

If you are using social media sites such as Facebook or Twitter, there are some simple steps you can take to manage your reputation and protect your identity. Even if you are not using these sites, it is important to manage your digital footprint and identify any false or misleading information about you online.

In this booklet you will find our top 10 tips for protecting your reputation online. We also provide practical guides for setting up Facebook, Twitter, Instagram and mobile devices to help you ensure your information is safe online.

Contents

Top 10 tips for protecting your reputation online . . .	2
Managing your Facebook account	5
Make sure your profile is set to private	5
Only accept friend requests from people you know and trust and learn to block offensive users	8
Report fake profiles	9
Delete unused accounts	10
Managing your Twitter account	12
Make sure your profile is set to private	12
Only accept friend requests from people you know and trust and learn to block offensive users	12
Report fake profiles	13
Delete unused accounts	15
Managing your LinkedIn account	16
Make sure your profile is set to private	16
Limiting who can view your activity feed and connections	16
Limiting certain people from communicating with you	17
Protecting your account information	17
Delete your account	17
Managing your Instagram account	18
Make sure your profile is set to private	18
Only accept friend requests from people you know and trust and learn to block offensive users	19
Report fake profiles	19
Managing your Snapchat account	20
Does an image really delete on Snapchat?	20
Managing your privacy settings	20
Delete your account	21
Protecting your mobile devices	22
Disable geotagging for applications and cameras on your mobile device	22
iPhone	22
Samsung Galaxy S Series	23
To turn off Geo-tagging on Android phones	24
To turn off GPS functionality on Android phones	24

Top 10 tips for protecting your reputation online



Tip 1: Make sure your profile is set to private

To manage your privacy on social media such as Facebook, Twitter or Instagram, you have the option of making your profile either private or publicly accessible. You can check this through the Settings option on your profile and/or accounts.



Tip 2: Only accept friend requests from people you know and trust and learn to block offensive users

People aren't always who they say they are. Before you accept a friend request from someone, ensure that you know who they are offline and that you trust them to protect the personal information you share on your profile. Just because you share a mutual friend, doesn't mean you actually know the person.

If people harass or threaten you online, you can block them from communicating with you.



Tip 3: Regularly search for yourself online

Regularly search for your name, email addresses and any usernames you operate in online search engines such as Google, Bing or Yahoo. You can also look up your name using www.pipl.com which brings back many social media results. Also try searching your name using the search functions on Facebook and Twitter.

These searches will allow you to identify fake profiles and/or accounts, as well as gain a better understanding of what your digital footprint looks like.



Tip 4: Report fake profiles

Fake accounts or accounts impersonating others on Facebook, Twitter and Instagram can be reported. Forms can be found on these social media sites which you can complete to report these incidences.



Tip 5: Do not join offensive online groups or 'like' offensive online content

Depending on your privacy settings, the groups which you belong to on Facebook can be publicly available information. Your name is then linked with the objectionable content shared on those Facebook groups, which you have no control over.



Tip 6: Do not post inappropriate content online

Think before you post any content online as it is impossible to permanently delete digital content once it has been shared.



Tip 7: Delete unused accounts

If you are no longer using your online accounts, it is best to deactivate or delete them.

Before you delete your accounts:

- Type your full name into a search engine such as Google or www.pipl.com to find out which social media accounts you have. Also try searching your email addresses in these search engines. You may have an old Myspace or Bebo profile which you've forgotten about, but this could still contain personal information or photos of you.
- Make sure you know your log-in details for each account. If you've forgotten which email address you used to start up the account, have a search in your email accounts for Facebook, Bebo, Myspace and Twitter to see which email account is linked to each profile.
- If you have forgotten the password to access your social media accounts, follow the directions in the 'Help' or 'Safety' section of the social media website to find out how to recover a forgotten password.
- Have a look at the photos on your profile in which you're tagged. Photos uploaded by friends will still be available after you've deleted your account. Contact your friends and ask them to remove these photos and, if they do not take them down, you can report the photo to the site on which it appears.

Facebook and Twitter give you the option of downloading a copy of all the information you have on your profile including photos, comments and your wall posts. Before deleting your account, it's a good idea to keep a copy of your information for your own records, but also to make sure you don't lose any of your photos.



Tip 8: Turn off your Bluetooth when not in use and change the name of your device

Bluetooth creates a wireless network between paired devices within a limited range. There are ways in which vulnerabilities in Bluetooth can be exploited, providing access to your address book, calendar, messages, photos and other content on your mobile phone.

To reduce your exposure to this risk, ensure that Bluetooth is disabled or hidden when not in use and that the name of the device is changed to something which doesn't identify you, or the model of the phone.



Tip 9: Disable geotagging on your mobile device

Geotagging is the process whereby location data is added to an image or other content.

When this geotagged material is shared online, it is possible for others to read the metadata and identify the location where that image was taken.

Steps for disabling geotagging or location services for the camera on your smartphone can be found on page 18 of this booklet.

18+ Tip 10: Do not take, accept or forward nude images of someone under the age of 18

Do not generate, accept or forward on any naked images on your phone or online of someone who is under the age of 18 as they may be considered child pornography. By having these images on your phone or computer you could be deemed as having possession of child pornography. Forwarding them onto others could also be considered to be distribution of child pornography. These are serious criminal offences which can carry gaol terms of up to 15 years. You should report these images to your local police.

A conviction of child pornography-related offences can have serious long term consequences including being placed on a sex offenders' register and imprisonment.

Taking and distributing explicit images of people over the age of 18 may also constitute criminal offences. It is important to treat these images as you would their body and have their consent for any action you take.

Managing your Facebook account



Make sure your profile is set to private

To manage your privacy on Facebook, access the privacy settings by clicking on the cog wheel on the upper right-hand side of the page and select **'Privacy Settings'**.

