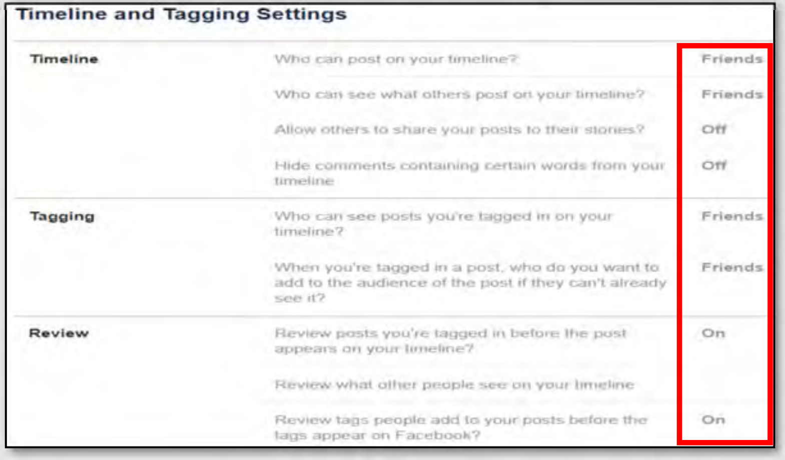
Set each category except "See My Location" to "My Friends".

Set "See My location" to "Only Me (Ghost Mode)".

facebook


Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with	


Timeline and Tagging Settings

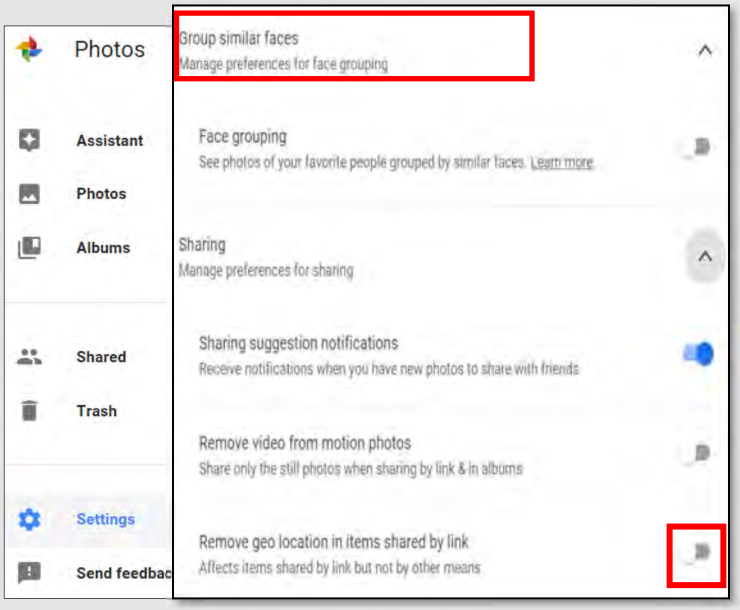
Timeline	Who can post on your timeline?	Friends
	Who can see what others post on your timeline?	Friends
	Allow others to share your posts to their stories?	Off
	Hide comments containing certain words from your timeline	Off
Tagging	Who can see posts you're tagged in on your timeline?	Friends
	When you're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

From your smart phone, tap the ≡ at the top right corner.

Select "Privacy" then "Settings".

Navigate to "Privacy Settings and Tools" and "Timeline and Tagging Settings" to adjust who can see your posts and pictures.

Google Photos



Group similar faces
Manage preferences for face grouping

Face grouping
See photos of your favorite people grouped by similar faces. Learn more

Sharing
Manage preferences for sharing

Sharing suggestion notifications
Receive notifications when you have new photos to share with friends

Remove video from motion photos
Share only the still photos when sharing by link & in albums

Remove geo location in items shared by link
Affects items shared by link but not by other means

Tap ≡ on the top left corner.

Tap "Settings".

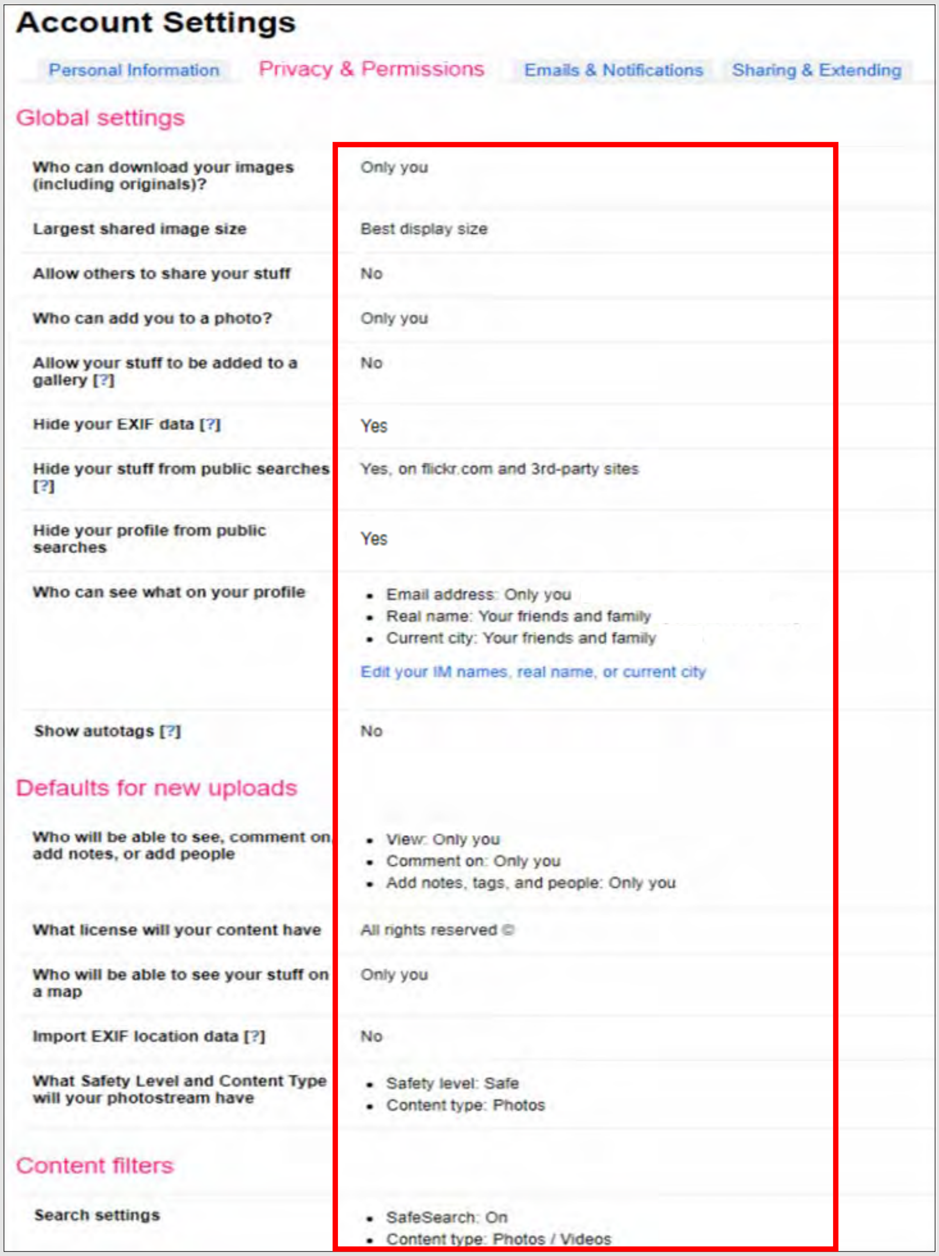
Ensure that the toggle is *on* for "Remove geolocation" from the Share section. Ensure that the toggle switch is

Android devices typically automatically backup photos with your EXIF data, so be sure to check your settings! #KeepGoogleInCheck

PHOTO SHARING SERVICES CARD

Privacy Settings Continued

flickr



Account Settings

Global settings

Who can download your images (including originals)?	Only you
Largest shared image size	Best display size
Allow others to share your stuff	No
Who can add you to a photo?	Only you
Allow your stuff to be added to a gallery [?]	No
Hide your EXIF data [?]	Yes
Hide your stuff from public searches [?]	Yes, on flickr.com and 3rd-party sites
Hide your profile from public searches	Yes
Who can see what on your profile	• Email address: Only you • Real name: Your friends and family • Current city: Your friends and family Edit your IM names, real name, or current city
Show autotags [?]	No

Defaults for new uploads

Who will be able to see, comment on, add notes, or add people	• View: Only you • Comment on: Only you • Add notes, tags, and people: Only you
What license will your content have	All rights reserved ©
Who will be able to see your stuff on a map	Only you
Import EXIF location data [?]	No
What Safety Level and Content Type will your photostream have	• Safety level: Safe • Content type: Photos

Content filters

Search settings	• SafeSearch: On • Content type: Photos / Videos

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

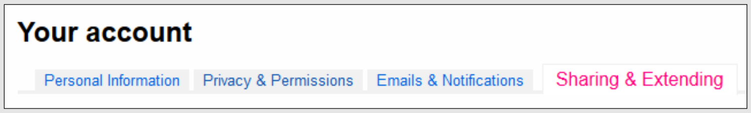
Tap the at the top right corner.

