INSTAGRAM

- **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.
- **Don't** use geo-location tags — Geo-tags that give your location pose a personal security risk. Although Instagram deletes metadata (including geo-tags) from photos during uploading, disabling them on your devices is good general safety practice.
- **Don't** establish connections with people you do not know. Understand that people are not always who they say 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.

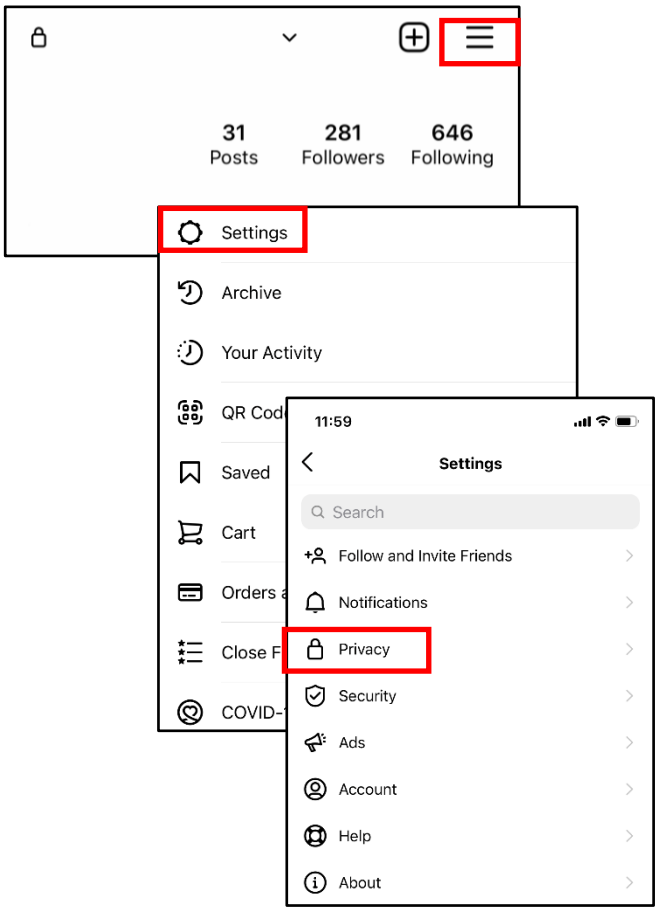
Privacy Settings

It is highly recommended that you set your account to "Private."

Select the "Menu" icon located at the top or the bottom of your screen. Select the first option, "Settings," then select "Privacy."

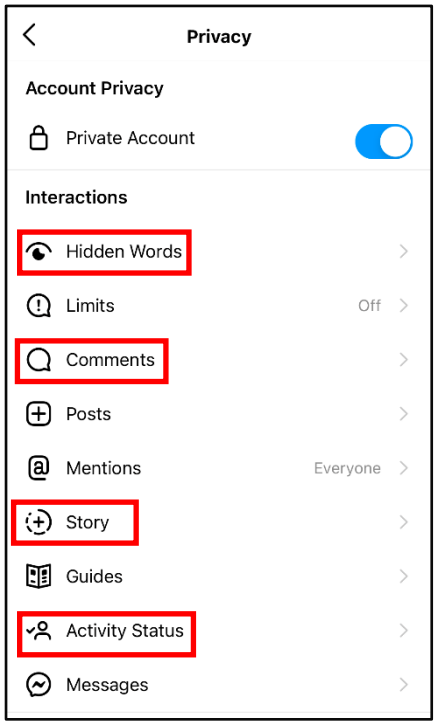
At the top, you'll see the "Account Privacy" section, then toggle "Private Account" to "On." If you are on your computer, the "Settings" tab will be located under your profile icon in the top right.

