Dark patterns: A step-by-step guide to protect your privacy

By Isabel Brown, Consumer Watchdog Associate

Apps and social media are a part of everyday life. They help us stay connected to the. world around us. But it can be easy to overlook the risk involved with making personal information accessible online, especially when that information can be recorded, bought and sold by the companies running the apps.

Dark patterns are one way that apps and websites steer consumers into making the choice that's right for the app or website -- but wrong for the consumer. Dark patterns make it harder for you to select higher privacy or security settings so they can collect more of your data and monetize your engagement. Also, while apps and websites make it as easy as possible -- often, one-click! -- to subscribe to paid services, dark patterns often make it much harder to cancel services.

It's important that consumers protect their own privacy. Federal passage of a strong privacy law has stalled due to industry demands that any new law allow unfettered collection and monetization of your data with no consumer enforcement rights against unfair practices. After a promising start with passage of the California Consumer Privacy Act in 2018, subsequent new state laws in Virginia and Colorado and proposals in numerous other states from Washington State to Florida, have followed an industry-approved pattern of providing only opt-out rights some of the time, but no real consumer protections.

Taking control of how public your information is – and how data companies like Google and Meta are able to use that information – is key to protecting your privacy.

You can take some control by changing your account settings. Finding exactly where those settings are can be difficult, so here are some recommendations and step-by-step instructions for how to set up your accounts and devices for four popular apps: Instagram, Facebook, YouTube and Twitter.

CONTENTS

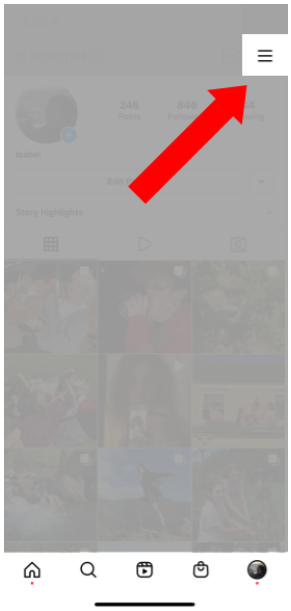
How to set up security preferences by platform

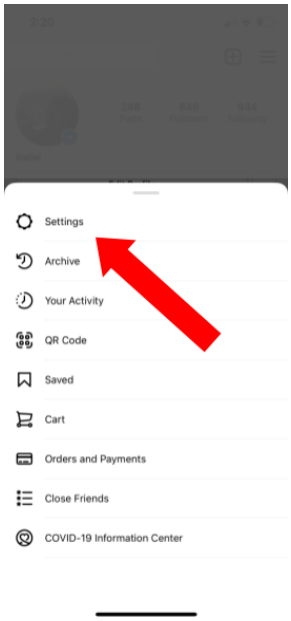
Instagram

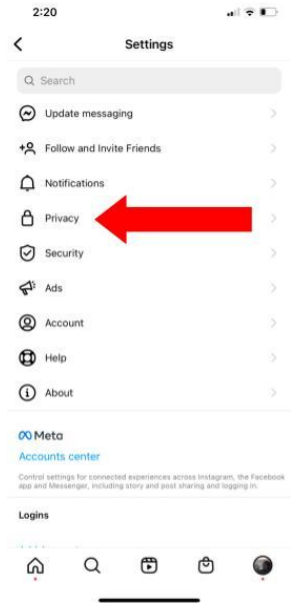
Make your account private

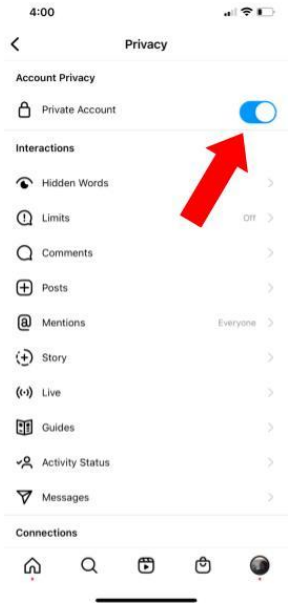
When you make an individual Instagram account, your account will be set to “Public” as a default, meaning that anyone who finds your profile can see what you post. Making your account private means that only people who follow you are able to see the photos that you post. It also means that people have to request to follow you, so you can be sure that only the people who you know and trust are able to see and interact with your posts.

You can do this on the Instagram app. Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Privacy. Switch on the Private Account toggle.





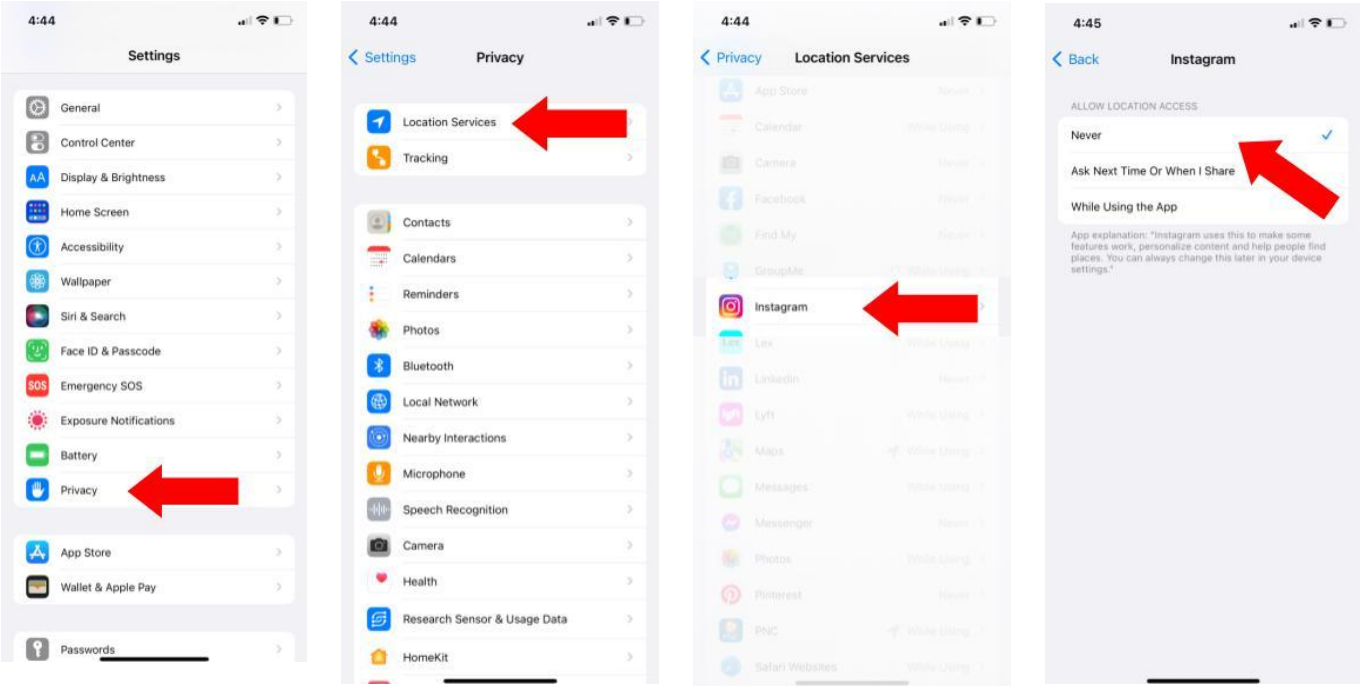




Turn off access to your location

When Instagram has access to your location, it can use it to suggest posts and accounts that are in your area that may be of interest to you. It can also use your location to show your content to other people in your area. While this can be helpful for small businesses trying to expand their reach within their community, for regular personal Instagram accounts, giving the app access to your location may be sharing more personal information than you want to, especially when your location information is used to send you targeted ads, or what that information is used or sold to other.companies.

You can turn off Instagram's access to your location on an iPhone: Go to the phone's Settings → Privacy → Location Services → Instagram → Never.

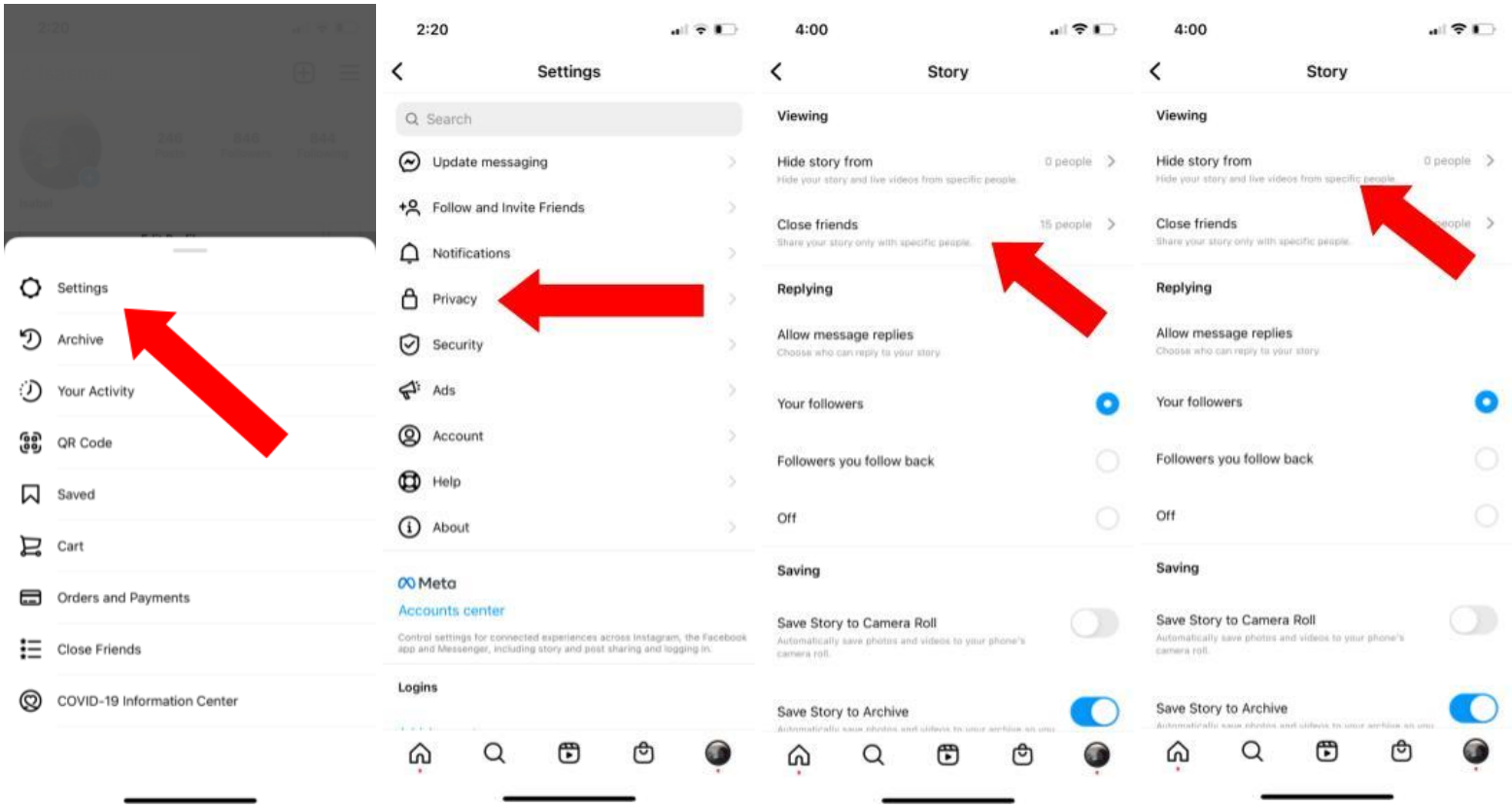


For Instagram Stories, make “Close Friends List” to control who sees them

Even if your account is private, you can take more control over who sees your Instagram stories. Making a “Close Friends List” means that you can individually select the followers that you want to share your Story with.

You can do this on the Instagram app. Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Privacy → Story → Close Friends → Select the people you want to be in your close friends group. The next time you post a Story, tap Close Friends on the bottom so that only the people on your list will see it. You’ll see a green circle with a start icon.

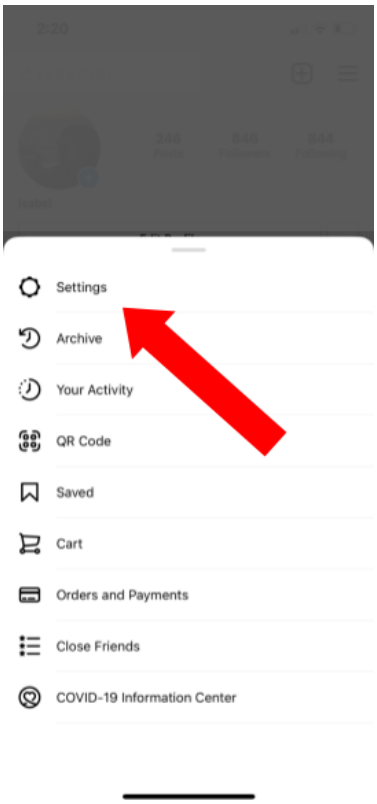
You can also block specific people from seeing your stories. Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Privacy → Story → Hide story from → Select the people you want to hide your stories and live videos from.

