



Privacy Settings

The internet offers a wealth of knowledge and ways to connect with people. However, as we explored last week, it can lead to people to search personal information on you or people you know.

No matter how you access the internet or internet-connected apps, there are privacy settings that you, as a user can use to protect your personal information. Here are some examples that you can explore. Even though you may not use certain apps or browsers, someone you know (family and friends) may use them. Helping them understand how and who they choose to share information can help their information stay safe and secure.

Browser Settings

(This can look different on how your browser is set up on your computer)

It may seem like a lot but for not, focus on the privacy menu(s). Here, you can change how you interact with your internet browser, search history, and what information it collects to make searching for something easier. Easier does not mean secure!

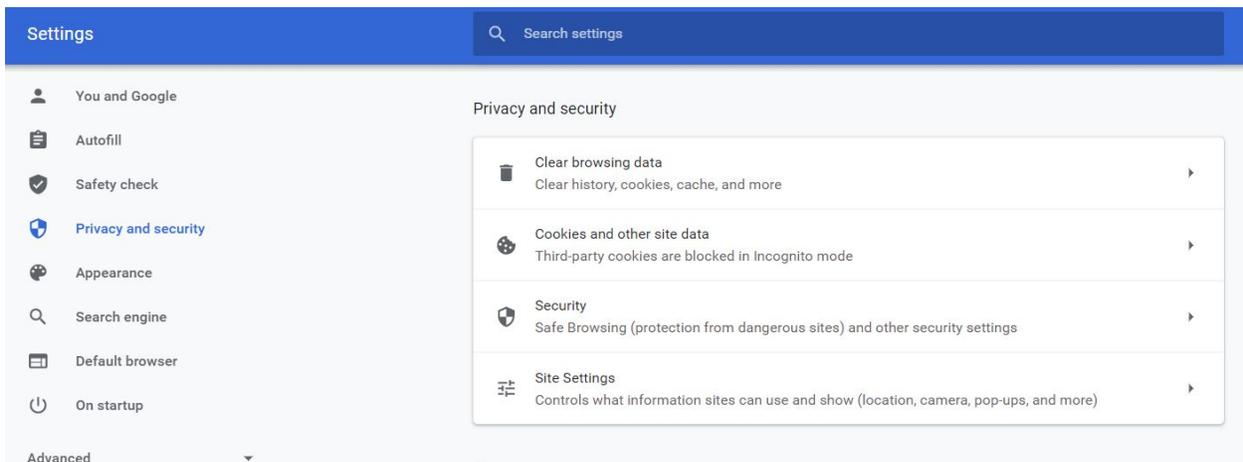
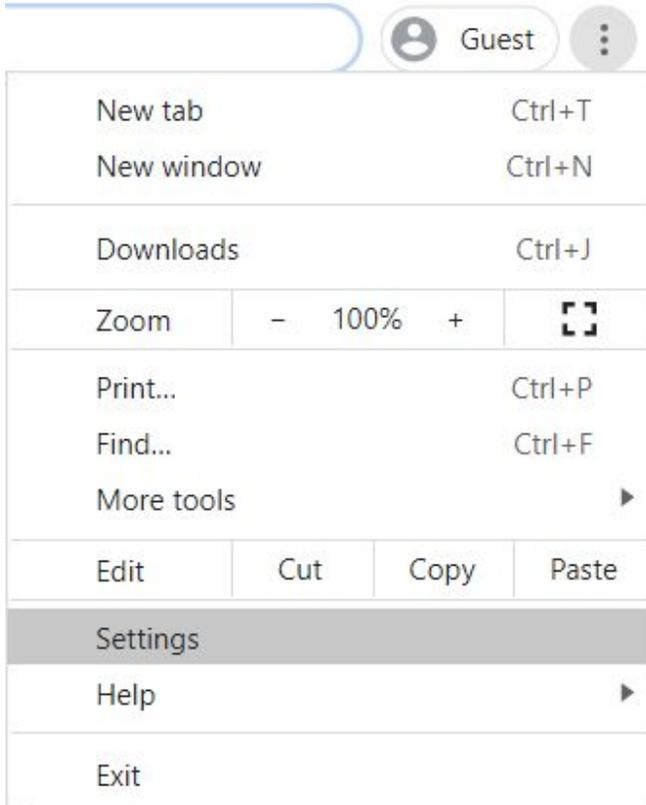
Explore the different settings on your browser to tune what kind of information your browser keeps or deletes when you close your browser, how to clear your search history, cookies (how websites remember what you do so it tailors searches to your preferences), cache (data to store temporary data so the next time you load up a website or app, it will load faster), and permissions (microphone, camera, notifications, and location) and more.