The screenshot shows the Facebook homepage interface. In the top right corner, a settings cog wheel is visible. A dropdown menu is open, showing options: 'Create Page', 'Advertise', 'Privacy Settings', and 'Log Out'. The 'Privacy Settings' option is highlighted with a thick orange border. An orange arrow points from the settings cog wheel to the dropdown menu.

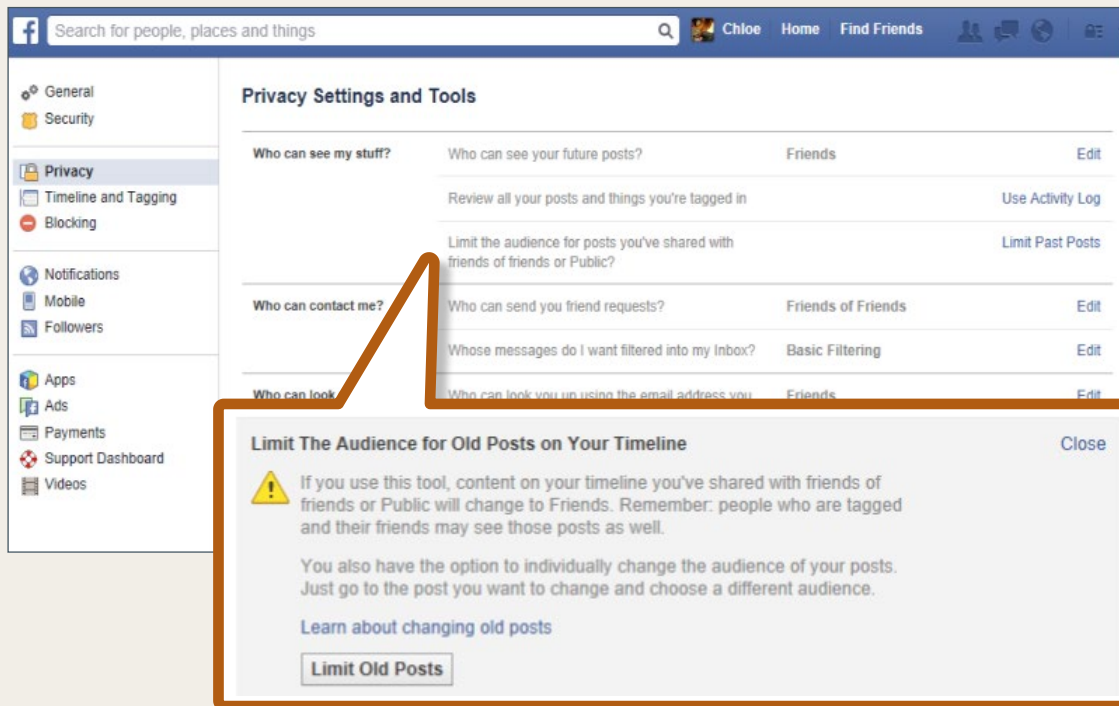
Under the **'Who can see my stuff?'** section, you can manage who is able to access your timeline.

Next to **'Who can see your future posts?'**, click on **'Edit'** to ensure that **'Friends'** is selected.

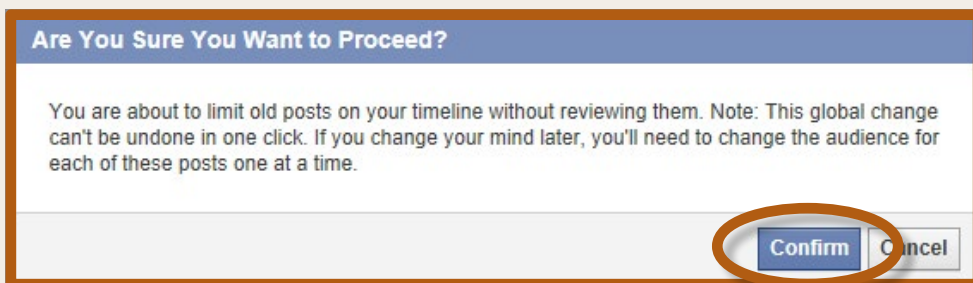
The screenshot shows the Facebook 'Privacy Settings and Tools' page. The left sidebar contains navigation options: General, Security, Privacy (selected), Timeline and Tagging, Blocking, Notifications, Mobile, Followers, Apps, Ads, Payments, and Support Dashboard. The main content area is titled 'Privacy Settings and Tools' and contains a table of settings. The 'Who can see my stuff?' section is highlighted with an orange box.

Section	Setting	Current Value	Action
Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of Friends	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want other search engines to link to your timeline?	Off	Edit

Some of your earlier posts may have been shared more broadly so it is important to ensure these are now only accessible by Friends. Click on **'Limit Past Posts'** next to **'Limit the audience for posts you've shared with friends of friends or Public?'**.



Click on **'Limit Old Posts'** after which a dialog box will appear. Select **'Confirm'** to limit past posts to Friends.



You can manage who can locate your timeline on Facebook under the **'Who can look me up?'** section.

Next to **'Who can look you up using the email address you've provided?'**, click on **'Edit'** and select either **'Friends'** or **'Friends of Friends'**.

The screenshot shows the Facebook 'Privacy Settings and Tools' page. The left sidebar lists categories like General, Security, Privacy, and Notifications. The main content area is titled 'Privacy Settings and Tools' and contains several settings:

- Who can see my stuff?** (Friends) - Edit
- Who can see your future posts?** (Friends) - Edit
- Review all your posts and things you're tagged in - Use Activity Log
- Limit the audience for posts you've shared with friends of friends or Public? - Limit Past Posts
- Who can contact me?** (Friends of Friends) - Edit
- Who can send you friend requests? (Friends of Friends) - Edit
- Whose messages do I want filtered into my inbox? (Basic Filtering) - Edit
- Who can look me up?**
 - Who can look you up using the email address you provided?** (Friends) - Close
 - This applies to people who can't already see your email address.
 - Who can look you up using the phone number you provided? (Friends)
 - Do you want other search engines to link to your timeline? (No)

A callout box with an orange border highlights the 'Who can look me up?' section, showing the 'Who can look you up using the email address you provided?' setting set to 'Friends'.