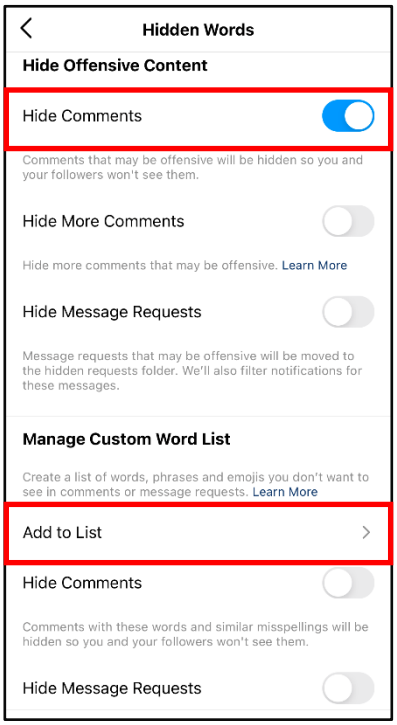
In "Privacy Settings," you can update settings for "Comments," "Tags," "Mentions," etc.



Instagram now provides you with the ability to update your settings on either your mobile device or computer. It is important to note that while some settings are available only on your smart device and a few are only available on your computer, but security settings on mobile devices are typically more robust! Any device used to access Instagram should be checked. * Images are of iPhone (iOS)

INSTAGRAM





Comment Controls

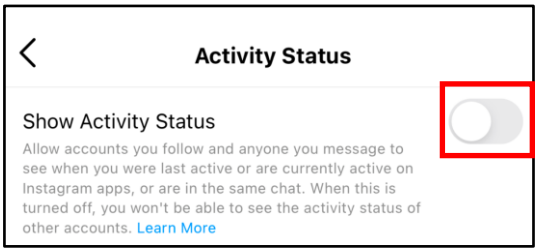
There are many useful features under the "Privacy" tab. First choose "Hidden Words," then adjust the settings under "Hide Offensive Comments."

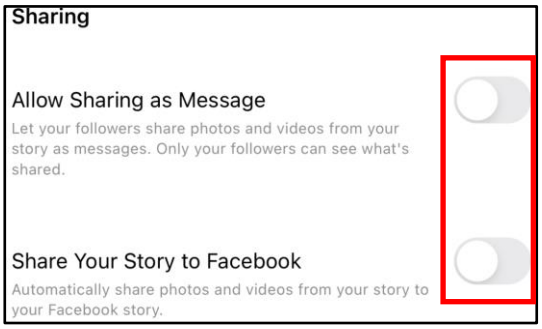
Especially for children's or teen's Instagram accounts, you may want to filter the kinds of feedback allowed on their posts. Here, you can block comments from certain people and filter out offensive comments including specific words you designate yourself.

Sharing and Activity Status

You will also see "Activity Status." This function allows users to see when you are active on Instagram. If you do not want users to know when you are active you can select "Activity Status" and toggle to "Off."

In "Story," identify the section titled "Sharing," toward the bottom of the page. Here you will be able to turn off the "Allow Sharing as Message" function, which allows others to share stories that you have posted. It is also recommended that you take a second to ensure the "Share Your Story to Facebook" function is "Off."



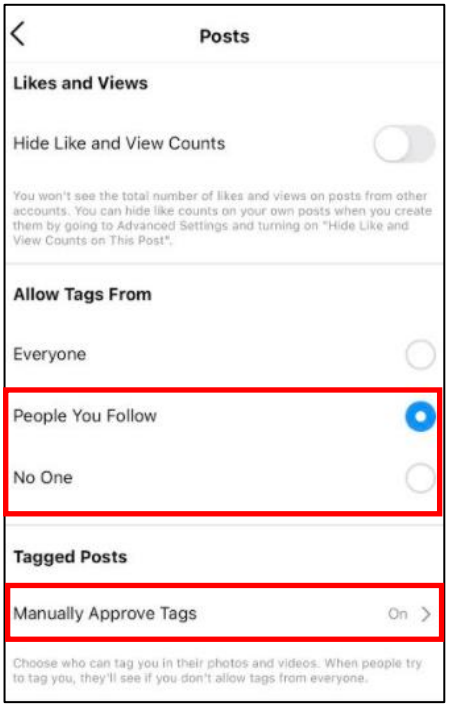


87% of Instagram users are from outside of the US. Therefore, it is extremely important to vet your followers before you trust them with your profile.