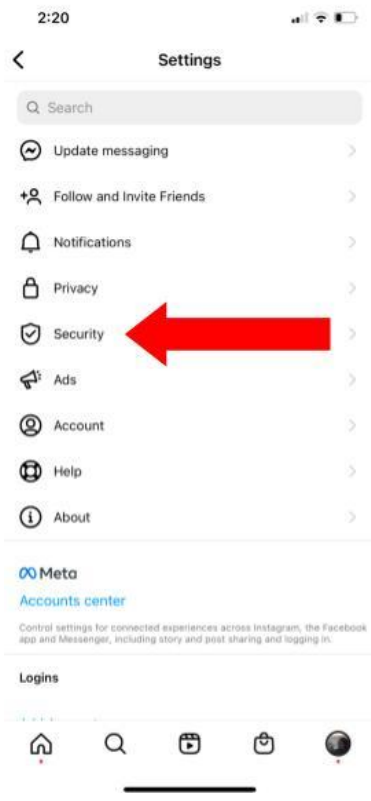


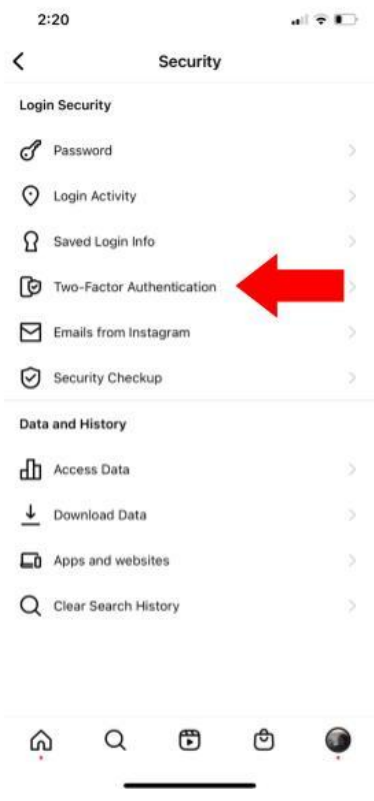
Turn on multi-factor authentication to prevent your account from getting hacked

Multi-factor authentication works by adding another step to log into your account, so you have to provide another piece of evidence, in addition to your account password, that proves that you are who you say you are.

You can set this up on the Instagram app. Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Security → Two-Factor Authentication → Tap the login method you want to use and follow the next instructions. You can download an authentication app, which you can use for all of your multi-factor authentication needs.



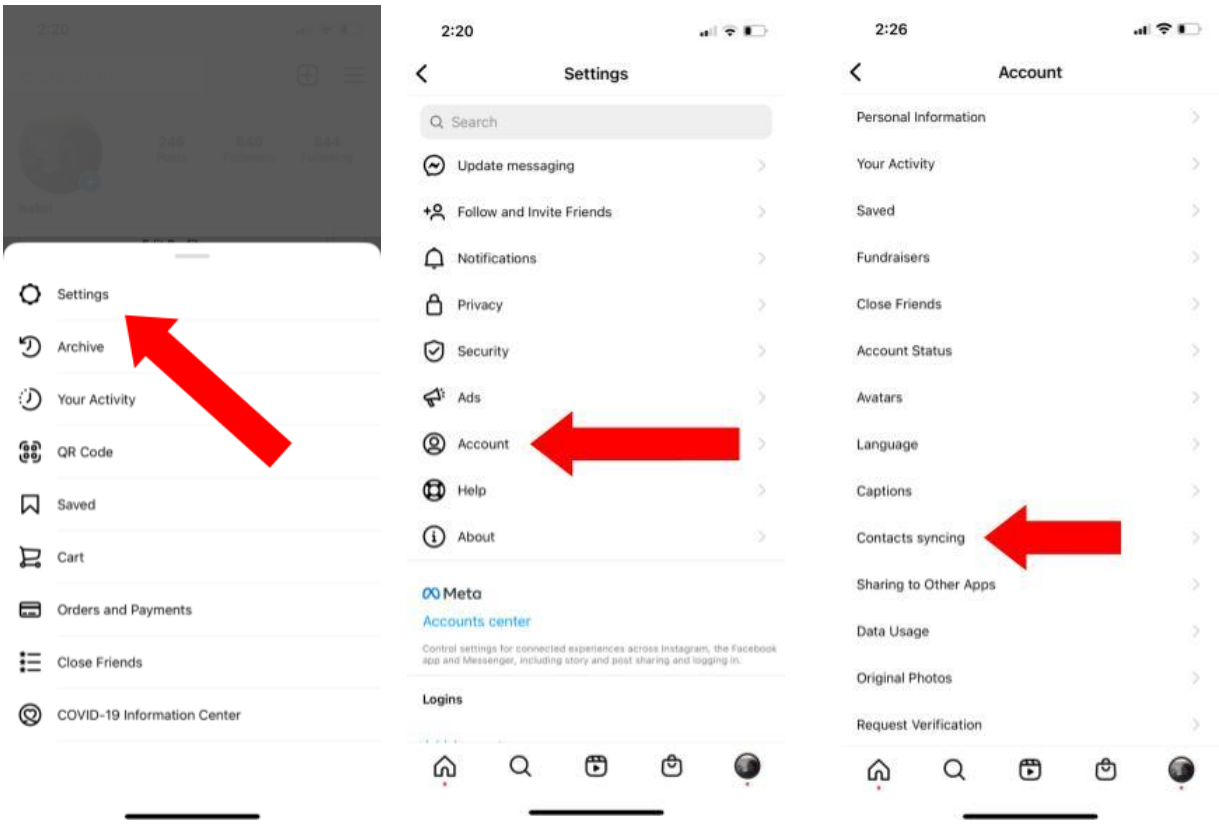




Don’t sync your contacts with the app. If you already have, you can delete them.

Instagram uses access to your contacts to help you find the people you know on Instagram. The downside is that access to your contacts means that Instagram knows the phone number, email and even home address of everyone in your contacts.

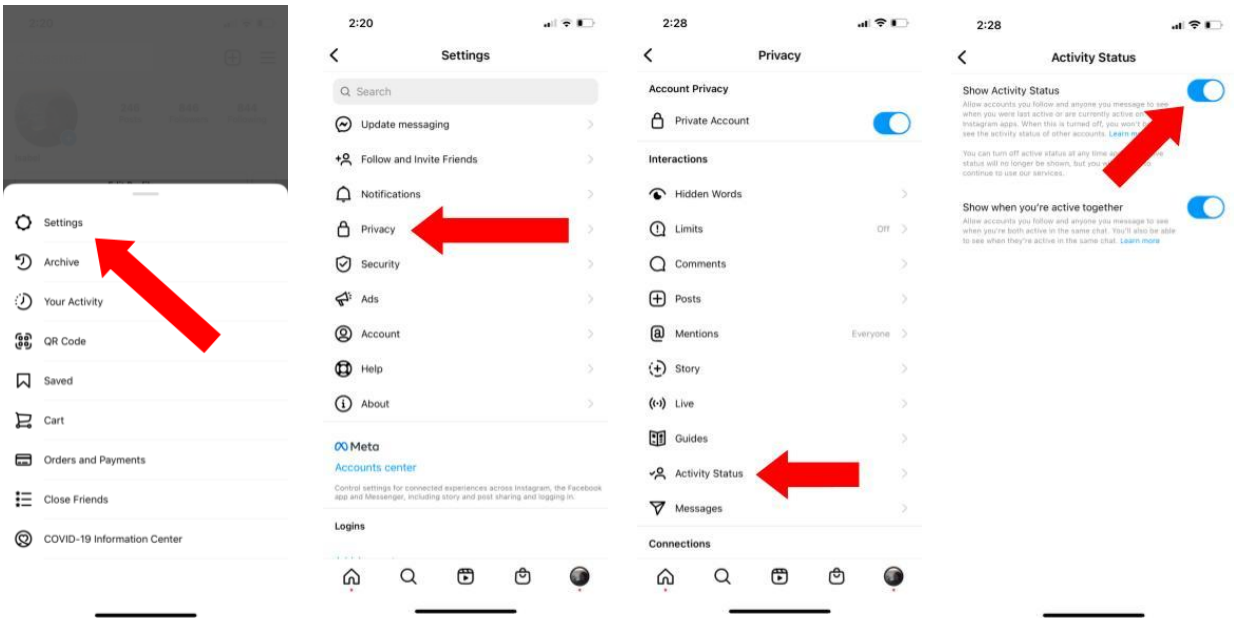
You can stop contact syncing on the app. Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Account → Contacts Syncing → Switch the toggle off.



Turn off activity status, which lets people know when you're online

When Activity Status is turned on, anyone who you have messaged on Instagram can see a little green circle next to your profile icon in the Messages section of the app. If you don't want your friends to be able to see when you're active online, you can turn this feature off.

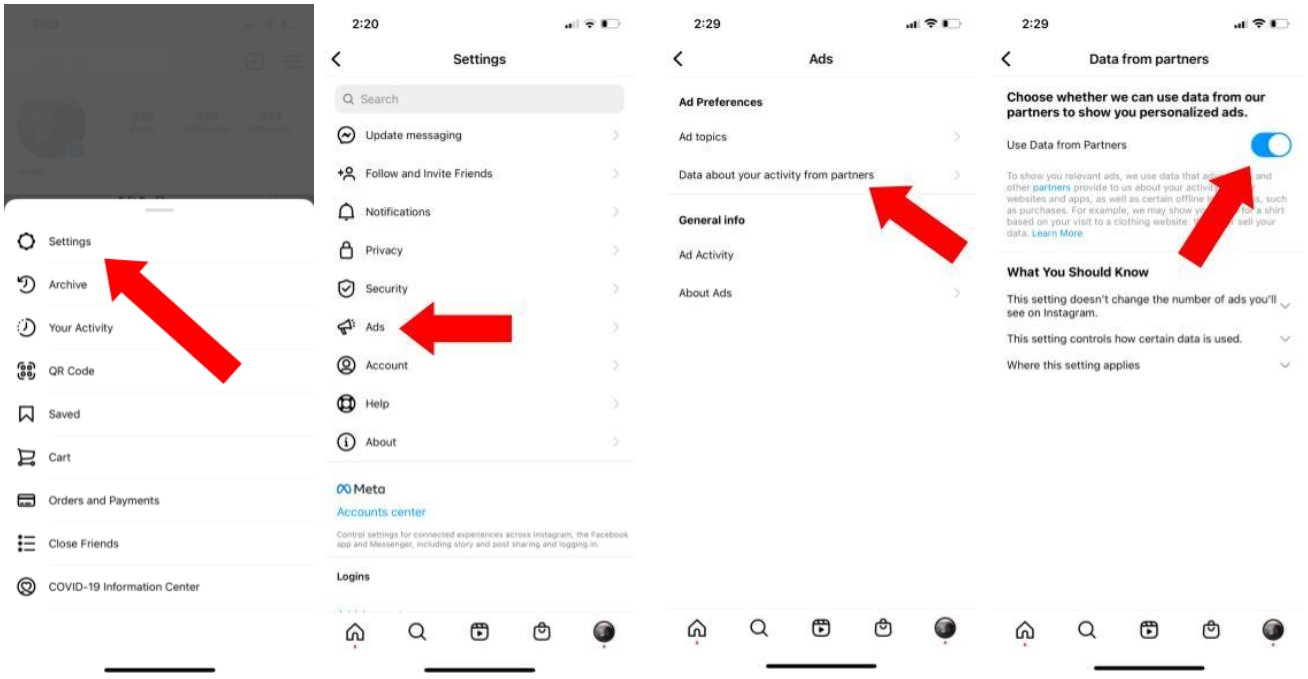
On the Instagram app, go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Privacy → Activity Status → Switch the toggle off.



Take some control over the targeted ads that Instagram shows you.