Click on **'Edit'** next to **'Who can look you up using the phone number you provided?'** and select either **'Friends'** or **'Friends of Friends'**.

The **'Do you want other search engines to link to your timeline?'** option should be set to **'Off'** and can only be switched to **'On'** by sharing your timeline with **Everyone**.



Only accept friend requests from people you know and trust and learn to block offensive users

On Facebook, you can block users by accessing the Privacy Settings page via the lock symbol on the upper right-hand side of the page and selecting 'See More Settings'.

Select 'Blocking' in the left-hand navigation page to list people and/or apps you wish to block.



Manage Blocking

Restricted List When you add friends to your Restricted list they can only see the information and posts that you make public. Facebook does not notify your friends when you add them to your Restricted list. [Edit List](#)

Block users Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Block users

■ Matthew Dawson Unblock

Block app invites Once you block app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request

Block invites from

Block event invites Once you block event invites from someone, you'll automatically ignore future event requests from that friend

Block invites from

Block apps Once you block an app, it can no longer contact you or get non-public information about you through Facebook. [Learn more.](#)

Block apps



Alternatively, you can block people through the Privacy Shortcuts menu by clicking on the padlock icon on the upper right-hand side of the page.

Select 'How do I stop someone from bothering me?' and type the person's name or email address in the space provided.

Privacy Shortcuts

Who can see my stuff? ▾

Who can contact me? ▾

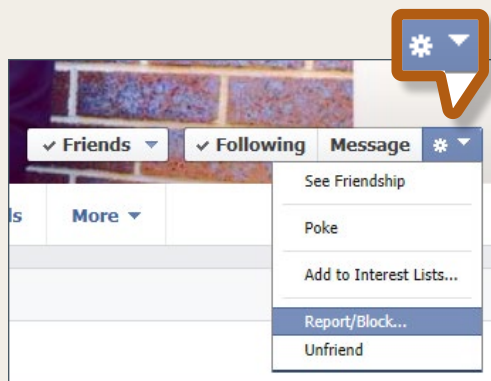
How do I stop someone from bothering me?

You can block someone to unfriend them and prevent them from starting conversations with you or seeing things you post on your timeline. [?]

[View All Blocked Users](#)

[See More Settings](#)

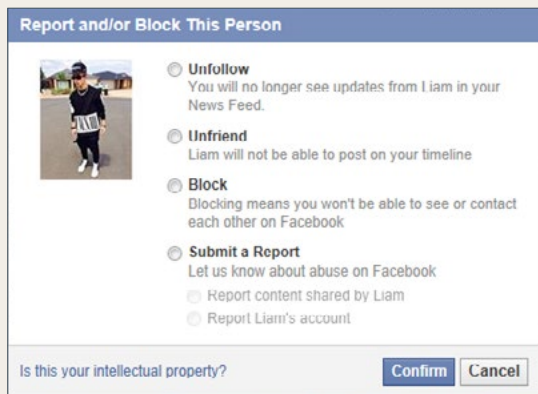
The third option for blocking someone on Facebook is to access their timeline and select the cog wheel under the person's cover photo, next to the 'Message' option. Select the 'Report/Block...' option in the menu which appears.



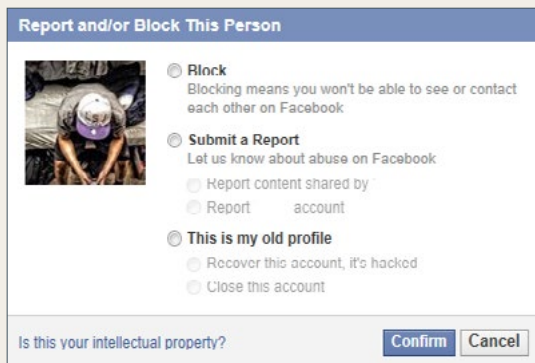
A dialog box will appear which provides options for dealing with the offensive user. This box will have different options depending on whether this person is already your friend.

Select the 'Block' option and, if you wish, you can report the user to Facebook by selecting the 'Submit a Report' option and clicking 'Confirm'. You will then be prompted to provide further details of your report.

Blocking options if currently friended



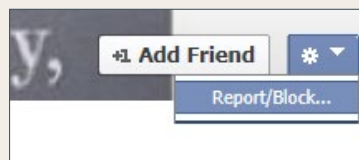
Blocking someone who is not a friend



Report fake profiles

To report a fake profile on Facebook, access the fake profile's timeline and select the cog wheel under the person's cover photo, next to the

'Message' option. In the menu which appears, select the 'Report/Block...' option.

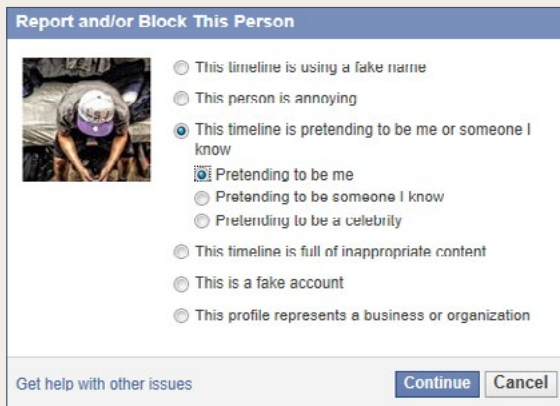


Select the 'Submit a Report' option, check the box next to 'Report ...'s account' and select 'Confirm'.



