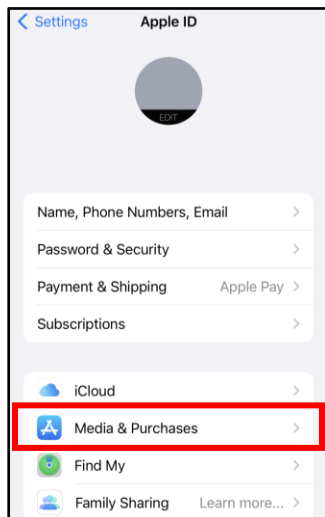
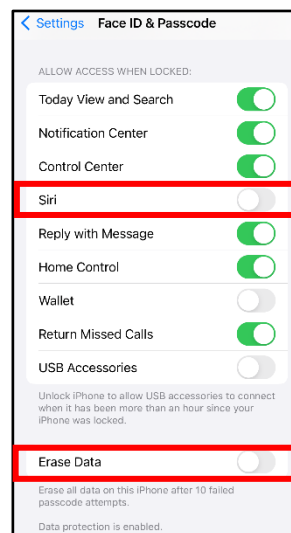
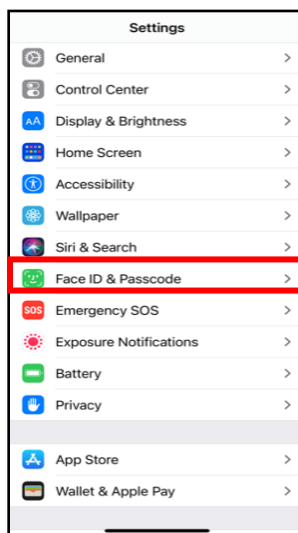


iOS PRIVACY SETTINGS

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

Physical Security

In the iOS “Settings” app find and select “Face ID & Passcode,” then select “Set Up Face ID” and “Turn Passcode On.” Ensure the password is strong such as an alpha-numeric passcodes. At the bottom, there is an option to “Erase Data” which will completely erase all data after 10 failed attempts. Additionally, it is recommended that you turn off “Siri” due to its listening capabilities and bugs associated with accessing your phone. Finally, scroll further down in this section to find, “Allow Access When Locked” and go through to ensure comfortability with each.



Find my iPhone

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

iOS PRIVACY SETTINGS

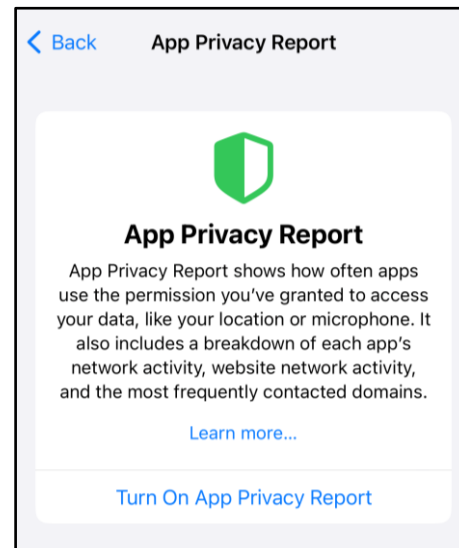
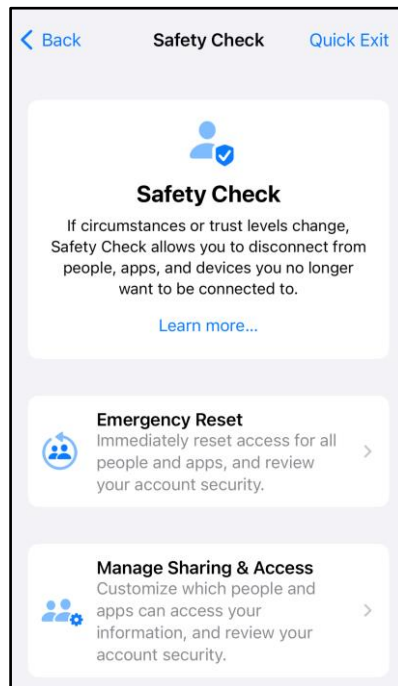
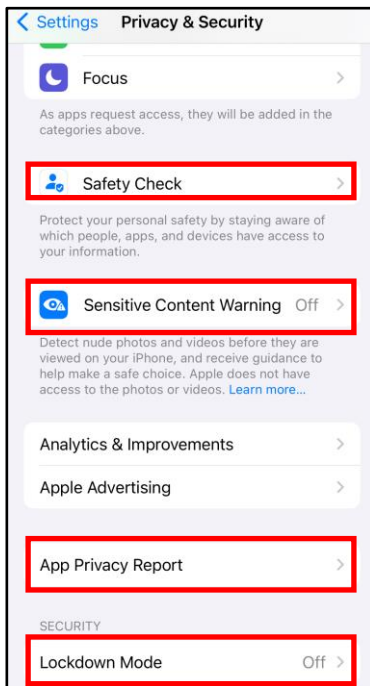
Sign-in & Security