There are other browsers you can download and use. Here are some examples that will help you navigate any browser you end up using. You can also research the browser you use by searching the “browser name + security settings.”



Google Chrome:

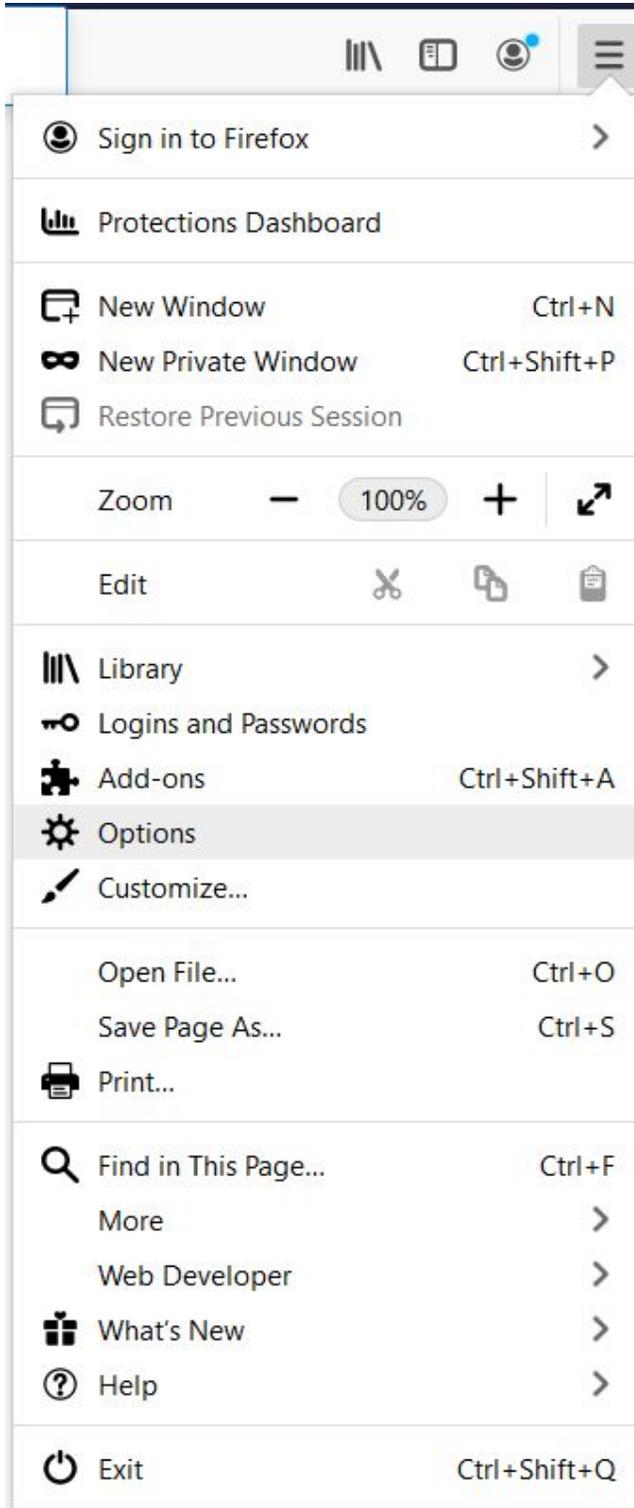
1. Click on the three vertical dots and select Settings





Mozilla Firefox:

1. Click the three horizontal lines and select “Options.”





2. Select "Privacy & Security."

The screenshot shows the Firefox browser's settings interface. On the left is a sidebar with navigation options: General (gear icon), Home (house icon), Search (magnifying glass icon), Privacy & Security (lock icon, highlighted in blue), Sync (refresh icon), Extensions & Themes (puzzle piece icon), and Firefox Support (question mark icon). The main content area is titled "Browser Privacy" and features "Enhanced Tracking Protection" with a shield icon. A text block explains that trackers follow users online and that Firefox blocks many of them, with a "Manage Exceptions..." button. Below this are three protection levels: "Standard" (selected with a radio button), "Strict", and "Custom". The "Standard" level is described as "Balanced for protection and performance. Pages will load normally." and lists several blocked items: Social media trackers, Cross-site tracking cookies, Tracking content in Private Windows, Cryptominers, and Fingerprinters. The "Strict" level is described as "Stronger protection, but may cause some sites or content to break." The "Custom" level is described as "Choose which trackers and scripts to block".