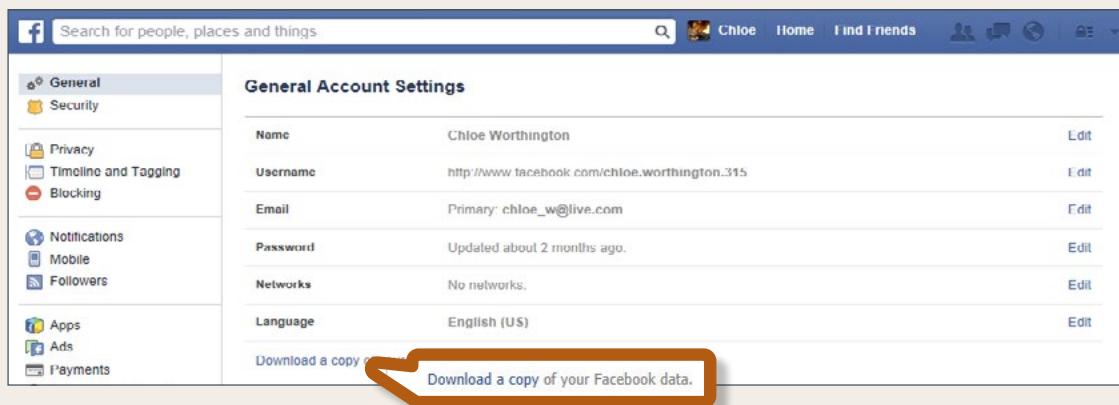
In the corresponding dialog box, select **'This timeline is pretending to be me or someone I know'** and select the option which corresponds with whom you are reporting on behalf of before clicking **'Continue'**. Follow the prompts to finalise your report.

If you don't have a Facebook account, you can still report a fake profile by completing the form at www.facebook.com/help/contact/?id=169486816475808

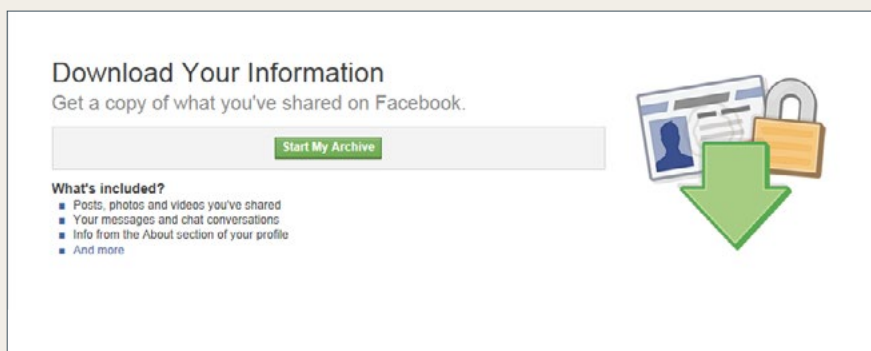


Delete unused accounts

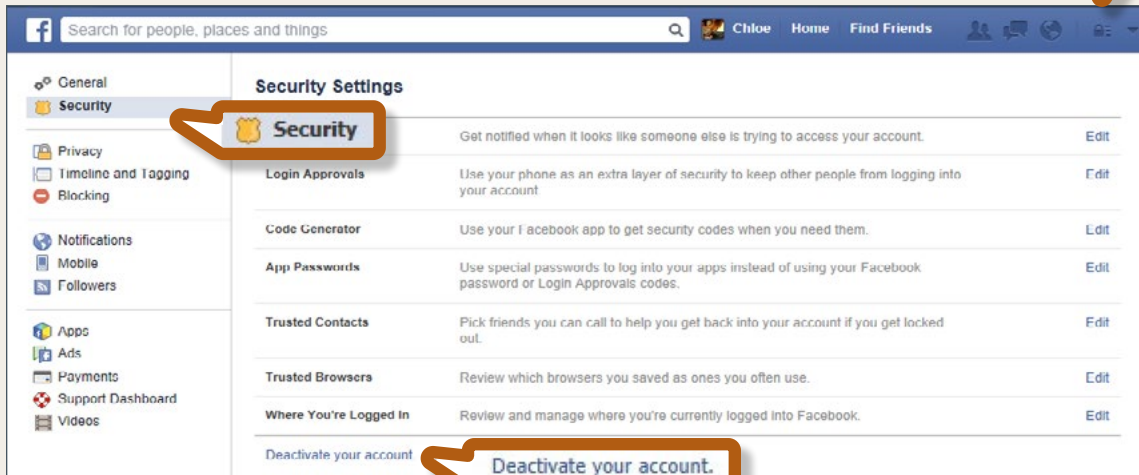
To download a copy of your Facebook content, access Account Settings by clicking on the cog wheel on the top right-hand side of your timeline. Click on **'Download a copy'** under the list of General Account Settings.



A new page will appear with information on how to download your information and some advice on protecting your security. Please follow the prompts and ensure that you have enough storage on your device to accommodate the potentially large volumes of data stored by Facebook about you.



To deactivate your Facebook account, access your Security Settings by clicking on the lock symbol on the right-hand side of your timeline. You can recover your account if you later change your mind.

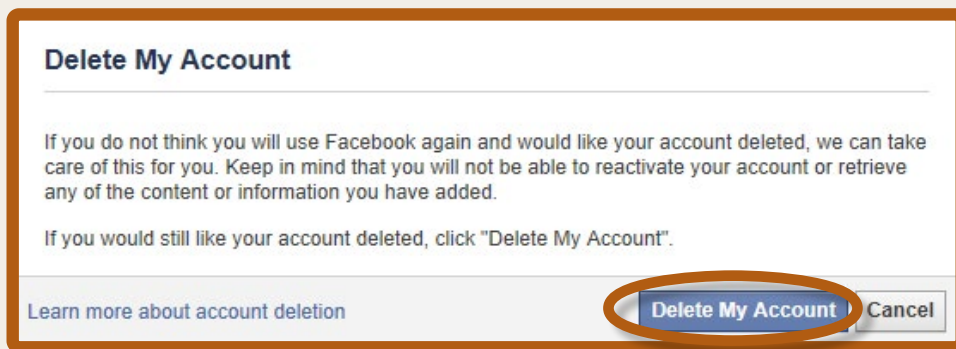


The screenshot shows the Facebook Security Settings page. A callout box with a lock icon points to the lock symbol in the top right corner of the Facebook interface. Another callout box points to the 'Security' link in the left-hand navigation menu. A third callout box points to the 'Deactivate your account' link at the bottom of the Security Settings list.