Tap “Settings”.

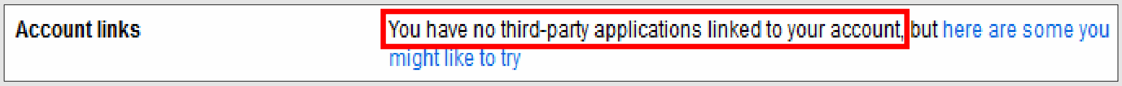
Tap the “Privacy & Permissions” tab and use the image to the left as an example for your security settings.

Now tap on the “Sharing & Extending” tab.

Make sure you do not have any third party applications such as Twitter or Tumblr linked to your Flickr account. You should see a message like the one outlined in red below.



Your account



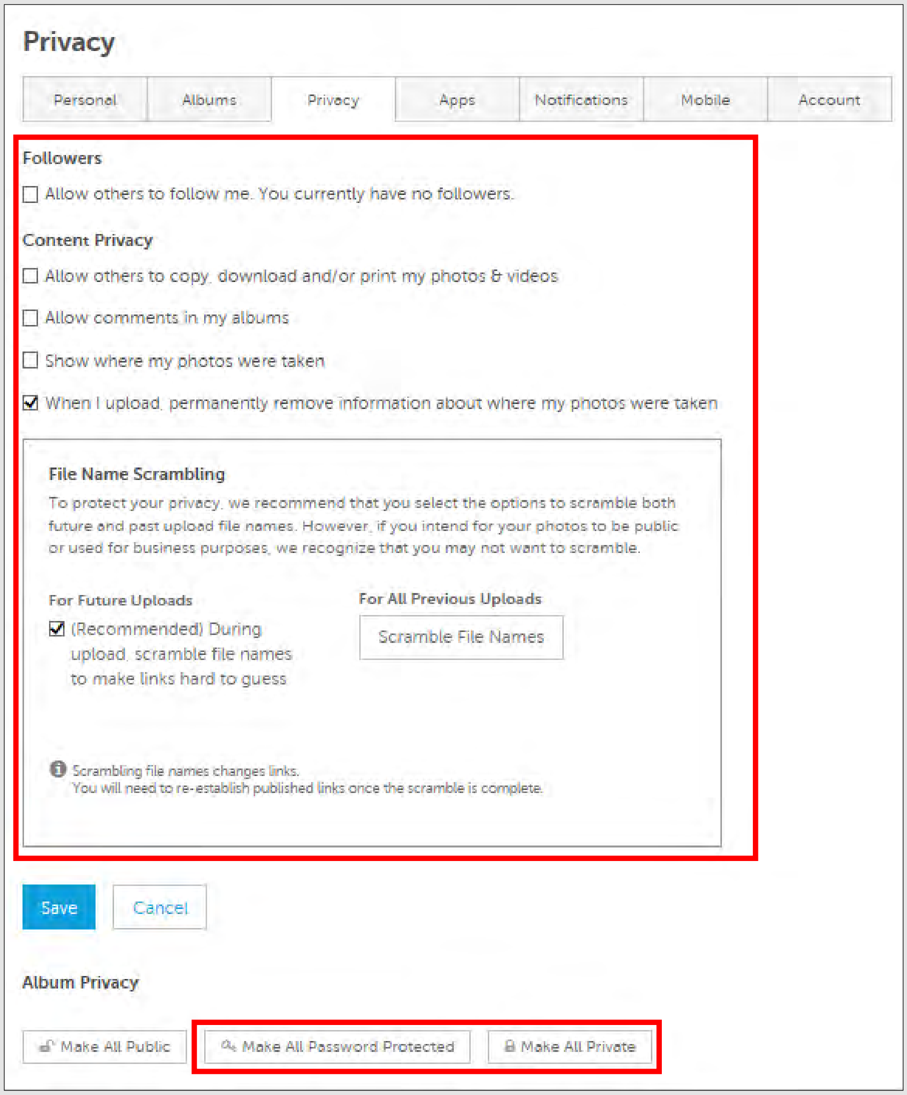
Account links	You have no third-party applications linked to your account, but here are some you might like to try

With proper security settings Flickr is a great web-based photo storage service, with 1 TB of free storage. #SecureMemories

Many photo sharing apps encourage you to link other social media accounts, but with convenience comes increased risk.

Privacy Settings Continued

photobucket



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

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

For All Previous Uploads

Scramble File Names

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

Album Privacy

Tap the 👤 at the top right corner.

Tap “Settings”.

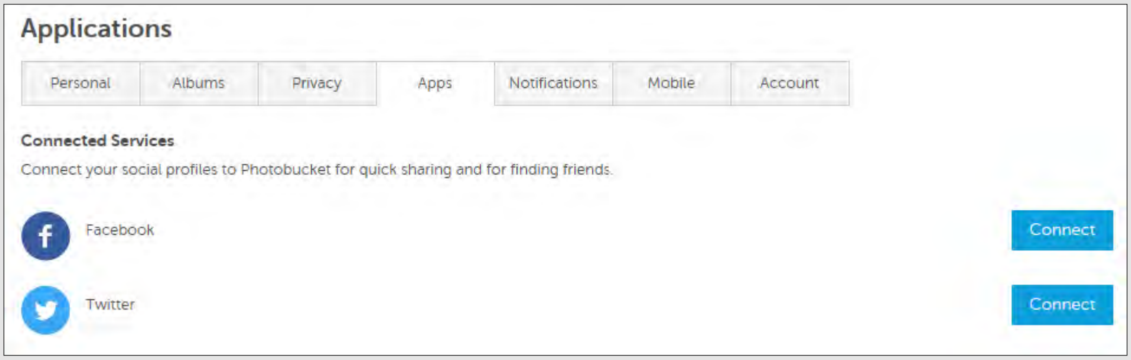
Tap the “Privacy” tab and use the image to the left as an example for your security settings.

Then tap the “Apps” tab.

Make sure you do not have any third party applications such as Twitter or Facebook linked to your Photobucket account.

Safety Fact: 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. Internet programs, such as Fuskers, have been created that can identify URL patterns and test for working photo URLs. This allows "private" photos on Photobucket being downloaded and distributed elsewhere on the Internet without the consent of their uploaders.

Photobucket monitors suspicious activity to prevent software from guessing URLs and downloading photos. It is recommended that Photobucket users scramble the links to photos and videos, and select the option to scramble the links of both past and future if there is no need to preserve the original file names.



Connected Services

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

UPDATED DEC 2019

SMARTPHONE EXIF REMOVAL SMART CARD

EXIF Data

EXIF—Exchangeable Image File Format—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, but may utilize the information internally. EXIF metadata are listed as tags that stores 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, GPSDateStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	Ability to reveal the exact location of private places, such as homes or offices. Some photosharing 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 sets 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.

Do:

- Prevent your device(s) from capturing geo-location data when taking pictures. Remove EXIF metadata from images taken by smartphones or digital cameras.
- Use privacy settings from the app to limit the audience to only yourself or close friends and family, before uploading pictures.
- Even with no EXIF data, the content of images may contain identifying information, including persons and locations. Assume that anyone can see, copy, or forward photos that are posted online.

Don't:

- Allow apps to automatically upload and share captured images (e.g. Instagram, Flickr).
- Assume that device settings remain the same after updates or over time. Verify the settings routinely.
- Upload pictures with landmarks, easily identifiable structures, or signs indicating location.
- Give apps used for sharing photos permission to access your device's location or other information.

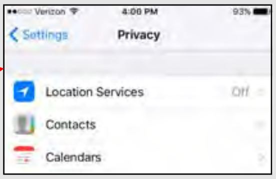
Prevent the Capture of Geolocation Data

iOS

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

❶ Select the "Settings" app. Click "Privacy" > "Location Services".