Under your “Apple ID,” navigate to “Sign-in & Security.” Here you can Change your password if needed. It is also suggested that you set up “Two-Factor Authentication” on your device. You can also enable “Account Recovery” here if you forget your password or device code to recover your data. Apple also offers a “Legacy Contact” option so that someone you trust will have access to your data after your death.



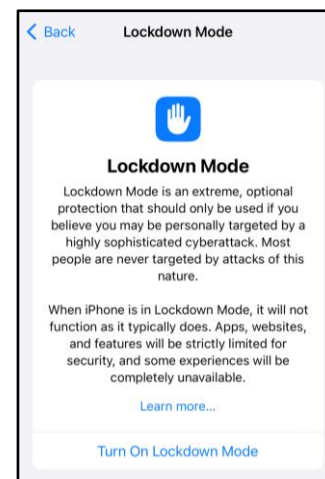
Privacy & Security

Go to “Privacy & Security” in your iPhone settings. From here you can do a “Safety Check” on your phone. It will allow you to reset access to apps and review your account security. If you have children, you should consider enabling the “Sensitive Content Warning.” You can also get an “App Privacy Report,” that shows how often apps use the permissions you’ve granted.

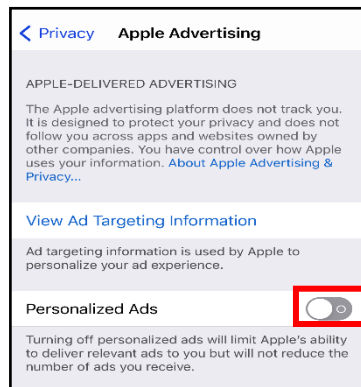
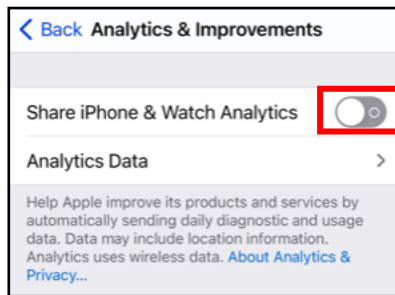
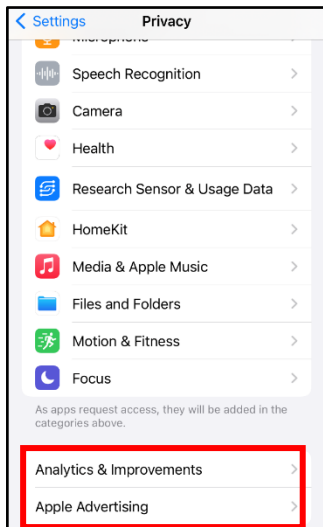


Lockdown Mode

Apple implemented a new tool called “Lockdown Mode.” It is a tool that limits functions on Apps, websites and features if you believe you're being targeted by sophisticated cyber security attacks.