General

Home

Search

Privacy & Security

Sync

Extensions & Themes

Firefox Support

Browser Privacy

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. [Learn more](#)

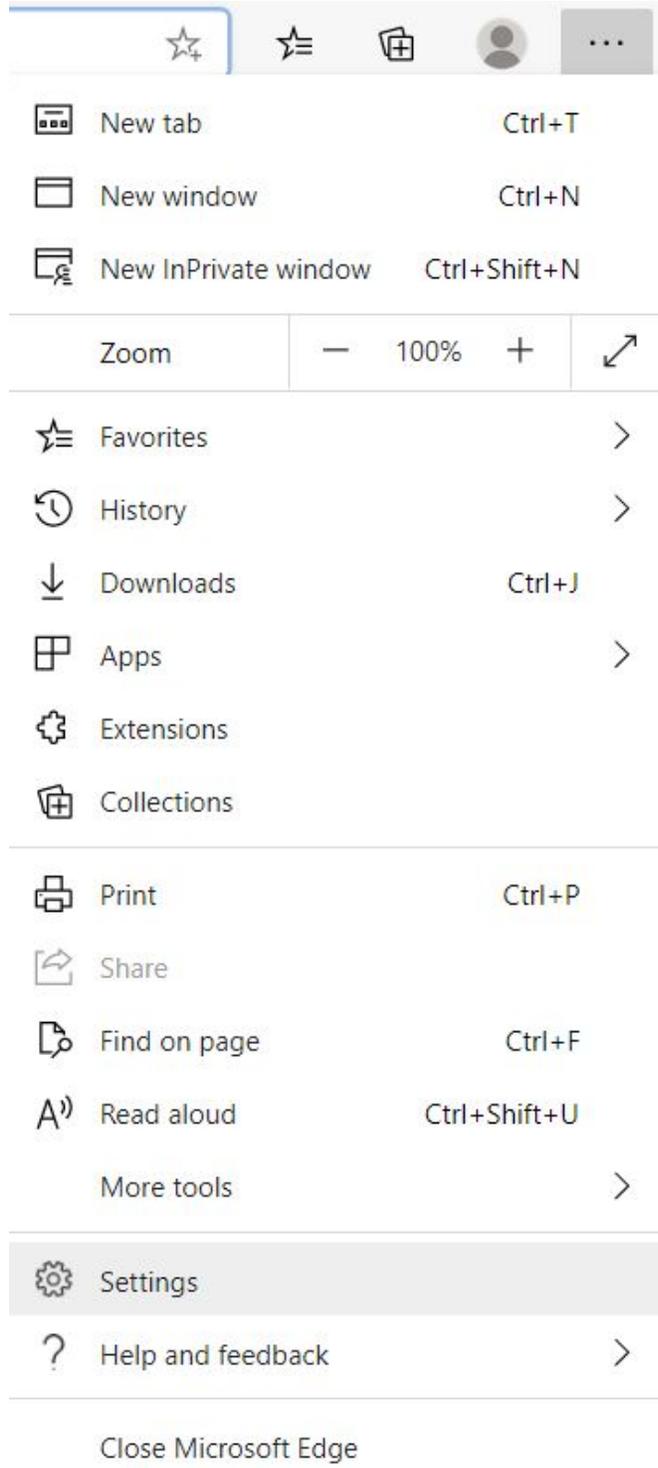
[Manage Exceptions...](#)

- Standard**
Balanced for protection and performance. Pages will load normally.
 - Social media trackers
 - Cross-site tracking cookies
 - Tracking content in Private Windows
 - Cryptominers
 - Fingerprinters
- Strict**
Stronger protection, but may cause some sites or content to break.
- Custom**
Choose which trackers and scripts to block



