

Internet Privacy

How to use websites and apps
safely and privately



What we'll cover

Some basics of online safety and privacy

Online Privacy

- Private browsing for
 - Safari (iPhone and Mac).
 - Google Chrome (iPhone and desktop)
- How to clear your Search History
 - Safari and Chrome, desktop and iPhone

App privacy

- Privacy run-downs for popular apps
- Which apps have Screenshot Alerts and record profile views

Online Surveillance

- How to check if somebody is accessing your emails (gmail and Outlook)
- How to turn off location sharing
 - via Share My Location and Find My iPhone
 - via Snapchat SnapMaps
 - How to respond to an AirTag notification





Private Browsing

What is it?

Private browsing is a feature on many web browsers that allows you to use the internet without saving the details of your searches; the websites you visit will not be recorded in your regular search history, and will not be shared with other devices.

That means when you go back to regular browsing, there will be no record of what you searched in your history.

Private browsing is a safe way to use the internet without leaving the same footprints as regular browsing. Most browsers (like Google Chrome or Safari) have this feature, and you can access it on your phone or computer.

You can sometimes even set your browser up to search privately every time. Learn about how to privately browse on desktop computers and phone apps in the following pages.






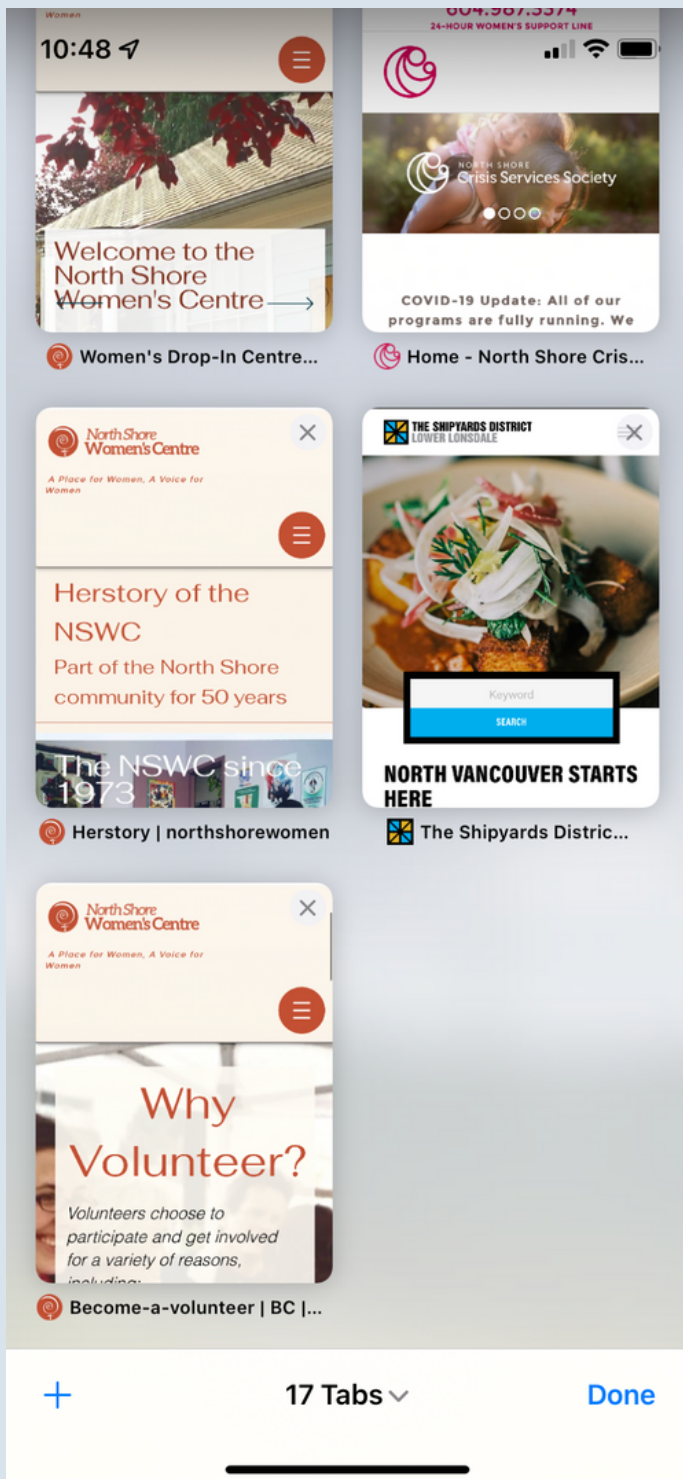
Private Browsing



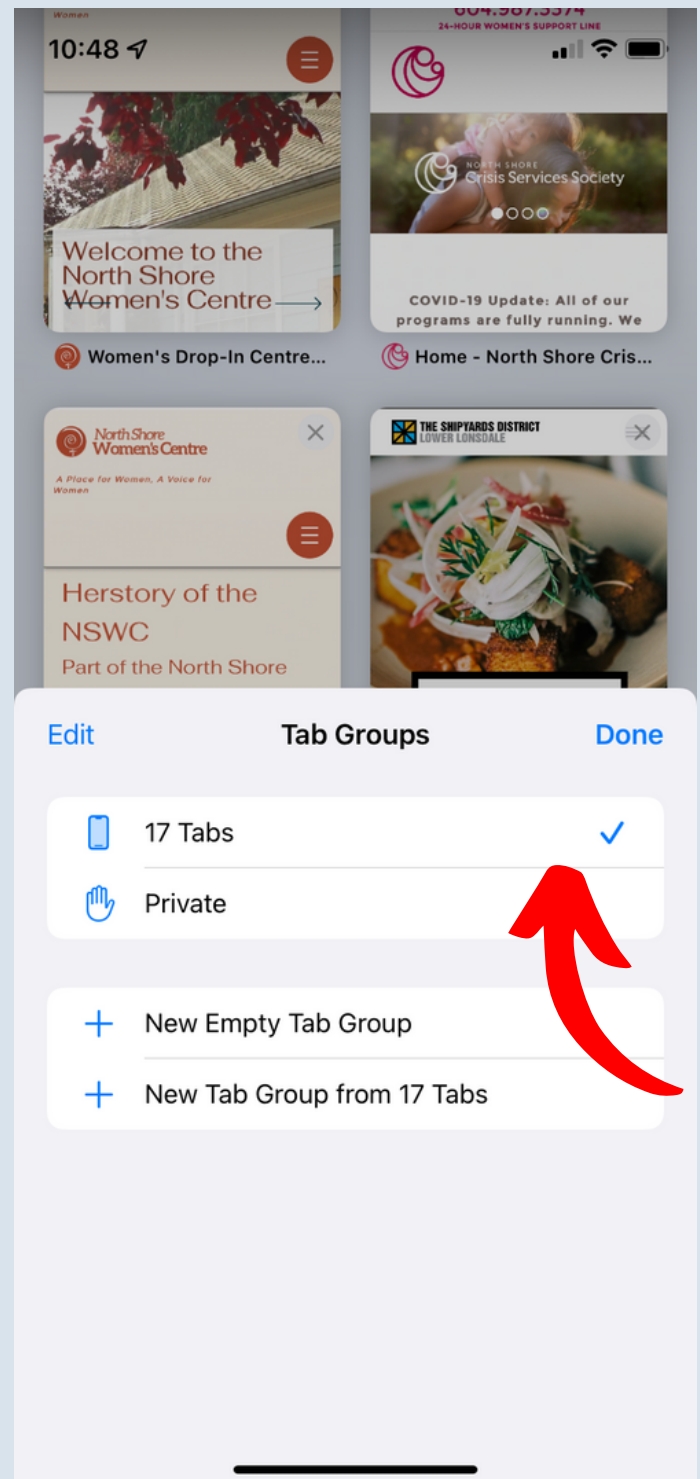
Safari for iPhone

Step 1: Open your Safari App and view your open tabs by clicking the button on the bottom right that looks like this: 

This is tab view.



Step 2: Click the middle text on the bottom that says "# Tabs" to see your tab options. In the example, it says "17 Tabs" but yours might have more or less. This is tab options.





Private Browsing

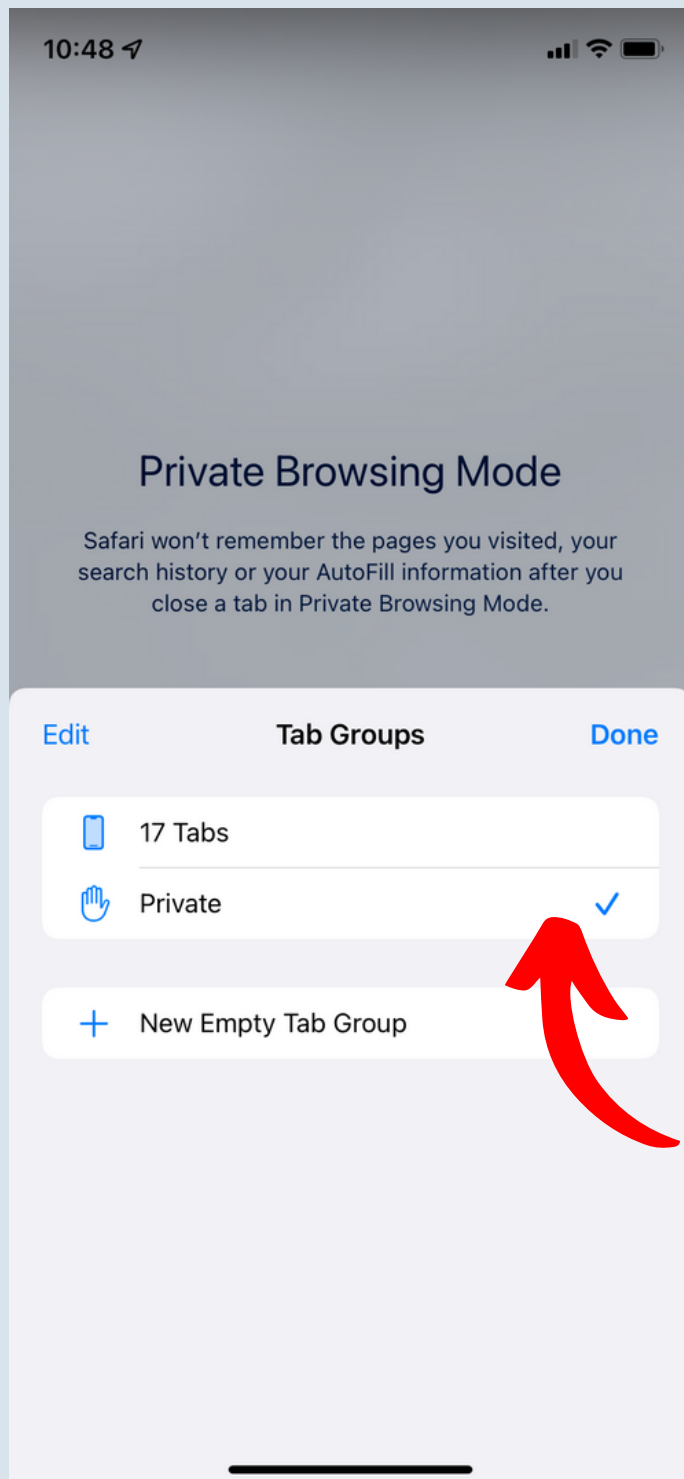


Safari for iPhone

Step 3: Click the button that says "Private" to open private browsing. The button looks like this:

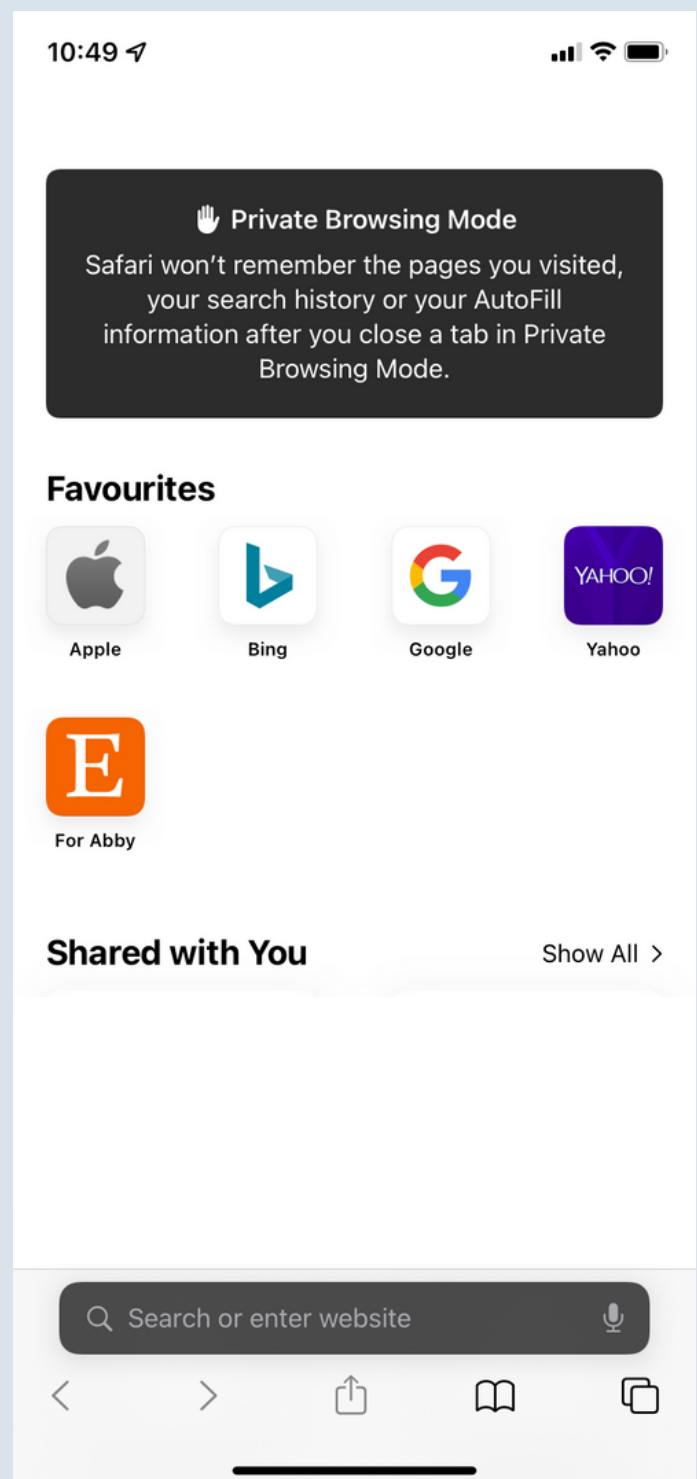


This is the private button.