iOS PRIVACY SETTINGS

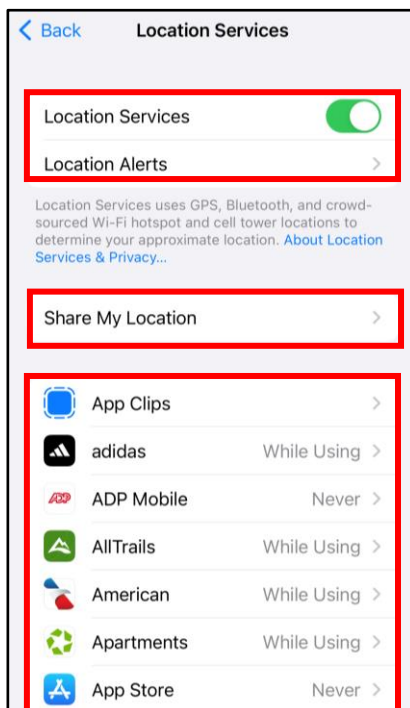


Analytics and Advertising

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

Location Based Services

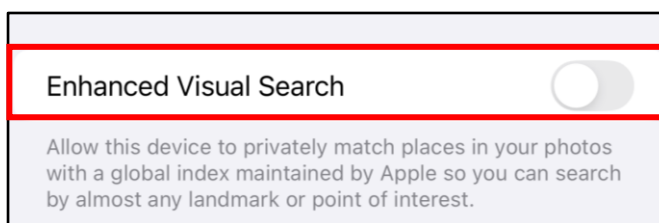
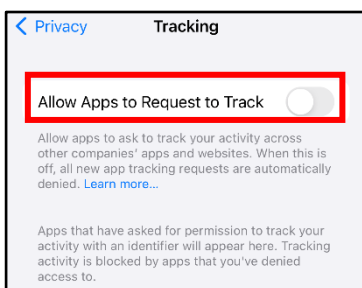
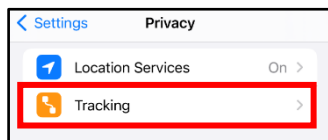
Navigate to "Location Services." From here you can control what apps are able to see your location, if at all. It is recommended that you keep the settings at "Never" or "While Using" only. Next, navigate down to "Share My Location." Here you can toggle "Find My iPhone," which allows you to Locate, Lock, or erase the device. You can also choose to toggle "Share My Location" on or off.



iOS PRIVACY SETTINGS

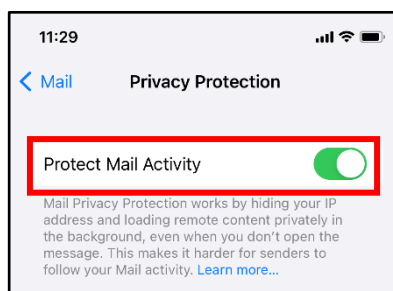
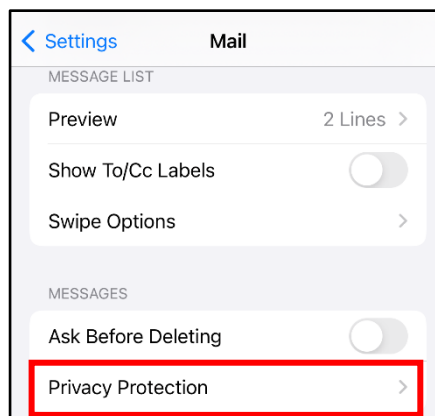
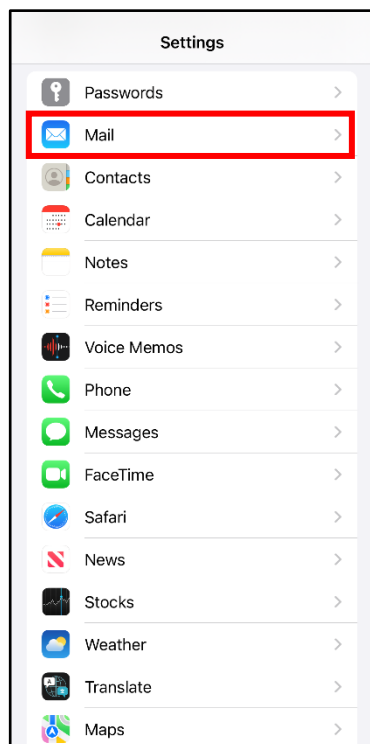
Tracking

Locate and select “Privacy” under “Settings” then select “Tracking.” Under “Tracking,” ensure that “Allow Apps to Request to Track” is off. This will make it so apps won't have permission to track your activity, and so you won't have continuously click deny every time a new app asks. Also related to tracking, if you go back to your settings and scroll down to the “Apps” portion, then go to “Photos.” Here at the bottom, there is an option called “Enhanced Visual Search.” It is recommended you turn this off as it gives apple access to privately match places in your photos to a global index.