INSTAGRAM

Tagging

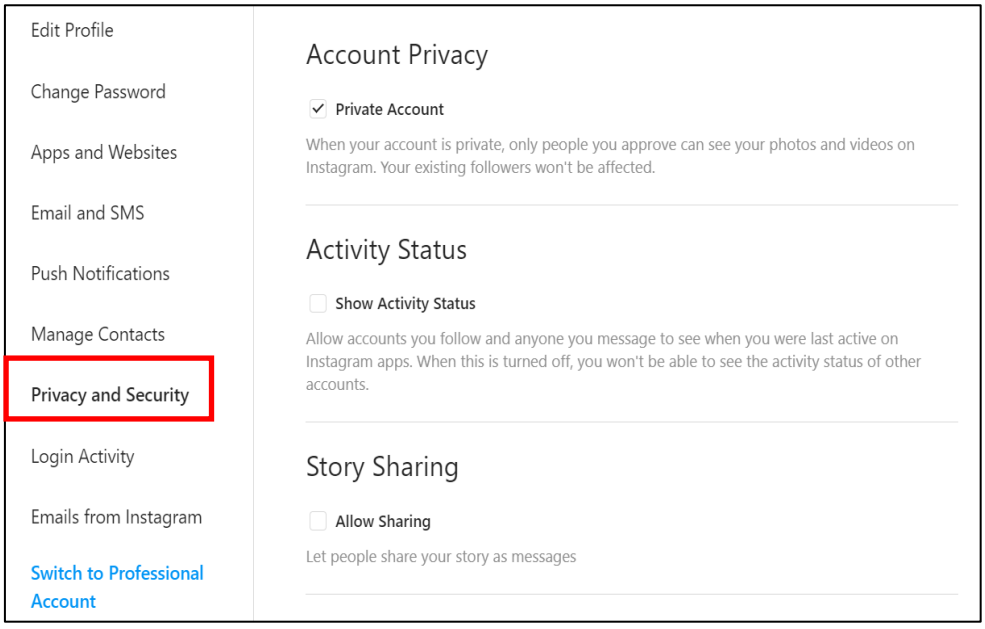
Next, you want to make sure you are in full control of pictures of you that are online - for this, review the “Tags” menu. From the “Privacy” menu, select “Posts.” For best security, identify “Allow Tags From” and select “No One,” which will allow no one to tag you in their photos. Alternatively, choose “People You Follow.” Also, under “Tagged Posts,” ensure that “Manually Approve Tags” is set to “On,” or select this option and toggle it “On.”



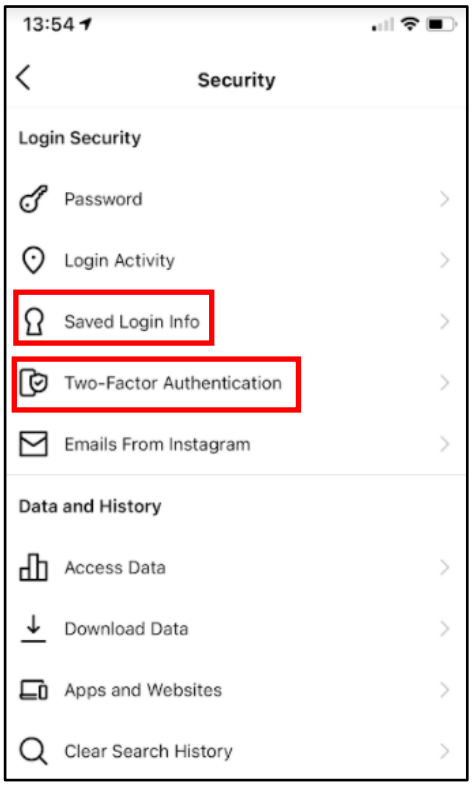
Additional Privacy Setting Considerations

The remaining items under the “Privacy” tab allow you to restrict, block, and mute Instagram accounts as you see fit.

Once you have adjusted the “Privacy” settings on your mobile device, it is a good idea to check them on your computer application. Ensure your preferences have been updated and any unique settings reviewed and set accordingly.