Step 4: Make your searches! The regular features might change colour to black.

This is what it looks like!





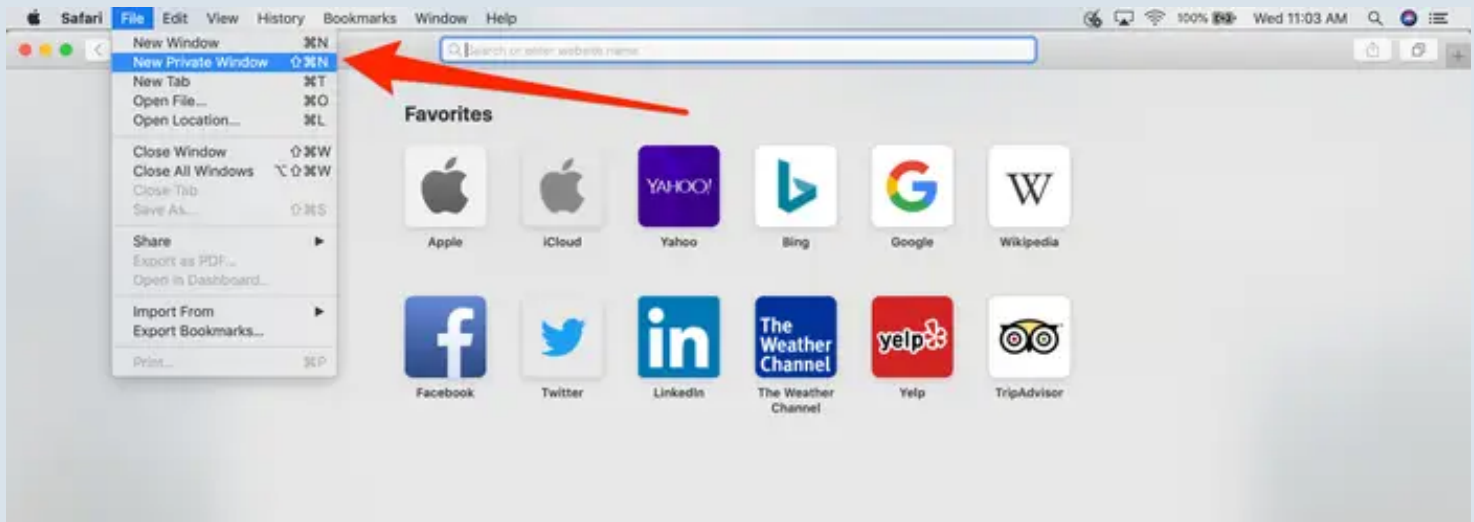
Private Browsing



Safari for Mac.

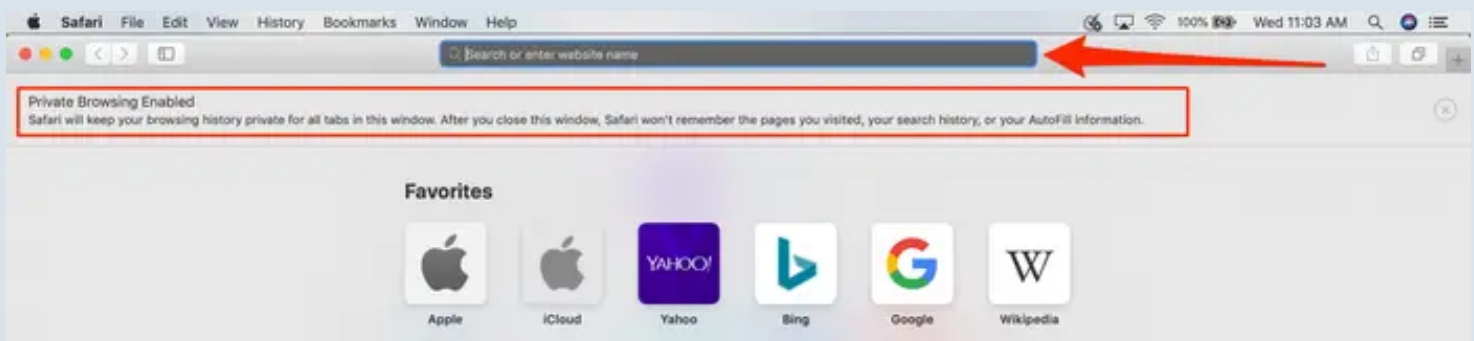
Step 1: Open your Safari App and click "File" in the top toolbar. Then, select "New Private Window"

This is New Private Window in File.

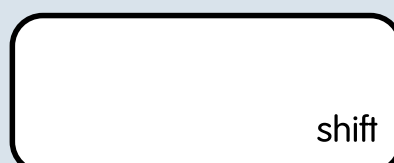


Step 2: Make sure the search bar changes colour from light to dark, and you see the banner that says "Private Browsing Enabled"

This is Private Browsing Enabled.



Tip: You can use the keyboard shortcut Command + Shift + N (Mac) to open a new private window.





Private Browsing

Clearing your history on Safari



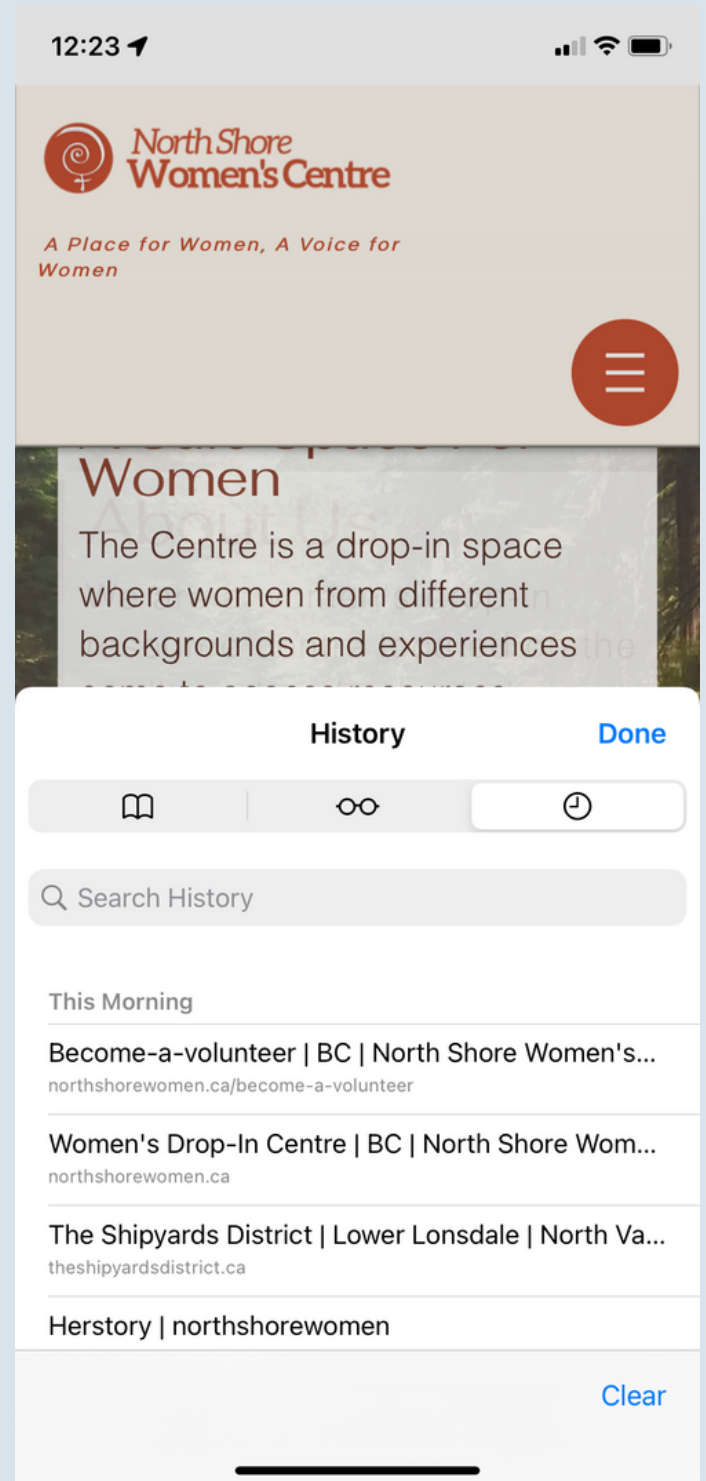
Step 1: Open your Safari App and click the History button on the bottom bar, which looks like this:

This is the History button.



Step 2: View your history to see what sites your browser recorded, and click "Clear" on the bottom left.

This is your History page.