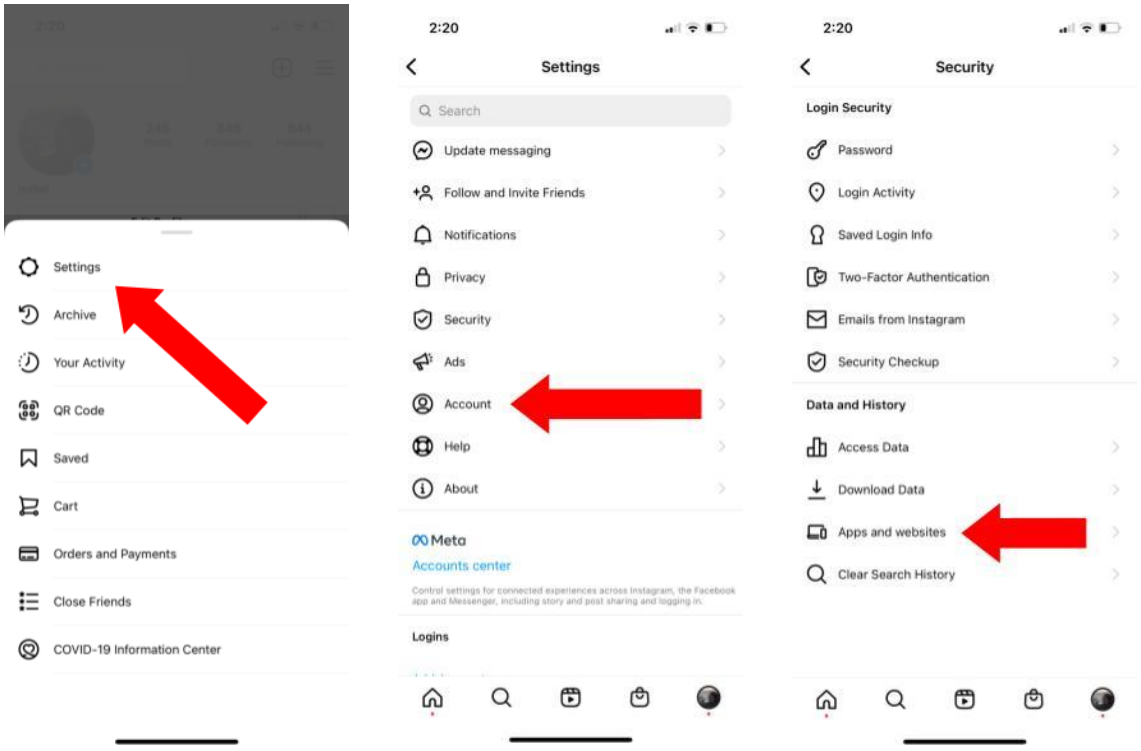
You can control whether Meta (Instagram and Facebook's parent company) can use information that other companies have gathered about you to send you targeted ads on Instagram or Facebook, and you can control whether Meta sends their information to other companies that would use it to send you targeted ads elsewhere.

To stop Instagram from getting your information from other companies in order to send you targeted ads, Open the app → Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Ads → Data About Your Activity From Partners. Now, switch the "Use Data from Partners" toggle off.



If you've connected your Instagram account to other apps for tracking your followers' activity or scheduling posts, those apps have access to everything on your Instagram account. You can remove their access to your account in Instagram's settings.

On the app: Go to your profile by clicking the icon in the bottom right → Open the menu in the top right by clicking the icon with three horizontal lines → Settings → Security → Apps and Websites → Active → Next to a particular app, tap Remove.

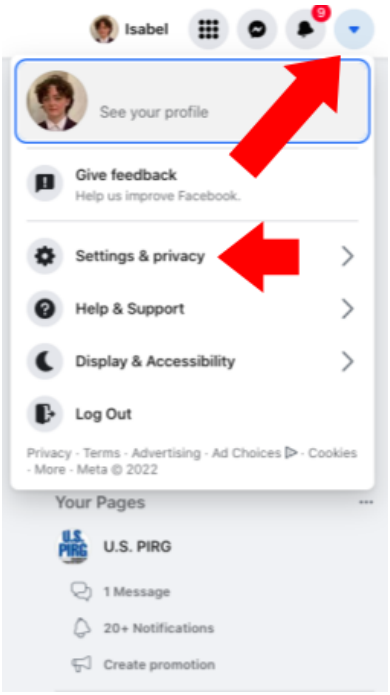


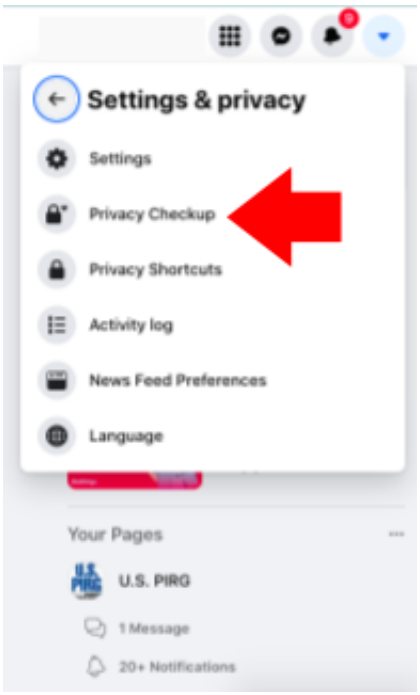
Facebook

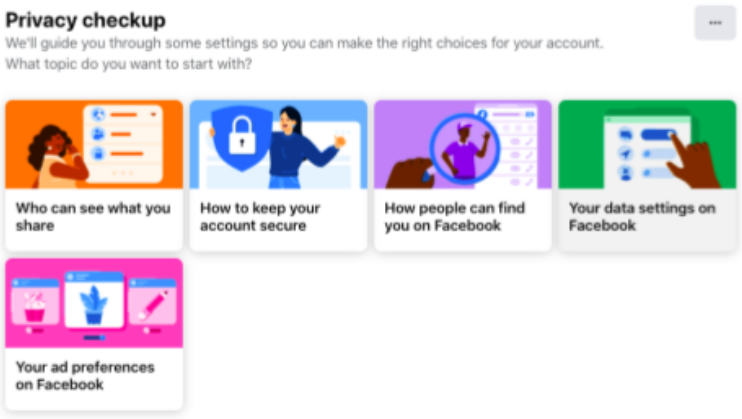
Start with a “privacy checkup”

Facebook added a new tool for managing your account privacy. It’s more streamlined than going through all of the privacy settings, making it a good place to start. You can find it when you’re logged into Facebook on your computer.

On a computer: Click the down arrow in the top right of the Facebook home page → Settings & Privacy → Privacy Checkup → Choose from the provided options. It’s good to go through all of the options to get the lay of the land and to cover all of the basics.







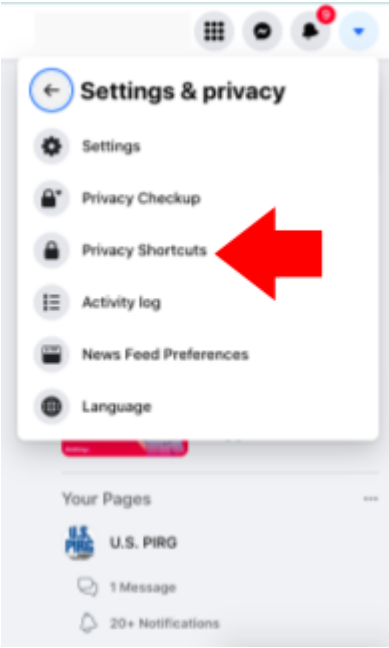
There are some privacy settings that you can’t find through the Privacy Checkup feature.

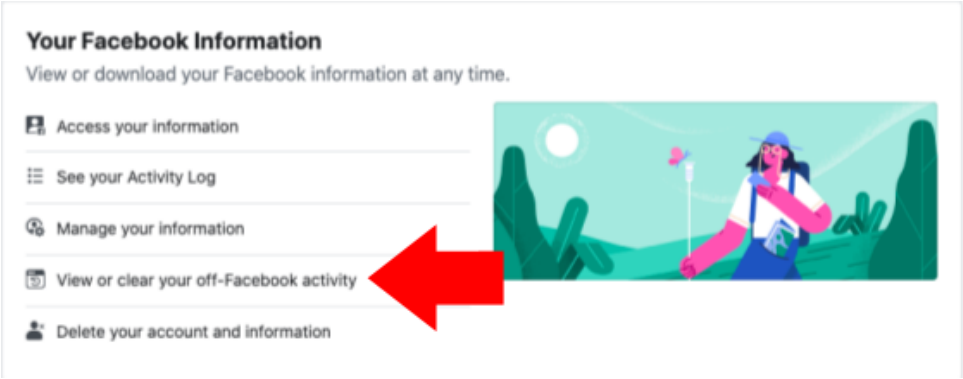
Changing these settings takes a bit more digging. The Privacy Checkup is a good place to start, but you need to delve a bit more into the settings to really make sure your information is secure.

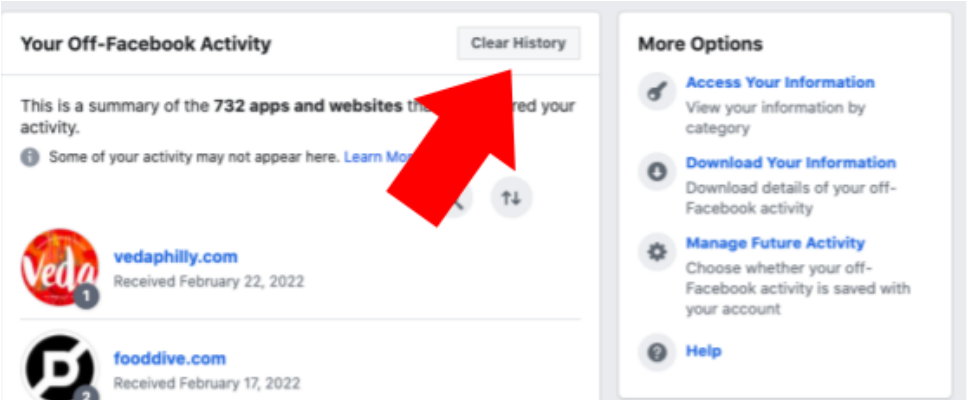
Clear out the information that Facebook has collected about you from other websites

If you use Facebook to sign in to other accounts and websites, be aware that this lets Facebook and the other company exchange information about you. You can find what other websites are connected to Facebook and currently collecting information about you, and you can remove them

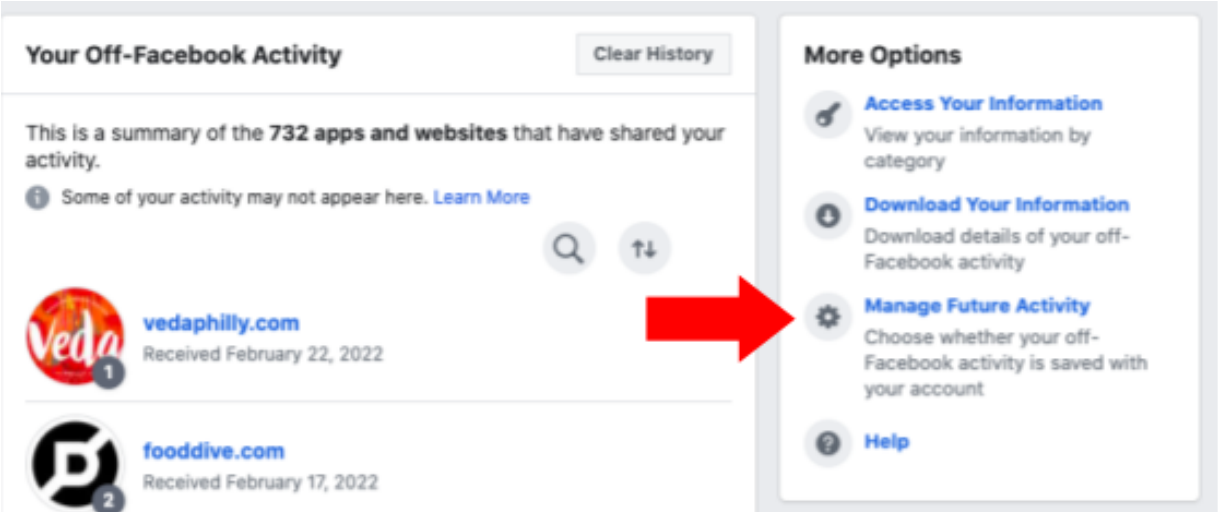
On a computer: Click the down arrow in the top right of the Facebook home page → Settings & Privacy → Privacy Shortcuts → Scroll down to Your Facebook Information → View or clear your Off-Facebook Activity. The “Clear History” button will disconnect your Facebook account from the other apps that would use that information to send you targeted ads.