Microsoft Edge:

1. Click on the three horizontal dots and select Settings.





2. Microsoft Edge expands its privacy settings into two tabs, “Privacy, search, and services” and “ Site permissions.”

Settings

Search settings

- Profiles
- Privacy, search, and services**
- Appearance
- On startup
- New tab page
- Site permissions
- Default browser
- Downloads
- Family safety
- Languages
- Printers
- System
- Reset settings
- Phone and other devices
- About Microsoft Edge

We value your privacy.
We will always protect and respect your privacy, while giving you the transparency and control you deserve. [Learn about our privacy efforts](#)

Tracking prevention ?

Websites use trackers to collect info about your browsing. Websites may use this info to improve sites and show you content like personalized ads. Some trackers collect and send your info to sites you haven't visited.

Tracking prevention

Basic	Balanced (Recommended)	Strict
<ul style="list-style-type: none">Allows most trackers across all sitesContent and ads will likely be personalizedSites will work as expectedBlocks known harmful trackers	<ul style="list-style-type: none">Blocks trackers from sites you haven't visitedContent and ads will likely be less personalizedSites will work as expectedBlocks known harmful trackers	<ul style="list-style-type: none">Blocks a majority of trackers from all sitesContent and ads will likely have minimal personalizationParts of sites might not workBlocks known harmful trackers

Blocked trackers
View the sites that we've blocked from tracking you

Exceptions
Allow all trackers on sites you choose

Always use "Strict" tracking prevention when browsing InPrivate

Settings

Search settings

- Profiles
- Privacy, search, and services
- Appearance
- On startup
- New tab page
- Site permissions**
- Default browser
- Downloads
- Family safety
- Languages
- Printers
- System
- Reset settings
- Phone and other devices
- About Microsoft Edge

Site permissions

- Cookies and site data** Allowed
- Location** Ask first
- Camera** Ask first
- Microphone** Ask first
- Motion or light sensors** Allow sites to use motion and light sensors
- Notifications** Ask first
- JavaScript** Allowed
- Adobe Flash** Always block Flash (recommended)
- Images** Show all
- Pop-ups and redirects** Blocked
- Ads** Blocked



Social Media

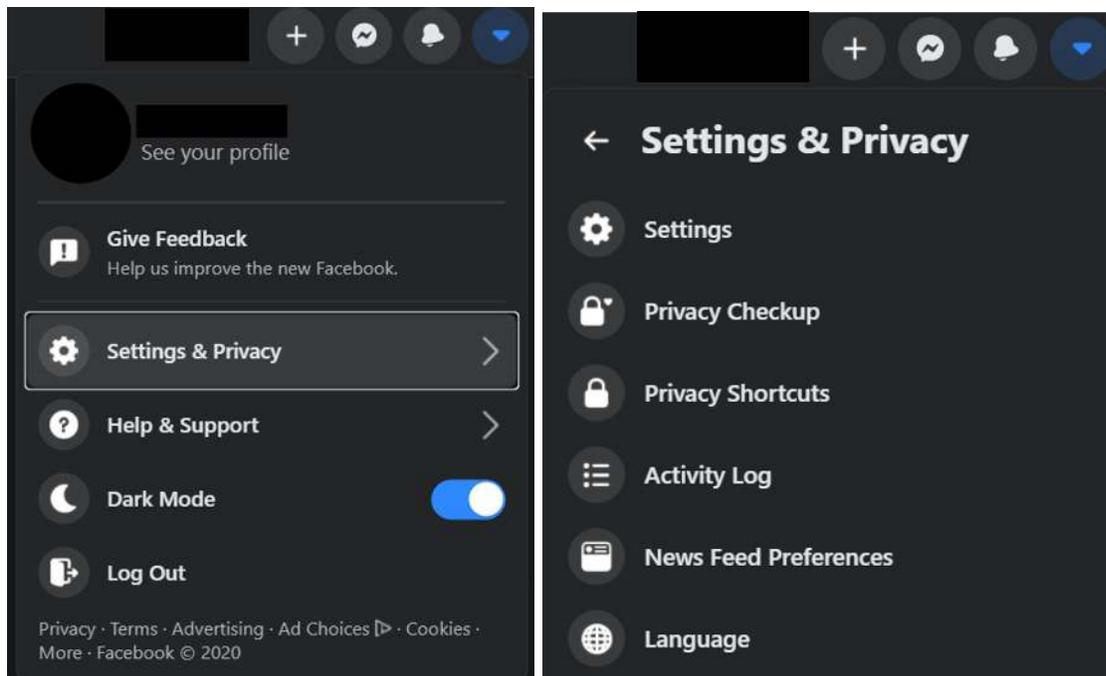
Social media can be a useful tool to help you with friends and family and share your life. However, you should know who is able to access this information and if they can be trusted.