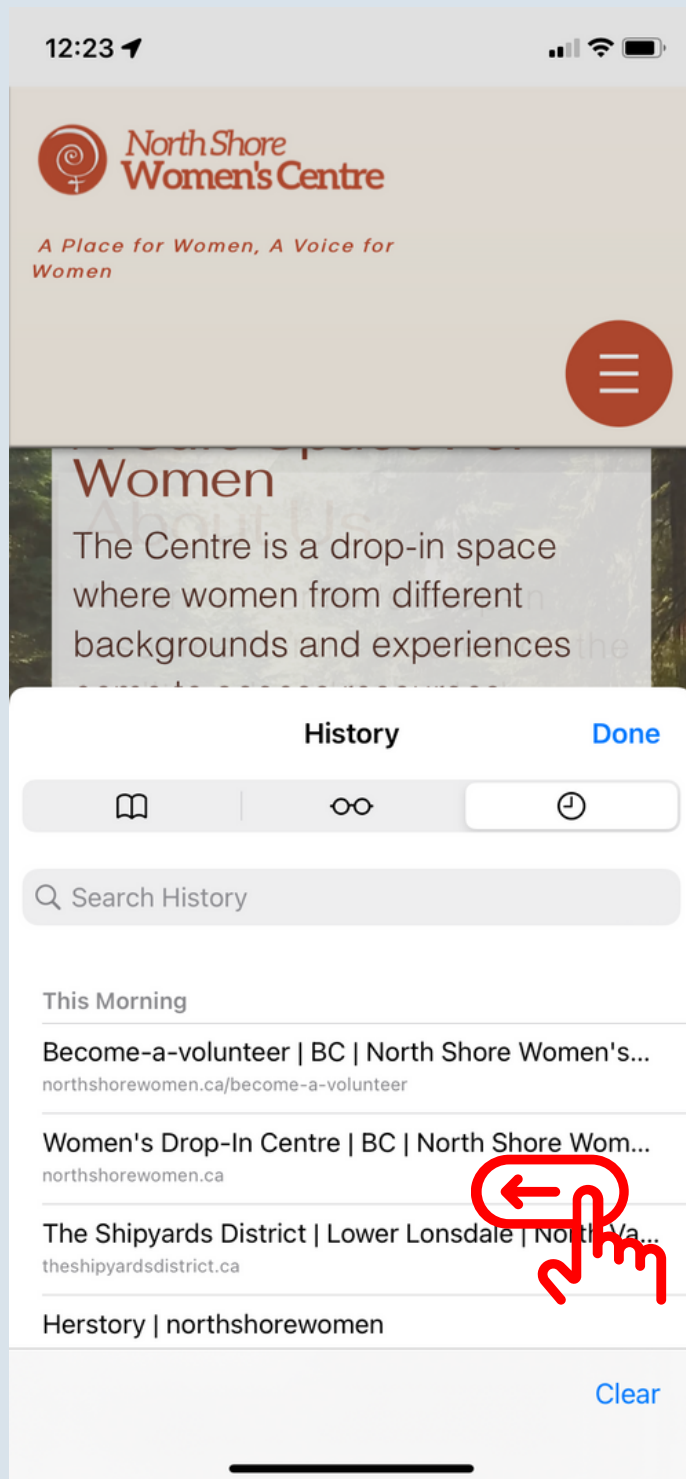
Private Browsing

Clearing your history on Safari



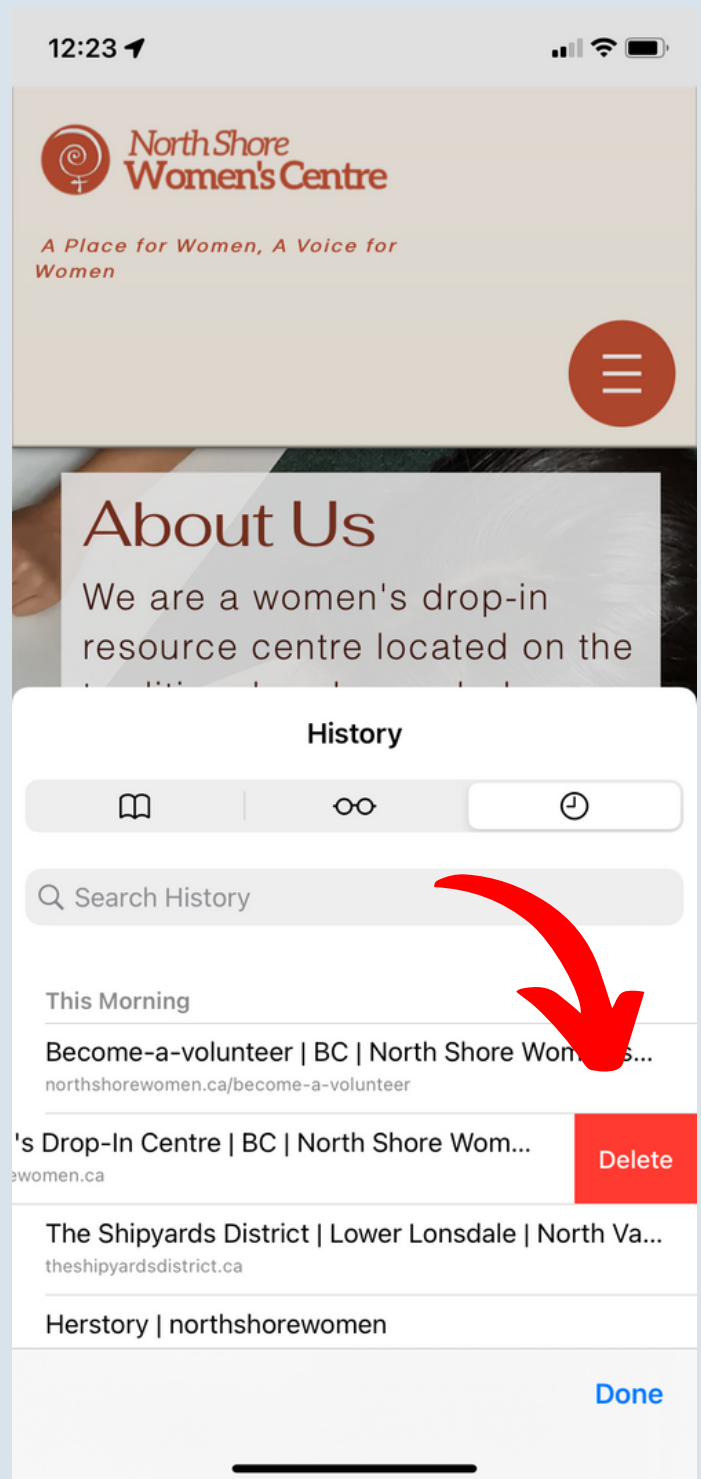
Step 3: If you want to delete just one search, tap and slide that search to the left.

This is the process.



Step 4: When you see a red button that says "Delete," click that to delete an individual search.

This is the Delete button.





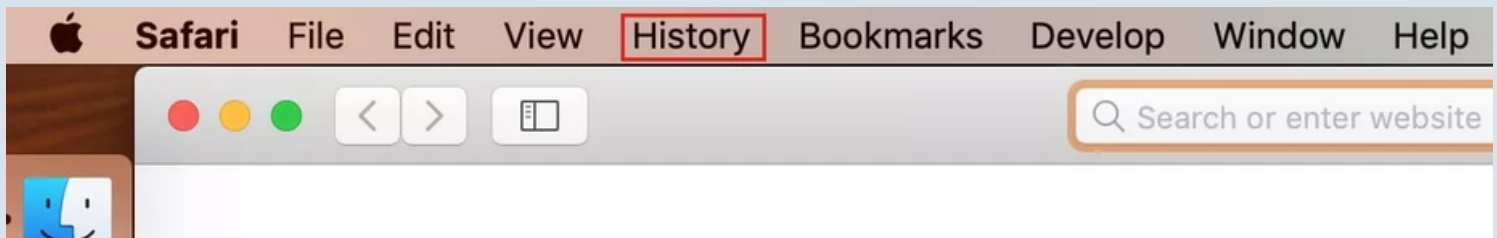
Private Browsing



Clearing your history on Safari

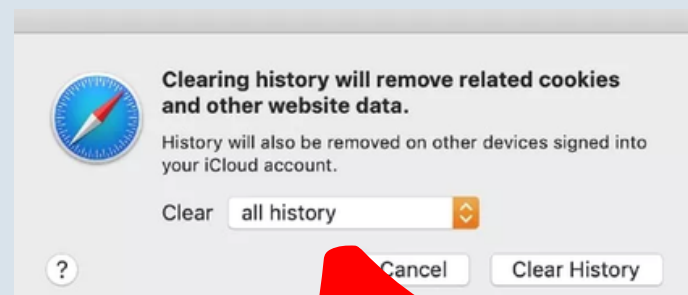
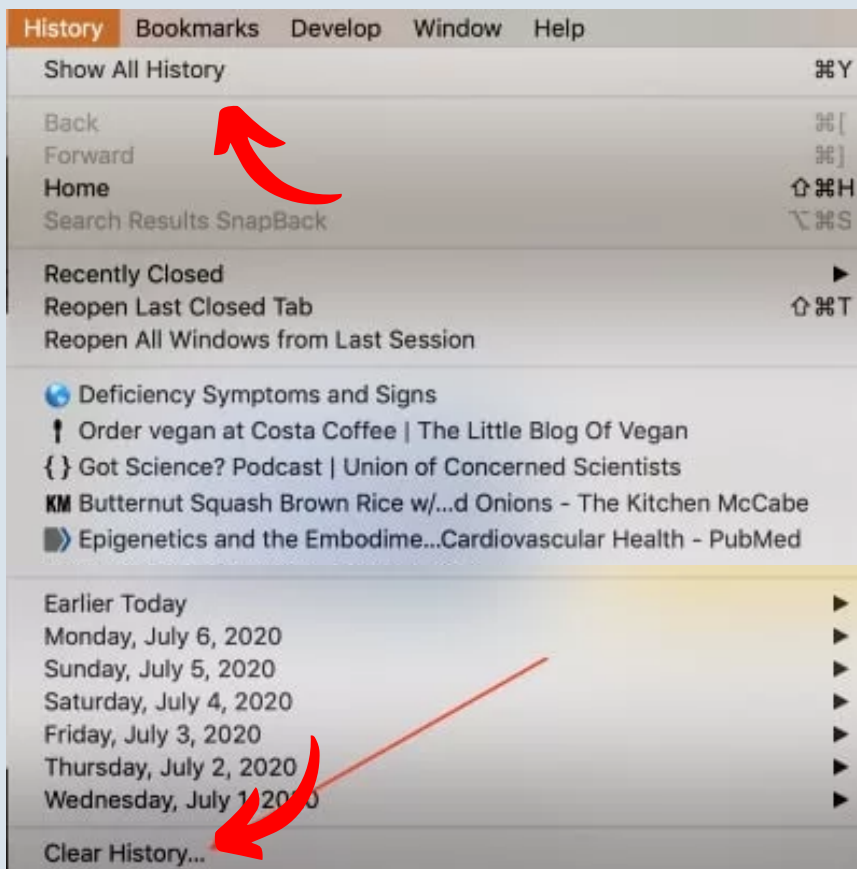
Step 1: Open your Safari App and click "History" in the top toolbar. It is between "View" and "Bookmarks"

This is History in your toolbar.



Step 2: A menu will drop down when you click History. To delete all searches, click "Clear History" at the bottom, and then "all history" from the pop-up.

To delete one search, click "Show All History" at the top, and right click the website you want to delete. Then, click delete from the drop-down menu.



Tip: You can clear your search history on a Mac with the keyboard shortcut command + shift + delete







Private Browsing

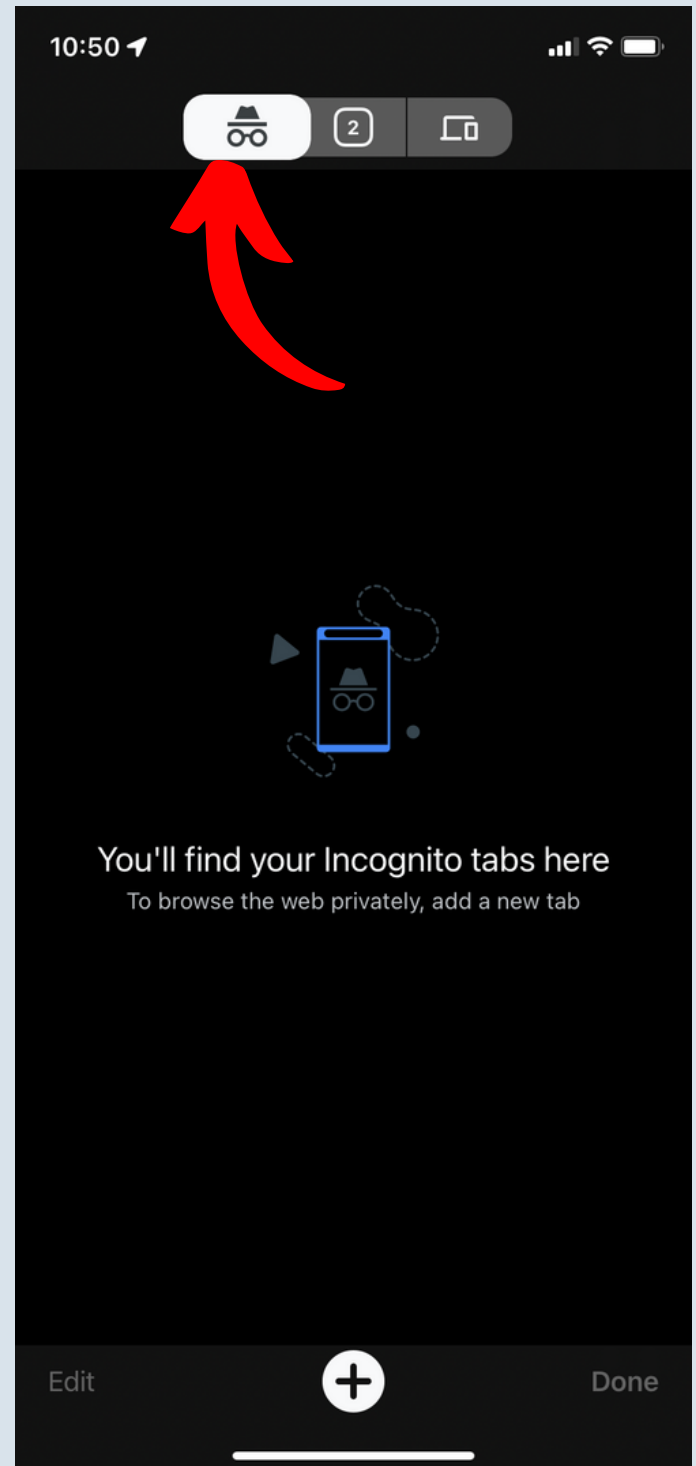
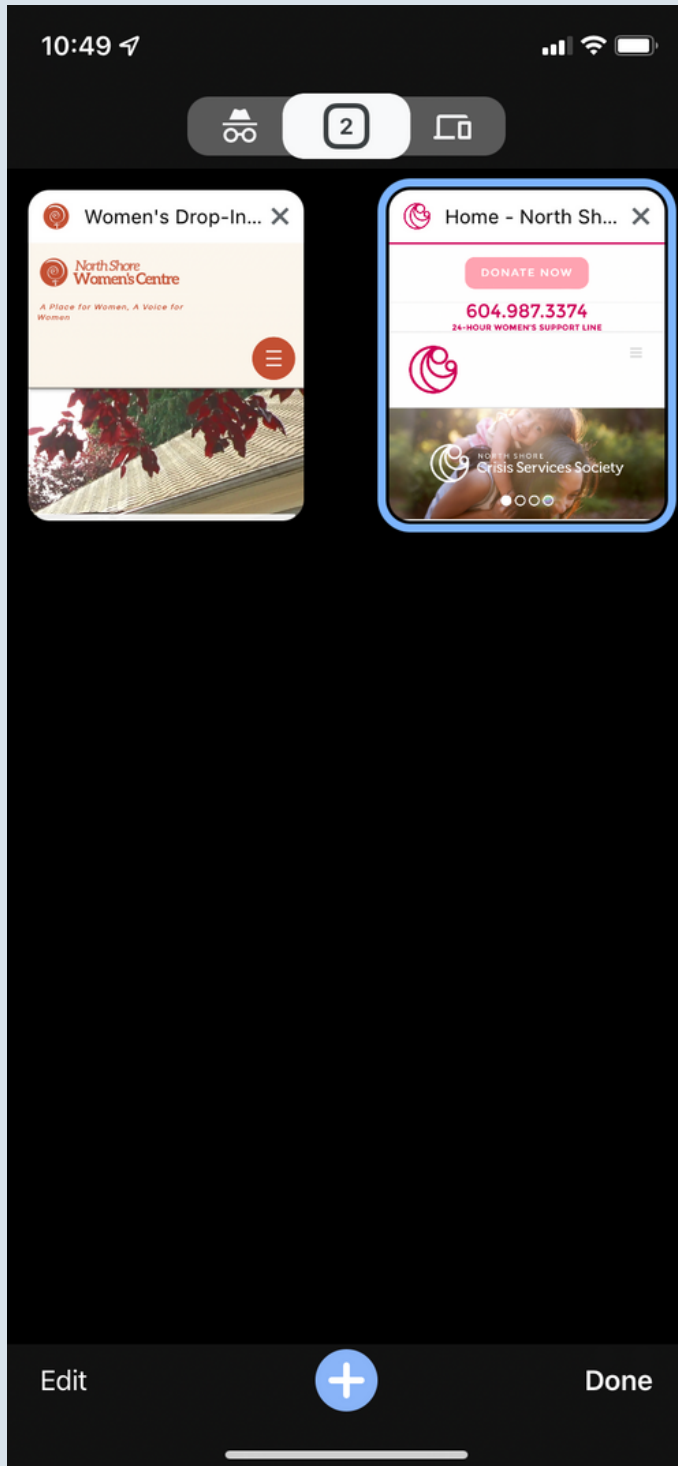