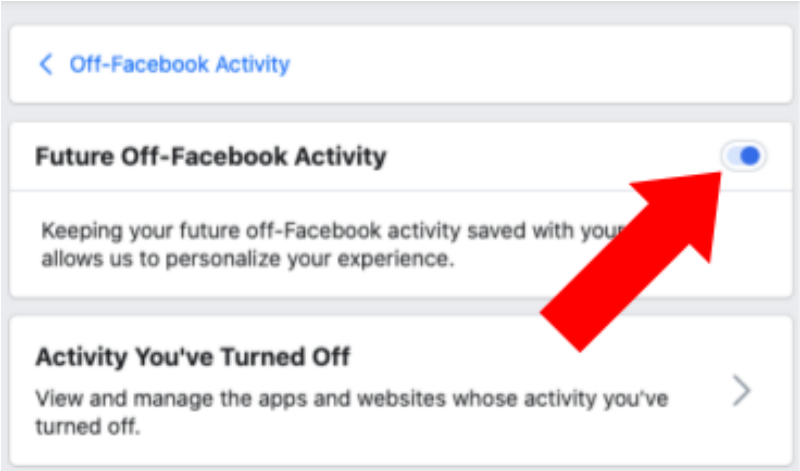






To prevent your information from being used for targeted ads in the future, click Manage Future Activity on the right-hand side, click the Manage Future Activity button on the next screen and then switch the toggle off. Be aware that turning off Future Activity means that you won't be able to use Facebook to log in to other accounts.





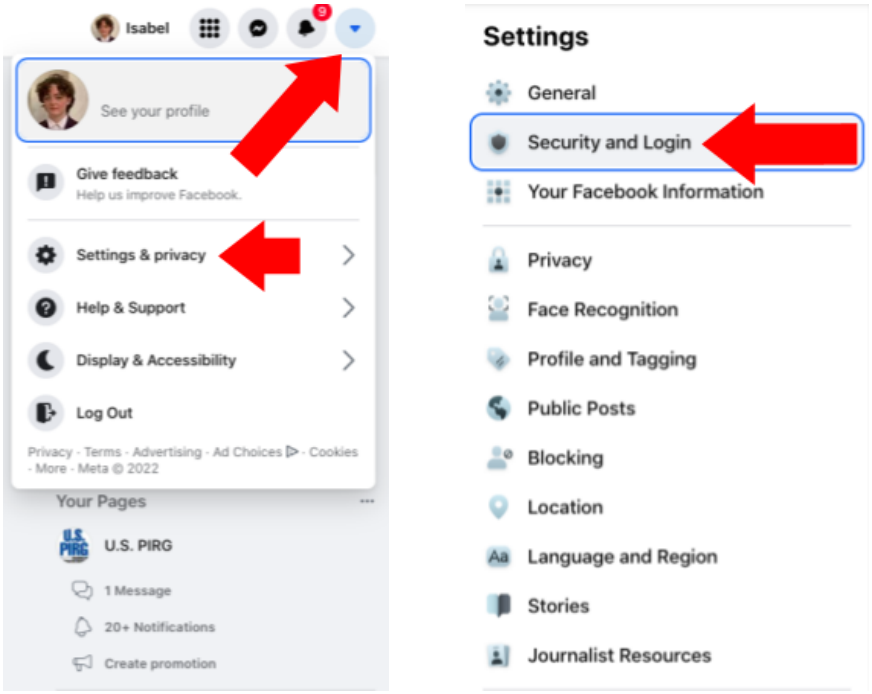
Prevent Facebook from following you on other sites

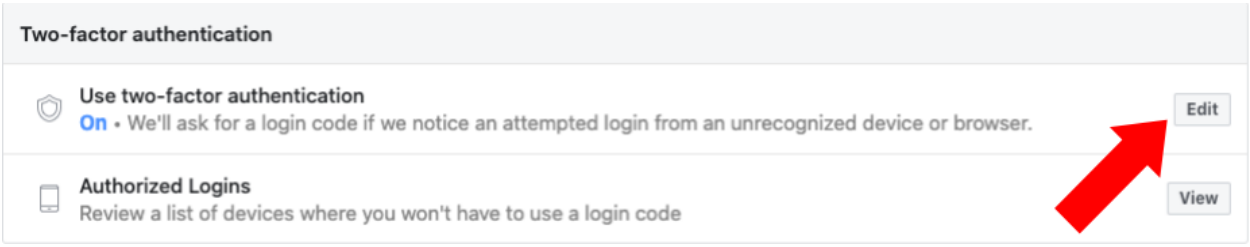
When using the Facebook web browser, get an ad-blocking extension to limit how Facebook and other apps that partner with Facebook from collecting your information.

Set up multi-factor authentication to keep you account safe from hackers

Multi-factor authentication works by adding another step to log into your account, so you have to provide another piece of evidence, in addition to your account password, that proves that you are who you say you are.

On a computer: Go to Settings → Security and Login → Set Up Two-Factor Authentication → Get Started.

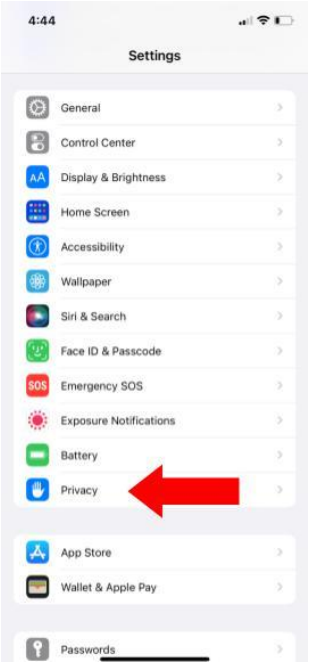


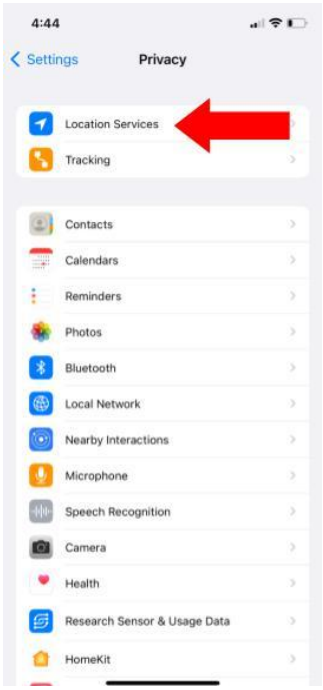


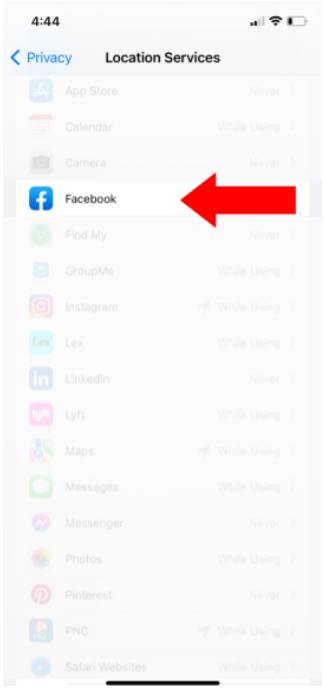
Turn off access to your location

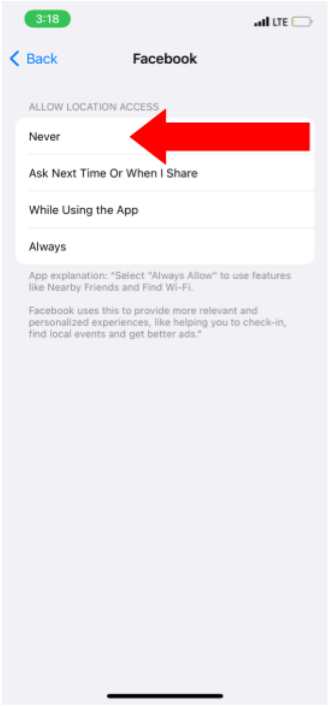
When Facebook has access to your location, it can use it to suggest posts and accounts that are in your area that may be of interest to you. But giving the app access to your location may be sharing more personal information than you want to, especially when your location information is used to send you targeted ads, or what that information is used or sold to other companies.

On an iPhone: Go to the phone's Settings → Privacy → Location Services → Facebook. Then click either "While Using the App" or "Never."





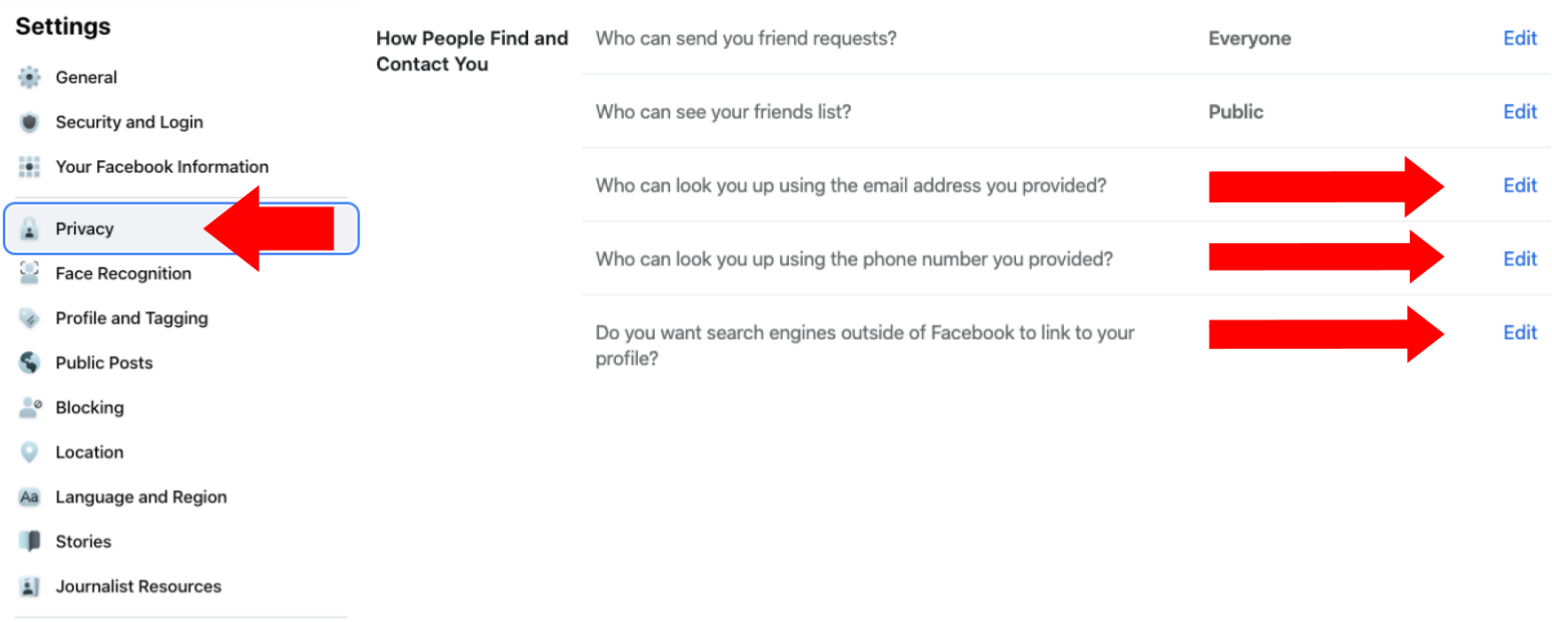




Make your profile more difficult to find on the internet

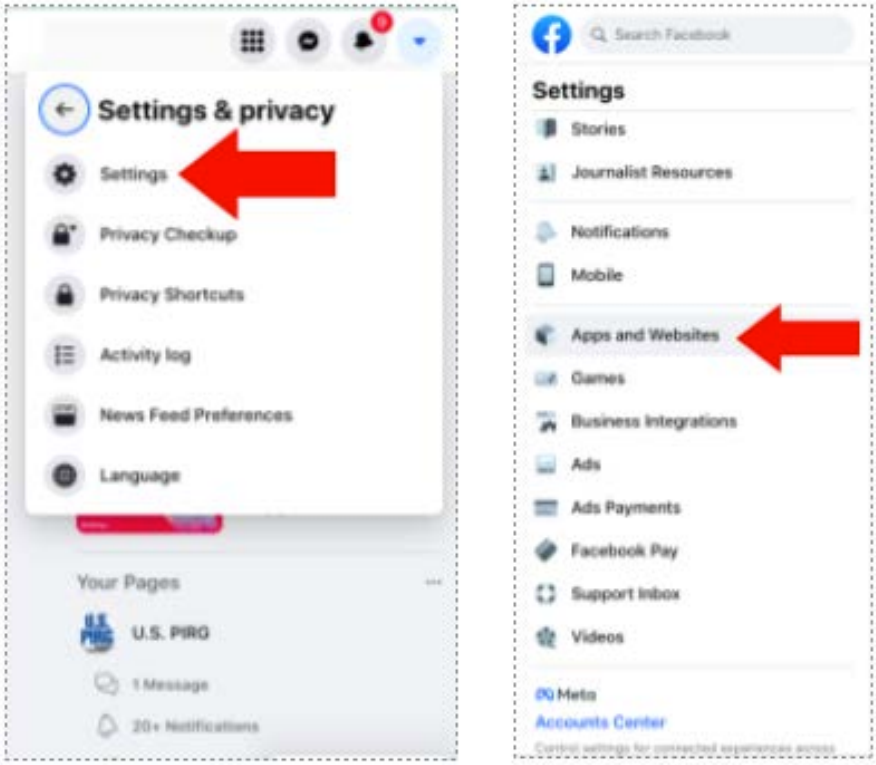
On a computer: Go to Settings → Privacy → "Do you want search engines outside of Facebook to link to your profile?" → Edit → Unclick the checkbox on the bottom → No.