Mail

Mail now offers “Privacy Protection” to your email. It will now encrypt your messaging, hide your IP address, and load remote content privately in the background. This setting will automatically appear when you update to IOS 16. However, if you opted out of it during the initial setup, you can turn it on by going to “Mail” under “Settings.” Under “Mail” go to “Privacy Protection.” Then turn on “Protect Mail Activity.”



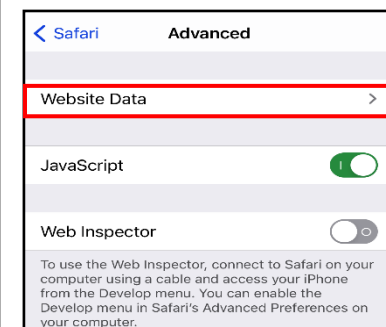
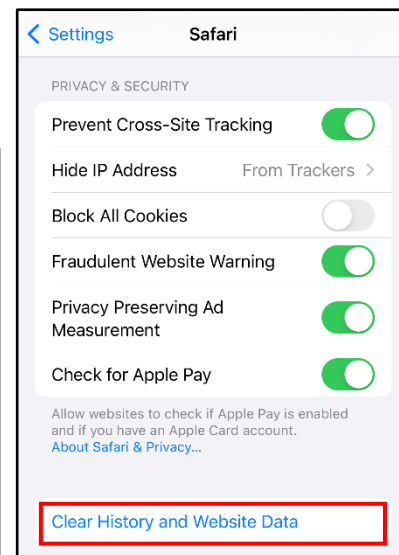
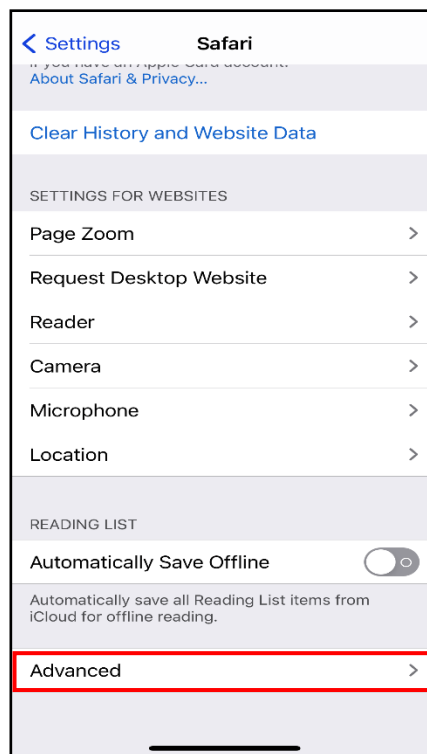
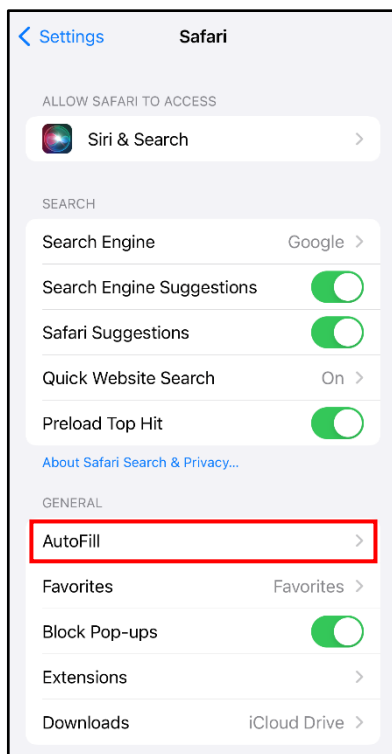
IOS PRIVACY SETTINGS

Safari

Safari's "Do Not Track" is a universal web tracking opt-out initiative that allows users to prevent advertisers from tracking your browsing habits. There are several sections to look through and adjust the settings, but it is recommended to turn off "Frequently Visited Sites" under the section titled "General." This prevents Safari from tracking sites you regularly visit. Next, under the "Privacy & Security" section on the "Safari" page, turn on "Prevent Cross-Site Tracking" and "Fraudulent Website Warning."