Google Chrome for iPhone

Step 1: Open your Chrome App and view your open tabs by clicking the top button that looks like this. We have a 2 inside the box, but you might have more or less:  This is tab view.

Step 2: Click the left top tab to open a private browsing tab, which Google calls "Incognito." It looks like this: 

This is the incognito tab.





Private Browsing



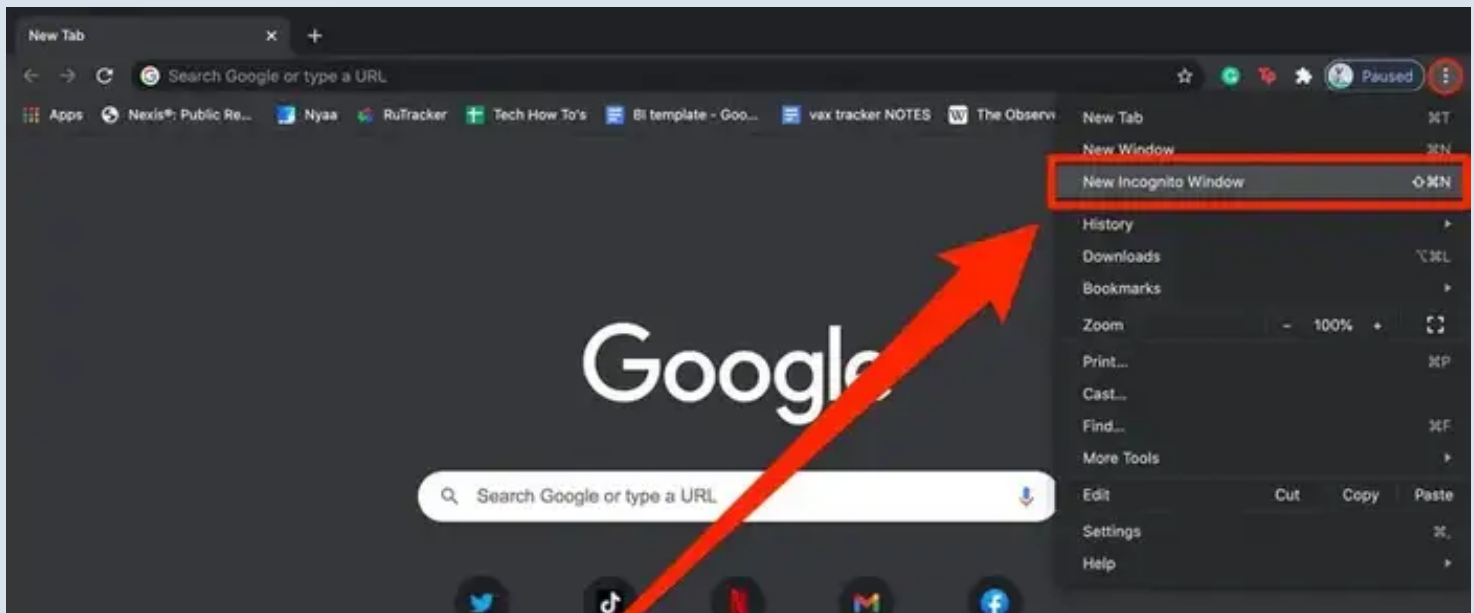
Google Chrome for Desktop

Step 1: Open your Chrome App and click the three dots on the top left of your toolbar. The button looks like this:

Then, select "New Incognito Window"



This is New Incognito Window in Menu.



Tip: You can use the keyboard shortcut Ctrl + Shift + N (PC) or Command + Shift + N (Mac) to open a new incognito window.

Ctrl

⇧ Shift

N





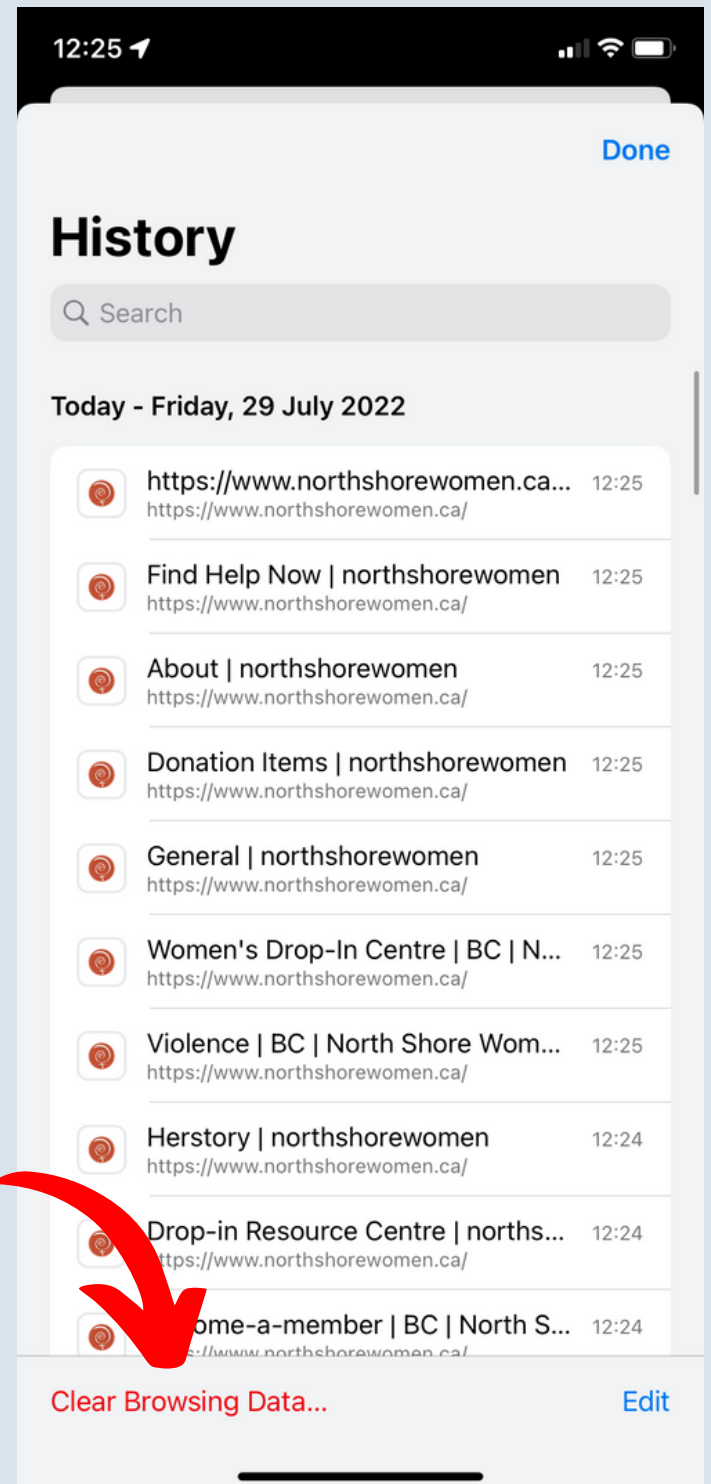
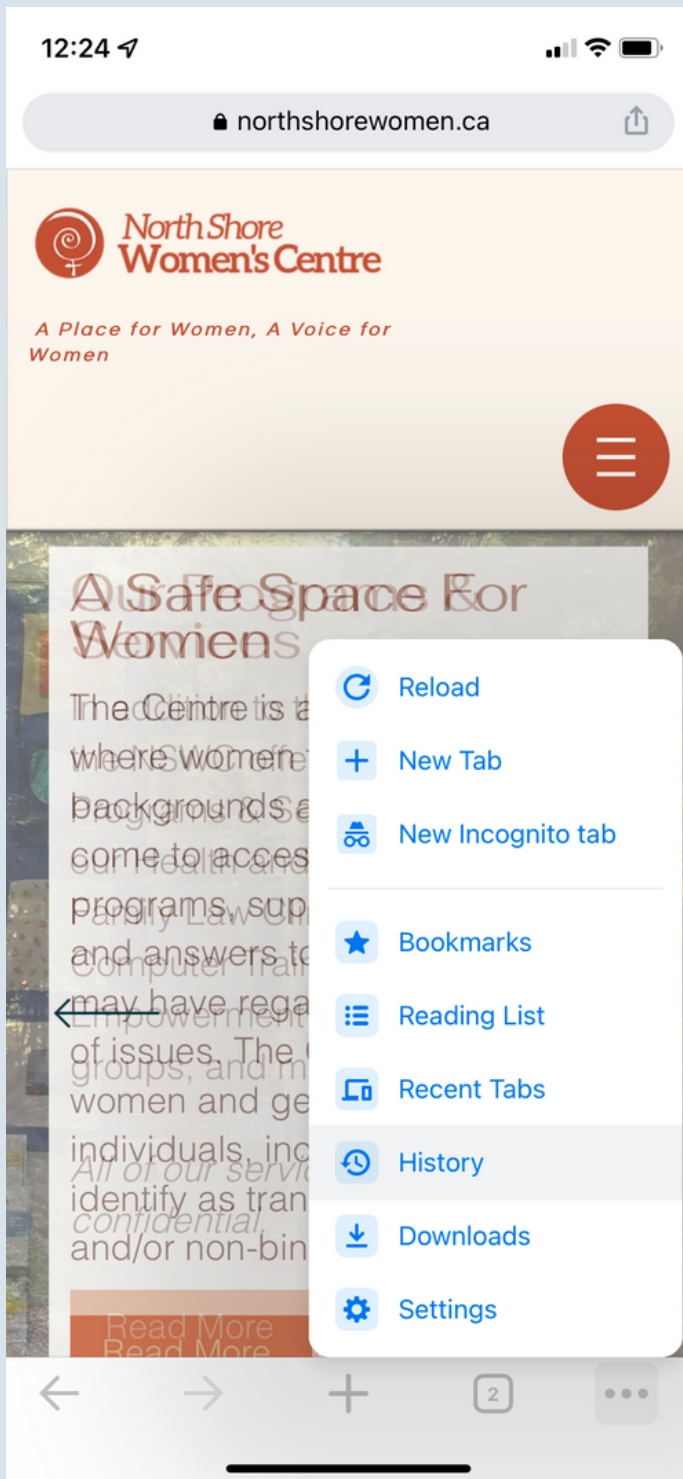
Private Browsing



Clearing your history on Chrome

Step 1: Open Chrome and click the three dots on the bottom left to reveal the menu. The button looks like this: ● ● ●
Then, click "History"

Step 2: View your history to see what sites your browser recorded, and click "Clear Browsing Data" on the bottom right.
This is your History page.