It is a hassle but it's important to use different passwords with every account. In case one account is compromised, hackers can't access all your information if your passwords are different.

Some websites offer two-way authentication (2FA) where you have to verify your identity via phone call, text message, or email. Some sites also let you know when your account is logged in on a new device. If it's not a device you know of, you should change your password immediately to prevent information from leaking.

Facebook: (screenshots taken from a computer)

1. After you (or your family members) login, click on the upside-down triangle to open the Settings menu. Here, click on "Settings & Privacy" to explore the different settings you can tweak how people see your profile.



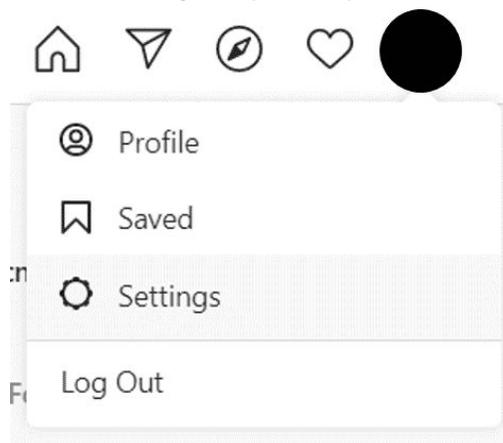
2. There are a lot of menus within Facebook to explore. The "Settings" option takes you to the "General Account Settings" page. It's a lot of information to take in but taking time to go through them will help you protect your privacy from people you don't know.



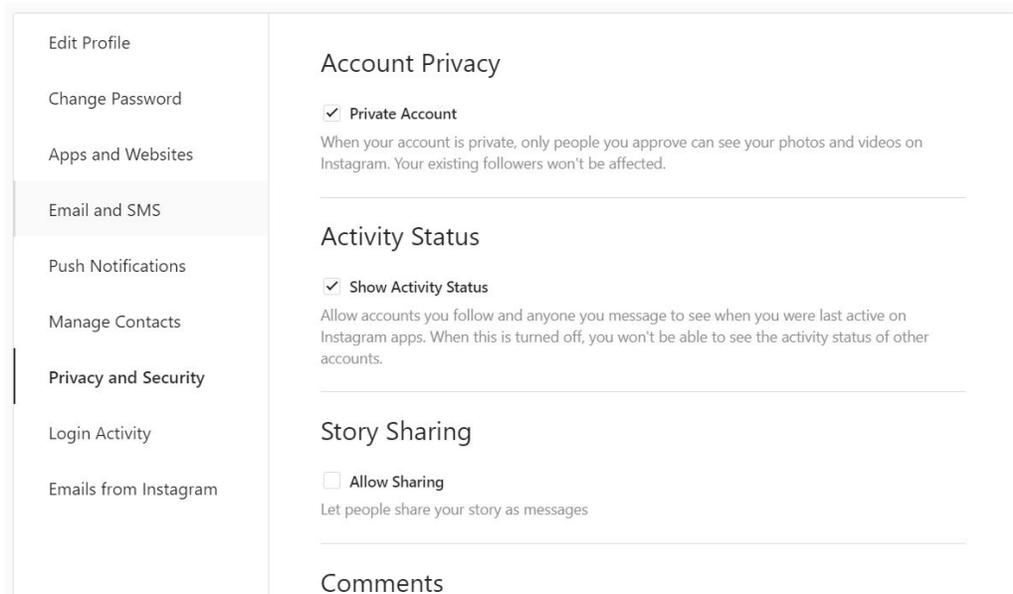
- a. Facebook lists who you choose to view information as:
 - i. Only Me - only you can view any information you put on your profile
 - ii. Friends - the people you choose to friend
 - iii. Public - anyone on or off Facebook (least secure)
 - iv. Custom - include and exclude friends and lists
3. Settings can be accessed from mobile devices as well under the same settings.