❷ Turn off location services altogether or for the iPhone's camera applications.



Verizon 4:00 PM 93%

< Settings Privacy

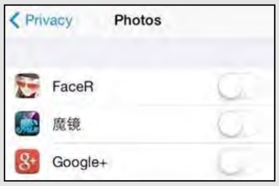
Location Services Off

Contacts

Calendars

❸ Return to the "Settings" app. Click "Privacy" > "Photos".

❹ Disable permissions for other apps to have access to the photos stored in the device's camera roll.



< Privacy Photos

FaceR

魔镜

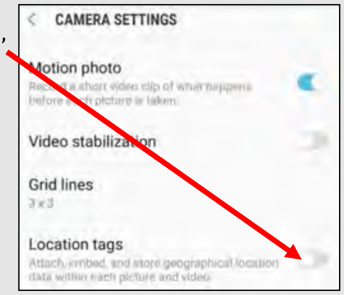
Google+

Android

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

❶ 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.

❷ 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.



< CAMERA SETTINGS

Motion photo

Record a short video clip of what happens before each picture is taken.

Video stabilization

Grid lines

3 x 3

Location tags

Attach, embed, and store geographical location data within each picture and video.

Twitter doesn't share your EXIF data, but it will geo-tag your post if location services are enabled. #DisableLocationServices

UPDATED DEC 2019

SMARTPHONE EXIF REMOVAL SMART CARD

Remove EXIF data before sharing or posting images, especially images captured in private homes or businesses. #PhotoSafety

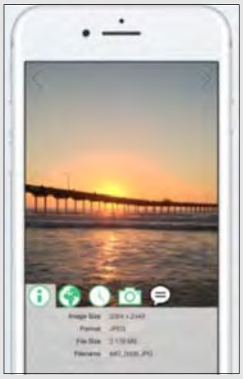
Prevent the Capture of Geolocation Data Continued

- 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 for your smartphone's camera application, as shown on the previous page.
- Remember that uploading or sharing a lower quality image will still 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 the select "Remove".

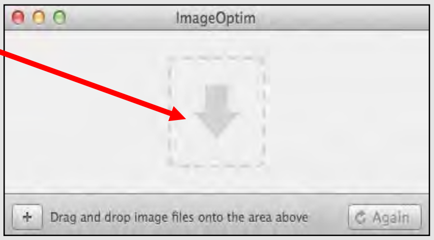


5. An easy way to identify photos that have EXIF data with geo-locations is to view your "Places" folder. Any images that appear in this folder have geolocation data, once you disable the geotagging feature and remove your EXIF data, this folder should be empty.

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.

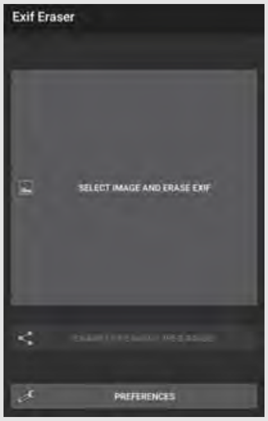
1. Drag the photos for EXIF removal into the app window and wait for a green check mark to appear next to the file name.



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".

EXIF Eraser for Android

EXIF Eraser is a free US-based app that deletes all EXIF data from image files stored on your Android

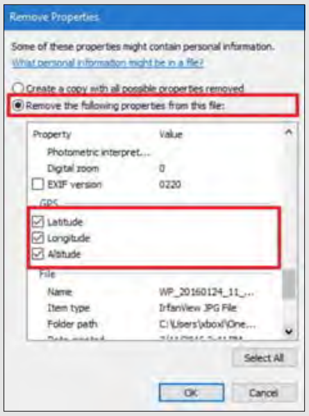


1. Download an EXIF Eraser app from the Play Store.
2. Open the app and select an image.
3. The EXIF data will be removed.
4. Processed images will be saved separately from the original file.

Reviewing & Removing EXIF Data in 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".



Remove Properties

Some of these properties might contain personal information.
What personal information might be in a file?

○ Create a copy with all possible properties removed
● Remove the following properties from this file:

Property	Value
Photometric interpret...	
Digital zoom	0
□ EXIF version	0220
GPS	
☑ Latitude	
☑ Longitude	
☑ Altitude	
File	
Name	WP_20160124_11_...
Item type	IrfanView JPG File
Folder path	C:\Users\xbox\One...

Select All

OK Cancel

Geo-localization

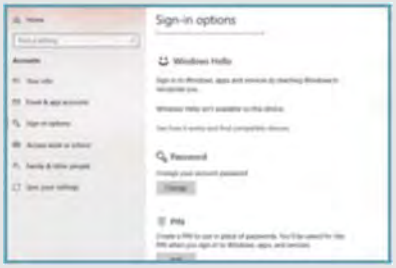
Even with the EXIF metadata removed, images containing, vegetation, addresses, business names, road markings, and landmarks, could allow someone to identify the location of where a photograph was taken. Geo-localization, the determination of a location of an image through visual information, is currently being researched and developed. This will allow computers to compare a picture without EXIF metadata to millions of other picture found on the internet that do have location metadata. Once the computer discovers a close match between two pictures the computer can apply the location metadata of one picture

UPDATED DEC 2019

LOCK DOWN YOUR LAPTOP SMART CARD

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.



Sign-in options

Windows Hello

Sign in to Windows, apps and services by teaching Windows to recognize you.

Windows Hello isn't available on this device.

See how it works and find compatible devices.

Password

Change your account password

Change

PIN

Create a PIN to use in place of passwords. You'll be asked for this PIN when you sign in to Windows, apps, and services.

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

Navigate to **Start Button > Settings > 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

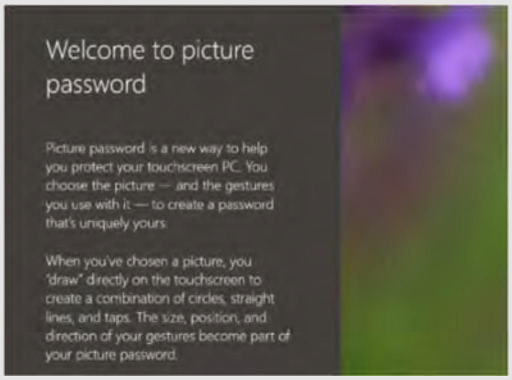
Windows 10 also has a number of additional log-in security features.

At the **Settings > 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 though likely 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 > Sign-in Options** menu by pairing your laptop to a Bluetooth device with the "Dynamic Lock" slider.



Welcome to picture password

Picture password is a new way to help you protect your touchscreen PC. You choose the picture — and the gestures you use with it — to create a password that's uniquely yours.

When you've chosen a picture, you "draw" directly on the touchscreen to create a combination of circles, straight lines, and taps. The size, position, and direction of your gestures become part of your picture password.

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.

Encryption Basics

Some versions of Windows 10 allow users to easily encrypt file, folder and hard drive data with BitLocker protection. To access BitLocker, navigate to **Start Button > Settings > System and Security** and select the BitLocker slider to secure your hard drive data.

If you'd rather use "on-the-fly" software to lock certain files or folders, you can also use a number of Freeware (Free Software) encryption services such as VeraCrypt, AxCrypt, GNU Privacy Guard, or 7-Zip.

Laptop Security Tip: If possible, set-up two factor authentication on your laptop by pairing it with a Bluetooth device you carry on your person.

UPDATED DEC 2019

LOCK DOWN YOUR LAPTOP SMART CARD

Virtual Private Network (VPN)

A Virtual Private Network (VPN) connection could save your life. No, really, it could. Well, maybe that's a bit dramatic, but it *can* safeguard your data and protect your personal 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 rarely 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. In fact, there are few reasons not to use VPN, whether you're connecting at home or on the go.

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 . It really is that simple.

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 ISP 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

Sources

http://www.pcworld.com/article/2025897/a-road-warriors-guide-to-locking-down-your-laptop.html

https://www.umass.edu/it/support/security/laptop-mobile-device-physical-security-dos-donts

http://www.pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

http://www.lehman.edu/itr/documents/computer-security-dos-donts.pdf

http://www.pcworld.com/article/223044/vpns_for_beginners_to_experts.html

https://laptop.ninja/5-dos-and-donts-for-laptop-owners/

https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up

Laptop Security Tip: Full-disk encryption can protect your data but only when used in combination with good password security practices.