Private Browsing

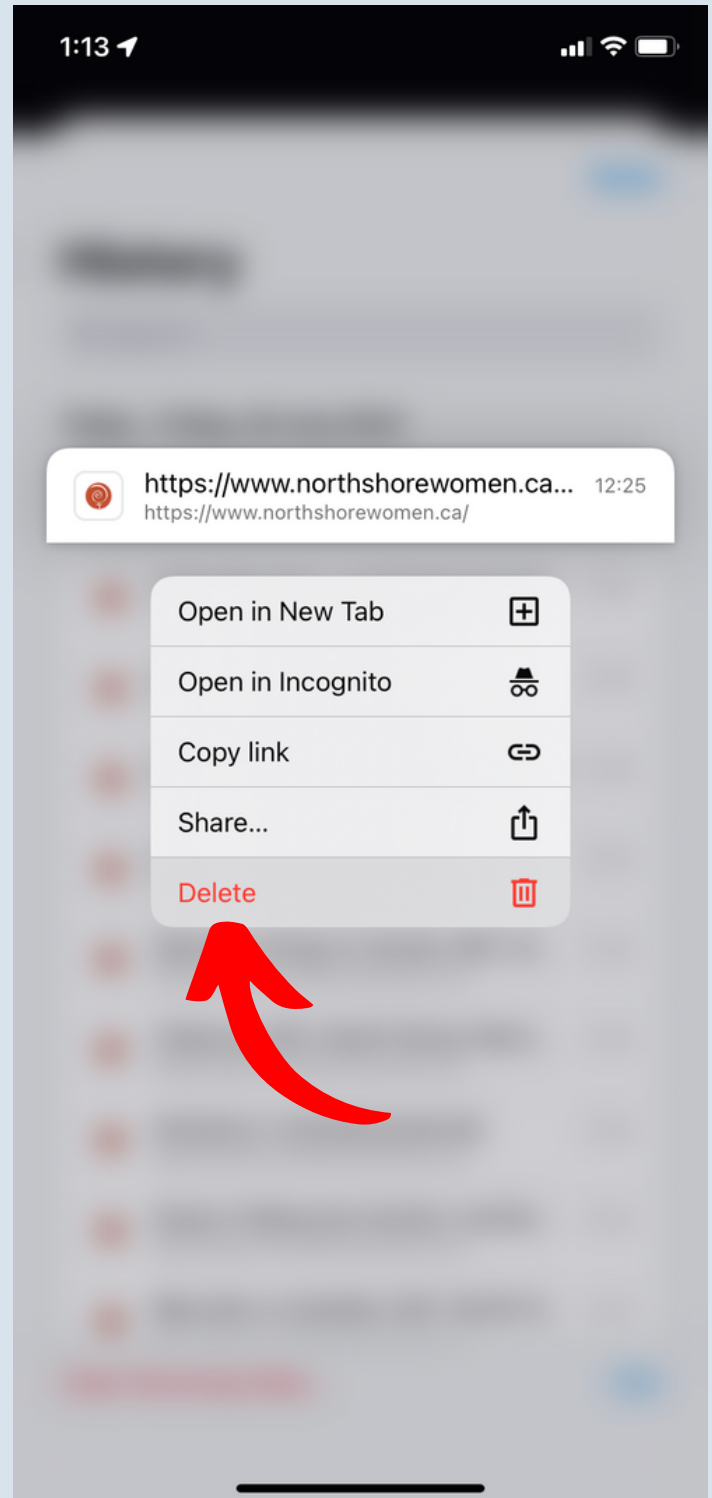
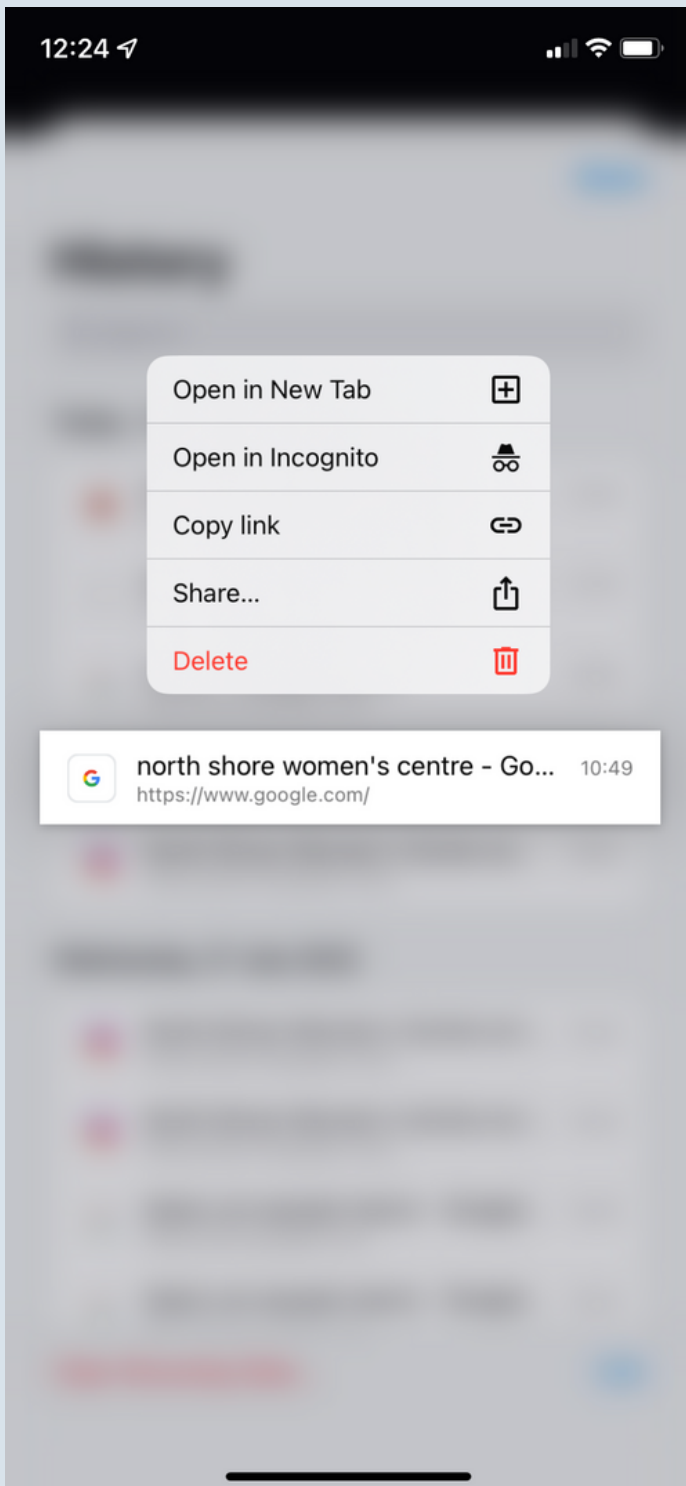


Clearing your history on Chrome

Step 3: If you want to delete just one search, hold down on the one you want to delete until the menu pops up.

Step 4: Click the "Delete" Button to remove the search from your history.

This is the Delete button.



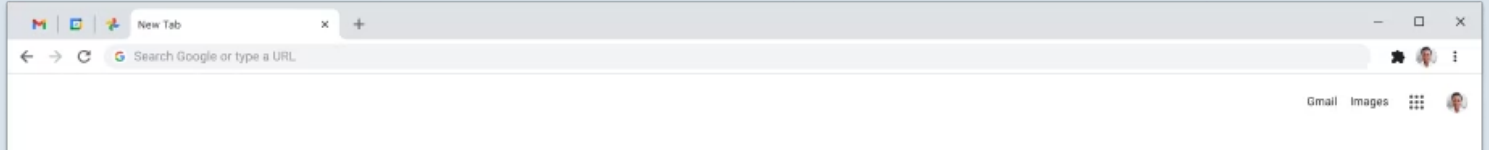


Private Browsing

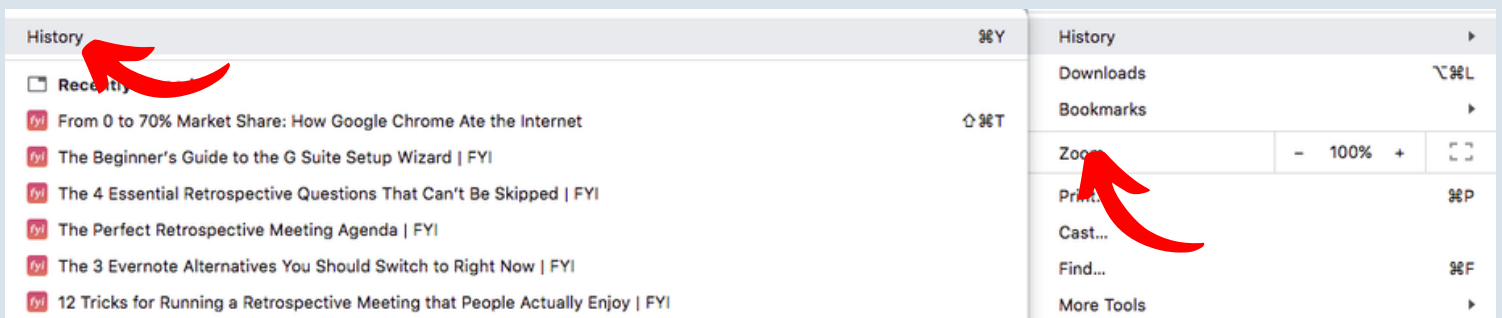


Clearing your history on Chrome

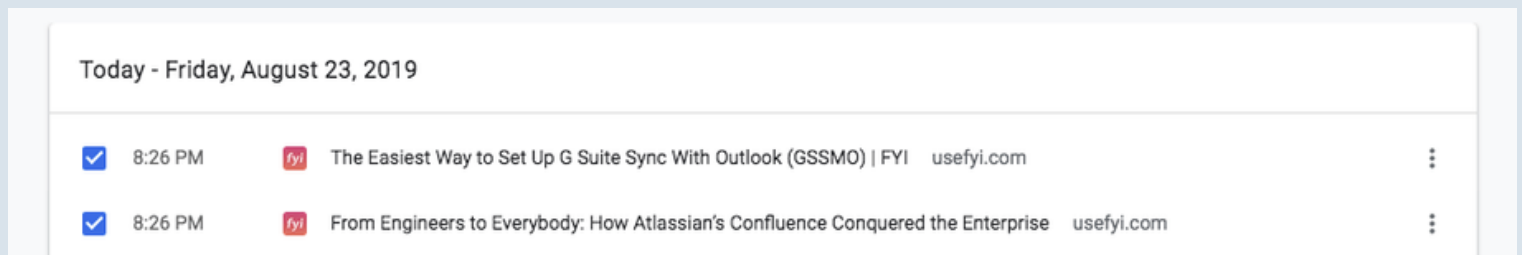
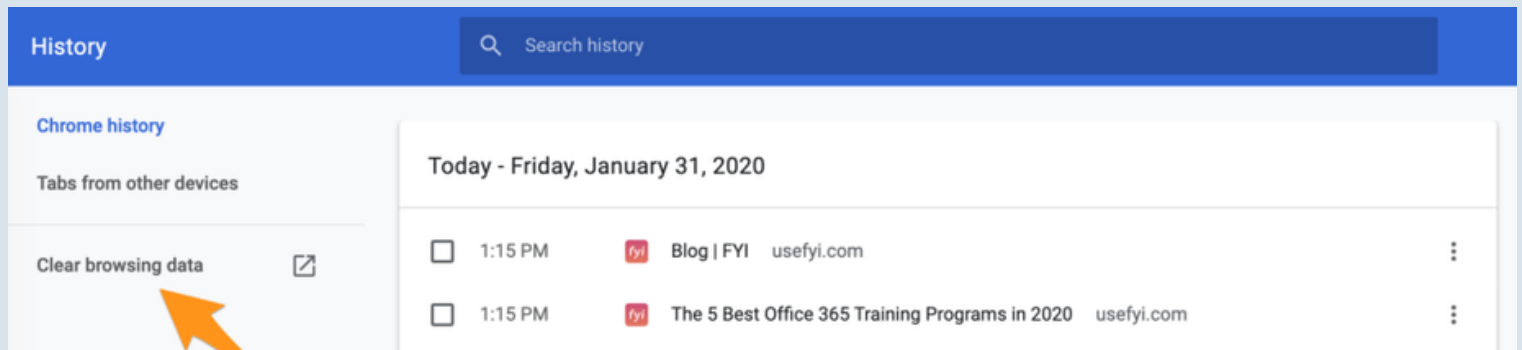
Step 1: Open your Chrome App and click the three dots on the top right to view your menu.