INSTAGRAM

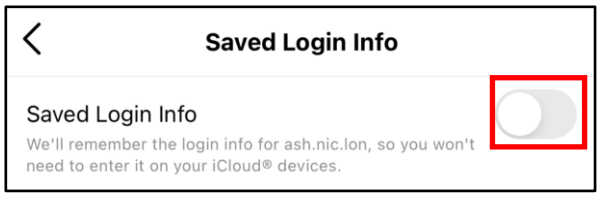


Security Settings

With your “Privacy” secured, the next important feature to address is “Security” on your Instagram account.

Saved Login Information

Back under “Settings,” select “Security,” located under the “Privacy” section you just completed. First, select “Saved Login Info,” then ensure the toggle is set to “Off.” This way, if someone steals your device, they will not also have instant access to your Instagram account.

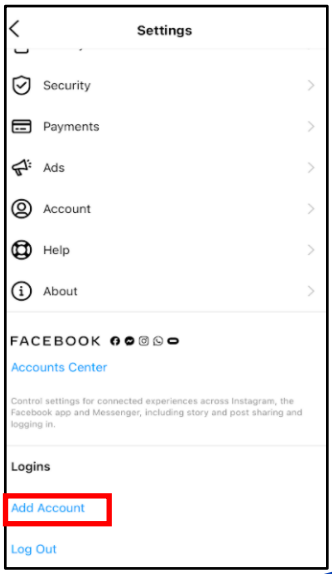


Two-Factor Authentication

“Next, under “Security,” select “Two-Factor Authentication.” It is recommended that you choose this function in order to better protect your account. On the following screen, select “Get Started,” then choose your preferred authentication method.

Adding Accounts

There is a function located in “Settings" called “Add Account,” where you can add unlimited additional accounts to your mobile device. For instance, a parent would be able to add a child’s account to theirs as a way of monitoring activity. Depending on the settings of the account, you may be able to access the added account without entering a password.

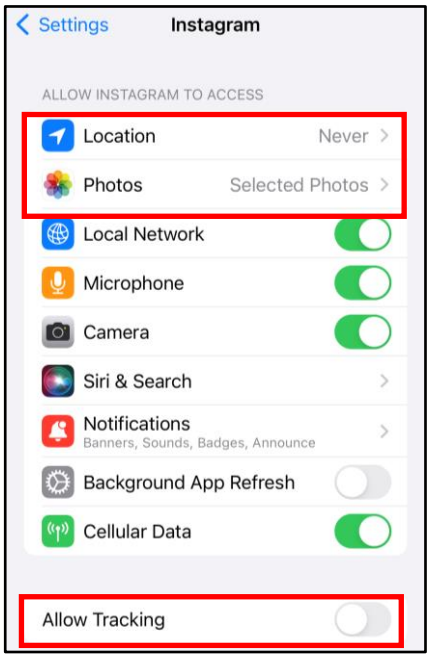


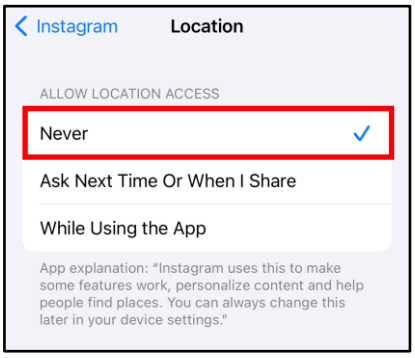
The dangers of the “Add Account” feature are significant for teenagers, who are less inclined to consider security. Only allow others you know and trust to “Add Account.” You should not try to access your account on someone else’s mobile device, and always remember to log out, especially when using a different device.