Security Settings	Description	Action
Security	Get notified when it looks like someone else is trying to access your account.	Edit
Privacy		
Timeline and Tagging		
Blocking		
Notifications		
Mobile		
Followers		
Apps		
Ads		
Payments		
Support Dashboard		
Videos		
Security Settings		
Login Approvals	Use your phone as an extra layer of security to keep other people from logging into your account.	Edit
Code Generator	Use your Facebook app to get security codes when you need them.	Edit
App Passwords	Use special passwords to log into your apps instead of using your Facebook password or Login Approvals codes.	Edit
Trusted Contacts	Pick friends you can call to help you get back into your account if you get locked out.	Edit
Trusted Browsers	Review which browsers you saved as ones you often use.	Edit
Where You're Logged In	Review and manage where you're currently logged into Facebook.	Edit
Deactivate your account		

Click on **'Deactivate your account'** under the list of Security Settings. Follow the prompts to complete the deactivation of your account.

If you wish to delete your Facebook account entirely, without the option of recovering your information, you can complete the form available at www.facebook.com/help/delete_account and follow the prompts.



The screenshot shows the 'Delete My Account' form. The title is 'Delete My Account'. The text reads: 'If you do not think you will use Facebook again and would like your account deleted, we can take care of this for you. Keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added.' Below this, it says: 'If you would still like your account deleted, click "Delete My Account".' At the bottom, there is a link 'Learn more about account deletion' and two buttons: 'Delete My Account' and 'Cancel'. The 'Delete My Account' button is circled in orange.

Managing your Twitter account



Make sure your profile is set to private

Most people use Twitter to improve their public profile and will often make their account publicly available. If you wish to use Twitter for more personal interactions, you may choose to make your account private. This can be done by clicking on the cog wheel on the upper right-hand side of the page and selecting **'Settings'**.



Next to **'Tweet privacy'**, check the box next to **'Protect my Tweets'**.

Tweet privacy Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more.](#)



Only accept friend requests from people you know and trust and learn to block offensive users

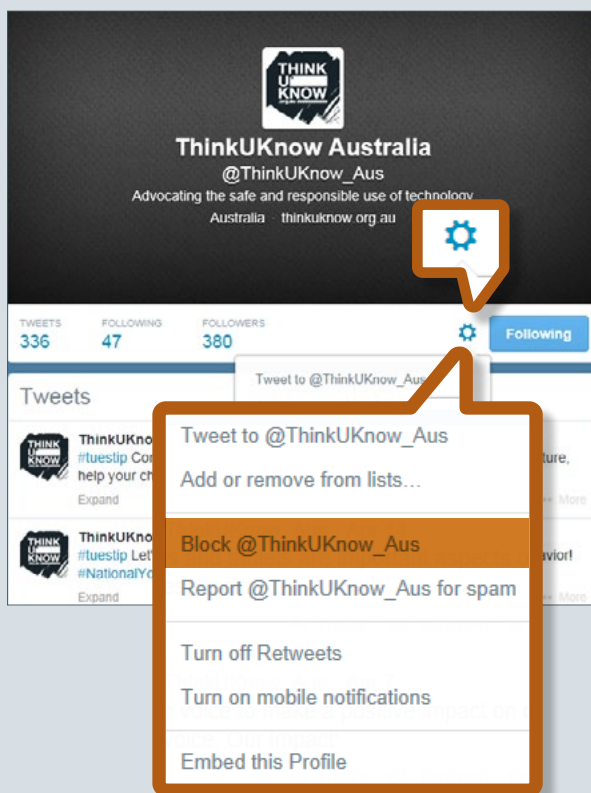
If you are using Twitter, you may be comfortable allowing people you don't actually know to be followers. If you do not know and trust a person, it is important that you exercise some caution when clicking on links contained in one of their Tweets. To fit into the character limit of tweets, URLs are shortened using services like <http://bit.ly/> which redirect you to an existing website. Unfortunately, this means that you cannot be sure of where the

link will take you and you may end up at a phishing site or falling victim to a drive-by download of malware and viruses.

Please use caution when clicking on links in Tweets, especially if you do not know the person.

You can use URL expanders such as <http://real-url.org> or others listed on the Twitter Help Centre to see what the actual URL is, and decide whether you are comfortable viewing the site.

On Twitter, you can block users by accessing their profile and selecting the Interaction menu, which looks like a person's silhouette, next to the 'Follow' status. Select the 'Block' option and follow the prompts.



Report fake profiles

Fake accounts or accounts impersonating others can be reported to Twitter via the form available at <https://support.twitter.com/forms/impersonation> and selecting 'I am being impersonated'.

 A screenshot of the Twitter Help Center page titled 'Report an account for impersonation.' The page has a blue header with the Twitter logo and 'Help Center' text. Below the header is a navigation bar with links: 'Welcome to Twitter', 'Me', 'Notifications', 'Discover', 'Mobile & Apps', and 'Troubleshooting'. The main content area has a white background with a blue border. It contains the heading 'Report an account for impersonation.' followed by the instruction 'Fill out the form below to request help.' Below this is a form with the question 'How can we help?' and five radio button options:

- My account was suspended.
- I can't sign into my account.
- My account has been hacked or compromised.
- Someone is using my email address without my permission.
- I am being impersonated.

 At the bottom of the form, there is a link: 'Not what you need help with? Choose another topic.'

Report an account for impersonation.

Fill out the form below to request help.