On the same page, select "Who can look you up using the phone number you provided?" → Only me. Do the same for "Who can look you up using the email address you provided?"



Manage how much access to your Facebook account information that other apps and websites have

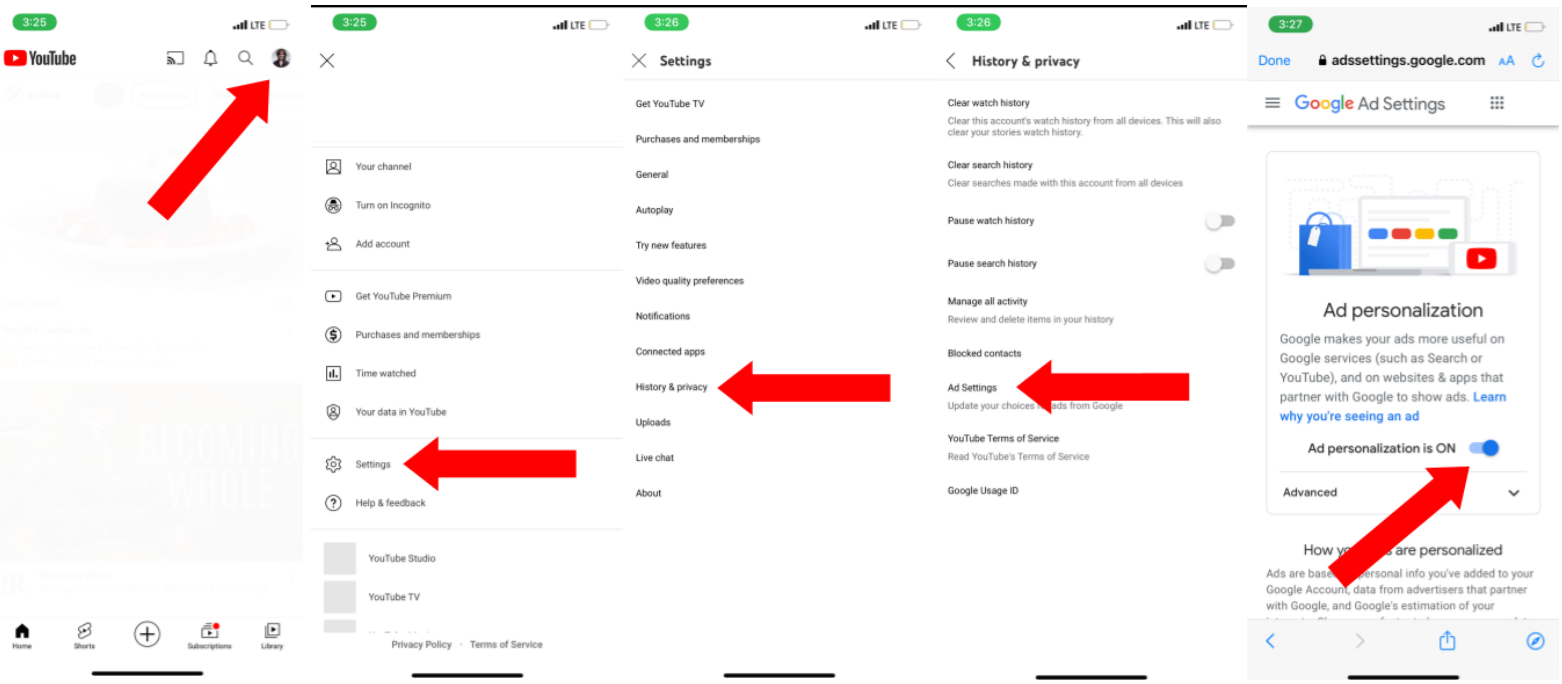
On a computer: Click the down arrow in the top right of the Facebook home page → Settings & Privacy → Settings → Apps and Websites → See More → Click on the box next to the app's name → Remove.



YouTube

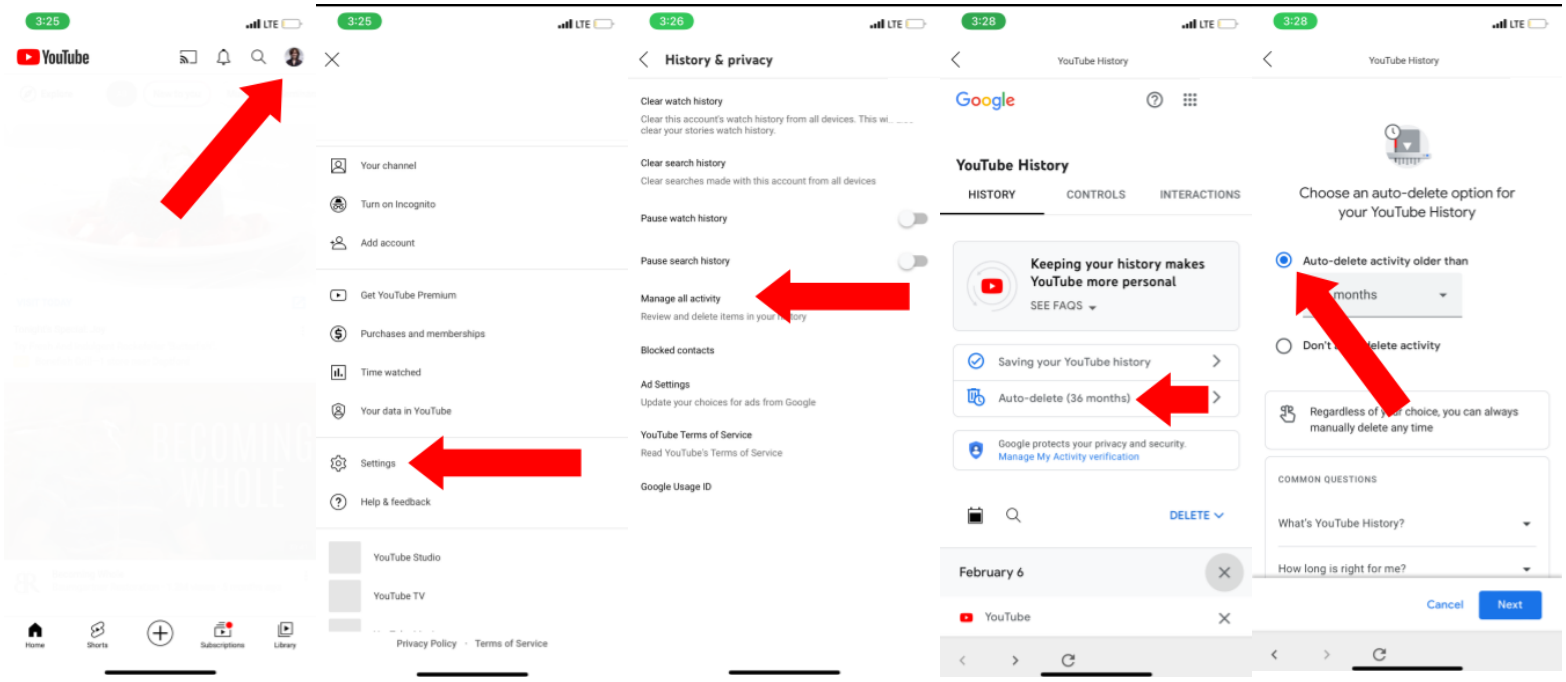
Turn off personalized ads

YouTube works with Google to collect information from the videos that you watch to send you related ads. You can turn off personalized ads in the Youtube app. Click on your profile picture (if you don't have a photo uploaded, it will just be your initial) in the top right corner → Settings → History & privacy (or Privacy on a computer) → Ad settings. This will take you to the web version of Google. From here, you can turn off Ad personalization. You can also scroll down and see how your ads are personalized, including demographic information that Google has collected about you like your age, as well as areas that it thinks you're interested in. If you don't want to turn off personalized ads entirely, you can control the type of content that your personalized ads are about.



Set your Youtube history to automatically delete

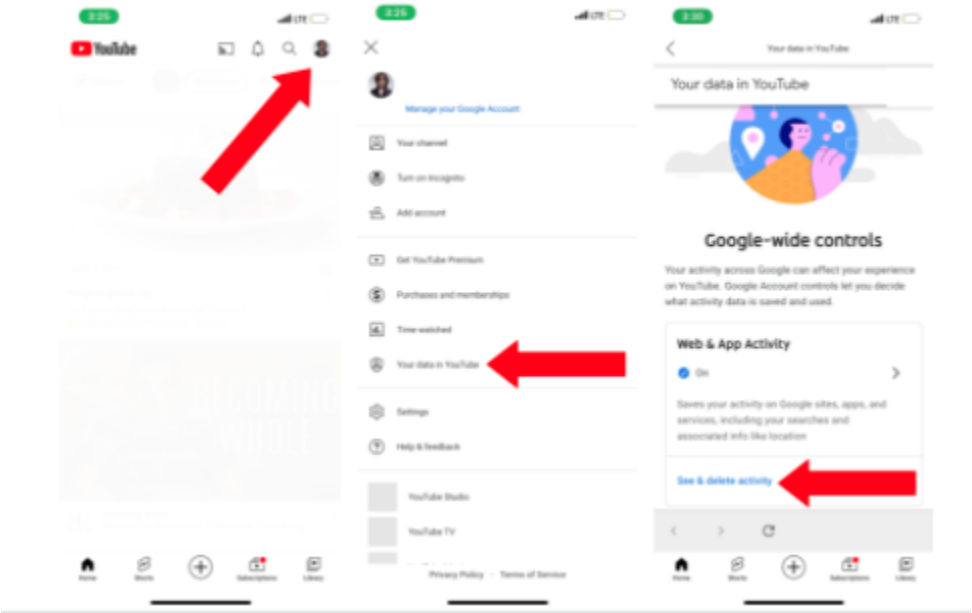
In the YouTube app, click on your profile picture in the top right corner → Settings → History & privacy → Manage all activity → Controls. From here you can turn YouTube History off completely, or under the subsettings you can change whether the videos you watch or the things you search for on YouTube are included in your YouTube History. You can also choose an Auto-delete option that will delete any YouTube activity history after a period of time that you set.



Don’t let Google track you across different apps

YouTube is part of Google. Google can track your activity across its various apps and platforms, including YouTube. It can even track your location. You can turn this off and see more details about the information that Google has collected about you through the Google settings that you can access through YouTube.

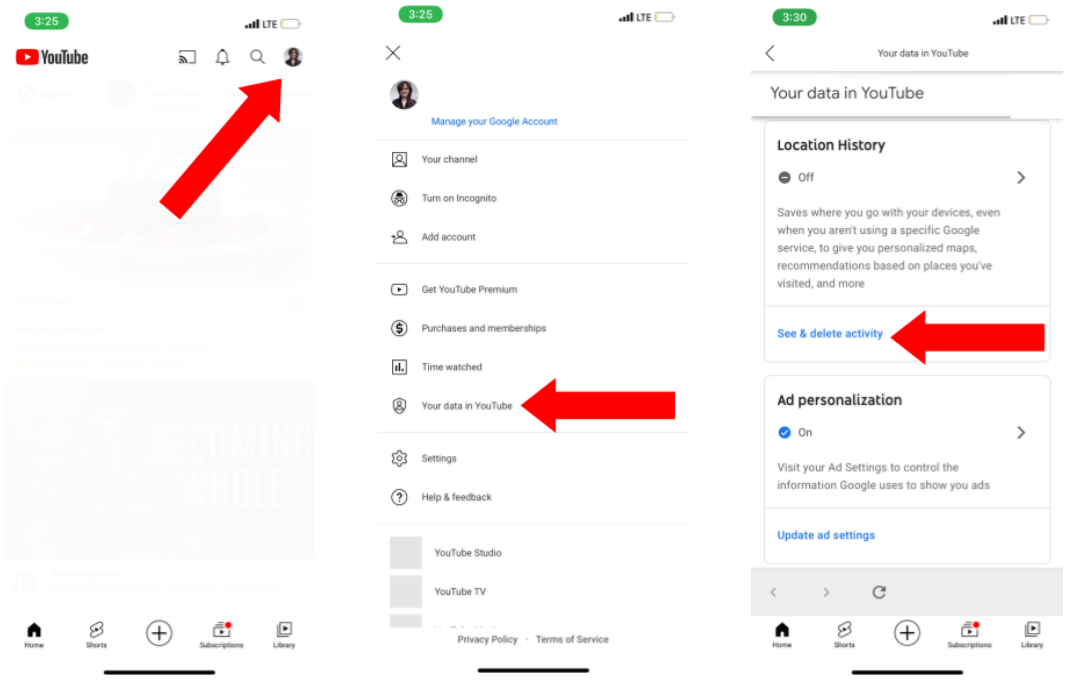
In the YouTube app, click on your profile picture in the top right corner → Your data in YouTube → scroll down to find the Google-wide controls → Web & App Activity → Switch the toggle off. From here you can also see and delete any information that YouTube or Google have collected from other apps.