Step 2: Click "History" on the drop-down menu, and then click History again on the next pop-up.

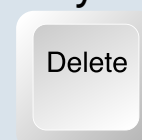
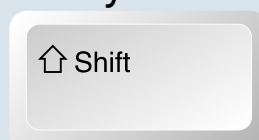
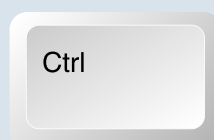


Step 3: Click "Clear browsing data" on the right side menu to delete "all time" history, or click the check-box next to the search you want to erase.



NOTE: you must separately delete your Google Account search history.

Tip: you can erase your search history with the keyboard shortcut
Ctrl+shift+del





App Privacy

What is it?

When you agree to the terms and conditions while signing up for a service or into an app, do you read the whole document? Many people do not, and the terms and conditions can contain valuable information about the safety and privacy of the app and your data.

Sometimes we also want to use apps in a way that make us wonder about how private they are for *other* people. For instance, can someone see if someone views their profile? Can they see if someone searches them? Will they be notified of *who* did the viewing/searching?

Read on to learn about how different apps handle your privacy.





App Privacy

App rundown

Key terms

End-to-end encryption:
data can't be secretly
read or modified



WhatsApp: 7/10

Key benefits: End-to-end encryption, company doesn't store delivered messages, third parties can't read your messages

Key concerns: You have to be careful about connecting this app to your contacts, as it will automatically add you to their contact list if you do.



Telegram: 9/10

Key benefits: Very strong end-to-end encryption through "secret messages", Secret chat messages cannot be forwarded, self-destruct messages, screenshot alerts, not a very well-known app, so can be easier to go unnoticed by others.

Key concerns: Non-secret-chat messages are not encrypted



Facebook/Meta messenger: 4/10

Key benefits: End-to-end encryption in secret messages, clearable search history, remove a message you've sent.

Key concerns: Very recognizable, Meta privacy concerns (third party access)



App Privacy

App rundown



Snapchat: 2/10

Key benefits: Screenshot alerts, basic idea of messages/photos disappearing forever

Key concerns: NOT encrypted, photos and messages do NOT really "disappear" but are held on a server, even "my eyes only" can be accessed by third parties via servers, people can find workarounds to screenshot without alerting, location tracking



Twitter: 6/10

Key benefits: You can make a private account that can't be followed without you approving a request, blocking hides you from the person you block, private accounts can't be found via internet search.

Key concerns: Twitter can store information you've sent through DMs with third parties, followers can still screenshot private accounts and share them without an alert, your likes are always visible to followers.



Instagram: 4/10

Key benefits: Private mode for messaging, can create a private account, your likes can't be scrolled through, blocking hides you from the person you block

Key concerns: Not very secure, easily hacked, screenshots of DMs can be taken without alert, collects lots of personal data



App Privacy

What can others see?

Can a user see if I save/take a screenshot of our messages or their posts/page?

Can I see if they take one from my messages or page?

Yes



No



Sometimes



Can a user see if someone views their profile/page?

Can I see if they view mine?

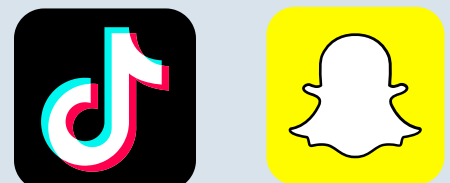
Yes



No



Sometimes





Online Surveillance

Is someone seeing my activity?

On some websites and applications, you can enable another person to see your activity, like your location, your banking notifications when you make a purchase, or your emails.

While this is meant to increase productivity and safety, it can be dangerous if someone else activates that feature without your knowledge and/or consent.

Scroll on to see how to tell if someone is forwarding your email inbox, tracking your location via your phone or a tracker, or following your purchases. And, what you can do to increase your security.




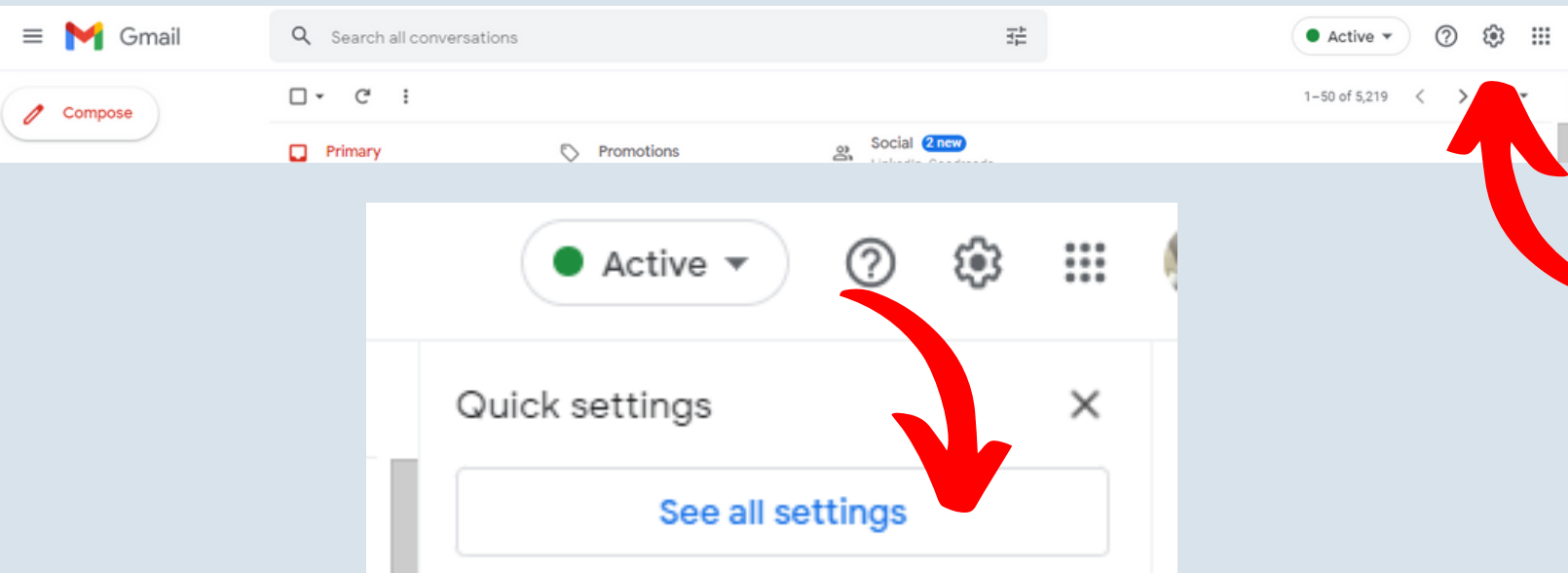


Online Surveillance

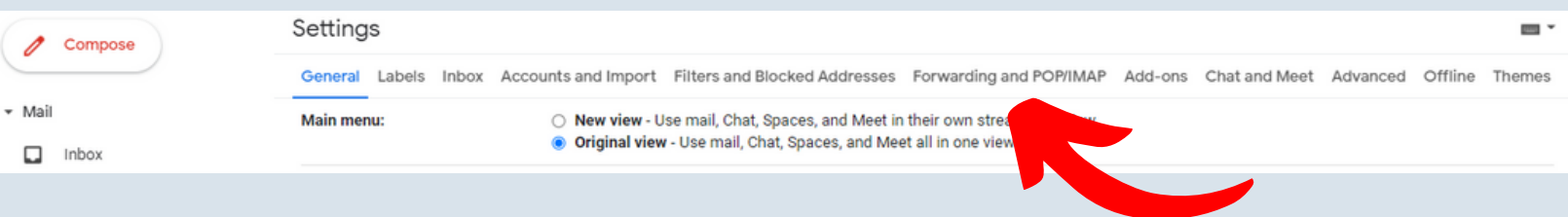


Is someone seeing my Gmail inbox?

Step 1: Open Gmail and click "Settings" which looks like this: 
Then, click "see all settings"



Step 2: Click the tab in the toolbar that says "Forwarding and POP/IMAP"



Step 3: View the top category, "Forwarding," and see if there is an email address in that section. If there is, then some or all of your emails might be forwarded to that address. If it says "add a forwarding address," then there is no mail being forwarded.

NOTE: this does not necessarily mean nobody is reading your emails-- they can be read and marked "mark as unread" by anybody who has access to your computer or phone where your email is logged in. Be vigilant about where you leave logged-in accounts, and keep varied and complex passwords between accounts.

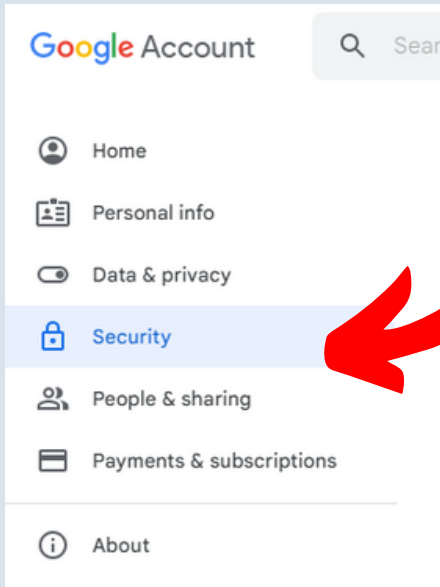


Online Surveillance

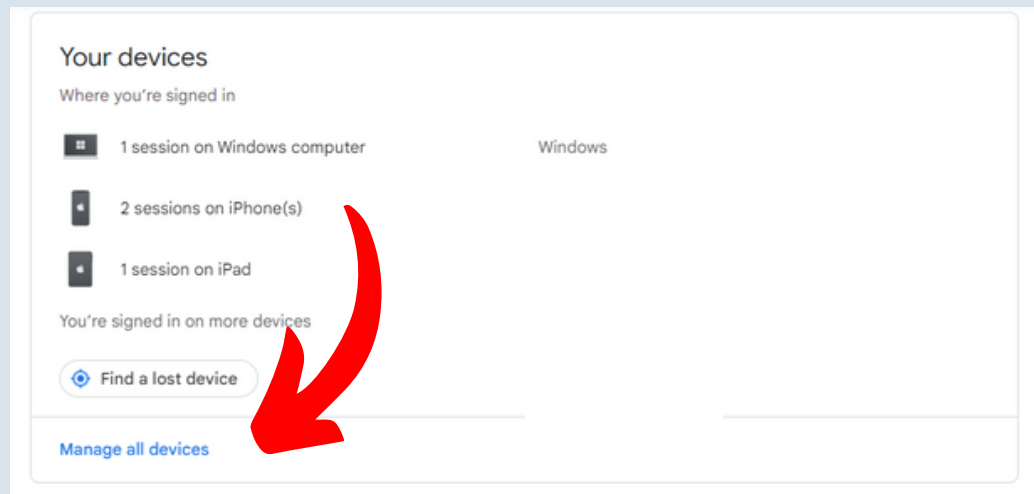


Is someone logged into my Google Account?

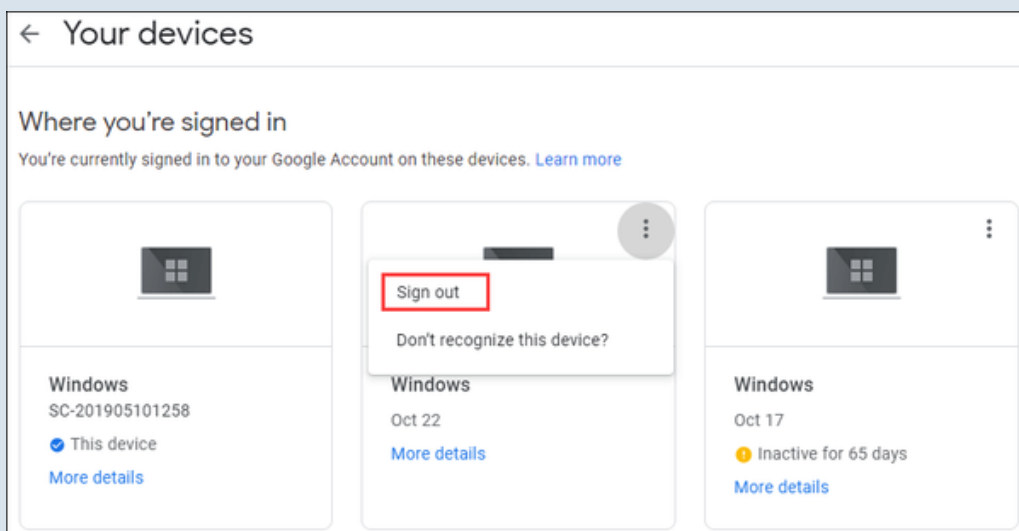
Step 1: Open your Google account/user profile, and click "Security" on the right side toolbar, which looks like this:



Step 2: Scroll down until you see "Your Devices: Where you're signed in" and click "Manage All Devices"



Step 3: Manage your devices by clicking the three stacked dots on the corner of each session profile and signing out individually, or saying "Don't recognize this device?" if the session does not belong to you.