- How can we help?
- A user is pretending to be me or someone I know.
 - I am the person being impersonated.
 - I am an authorized representative of the person being impersonated.
 - I am a friend or fan of the person being impersonated.
 - A user is pretending to be or represent my company, brand, or organization.

Your Information

We may provide third parties, such as the affected user, with a copy of this complaint.

Your first and last name

Your Email address

Legal alias

Common nickname

Your Twitter username
(optional)

Twitter account not required to submit a ticket

Have you previously filed reports regarding impersonation from this email address and faxed a copy of your government-issued photo ID to Twitter as part of that process?

- Yes
- No

Wrapping up

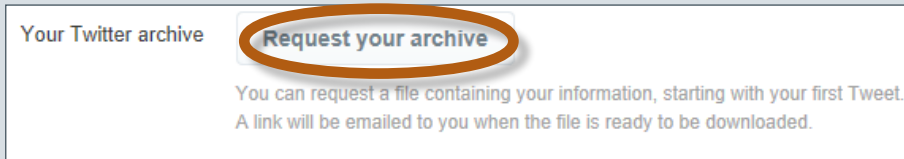
Anything else? (optional)

Security reminder: Do not include private information (address, home phone) in this request. **Never** include your password.

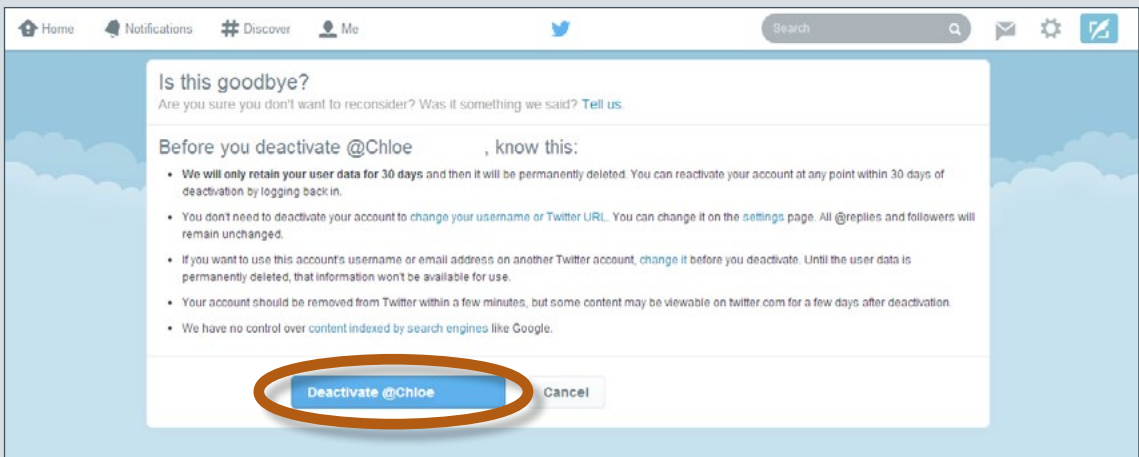
Select the 'A user is pretending to be me or someone I know' option and then select the option which corresponds with whom you are reporting on behalf of. Complete the form with the information requested. You do not need a Twitter account to report a fake profile.

X Delete unused accounts

To download your Twitter account, access your Settings by clicking on the cog wheel on the top right-hand side of your account, select **'Request your archive'** and follow the prompts.



To deactivate your Twitter account, access your Settings by clicking on the cog wheel on the top right-hand side of your account. From the bottom of the Settings menu select **'Deactivate my account'**. On the next page that appears, select the **'Deactivate'** button.



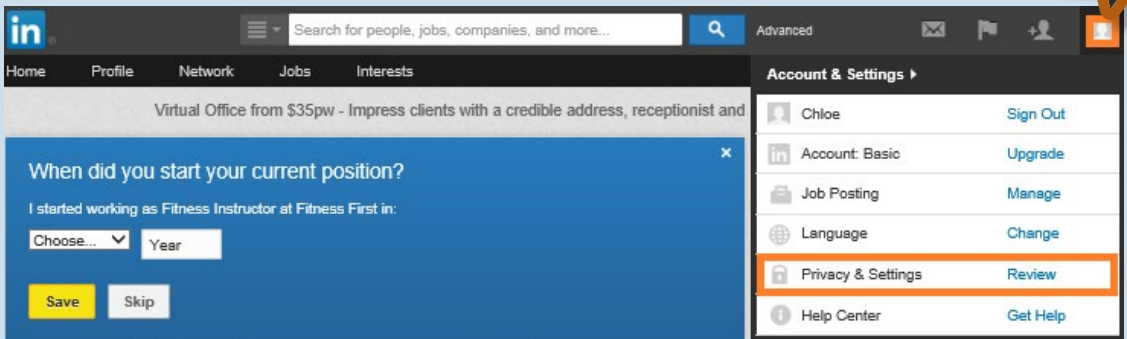
Managing your LinkedIn account



Make sure your profile is set to private

Many people use LinkedIn to connect with professionals around the world. If you want to use LinkedIn to improve your public profile and interact with other professionals, you can make your account private.

This can be done via your profile picture icon located in the top right hand corner. Select **'Privacy & Settings'** to view your privacy settings.



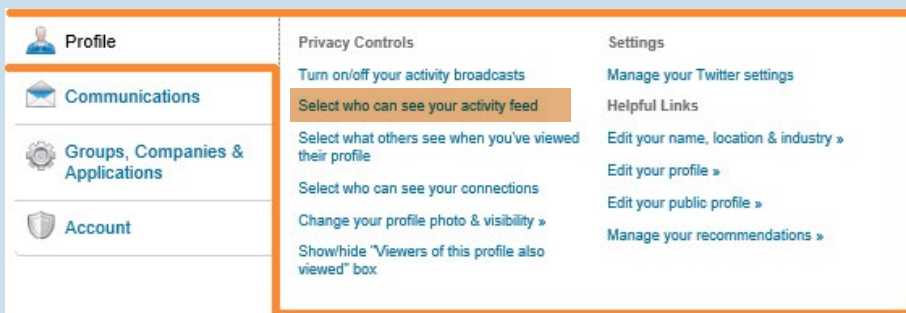
Accessing your **'Privacy & Settings'** allows you to protect your profile and sensitive information by:

- Limiting who can view your activity feed and connections,
- Limit certain people from communicating with you, and
- Protect your account information.