Instagram: (screenshots taken from a computer)

1. Click your profile picture and select “Settings.”



2. Click “Privacy and Security” to explore how people can view your profile.

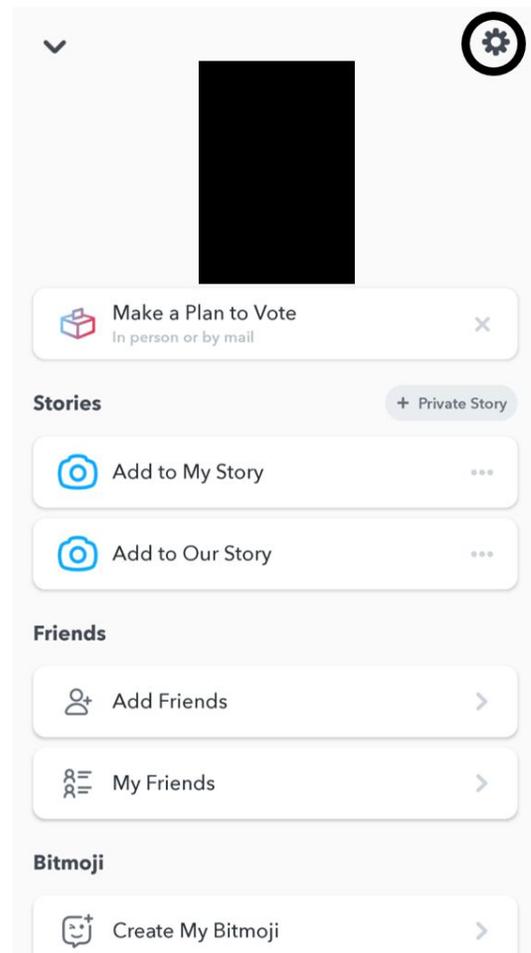


3. Settings can be accessed from mobile devices as well under the same settings.



Snapchat: (screenshots taken using an Android device)

1. Press on your profile picture and select the gear icon to enter the Settings.

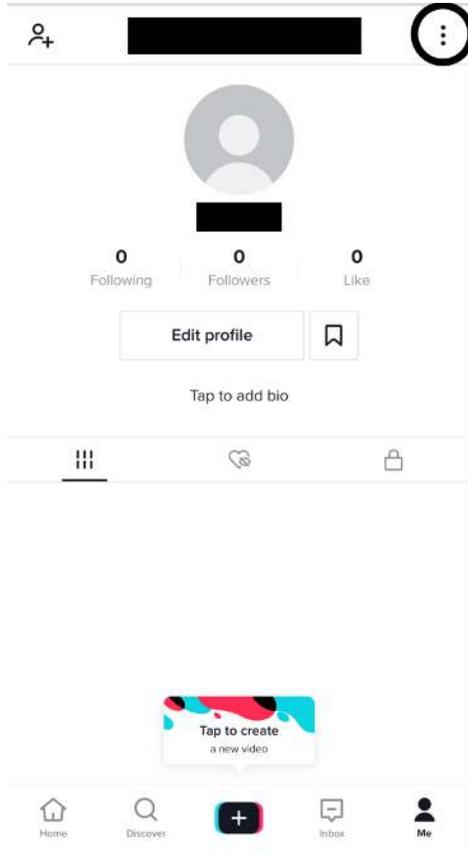


2. Go through each option to check that your Snaps are being viewed only by the people you want to see. Snapchat also allows you to set up Two-Way Authentication in case your account is compromised.