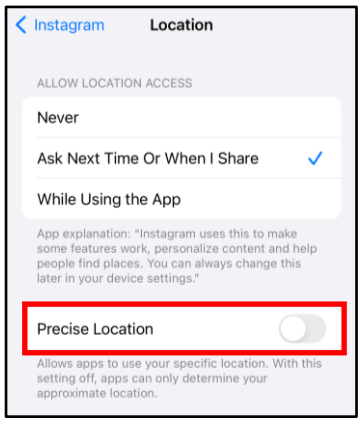
INSTAGRAM

Access to Photos/Location

There is an option in the settings tab to deny Instagram having persistent access to all your photos. It is recommended you only allow Instagram access to the photos/videos on your device(s) at the time you want to upload them. It is also recommended that you turn your "Location" settings to "Never." If not, it is strongly suggested you turn off "Precise Location." "Allow Tracking" should also be turned off, so that you're not being tracked across other apps and websites. (Android automatically defaults to turned off.)

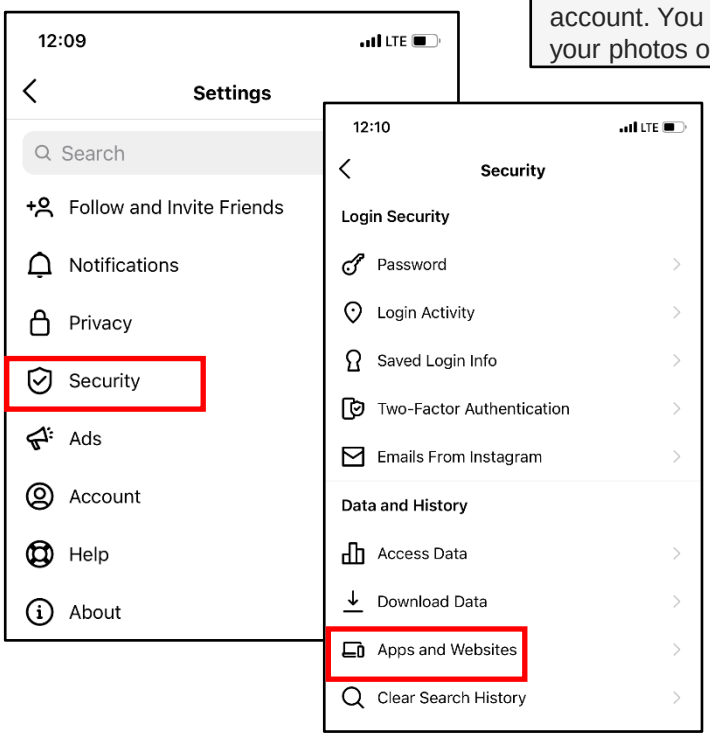


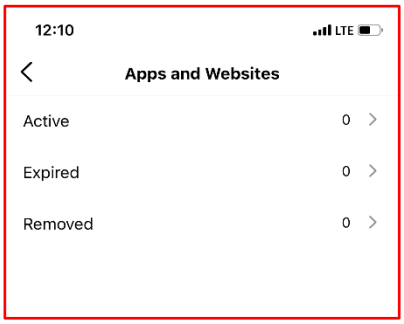




Google Photos

If you don't want your Instagram photos or videos to appear on Google, It is recommended you revoke access to third-party apps and websites and set your account to private. It may take time for these sites and Google to re-index and remove the images, even if you delete your account. You can also contact the app that's displaying your photos on Google to expedite the process.





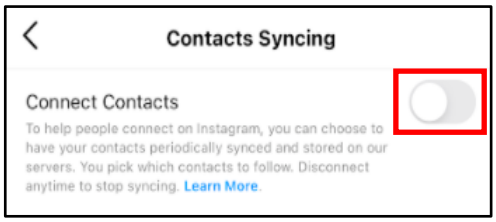
If your account is secured according to the recommendations in this card, it will show zero apps and websites registered.