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

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



IOS PRIVACY SETTINGS

Siri and Apple Intelligence

This is only if you have the Apple iPhone 15 and newer models WITH iOS 18 installed. Under your “Settings” tab, navigate to “Apple Intelligence & Siri.” Once here, you will see the option “Turn on Apple Intelligence.” It is recommended that you do not enable this. Below that you can see “Talk to Siri” which is recommended to keep off, and “Siri & Dictation History” where if you have Siri enabled, you can delete the transcripts it records locally on your device. Below that is the “Suggestions” portion. It is recommended that you keep all of these off as well. Keep scrolling and you will see the “Siri App Access.” Under here, you will see “App Clips” and “Apps.” It is recommended that you go through both off these and make sure the settings are turned off as depicted below. **Apple paid out \$95 million in lawsuit due to Siri listening in on conversations and selling that data to third party entities.**

Settings

Bluetooth

Cellular

Battery

General

Accessibility

Action Button

Apple Intelligence & Siri

Apple Intelligence & Siri

A personal intelligence system integrated deeply into your iPhone, apps, and Siri.

Turn On Apple Intelligence

SIRI REQUESTS

Language

Talk to Siri

Voice

Siri & Dictation History

Siri & Dictation History

Delete Siri & Dictation History

Delete the transcripts of your Siri & Dictation requests that are stored on this iPhone and used to personalize your experience.

SUGGESTIONS

Suggest Apps Before Searching

Reset Hidden Suggestions

Allow Notifications

Show in App Library

Show When Sharing

Show Listening Suggestions

SIRI APP ACCESS

App Clips

Apps

Apps

App Store

App Clips

Learn from App Clips

ON HOME SCREEN

Show in Search

Suggest App Clips

Apps

App Store

Learn from this App

SUGGESTIONS

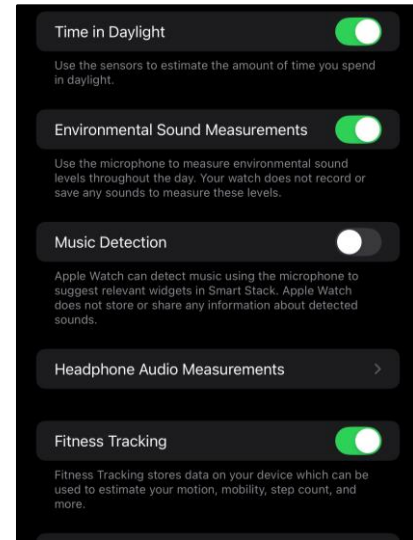
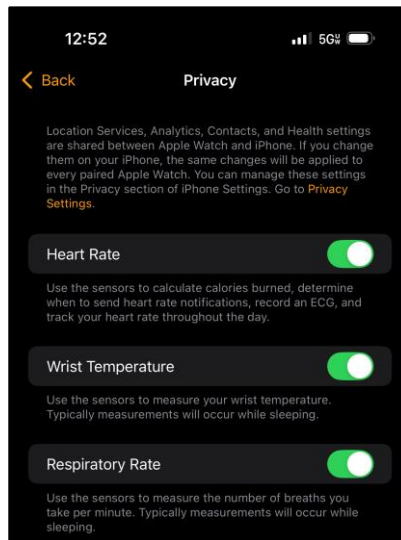
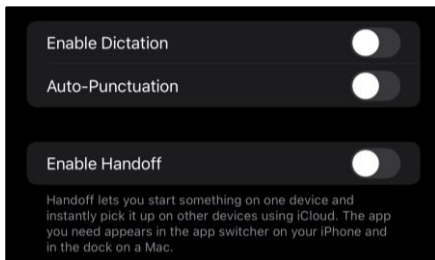
Show on Home Screen