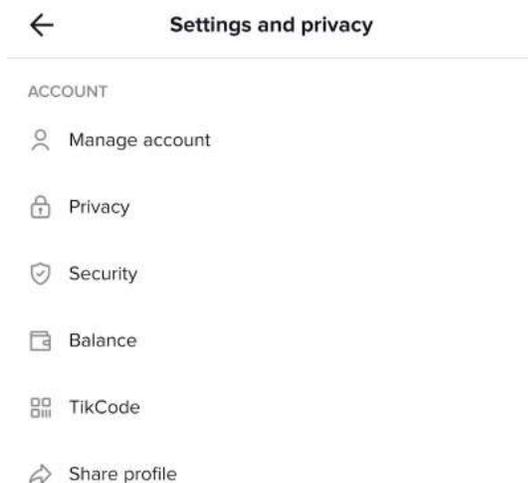


TikTok: (screenshots taken using an Android device)

1. Press on “Me” and the three vertical dots in the corner to go into the settings.



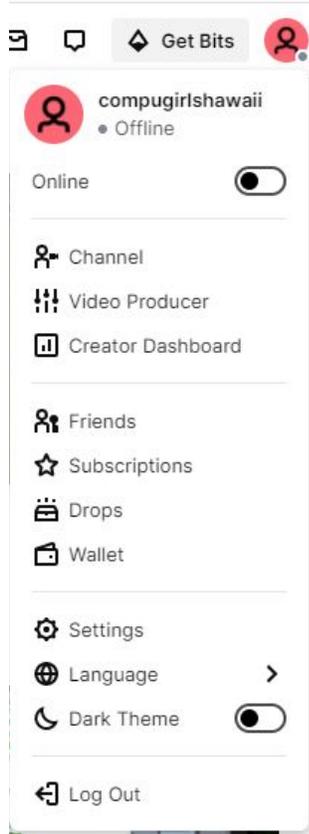
2. Look at the settings under Privacy and Security to make sure the settings are correct.



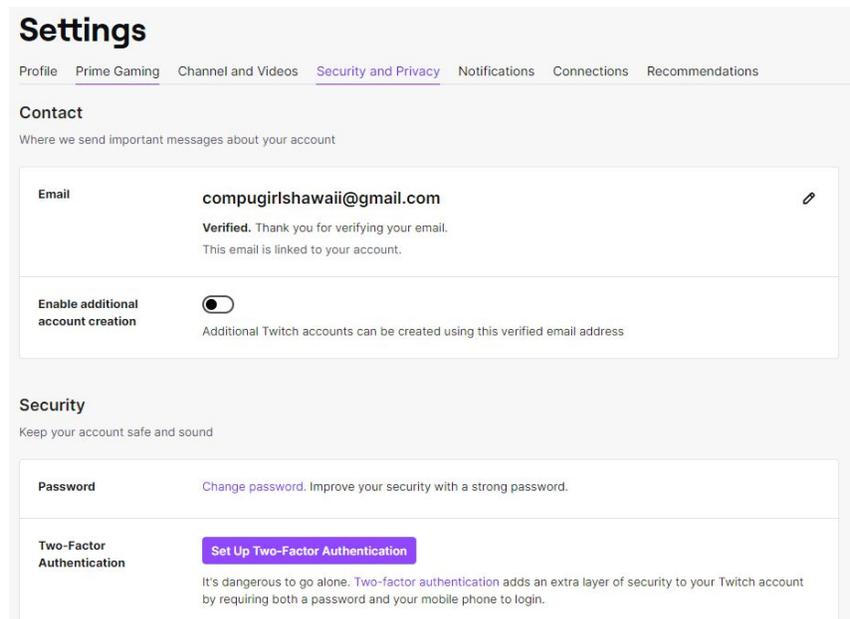


Twitch: (screenshots taken from a computer)

1. Click on your profile and click on settings.



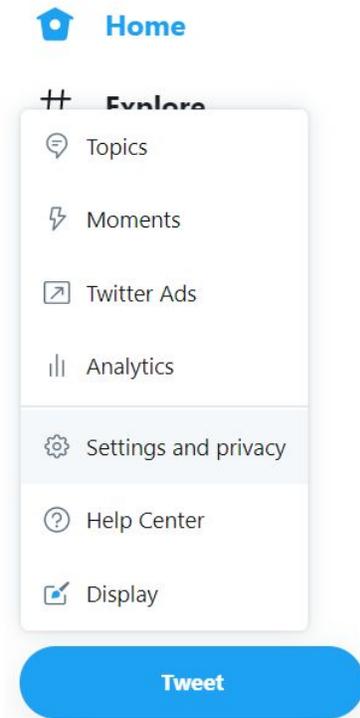
2. Click on "Security and Privacy" and explore the options.