NOTE: It is important to change your password if someone has been accessing your account without your knowledge or consent so that they cannot access it again after you log them out.



Online Surveillance



Is someone seeing my Outlook inbox?

Step 1: Open Outlook and select "Settings" which looks like this: Then, click "View All Outlook Settings"



Step 2: Click "Mail" and then "Forwarding."

Step 3: See if there is an email address listed. To turn off forwarding, clear "Enabled forwarding" and then save the settings.

NOTE: this does not necessarily mean nobody is reading your emails-- they can be read and marked "mark as unread" by anybody who has access to your computer or phone where your email is logged in. Be vigilant about where you leave logged-in accounts, and keep varied and complex passwords between accounts.

The screenshot shows the Outlook Settings interface. On the left, the 'Settings' sidebar has 'Mail' selected. The main area shows 'Forwarding' settings. A red box highlights the 'Enable forwarding' checkbox (which is checked), the 'Forward my email to:' text, the email address input field (containing 'Enter an email address'), and the 'Keep a copy of forwarded messages' checkbox (which is unchecked).

Settings	Forwarding
<input type="text" value="Search settings"/>	You can forward your email to another account.
<input checked="" type="checkbox"/> Enable forwarding	<input checked="" type="checkbox"/> Enable forwarding
Forward my email to:	Forward my email to:
<input type="text" value="Enter an email address"/>	<input type="text" value="Enter an email address"/>
<input type="checkbox"/> Keep a copy of forwarded messages	<input type="checkbox"/> Keep a copy of forwarded messages



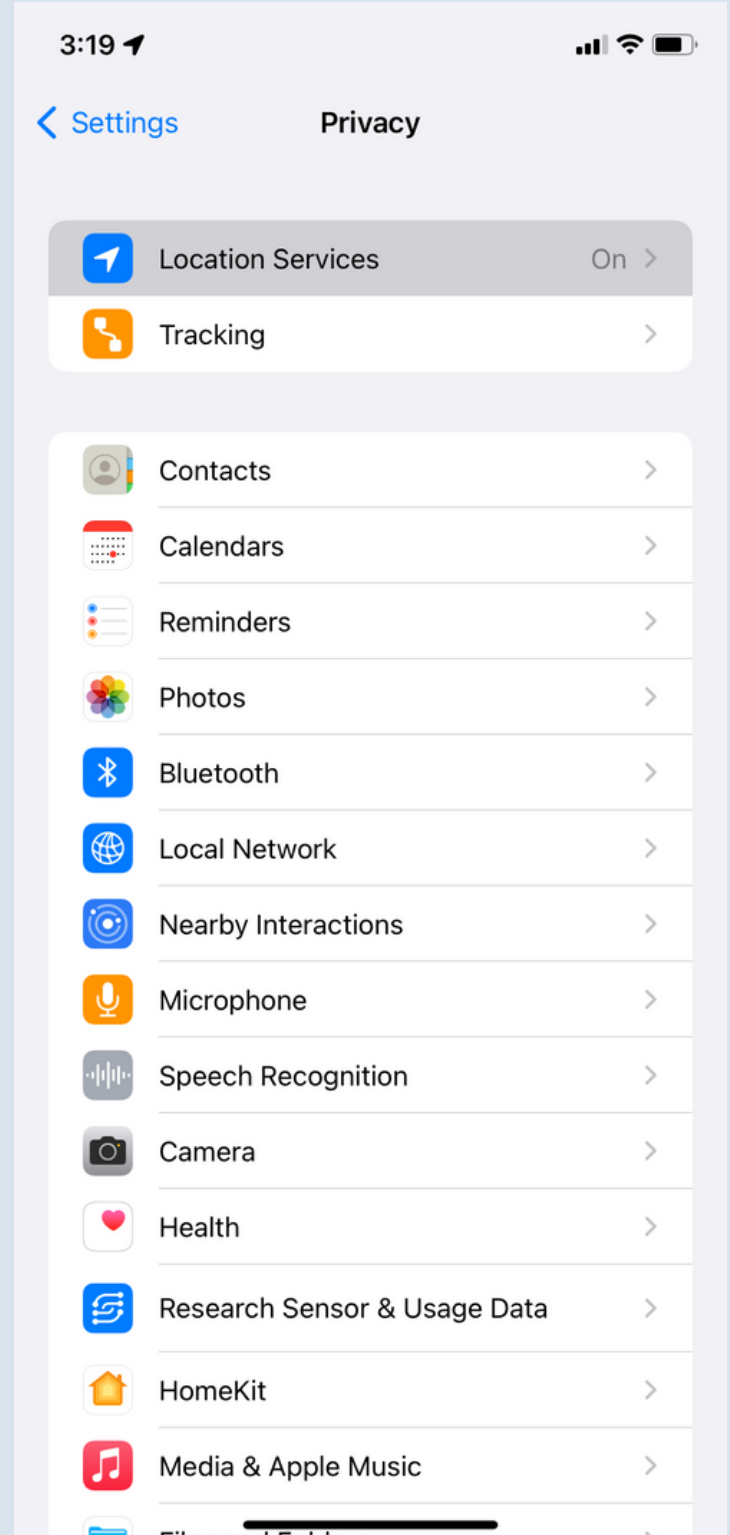
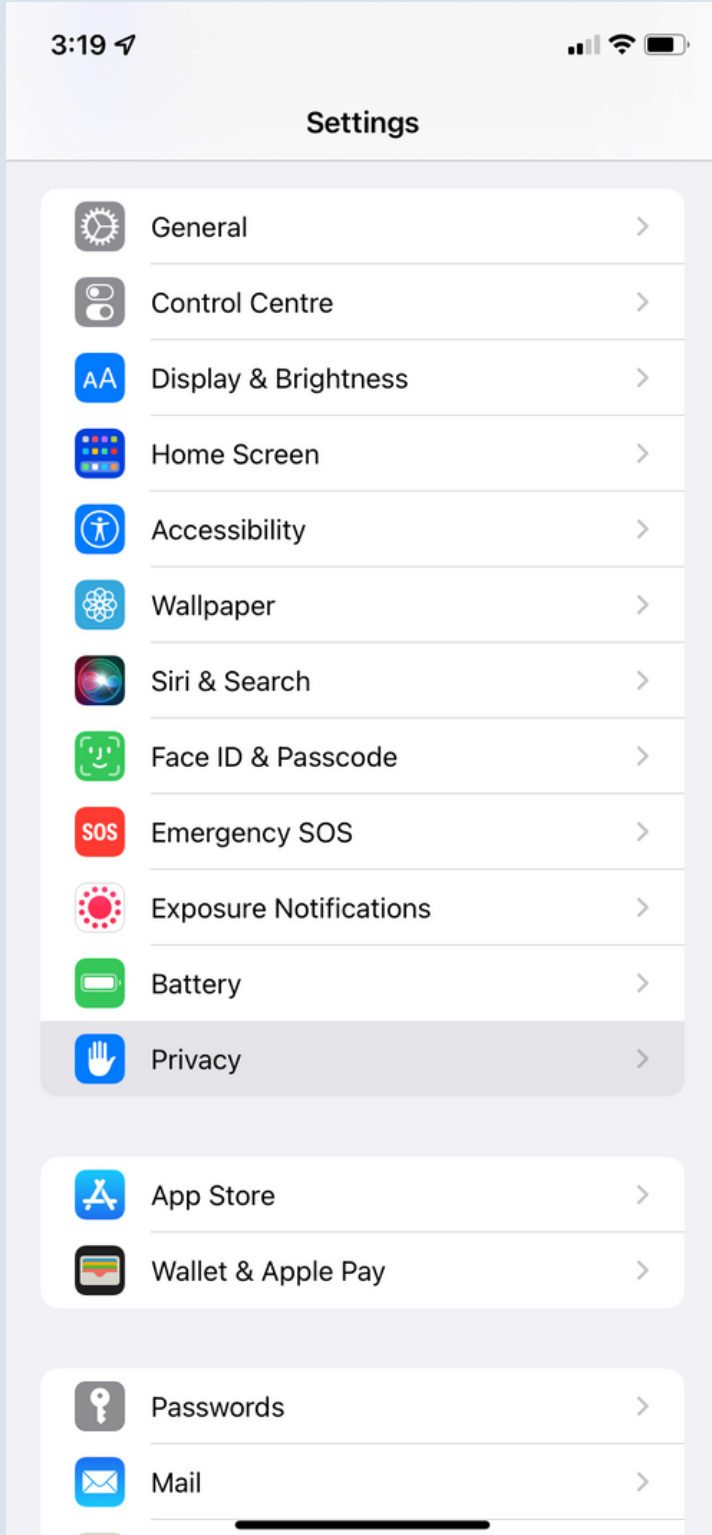
Online Surveillance



Is someone tracking my location from my iPhone?

Step 1: Open your iPhone settings app, and click on "Privacy"

Step 2: Click on "Location Services"