SAFEGUARD *Digital Identity Protection Toolkit*

INSTAGRAM

Contact Syncing

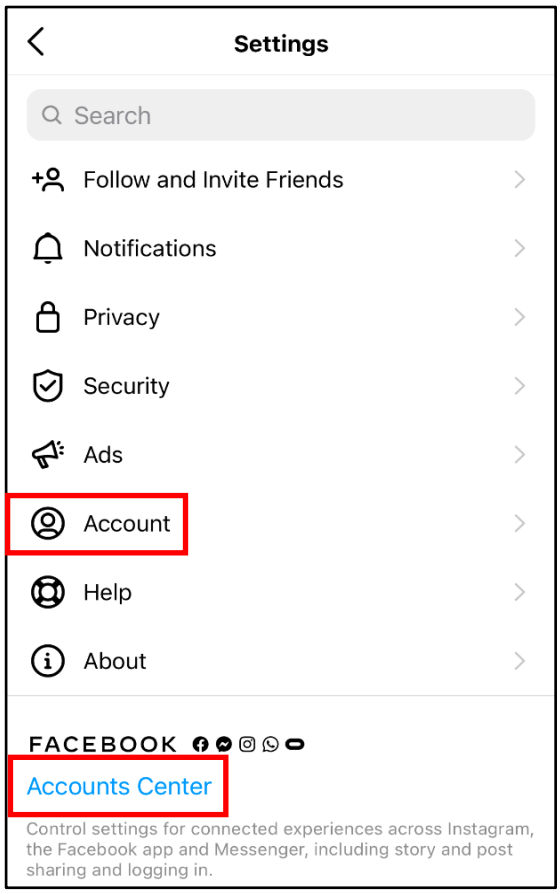
Back in the “Settings” menu, select “Account” then “Contacts Syncing.” It is recommended that you deny Instagram permission to upload your contacts by turning “Off” the “Connect Contacts” option.



Additional Account Setting Considerations

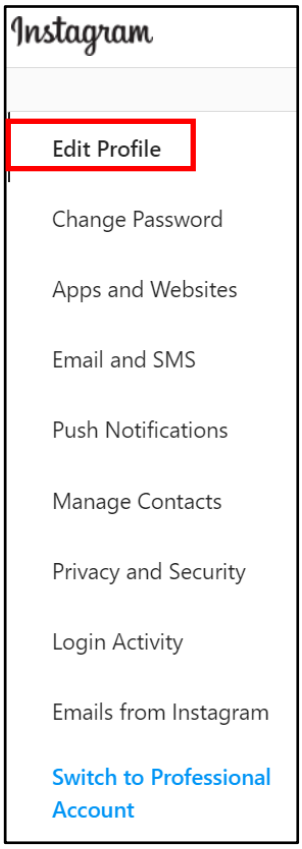
Another option in the “Accounts” tab is the “Sharing to Other Apps” (or Linked Accounts) feature. Here you want to make sure you have not linked any of your social media accounts to Instagram. You can also use the “Accounts Center” to access the “Sharing to other Apps” setting.

“Payments” feature allows you to add a payment method to your Instagram account for purchases made in the application. It is not advisable to store credit card or any other payment information on your account.



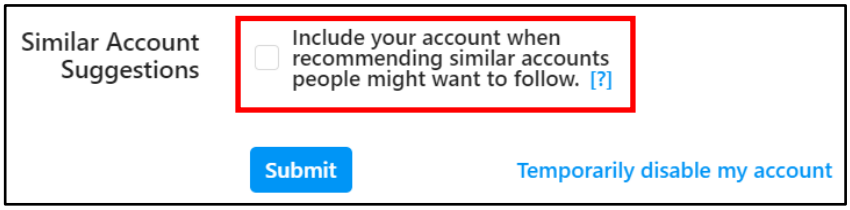
Instagram allows you to have more than one account loaded at a time. Talk to your kids about sharing their usernames and passwords with their friends.