UPDATED DEC 2019

SECURING YOUR HOME WIRELESS NETWORK

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 ILuvF00tb@77 from the phrase "I love football."
- Use a cable to directly connect any stationary computers / devices to your home network to limit vulnerabilities presented by wirelessly connected devices
- 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.

Glossary of Commonly Used Terms

Wireless Router	Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identifier (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.

Wi-Fi Security Level	Level of Security	Explanation
WEP	Low/Risky	Old encryption protocol. No longer considered a standard. Highest risk next to an "open" network.
WPA	Low-Moderate	Older encryption protocol. Better than WEP but should not be used when more modern encryption (WPA2) is available.
WPA2	Moderate-high	WPA2-PSK (AES) is the most secure option which uses the latest Wi-Fi encryption.
WPA3	High	Approved and replacing WPA2 by the end of 2018, as the new and more secure option for Wi-Fi Security.

Accessing Your Router

In order to change your WPA2 password you will need to access your router. In order to access your router, you must enter the appropriate IP address, username, and password. If you do not have this information, your Internet Provided should be able to provide it to you.

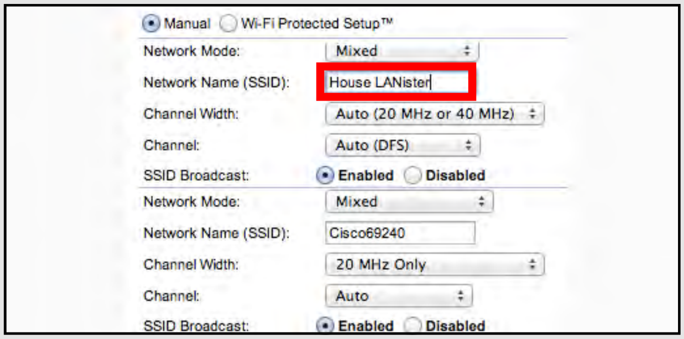
It is **important** to understand that when your internet is being set up by your Internet Provider, they are not required to set it up using WPA2 (see the chart to the left). Recommend you ensure they set it up for you and provide the IP address for the Router's settings. That way, once they leave you can change the user name and password.

When changing your username and password for the WIFI, it is important to consider the following: choose a username that does not include you or your family members' names; creating a password that is long and complex. Lastly, it is important to change any Guest account password to something other than your Admin/family account password.

Passwords provided by your internet provider are general in use; it is a good idea to change the password after everything is set up. #keepyourhomesecure

SECURING YOUR HOME WIRELESS NETWORK

Creating a Unique SSID



● Manual ○ Wi-Fi Protected Setup™

Network Mode: Mixed

Network Name (SSID): House LANister

Channel Width: Auto (20 MHz or 40 MHz)

Channel: Auto (DFS)

SSID Broadcast: ● Enabled ○ Disabled

Network Mode: Mixed

Network Name (SSID): Cisco69240

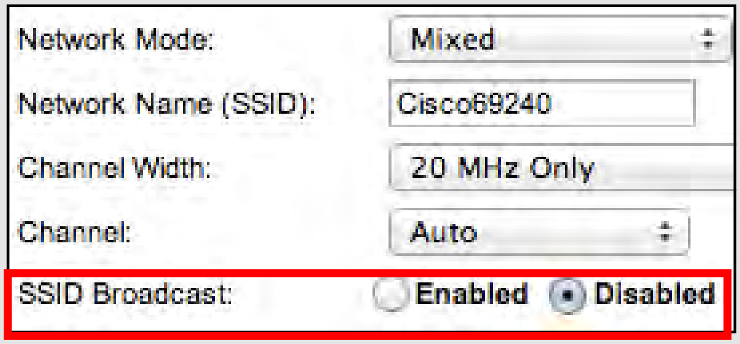
Channel Width: 20 MHz Only

Channel: Auto

SSID Broadcast: ● Enabled ○ Disabled

When creating a name for your Wi-Fi (your SSID), it is important to consider who will be seeing it and what information it may give away about you and your family. For instance, if you decide to give it the family name (last name and perhaps 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 specific network and entice nefarious individuals into attempting to hack into it. It is recommended that you chose a name for your SSID that is generic in nature, providing no information about your family, address, date of birth, etc.

Disabling the SSID Broadcast



Network Mode: Mixed

Network Name (SSID): Cisco69240

Channel Width: 20 MHz Only

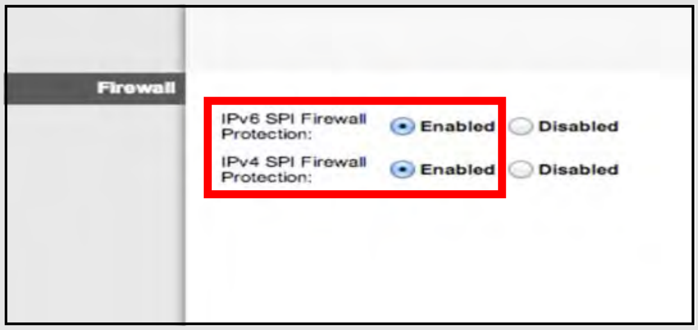
Channel: Auto

SSID Broadcast: ○ Enabled ● Disabled

If you would like to hide your SSID so that it does not broadcast to the public, you can do so by scrolling down from where you created your SSID name till you find what's pictured above. Remember, that while it is nice to be able to disable the broadcasting of your SSID, it is important to note that it can be easily unhidden should an individual request to find "hidden Wi-Fi's".

If you have smaller children in your home who have devices like the Leapfrog or Vtech games, and you disable your SSID broadcasting your child's device will not be able to find your network and connect to the internet. In order for those devices to connect, you will need to go back into your router settings and re-Enable the broadcasting of your SSID.

Router Firewall



Firewall

IPv6 SPI Firewall Protection: ● Enabled ○ Disabled

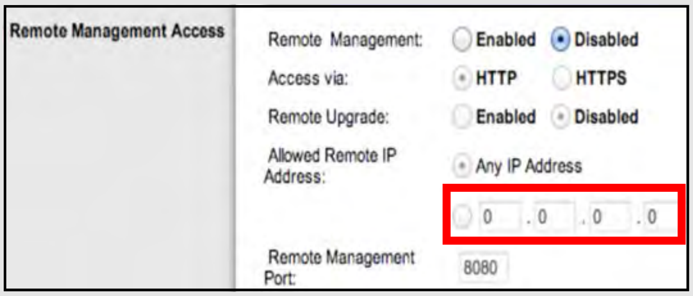
IPv4 SPI Firewall Protection: ● Enabled ○ Disabled

The next two settings are usually found in "Router Settings" but you may have to look around a bit to find them.

A firewall is a layer of security between your home network and the Internet. Since a router is the main connection from a home network to the Internet, the firewall function is merged into the router. Every home network should have a firewall to protect its privacy.

A firewall does not secure against every kind of attack. For example, you still need to run a virus-checker on all your computers.

Remote Access



Remote Management Access

Remote Management: ○ Enabled ● Disabled

Access via: ● HTTP ○ HTTPS

Remote Upgrade: ○ Enabled ● Disabled

Allowed Remote IP Address: ● Any IP Address

○ 0 . 0 . 0 . 0

Remote Management Port: 8080

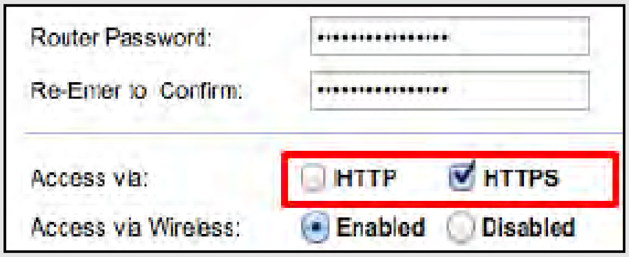
Check that the Remote Management IP Address is set to **0.0.0.0** to ensure that remote access is disabled. This will help to ensure that others cannot access your router remotely and without your permission.