Don’t give Google access to your location

If you have YouTube on your phone, Google can track your location even when you’re not using a Google app like YouTube. You can turn this off in the Google-wied controls that you can access through YouTube.

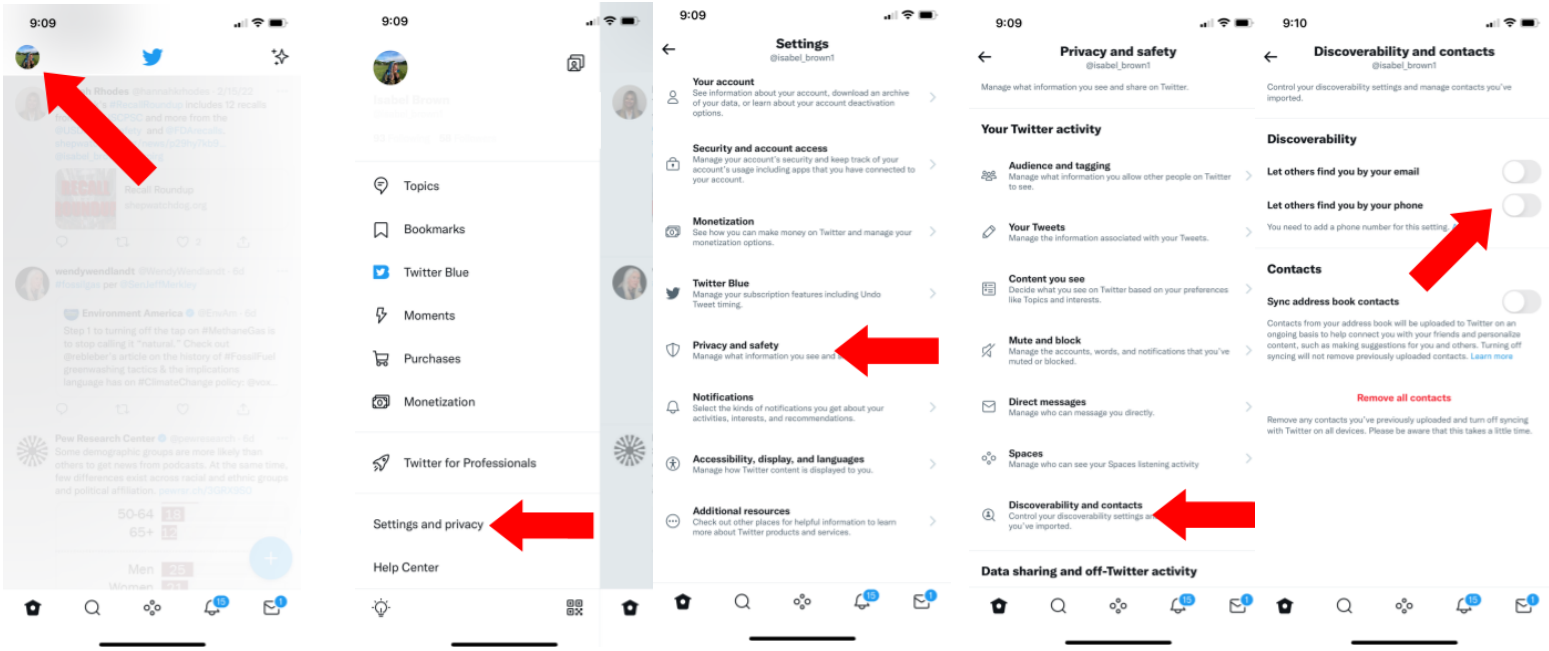
In the YouTube app, click on your profile picture in the top right corner → Your data in YouTube → scroll down to find the Google-wide controls → Location History → Switch the toggle off. From here you can also see and delete any location information that YouTube or Google have collected.



Twitter

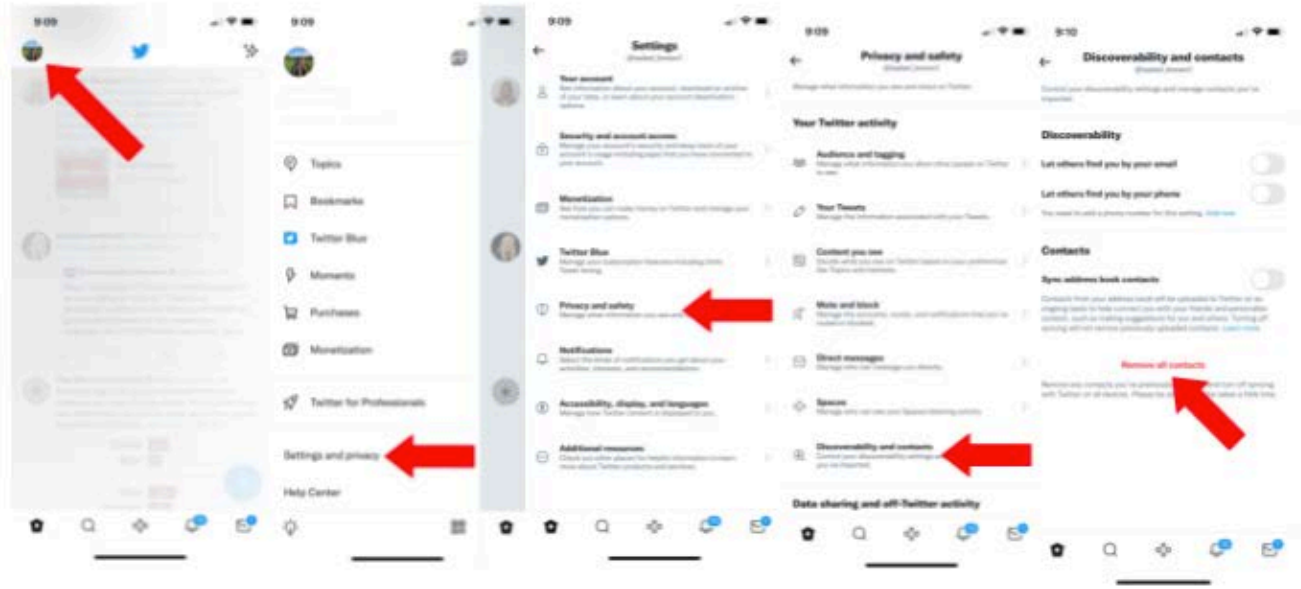
Control how easy it is to find your account

In the Twitter app, click on your profile picture in the top left corner → scroll down to Settings and privacy → Privacy and safety → Under “Your Twitter activity” → Discoverability and contacts. From here you can turn off whether you want people to be able to find you using your phone number or email.



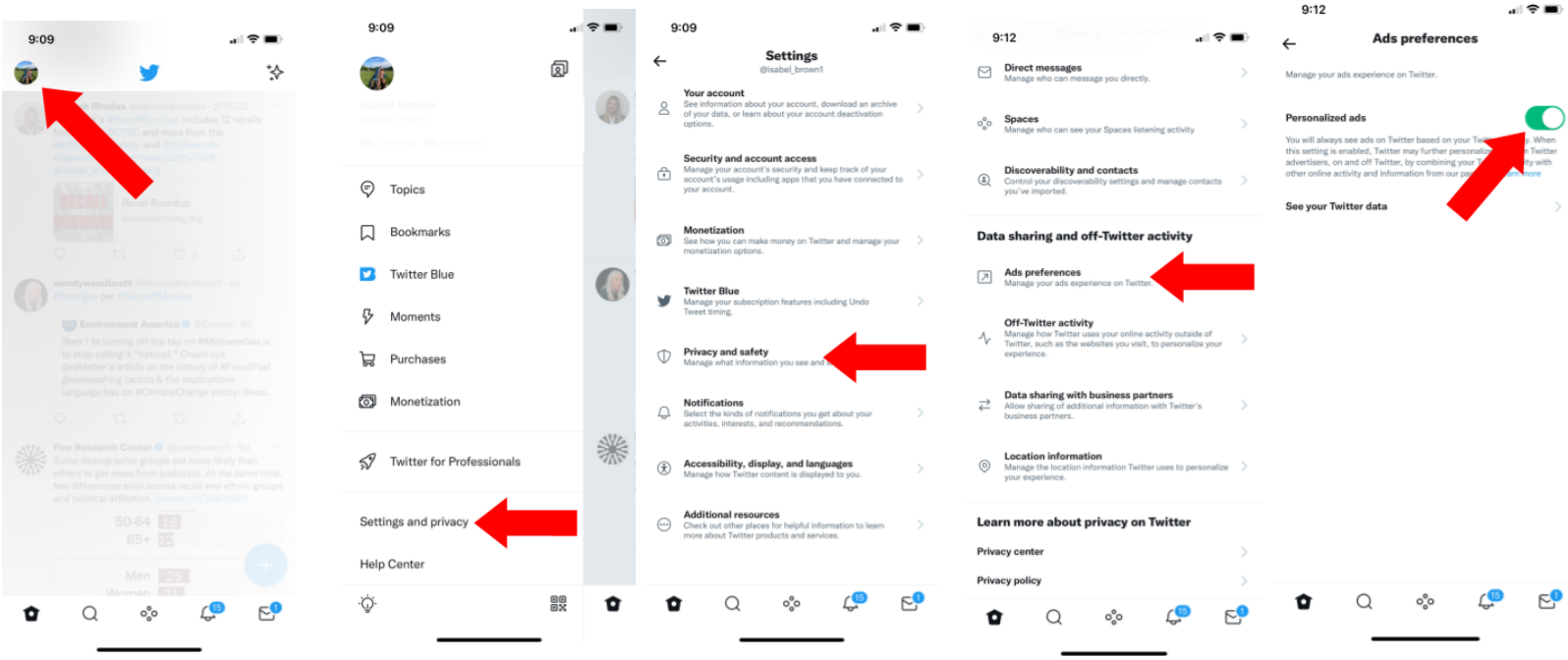
Don’t give Twitter access to your contacts if you don’t want it to

In the Twitter app, click on your profile picture in the top left corner → scroll down to Settings and privacy → Privacy and safety → Under “Your Twitter activity” → Discoverability and contacts. From here, you can also turn off whether your contacts are synced to Twitter, and you can Remove all contacts.



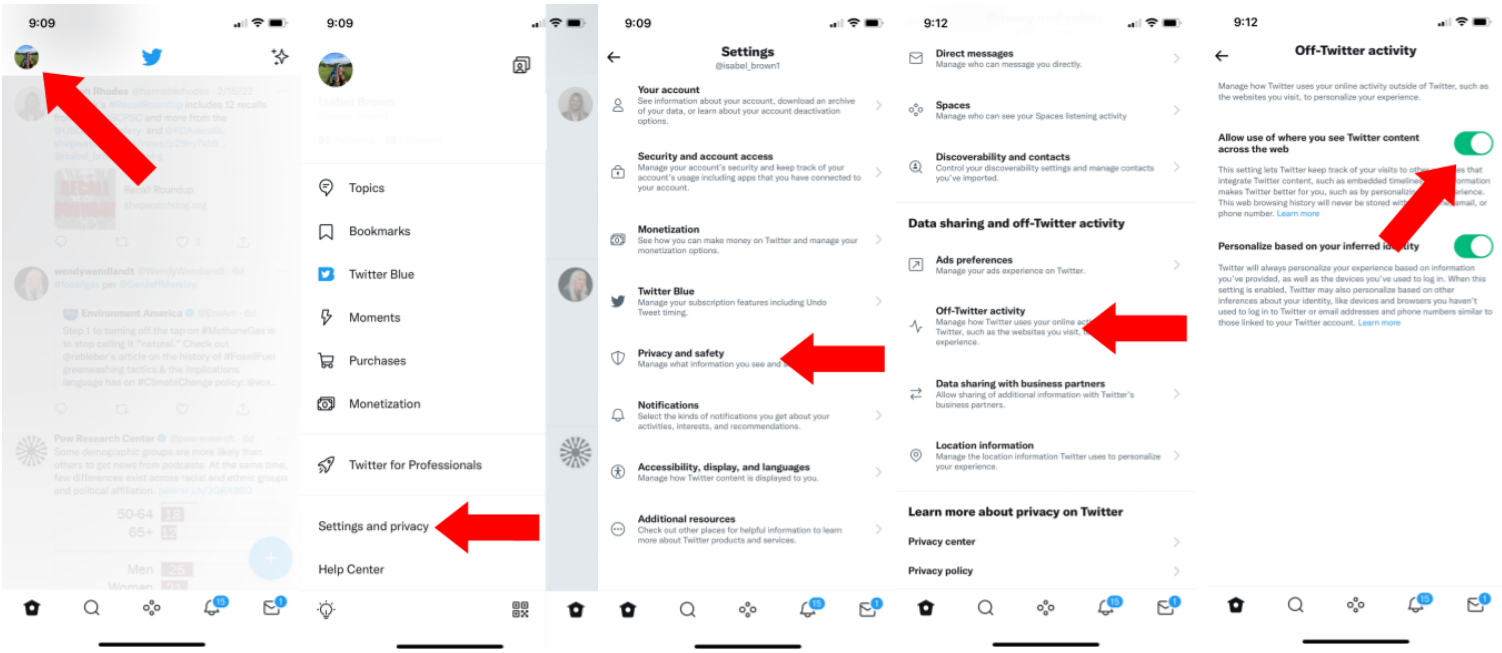
Turn off personalized ads

In the Twitter app, click on your profile picture in the top left corner → scroll down to Settings and privacy → Privacy and safety → Under “Data sharing and off-Twitter activity” → Ads preferences → Turn Personalized ads off.