Suggest App

iOS PRIVACY SETTINGS

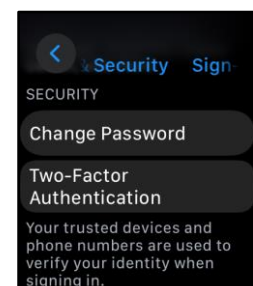
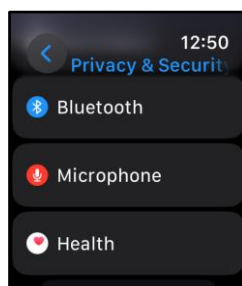
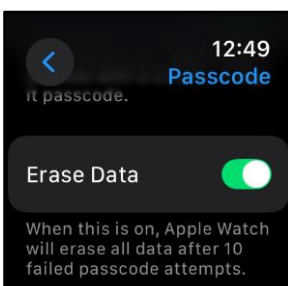
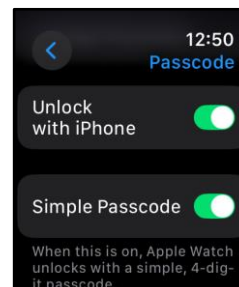
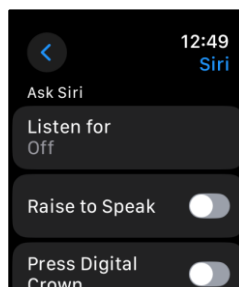
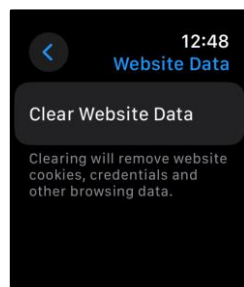
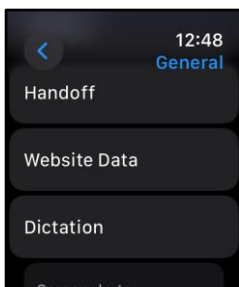
Apple Watch on iPhone

Some settings for the Apple watch are only available through the “watch” app on your iPhone Starting with going to your “Watch” app, under “General,” if you scroll down you will see where it says “Enable Dictation” and “Enable Handoff.” It is recommended that you keep both of these turned off. Next under “Privacy,” it is recommended to go through these settings and decide which ones you want enabled/disabled.



Apple Watch

Now on your apple watch, go to the “Settings” tab. Once here, scroll down to the “General” tab and scroll down to “Website Data.” Here you can “Clear Website Data.” After, go back and scroll down until you see “Siri.” Here it is highly recommended you turn Siri off. Next go back and scroll down to “Passcode.” It is recommended that you turn on “Simple Passcode,” “Wrist Detection,” and “Erase Data. Last, go scroll to “Privacy & Security” to access the “Microphone.” Turn off “Measure Sounds.” You can also change your password here and enable “Two-Factor Authentication.”

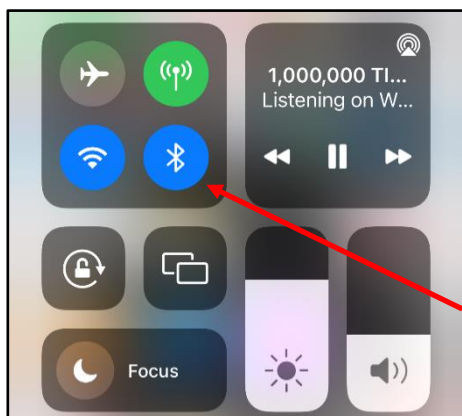


iOS PRIVACY SETTINGS

Wifi and Bluetooth

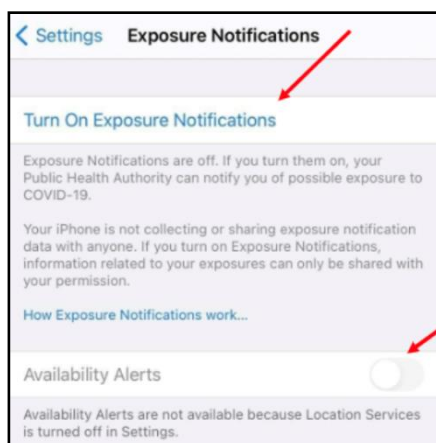
Where possible, public wifi networks should be avoided due to the vulnerabilities they present to your personal data. If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt on-line transactions. There are two ways to turn off wifi: 1)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

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



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

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



Note: The "Exposure Logging" toggle is disabled by default in iOS 15.1. It does not connect any data without you installing and authorizing a local health authority app, which will be available soon. Apple's exposure notification system will be completely opt-in.