Even if you have set up WPA2-PSK on your WI-FI it is still very important to have a virus and malware protection for your computer. #cybersecurity

SECURING YOUR HOME WIRELESS NETWORK

Routers need to be updated. We tend to take our Wi-Fi for granted, but just like taking the car in for an oil change we need to patch routers routinely. #themoreyouknow

Enabling HTTPS



Router Password: ••••••••••••••••

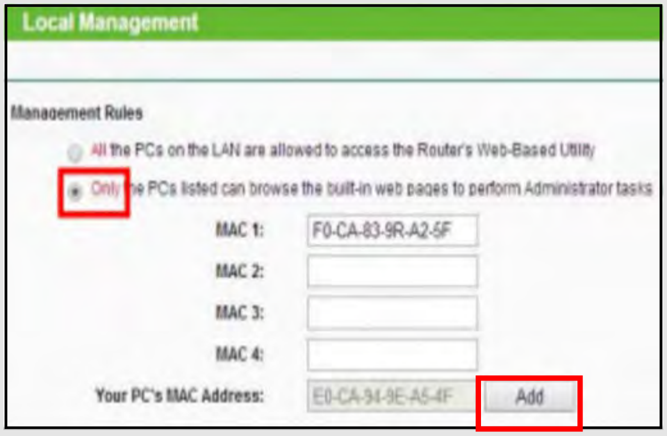
Re-Enter to Confirm: ••••••••••••••••

Access via: □ HTTP ☑ HTTPS

Access via Wireless: ● Enabled ○ Disabled

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 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.

Wireless MAC Filtering



Local Management

Management Rules

○ All the PCs on the LAN are allowed to access the Router's Web-Based Utility

● Only the PCs listed can browse the built-in web pages to perform Administrator tasks

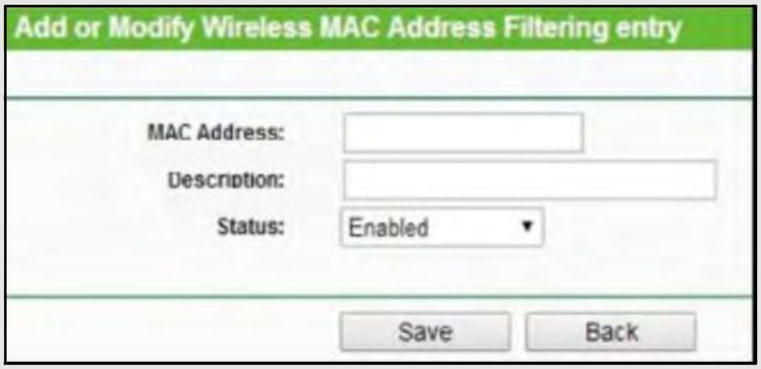
MAC 1: F0-CA-83-9R-A2-5F

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address: E0-CA-94-9E-A5-4F



Add or Modify Wireless MAC Address Filtering entry

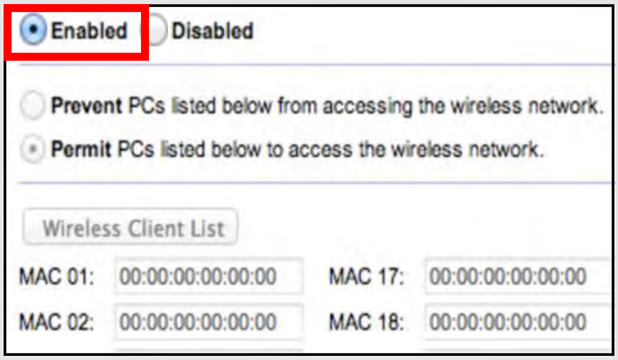
MAC Address:

Description:

Status: Enabled

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 (as highlighted above). 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 (as highlighted in the box to the right). Click the 'Add' button when done entering authorized devices.



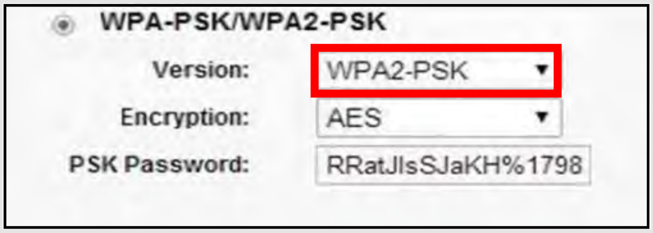
● Enabled ○ Disabled

○ Prevent PCs listed below from accessing the wireless network.

● Permit PCs listed below to access the wireless network.

MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00

Encryption



● WPA-PSK/WPA2-PSK

Version: WPA2-PSK

Encryption: AES

PSK Password: RRatJlsSJaKH%1798

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 examples, but different from the administrative router access password.

Useful Links

Practically Networked
www.practicallynetworked.com/support/wireless_secure.htm

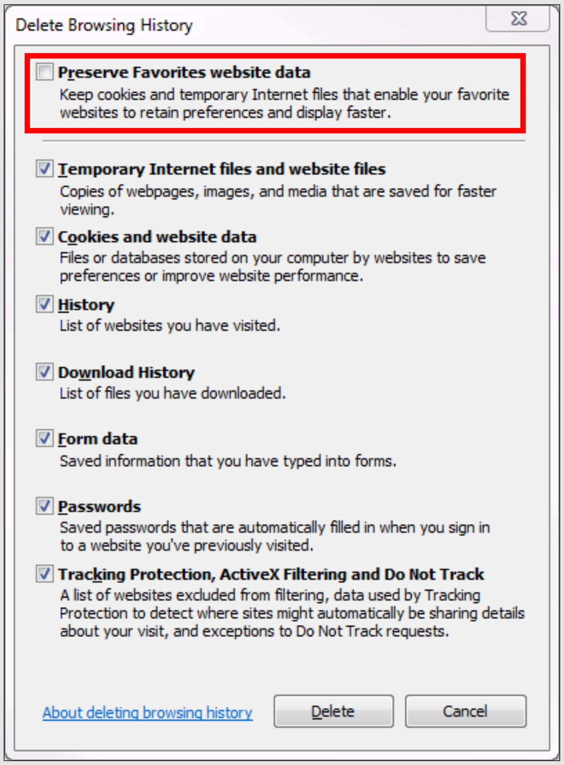
Wi-Fi.org
www.wi-fi.org/discover-wi-fi/security

DELETE BROWSER ARTIFACTS SMART CARD

Browser Artifacts—Cookies, Cache & History

Items such as browsing history, cache, and cookies are saved on your computer while you surf the Web. They are utilized in a number of ways to improve your browsing experience. These private data components, while offering conveniences such as faster load times and auto-populated fields, can also 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 can potentially be harmful if it fell into the wrong hands. For security and privacy purposes, delete these artifacts on a regular basis.

Deleting Internet Explorer Web Browser Artifacts



Delete Browsing History

□ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files and website files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies and website data**
Files or databases stored on your computer by websites to save preferences or improve website performance.

☑ **History**
List of websites you have visited.

☑ **Download History**
List of files you have downloaded.

☑ **Form data**
Saved information that you have typed into forms.

☑ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

☑ **Tracking Protection, ActiveX Filtering and Do Not Track**
A list of websites excluded from filtering, data used by Tracking Protection to detect where sites might automatically be sharing details about your visit, and exceptions to Do Not Track requests.

About deleting browsing history | Delete | Cancel

Make sure you are using the latest version of Internet Explorer (IE).

Click the Settings ⚙ button on the top right.

Click “Internet Options”.

Under the “General” tab’ locate the “Browsing History” section.

Click “Delete”.

You will see the window to the left. A useful keyboard shortcut to access this window is “*Ctrl-Shift-Delete”.*

Deselect “Preserve Favorites website data”.

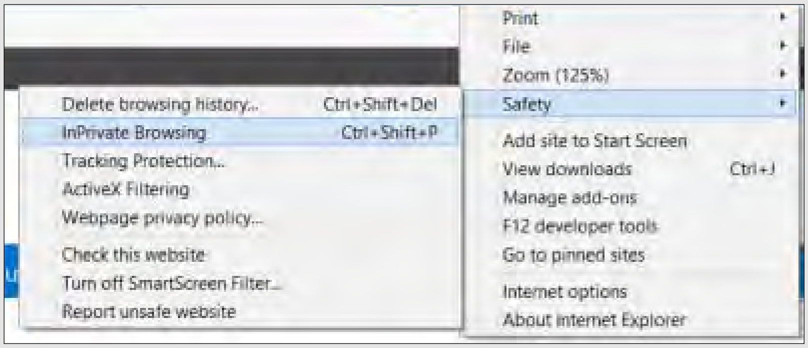
Select the boxes next to the history you want to remove and click “Delete”.

Exit/quit all browser windows and re-open the browser.

Internet Explorer is no longer supported on any mobile device.

As of March 2017, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on its Windows 10 devices. As of early 2018, IE versions 11, 10 and 9 still receive security updates.