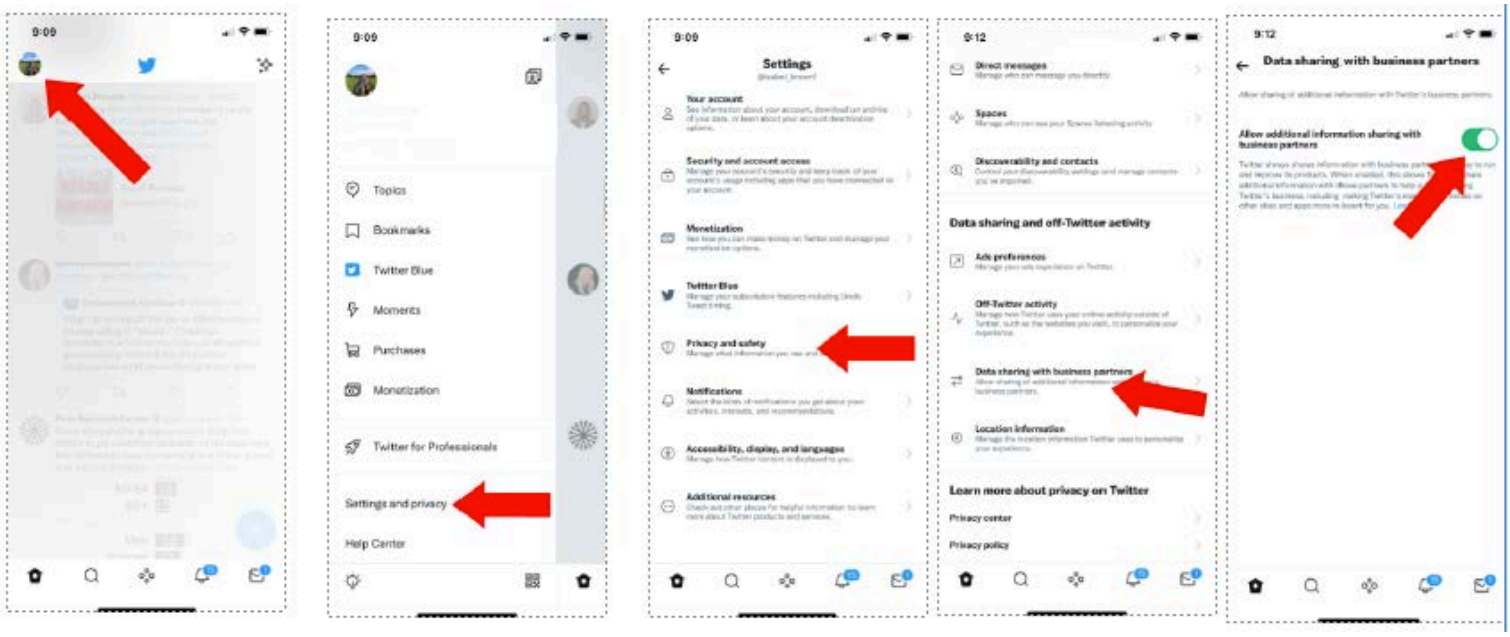
Don’t let Twitter track you across the web

In the Twitter app, click on your profile picture in the top left corner → scroll down to Settings and privacy → Privacy and safety → Under “Data sharing and off-Twitter activity” → Off-Twitter activity → turn off “Allow use of where you see Twitter content across the web” to keep Twitter from tracking your activity on websites that integrate with Twitter. Under Off-Twitter activity, you can also turn off “Personalize based on your inferred identity” to control whether Twitter gathers information about the browsers or devices you use to log in to infer things about your identity.



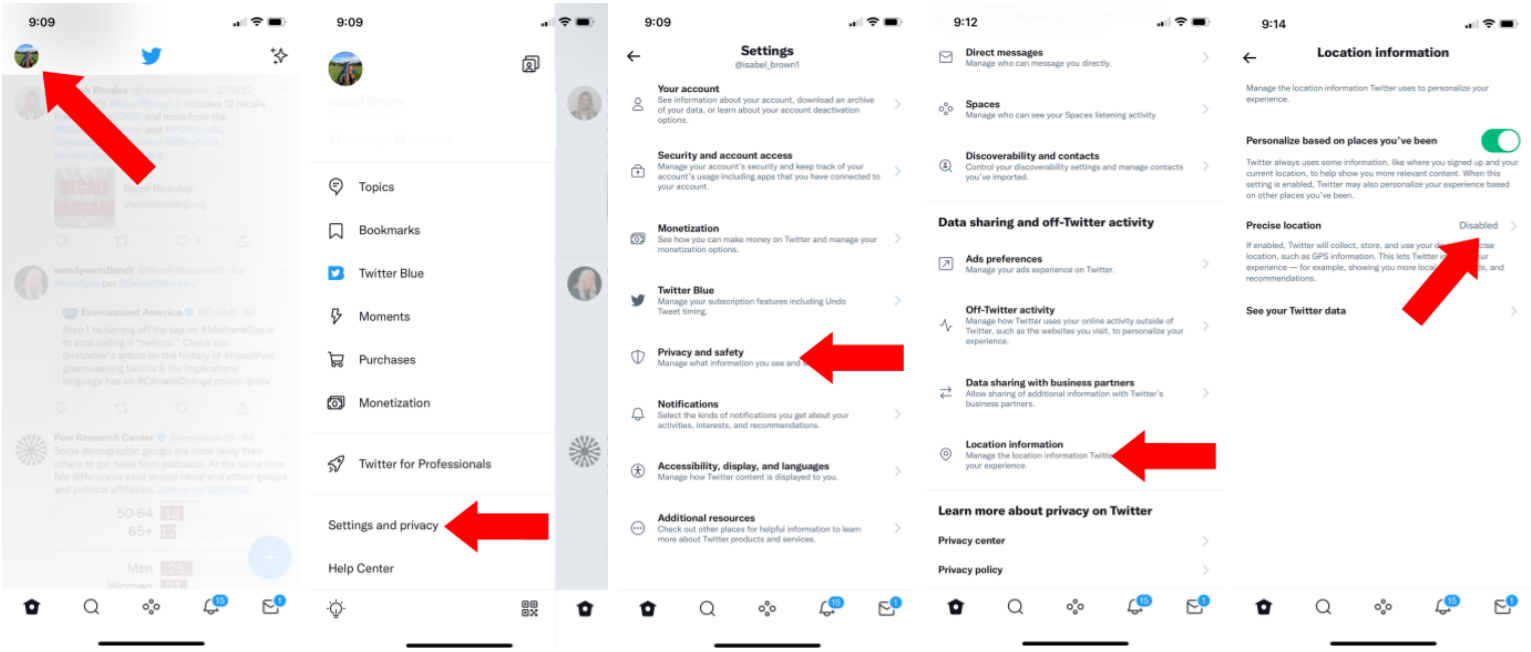
Don’t let Twitter share your information with other companies

In the Twitter app, click on your profile picture in the top left corner → scroll down to Settings and privacy → Privacy and safety → Under “Data sharing and off-Twitter activity” → Data sharing with business partners → Turn off “Allow additional information sharing with business partners”



Don’t give Twitter access to your location

You can do this from the settings on your phone or device, but you can also do this from within the Twitter app. In the Twitter app, click on your profile picture in the top left corner → scroll down to Settings and privacy → Privacy and safety → Under “Data sharing and off-Twitter activity” → Location information → Precise location → Turn off Precise location. From here, you can also turn off “Personalize based on places you’ve been” if you don’t want Twitter to send you any content tailored to your location.

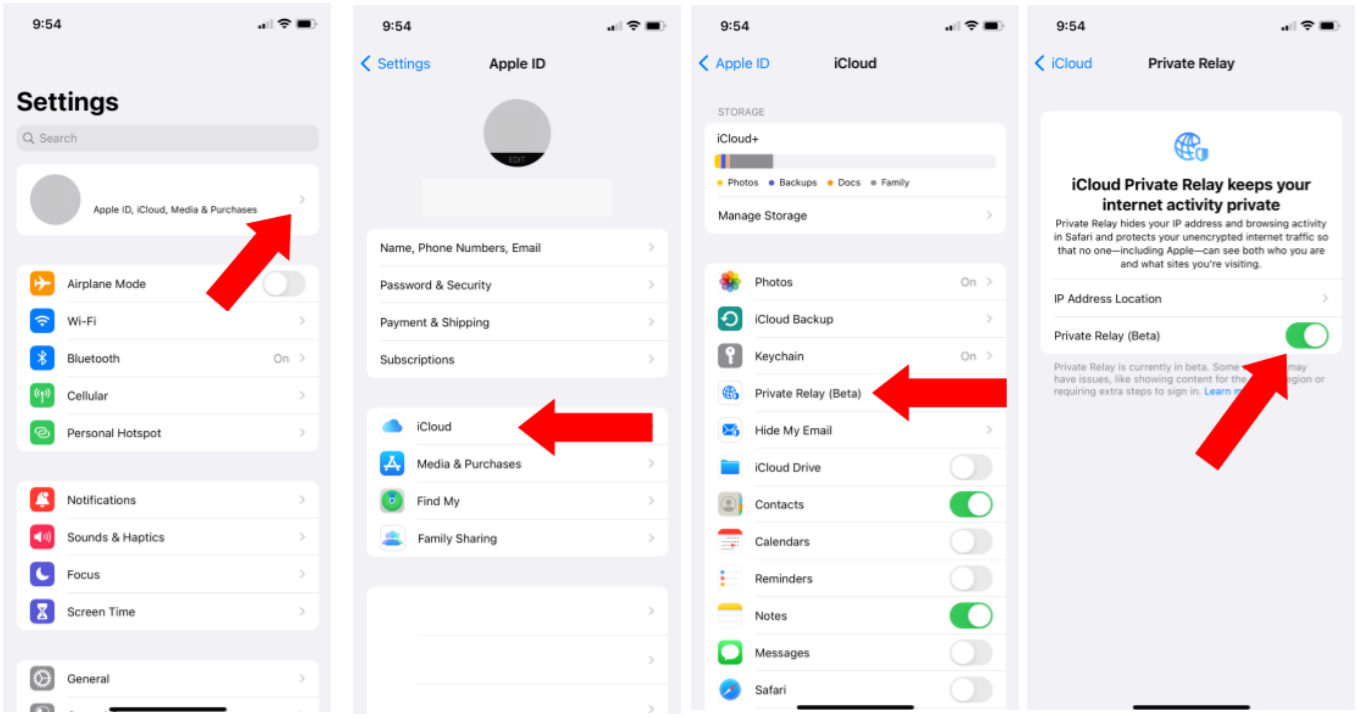


How to set up security preferences on your device

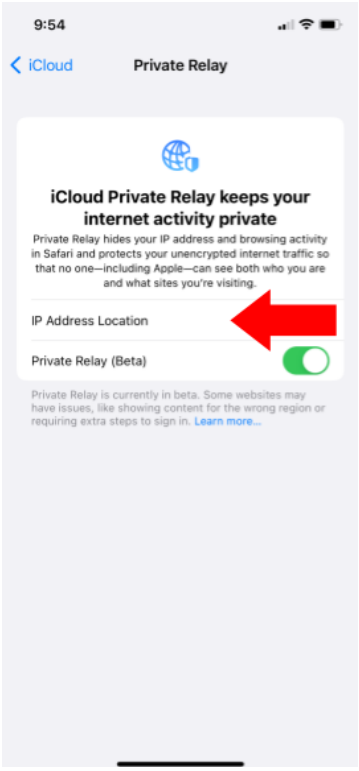
Apple devices

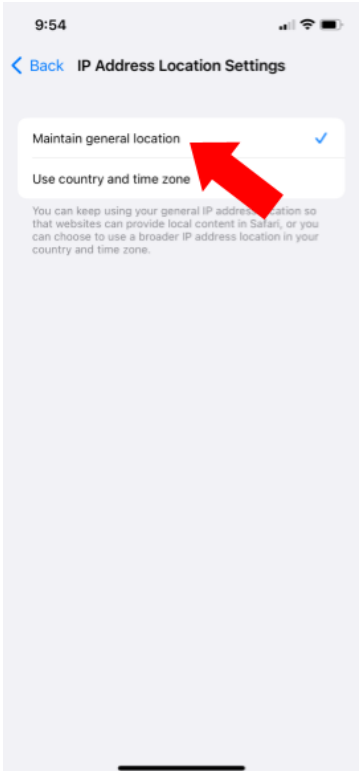
With iCloud+, Apple added Private Relay to protect your IP address from being tracked to see your online activity or your location. This means your Safari and unencrypted internet traffic will be protected from being tracked by Apple and anyone else. Private Relay is still in its Beta stage, so some websites may have issues knowing what region you're in or may ask for extra steps to sign in.