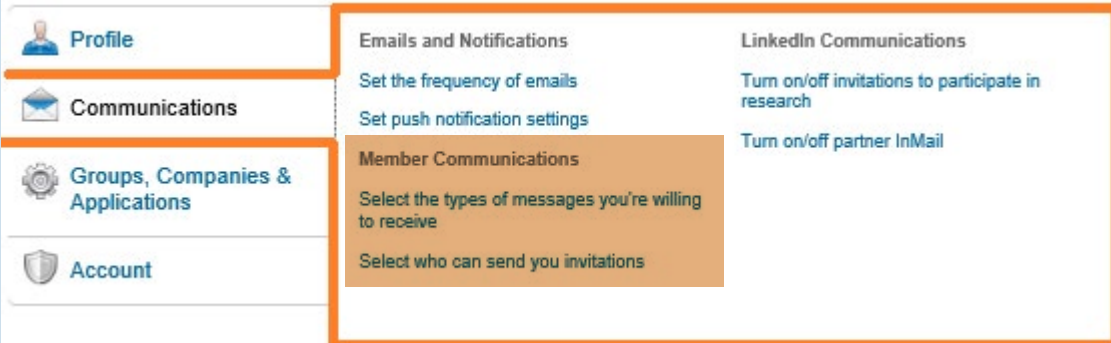
Limiting who can view your activity feed and connections

On LinkedIn you can limit who can view your activity feed and connections through your **'Privacy & Settings'**. Click on **'Profile'** in the left-hand navigation page, under **'Privacy controls'** click **'Select who can see your activity feed'**.



Limiting certain people from communicating with you

To limit people from communicating with you, access your **'Privacy & settings'**. In the left-hand side navigation page select **'Communications'** then click, **Member communications'**.



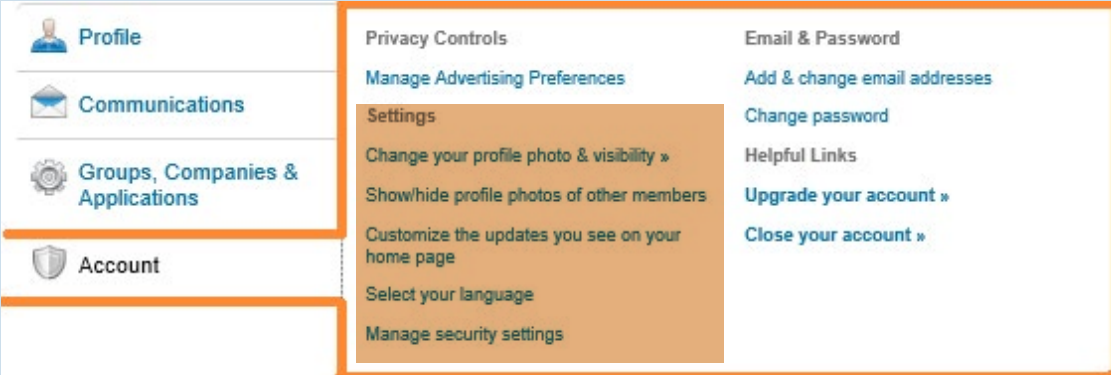
The screenshot shows the LinkedIn 'Privacy & settings' page. The left-hand navigation menu has 'Communications' selected. The main content area is divided into three sections: 'Emails and Notifications', 'LinkedIn Communications', and 'Member Communications'. The 'Member Communications' section is highlighted in orange and contains the following options:

- Select the types of messages you're willing to receive
- Select who can send you invitations



Protecting your account information

To protect your information on your account, access your **'Privacy & settings'**, select **'Account'** in the left-hand navigation page under **'Privacy Control'** to view your settings.



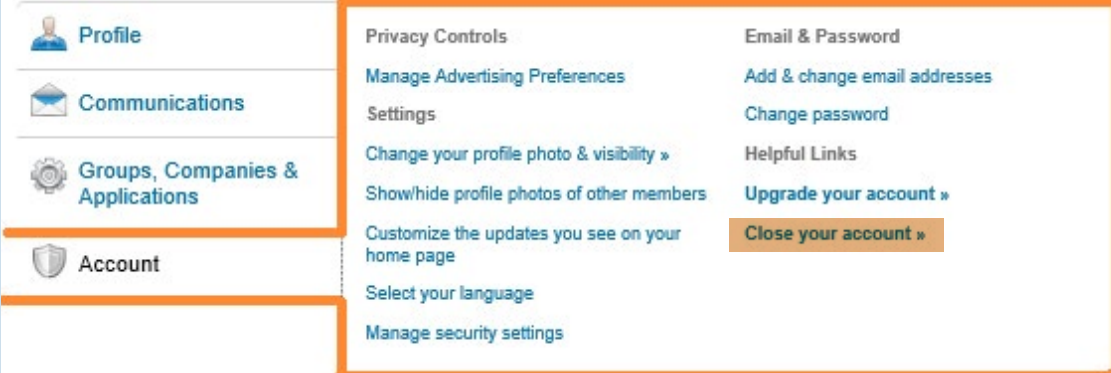
The screenshot shows the LinkedIn 'Privacy & settings' page. The left-hand navigation menu has 'Account' selected. The main content area is divided into three sections: 'Privacy Controls', 'Email & Password', and 'Settings'. The 'Settings' section is highlighted in orange and contains the following options:

- Change your profile photo & visibility »
- Show/hide profile photos of other members
- Customize the updates you see on your home page
- Select your language
- Manage security settings



Delete your account

To delete your account, access **'Privacy & settings'** click on **'Account'**, select **'Close your account'** and follow instructions.