Using Internet Explorer InPrivate Browser



To activate “InPrivate”, click the Settings ⚙ button on the top right.

Click “Safety”.

Click “InPrivate Browsing”.

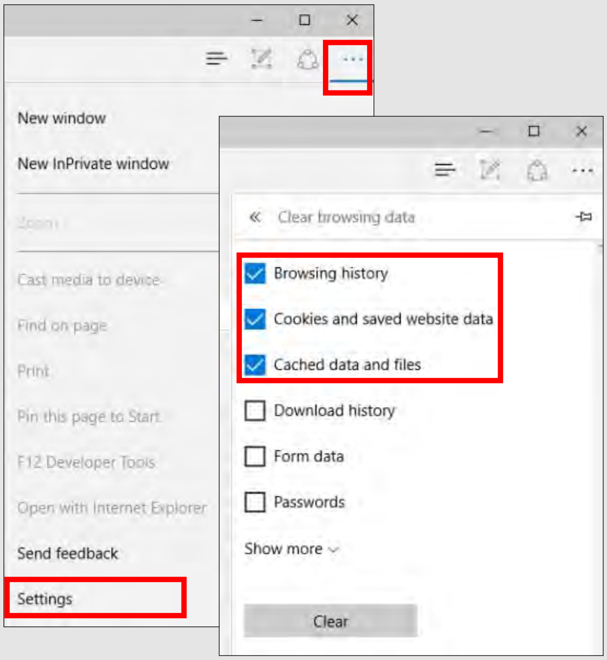
Alternatively, after opening Internet Explorer you can use the shortcut “*Ctrl-Shift-P*”.

An internet cookie is a small piece of data sent from a website and stored on a user’s computer while the user is browsing.

UPDATED DEC 2019

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Microsoft Edge Web Browser Artifacts



Clear browsing data

☑ Browsing history

☑ Cookies and saved website data

☑ Cached data and files

□ Download history

□ Form data

□ Passwords

Show more

Clear

Be sure to delete the browser artifacts regularly.

Click the three dots at the top right corner.

Click "Settings" followed by the "Privacy & security" tab..

Then click "Clear Browser Data".

Select the boxes next to the history you want to remove and click "Clear".

Mobile Browser

Open the Edge browser.

Tap the menu button ☆ on the top right.

Tap to 🕘 view history.

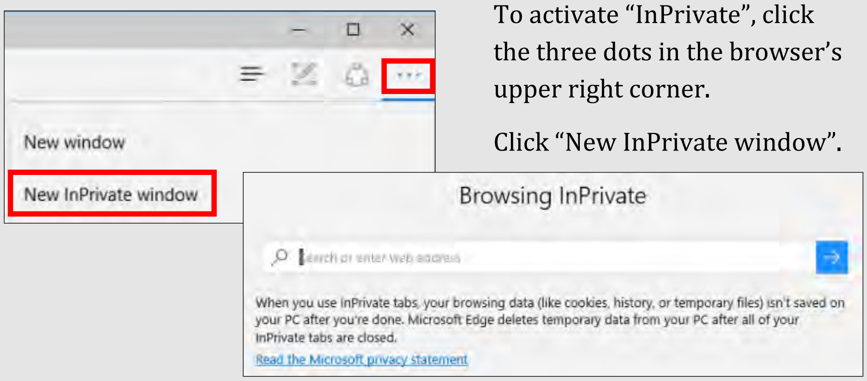
Tap to 🗑 clear all history.

Choose the types of data to remove from your phone and tap "Clear".

Using Microsoft Edge InPrivate Browser

Edge is Microsoft's new browser that comes with Windows 10. It is meant to eventually replace IE.

Edge comes with an option called "InPrivate", which is the browser's private mode that does *not* record your activities.



Browsing InPrivate

Search or enter web address

When you use InPrivate tabs, your browsing data (like cookies, history, or temporary files) isn't saved on your PC after you're done. Microsoft Edge deletes temporary data from your PC after all of your InPrivate tabs are closed.

Read the Microsoft privacy statement

To activate "InPrivate", click the three dots in the browser's upper right corner.

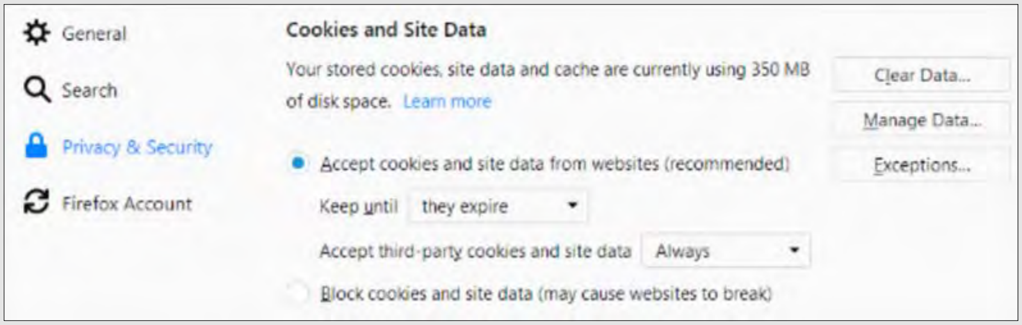
Click "New InPrivate window".

An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

UPDATED DEC 2019

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Firefox Web Browser Artifacts



Cookies and Site Data

Your stored cookies, site data and cache are currently using 350 MB of disk space. Learn more

Clear Data...

Manage Data...

Exceptions...

● Accept cookies and site data from websites (recommended)

Keep until: they expire

Accept third-party cookies and site data: Always

○ Block cookies and site data (may cause websites to break)

Click the menu button and click “Options”.

Click “Privacy & Security” on the left.

Then click “Clear Data”.

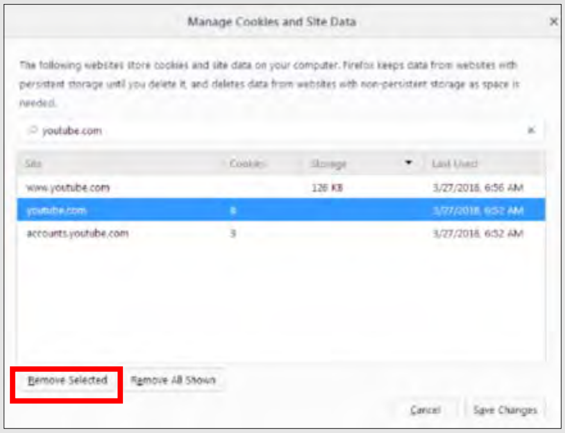
Individual Cookies

You can also remove individual cookies.

From the “Privacy & Security” screen, click “Manage Data”.

Select the site(s) you wish to clear data for.

Then click “Remove Selected”.



Manage Cookies and Site Data

The following websites store cookies and site data on your computer. Firefox keeps data from websites with persistent storage until you delete it, and deletes data from websites with non-persistent storage as space is needed.

youtube.com

Site	Cookies	Storage	Last Used
www.youtube.com		126 KB	3/27/2018, 6:56 AM
youtube.com	8		3/27/2018, 6:52 AM
accounts.youtube.com	3		3/27/2018, 6:52 AM

Mobile Browser

Tap the Menu icon on the top right.

Tap “Settings”. Scroll down to “Clear Private Data” and tap it.

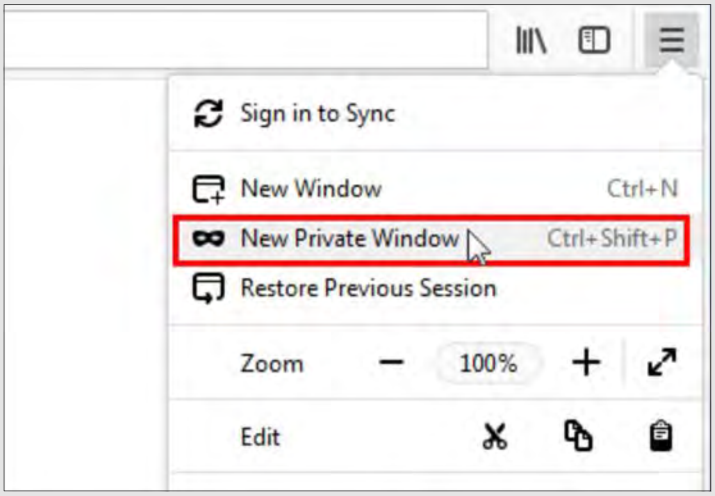
Selected data to be cleared. Tap “Clear Data.”