On an iPhone, open Settings → Click your name at the top where it says "Apple ID, iCloud, Media & Purchases → iCloud → Private Relay → Switch the toggle on.



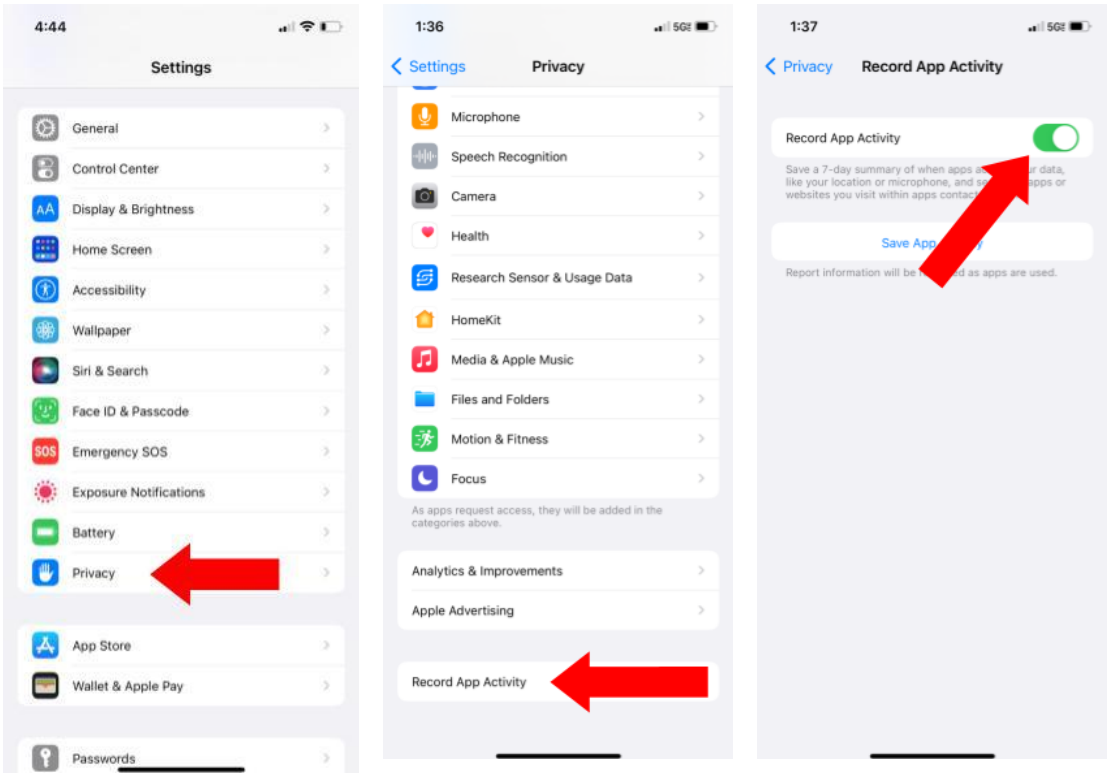
You can also control whether your IP address is linked to your location, or if you want Apple to use your country and timezone instead to have a less precise idea of where you are.





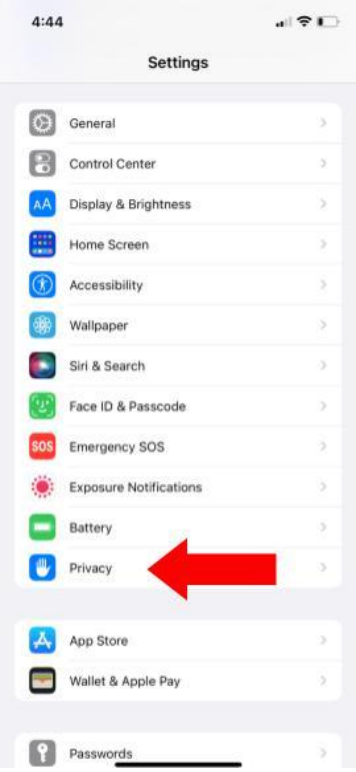
Use App Privacy Report to track what permissions you give each app, so you can decide how much information those apps actually need. You can get a weekly summary about apps that are accessing your information

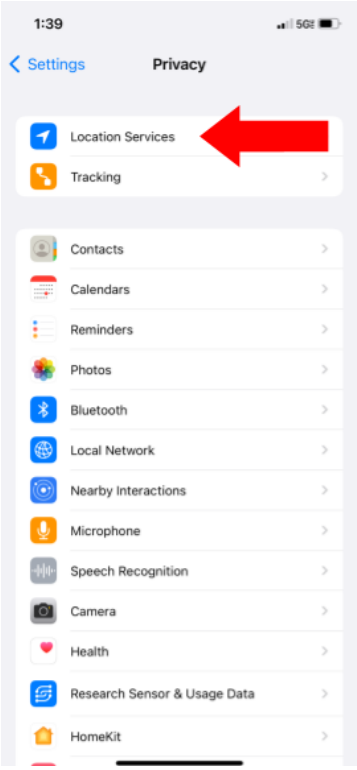
On an iPhone, open Settings → Privacy → scroll to the bottom, click Record App Activity → Turn on Record App Activity. You may also see an option to view your “App Privacy Report”. This will give you a summary of how your apps have been accessing your information.



Change or restrict which apps have access to your phone's location

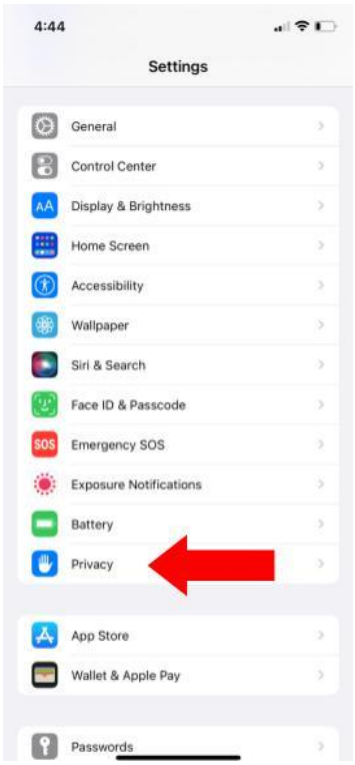
On an iPhone: Go to the phone's Settings → Privacy → Location Services → Click on an app → Click "Never" or "While Using the App."

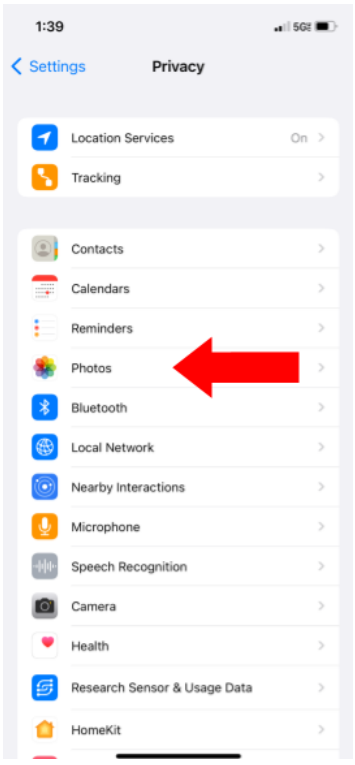


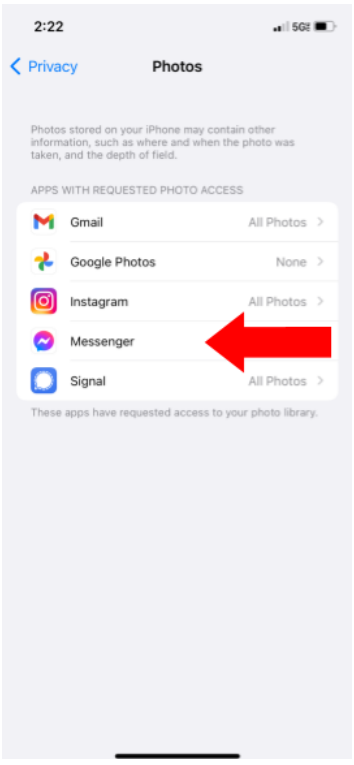


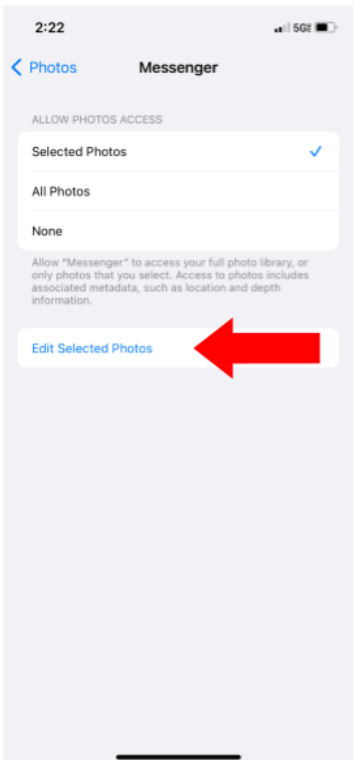
You can change which photos an app has access to, rather than granting access to your entire photo library

On an iPhone: Go to the phone's Settings → Privacy → Photos → Choose an app → Click Selected Photos → Edit Selected Photos → tap to choose the photos → Done.



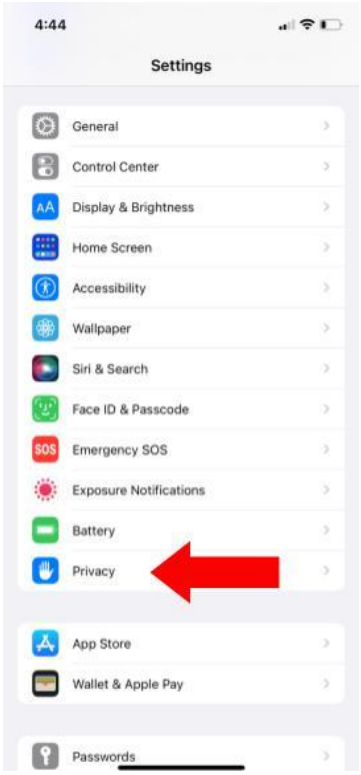


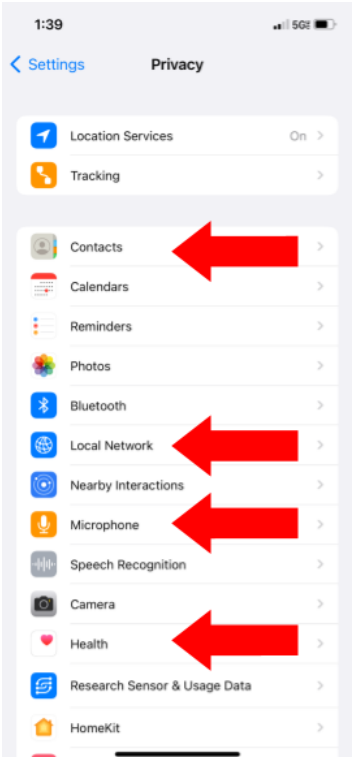




From your iPhone's privacy settings, you can also change whether an app has access to your camera, microphone, health app information, contacts and local internet network.

On an iPhone: Go to the phone's Settings → Privacy → choose the app you want to change access to, like Microphone or Camera → Click on a specific app to change its access to that information.





Disable cross-app tracking. On Apple devices, it's mandatory that an app get your consent before tracking you on other apps or websites.

To stop tracking for all apps, go to Settings on your phone → Privacy → Tracking → Turn off "Allow Apps to Request to Track."

If you want to allow an app to track you, go to Settings → Privacy → Tracking Settings, and from there you can turn on or off whether each app requests permission to track your activity.