INSTAGRAM



Discoverability

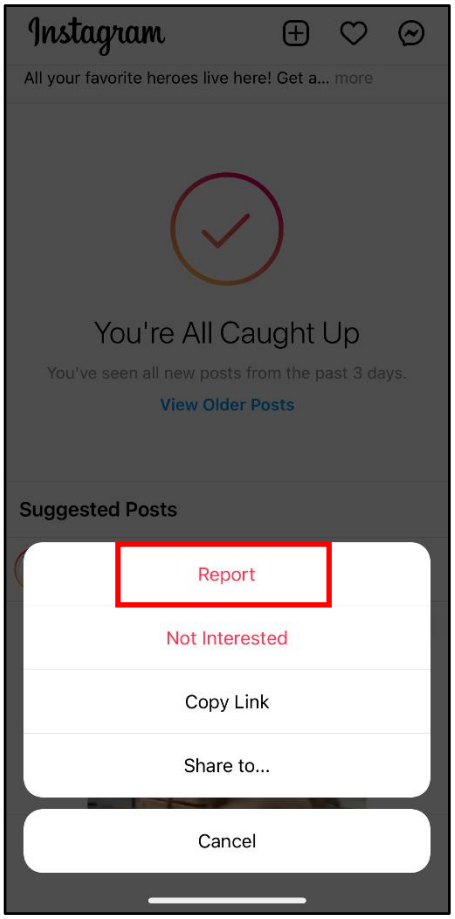
Instagram (personal computer/web-based version) has a feature that allows it to push your profile to other users as "suggested users to follow." It is recommended you disable this feature. First, select the "Profile" icon, then select the "Edit Profile" button. Once there, scroll to the bottom of the page. *This feature can only be locked down on your computer application.*



Report, Mute, or Unfollow

Instagram allows you to report or remove from your feed any offensive post you come across.

Simply select the menu button at the top right corner of the post and select from the drop-down menu which option best applies to that post. You have options to "Report" the offensive post, "Mute" the account that posted it for a select period of time, or "Unfollow" the person who posted it. When you report a post, Instagram will ask you for more information as to why you are reporting it, and then offer suggestions to improve your Instagram experience.

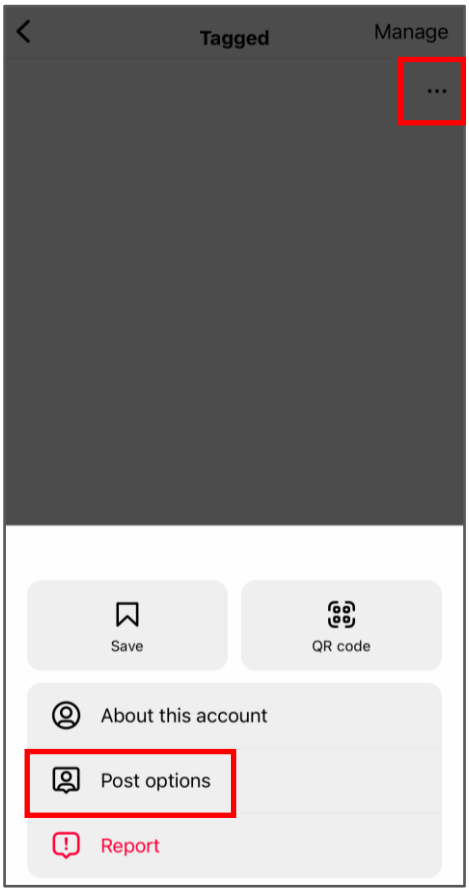


If someone is impersonating you on Instagram…
Go to https://help.instagram.com/, then go to "Privacy and Safety Center," "Report Something," and finally select "Impersonation Accounts."

INSTAGRAM

Removing Profile from Tagged Content

Removing unwanted tagged photos/posts is important. If you have a profile that is "Private," you are on the right track to controlling your online image. Understand that even if your profile is private, if you tag or comment on a post from a profile that is public, your tag or comment will be viewable to all.



To remove your profile from a tagged post, go back to your "Profile" icon and select the "Tagged" icon. Next, select the post you are tagged in that you wish to un-tag yourself from. Find and select the menu at the bottom of the post (shown to the left of the page by a red box,) then select "Post Options." Next, you can "Remove Me From Post" simply by selecting the link highlighted here in red.
This may not be available on all devices or the web-based version.

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

INSTAGRAM

Open Source Tracking

A significant reason for locking down your Instagram Account is due to projects like “The Follower.” The follower is a project by Dries Depoorter that uses open source cameras to track/find when and where you took an Instagram photo. The process he uses to do this is to first find open source cameras that are available to the general public, and record them with a software for a designated period of time. He then chooses locations on Instagram, like Wrigley field, that people have posted to Instagram. He then uses AI software to compare the Instagram photos with the recorded footage to see when and where you were there.