To manage how your data is shared and tracked, tap “Privacy” then tap “Tracking Protection” from the Settings menu.

“Enabled In Private Browsing” will inform sites that you do not want your browsing behavior tracked, but honoring this is voluntary.

Cookies can also be disabled from this screen.

Using Firefox Private Browsing Mode



To open a new Private Window, click the menu button on the top right.

Click “New Private Window”.

Alternatively, after opening Firefox you can use the shortcut “*Ctrl-Shift-P*”.

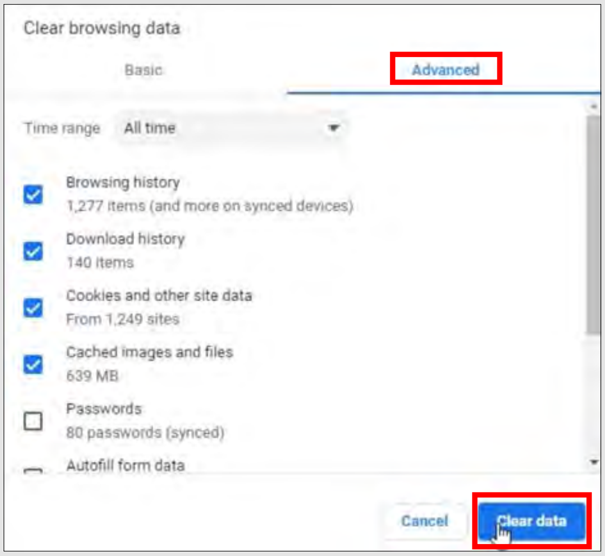
Important: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer.

Private Browsing also includes Tracking Protection, which prevents companies from tracking your browsing history across multiple sites.

DELETE BROWSER ARTIFACTS SMART CARD

Chrome doesn't have control over third party websites or their privacy practices, so be cautious when accessing websites.

Delete Google Chrome Browser Artifacts



Clear browsing data

Basic | Advanced

Time range: All time

☑ Browsing history
1,277 items (and more on synced devices)

☑ Download history
140 items

☑ Cookies and other site data
From 1,249 sites

☑ Cached images and files
639 MB

□ Passwords
80 passwords (synced)

Autofill form data

Click the ⋮ icon at the upper right corner.

Click "History" or hold *Ctrl-H*.

Click the menu on the upper left hand side.

Click "Clear Browsing Data". You can also hold C*trl-Shift-Delete*.

Click the "Advanced" tab in the pop-up window.

Select the Time range you desire.

Select the boxes next to the history you want to remove and click "Clear Browsing Data".

Exit/quit all browser windows and re-open the browser.

Mobile Browser

Tap the menu ⋮ icon.

Then tap "Settings".

Tap "Privacy".

Tap "Clear Browsing Data".

Select the boxes next to the history you want to remove and tap "Clear Data".

Individual Cookies

You can also remove individual cookies.

Click the ⋮ icon at the upper right corner.

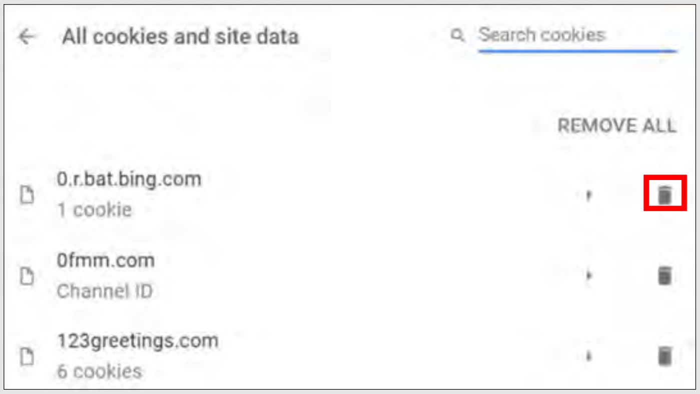
Click "Settings".

Scroll all the way to the bottom and click the "Advanced" button.

Under the "Privacy & Security" section, click the "Site Settings".

Click "Cookies and site data" and then "See all cookies and Data".

Click 🗑 for the sites you wish to clear.



All cookies and site data

0.r.bat.bing.com
1 cookie

0fmm.com
Channel ID

123greetings.com
6 cookies

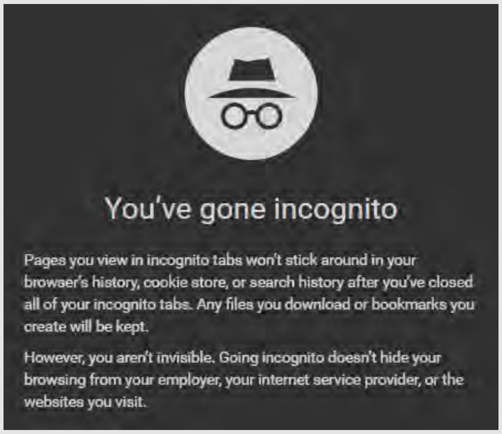
Using Google Chrome Incognito Mode

Chrome's Incognito mode will *not* save a record of what you visited or downloaded.

Be aware that Incognito is not available if you are using Window 10's "Family Mode."

Click the ☰ icon at the upper right. Select "New Incognito Window".

You can also use Incognito via the Chrome app on your iOS or Android device. Follow the same steps as above with the app.



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

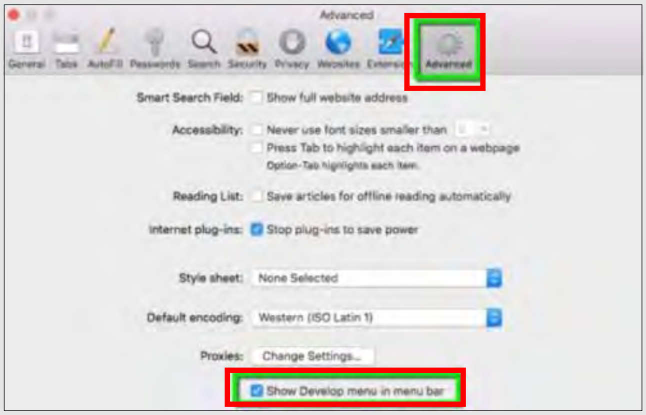
However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Like Microsoft Edge's InPrivate Browser, Chrome's Incognito will require you to constantly type in your password for logins. So you may prefer to use the regular Google Chrome browser out of convenience.

UPDATED DEC 2019

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Safari Browser Artifacts



Smart Search Field: □ Show full website address

Accessibility: □ Never use font sizes smaller than
□ Press Tab to highlight each item on a webpage
Option-Tab highlights each item.

Reading List: □ Save articles for offline reading automatically

Internet plug-ins: ☑ Stop plug-ins to save power

Style sheet: None Selected

Default encoding: Western (ISO Latin 1)

Proxies: Change Settings...

☑ Show Develop menu in menu bar

Click the “Safari” menu on the top left.

Click “Preferences”.

Click the “Advanced” tab.

Check the box at the bottom for “Show Develop menu in menu bar” and close the window.

Click the “Develop” menu at the top and click “ Empty Caches”.

Then click the “History” menu at the top and click “Clear History”.

Right click on the Safari icon in your App tray and select “Quit”.

Mobile Browser

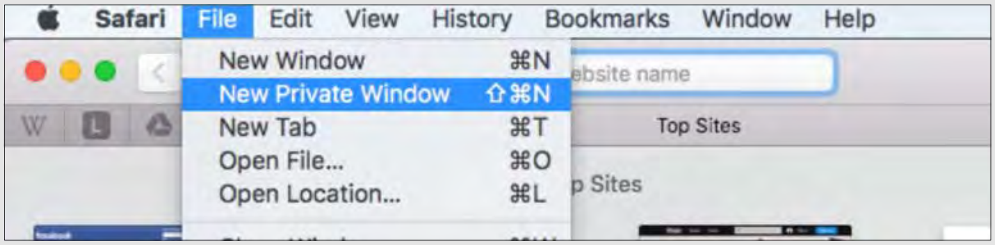
Open your iOS Settings app.

Scroll down and tap “Safari”.

Tap the “Clear History and Website Data” link in blue.