Twitter: (screenshots taken from a computer)

1. Once you log in, click on “More” to be taken to the “Settings and Privacy” page.



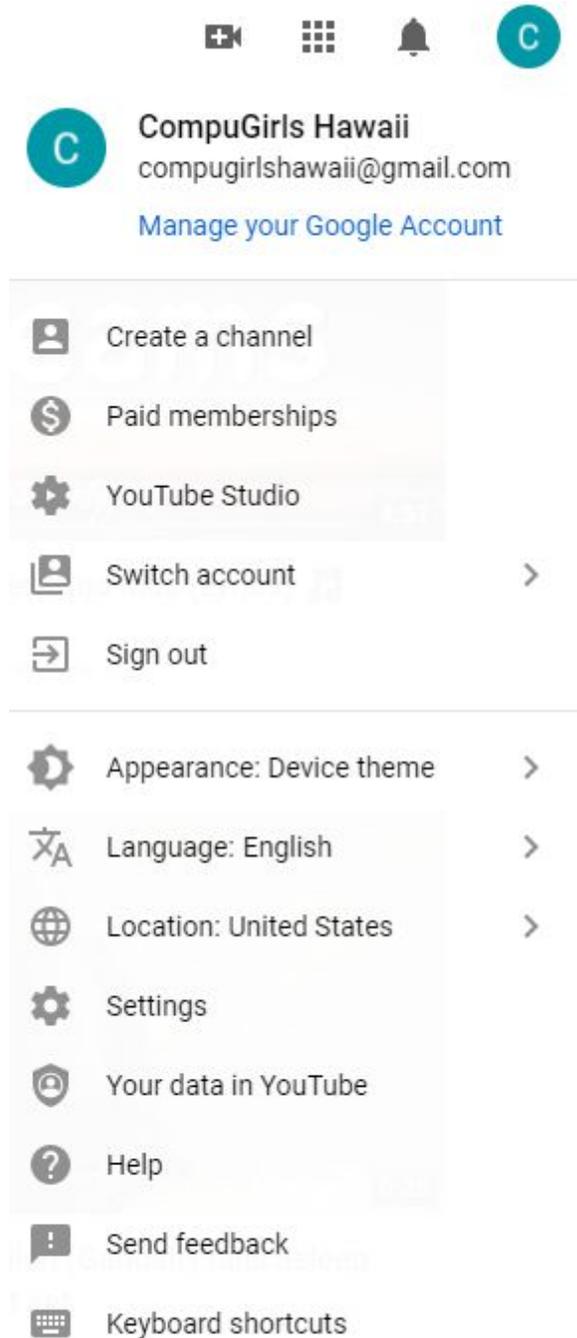
2. Select “Privacy and safety” and go through the different options to limit what information you share is available to the public.

Settings	Privacy and safety
Your account >	Manage what information you see and share on Twitter.
Security and account access >	Your Twitter activity
Privacy and safety >	<ul style="list-style-type: none"> Audience and tagging > Manage what information you allow other people on Twitter to see. Your Tweets > Manage the information associated with your Tweets. Content you see > Decide what you see on Twitter based on your preferences like Topics and interests Mute and block > Manage the accounts, words, and notifications that you've muted or blocked. Direct Messages > Manage who can message you directly. Discoverability and contacts > Control your discoverability settings and manage contacts you've imported.
Notifications >	
Accessibility, display, and languages >	
Additional resources >	
	Data sharing and off-Twitter activity



Youtube: (screenshots taken from a computer)

1. Click on your profile picture and select settings.





2. Select on “Privacy” to manage what you share on YouTube. Explore the different menu options to dive deeper into how Youtube works.

SETTINGS

- Account
- Notifications
- Playback and performance
- Privacy**
- Connected apps
- Watch on TV
- Billing and payments
- Advanced settings

Search

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**
Playlists created by others won't appear on your channel. Playlists created by you have separate, individual privacy settings. [Learn more](#)
- Keep all my subscriptions private**
Your subscriptions will not be visible to others. [Manage your subscriptions here.](#)

Ads on YouTube

You may see ads on YouTube based on general factors, like the topic of a video. The ads you see may also depend on your [Google Ads Settings](#). To learn more about how ads work for family accounts with kids, visit the [Google for Families Help Center](#).