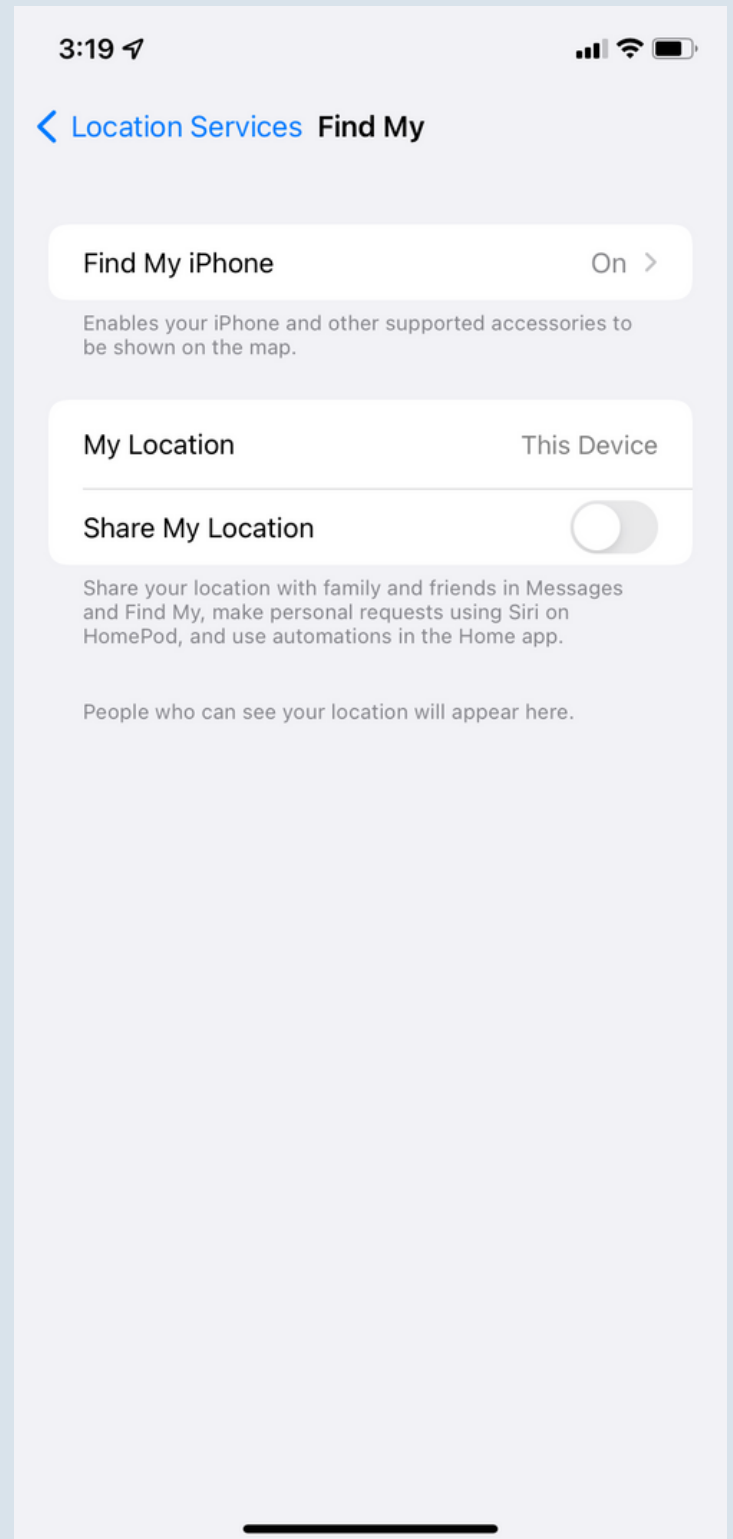
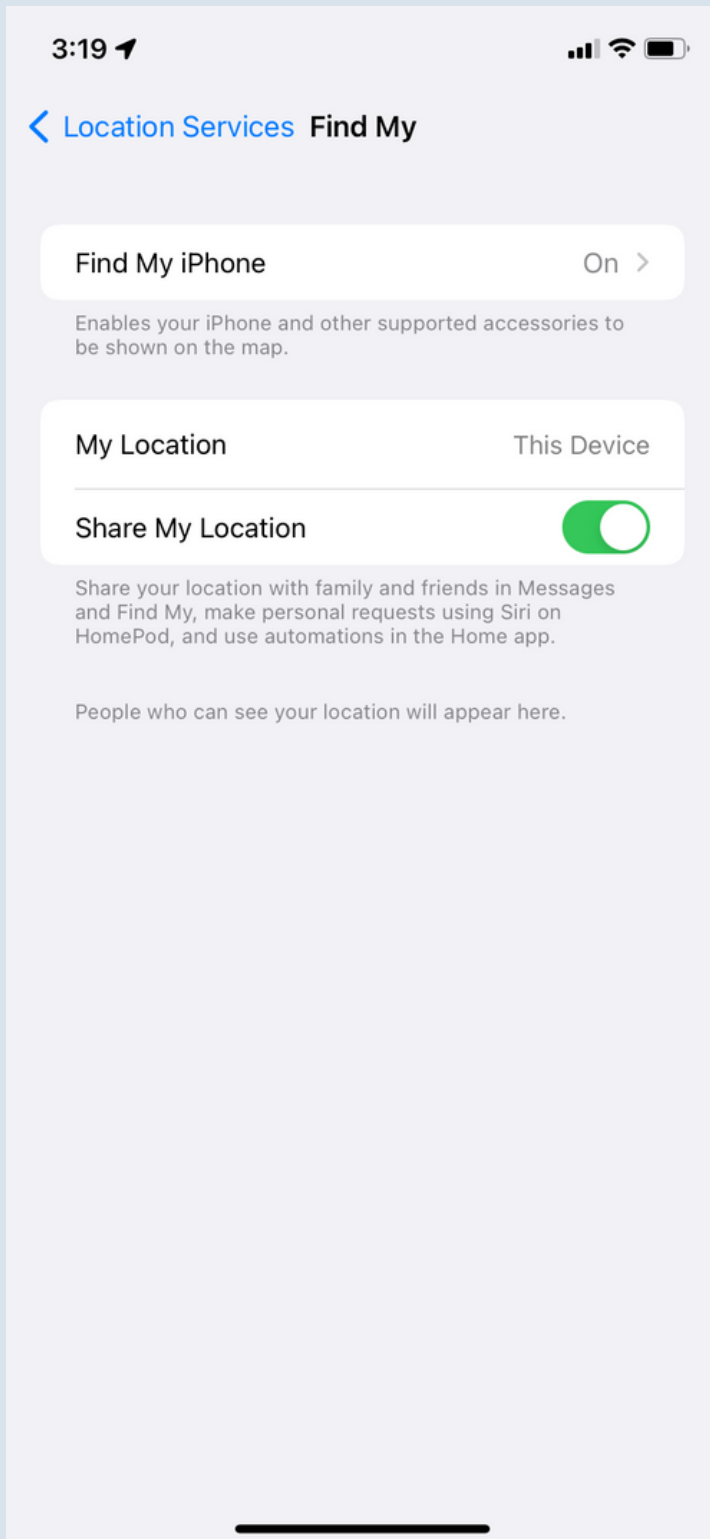
Online Surveillance



Is someone tracking my location from my iPhone?

Step 3: Click on "Find My" and then click on the button that says "Share My Location"

Step 4: Toggle the setting on or off as you wish. Repeat with any listed app.



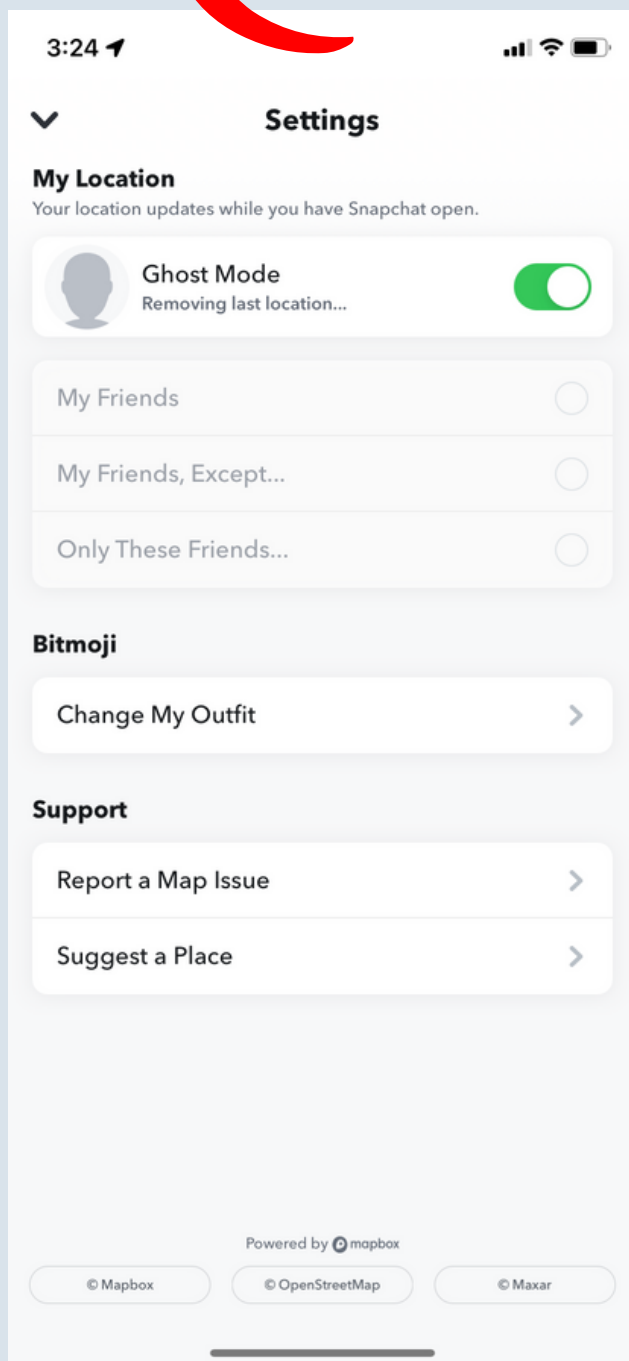
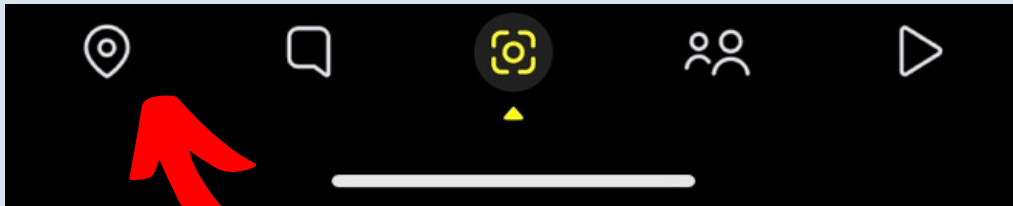



Online Surveillance



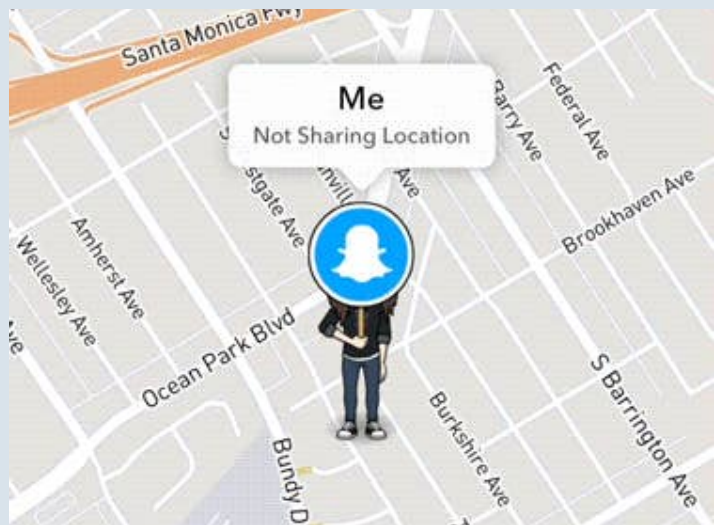
Is someone tracking my SnapMap location?

Step 1: Open Snapchat, and click on the SnapMap icon on the bottom right corner.



Step 2: Click the settings button in the top left corner that looks like this: 

Step 3: Click the button to turn on "Ghost Mode" and to turn off your location sharing. This will hide your bitmoji avatar from appearing on the map that your snapchat friends can see.



Now, only you can see your location. But, you can also turn off your location sharing with any app in the settings as shown in the previous page.



Online Surveillance



Is someone tracking my location with an AirTag?

An AirTag is a small GPS location tracking device made by Apple. It is about the size of a toonie, and can be very hard to find if it has been placed on you (such as in your purse, pocket, or hidden on your car)



When an AirTag that is not owned by you is too close to you for too long, Apple will notify iPhone users that there is a chance they are being tracked by an AirTag. The notification looks like this (below) and the AirTag owner can see the tag (and you) move on a map like this:





Online Surveillance



Is someone tracking my location with an AirTag?

Unfortunately, sometimes you cannot reliably turn off the tracking on an AirTag that you do not own, so these can be very dangerous. You should immediately check possible hiding spots, like your purse, handbag, backpack or anything you carry with you daily, your pockets, or keys.

People can buy magnetic attachments for AirTags, so it is also a good idea to check metal objects you may carry with you. For example, AirTags can be stuck with magnets to a car. Check hard-to-see places like your fender, bumper, behind your license plates, and in your wheel wells.

If you get an AirTag notification when you are outside, it is very important to try to locate it before you go home; the person tracking the AirTag can see where you go, so to stay safe try not to go to usual places like home or work while you search for it.

If you find a hidden AirTag (or similar device like a Tile Tracker), take out the battery and/or bring it to your local police station if you feel unsafe. Do not keep it or bring it home.





Online Surveillance

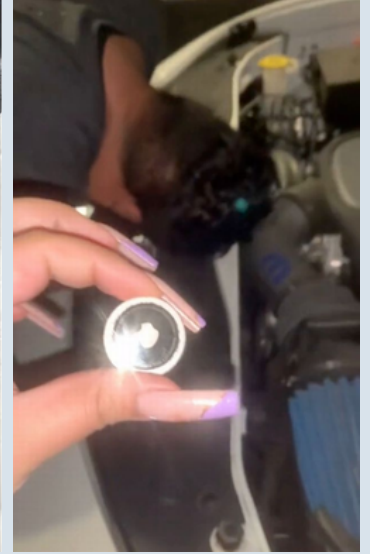


Is someone tracking my location with an AirTag?

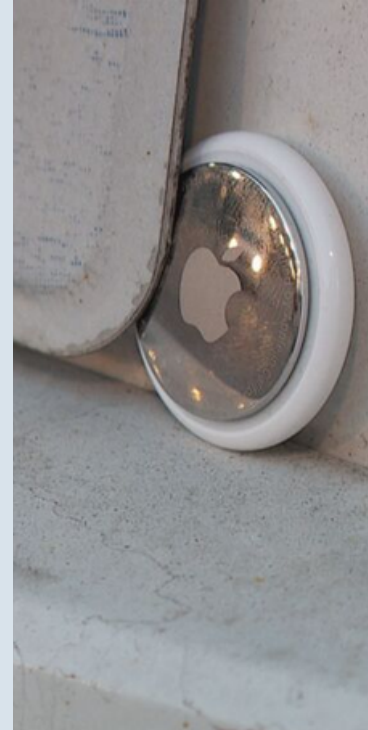
Some places on your vehicle that you can check for AirTags or Tile trackers if you get a notification that one is following you:



Under your windshield wipers



In and around your Gas Cap or your hood/engine



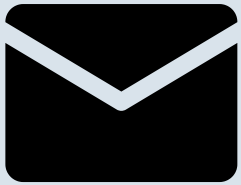
Under your car or in your wheel wells; under your license plate(s), other small and hard-to-see places



Have Questions?

Get in touch

If you have another question about online privacy, reach out to the NSWC. Our staff and volunteers may be able to help you, or direct you to another resource like our free [tech support](#) or [basic computer training](#) programs. We also offer a variety of online resources that staff can direct you to, or that can be accessed on our [website](#).



info@northshorewomen.ca



604-984-6009



northshorewomen.ca

Social media: @northshorewomen