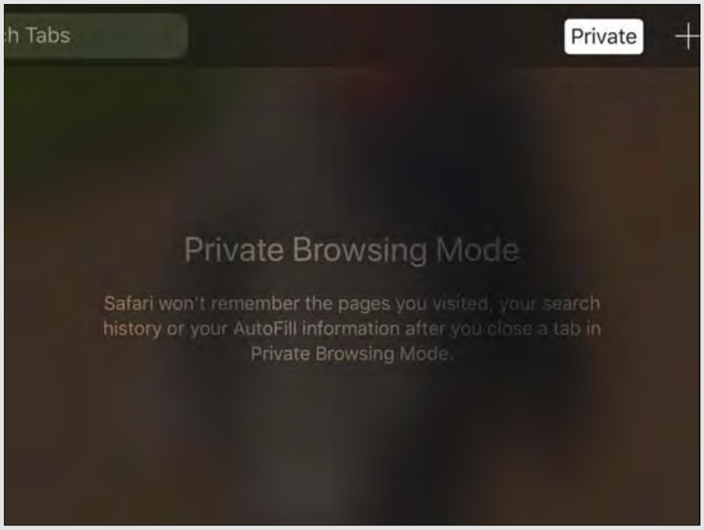
Exit/quit all browser windows and re-open the browser.

Deleting Safari Browser Artifacts



To open a Private Window, click “File” on the top left.

Click “New Private Window”.



Private Browsing Mode

Safari won't remember the pages you visited, your search history or your AutoFill information after you close a tab in Private Browsing Mode.

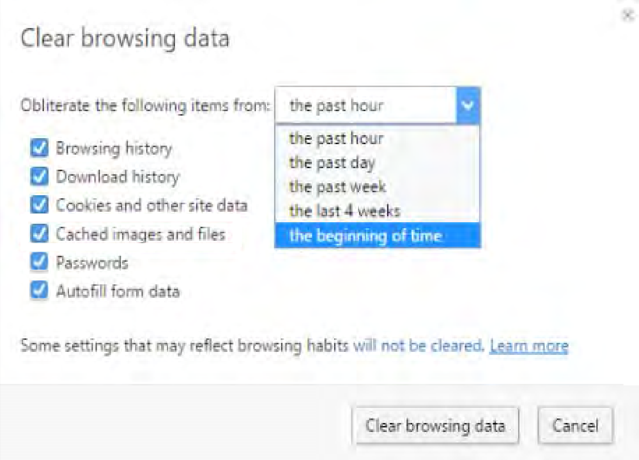
Enabling Private Browsing limits Safari in three important ways: It prevents the browser from creating a history of the pages you visit, it stops AutoFill information like website usernames and passwords from being remembered, and any tabs you open won't be stored in iCloud.

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.

When you are on a website that uses Apple Pay, the site can automatically check if you have Apple Pay set up if you haven't disabled this feature.

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Opera Browser Artifacts



Clear browsing data

Obliterate the following items from: the past hour

the past hour
the past day
the past week
the last 4 weeks
the beginning of time

☑ Browsing history
☑ Download history
☑ Cookies and other site data
☑ Cached images and files
☑ Passwords
☑ Autofill form data

Some settings that may reflect browsing habits will not be cleared. Learn more

Click the "Menu" button on the top left.

Click "History".

Click "Clear Browsing Data".

Select the Time frame and the boxes next to the history you want to remove and click "Clear Browsing Data".

Exit/quit all browser windows and re-open the browser.

Mobile Browser

Tap on the "Menu" button.

Tap "History".

Tap "Clear All".

Tap "Yes" to confirm.

Using a Private Tab in Opera Browser

Opera's Private Tab browsing deletes browsing history, cache, cookies, and logins when you close the tab.

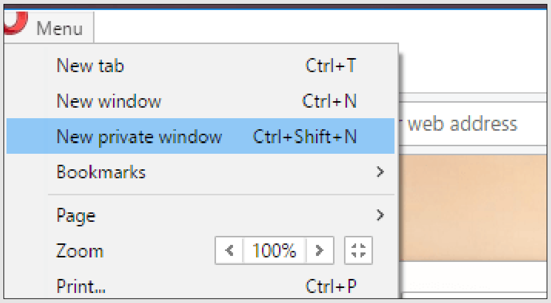
Please note that if you deliberately save data, such as a bookmark or a file, it will still be visible after the tab is closed.

You may prefer to use the regular Opera Browser window out of convenience. Be sure to delete browser artifacts regularly.

To create a Private Tab, click the "Menu" button on the top left corner.

Click "New Private Window".

Private browsing is also available on Opera Mini mobile browser as well.



Privacy is about much more than "hiding things". It's about protection. #ProtectYourPrivacy

DELETE BROWSER ARTIFACTS SMART CARD

Privacy and Security-Related Browser Tools

Ghostery is a German-owned freeware browser extension that allows you to choose what to block, on a tracker-by-tracker or site-by-site basis, or a combination of the two.

The tool also offers tracker profiles so you can learn about the companies collecting data on you as you browse the web.

Ghostery looks at the HTML code on each web page you visit to see if there are "tags" or "trackers" placed by a company that works with the website. The tool can determine if the company is showing you ads, collecting data, or giving you added functionality on the page.

The extension is available for Firefox, Chrome, Safari, Internet Explorer, Microsoft Edge, and Opera. It is also accessible via a mobile application for Android, iOS, and Firefox for Android.

AdBlock Plus is a German-based extension that blocks banner ads, pop-up ads, rollover ads, and more. It stops you from visiting known malware-hosting domains and disables third-party tracking cookies and scripts. It can even block video ads on Facebook and YouTube.

This extension works for Android, Chrome, Firefox, Internet Explorer, Maxthon, Opera, Safari and Yandex.

Blur protects your passwords, payments, and privacy from cyber criminals.

The US-based tool masks your passwords, email addresses, credit card numbers, and address information. It also has the ability to create strong passwords for new and existing accounts.

Blur blocks hundreds of companies from collecting your data online and blocks tracking that doesn't rely on cookies.

Free and Premium versions are available. Masked information is only available with the Premium version which costs $2—$5 a month based on length of subscription.

This extension is only available for Firefox on all devices.

Disconnect is a smart filter that stops third-party sites from tracking you. The companies that are collecting your information are shown in real-time as pages load. You can even see how those sites may be linked to other sites that track information.

Disconnect encrypts the data you exchange with common sites and helps to prevent visiting sites that have malware.

The extension is available for Chrome, Firefox, Safari, and Opera.

Before installing an add-on or extension, review the requested permissions. They may request to access and store to your data.

ADDITIONAL RESOURCES

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

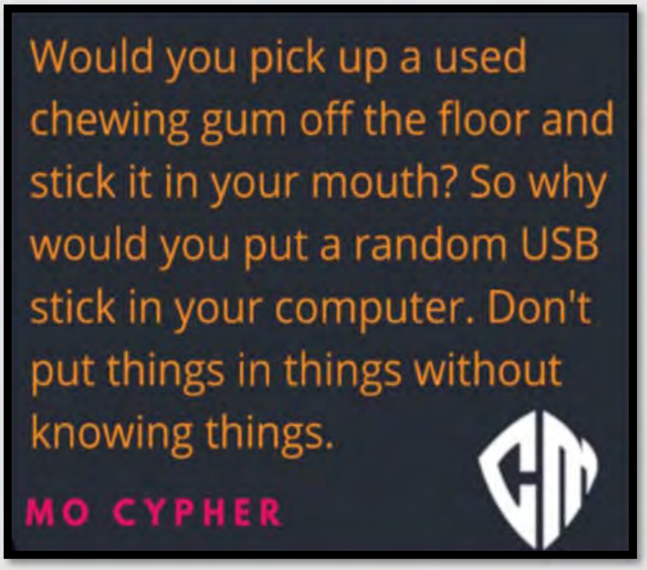
Equifax—ID Protection Kit
www.equifax.com/idtheftprotectionkit

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


Would you pick up a used chewing gum off the floor and stick it in your mouth? So why would you put a random USB stick in your computer. Don't put things in things without knowing things.

MO CYPHER

Netsmartz Workshop for Parent & Guardians
www.netsmartz.org/netparents.htm
www.netsmartz411.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.commonsensemedia.org

Opt Out of Interest-Based Advertising
www.networkadvertising.org/choices

Google Privacy
www.google.com/policies/privacy

DMA Choice
https://dmachoice.thedma.org

Social Media Help (for updated Privacy information)
https://www.facebook.com/help
http://search.twitter.com

Remember the more you know the easier it is to prevent something like Identity Theft from happening to you. #stopthinkpost #themoreyouknow