The screenshot shows the LinkedIn 'Privacy & settings' page. The left-hand navigation menu has 'Account' selected. The main content area is divided into three sections: 'Privacy Controls', 'Email & Password', and 'Settings'. The 'Settings' section is highlighted in orange and contains the following options:

- Change your profile photo & visibility »
- Show/hide profile photos of other members
- Customize the updates you see on your home page
- Select your language
- Manage security settings

The 'Close your account »' option in the 'Email & Password' section is highlighted in orange.

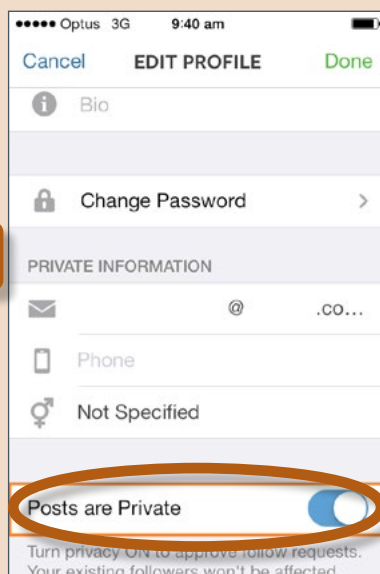
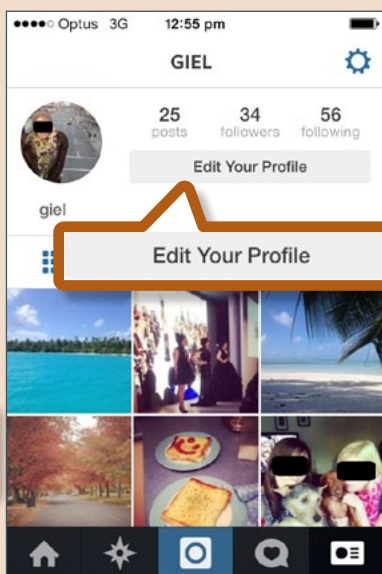
Managing your Instagram account



Make sure your profile is set to private

Many people use Instagram to improve their public profile and will often make their account publicly available. If you want to use Instagram for more personal interactions, you can make your account private.

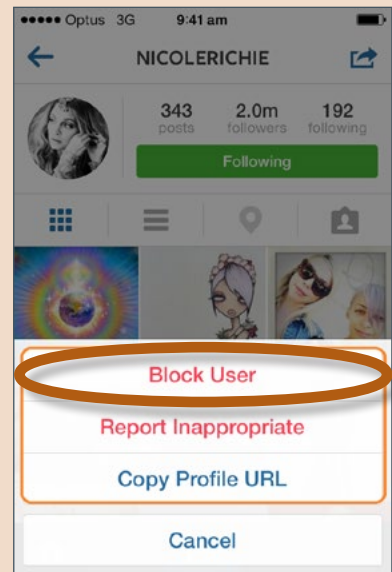
This can be done via the Instagram app on your mobile device. First select the **'Profile'** option on the lower right-hand side of the screen.



In the **'Edit Your Profile'** section scroll to the bottom of the screen and ensure **'Photos Are Private'** is in the **'On'** position and select **'Save'**.

Only accept friend requests from people you know and trust and learn to block offensive users

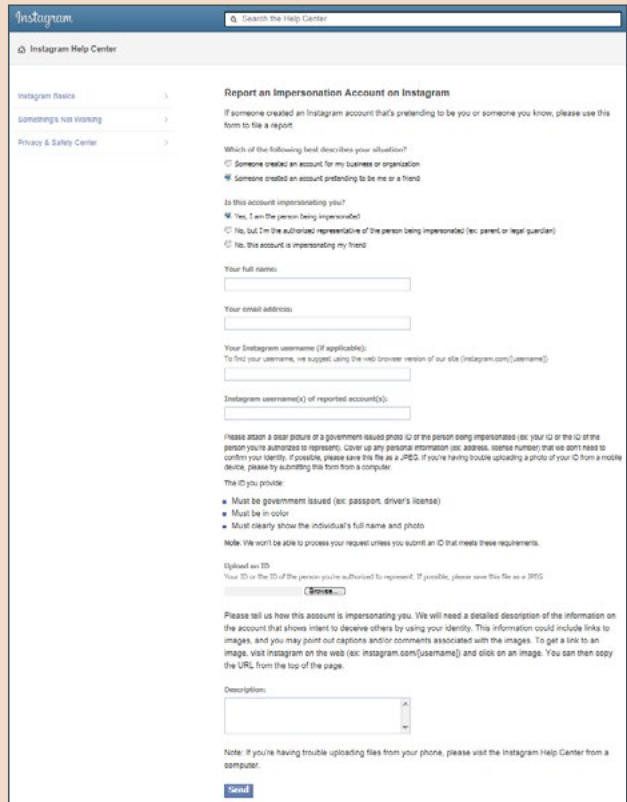
You can block users via the Instagram app on your mobile device. Open the profile page of the offensive user and select the **'Further Options'** icon on the upper right-hand side of the screen. Select the **'Block User'** option and when prompted by the dialog box, select **'Yes, I'm sure'**.



Report fake profiles

You can report fake or impersonation accounts to Instagram via their form at <http://help.instagram.com/customer/portal/emails/new>

You will need to attach two clear photographs from two different angles of a valid government issued ID. Attach these images directly in your reply to their initial email response and feel free to black out personal information.


 A screenshot of the Instagram Help Center website showing a form titled 'Report an Impersonation Account on Instagram'. The form includes several sections:

- Instagram Basics** (links to Instagram Basics, something's not working, Privacy & Safety Center)
- Report an Impersonation Account on Instagram**: A form to report someone pretending to be you or someone you know.
- Which of the following best describes your situation?**: Radio buttons for 'Someone created an account for my business or organization', 'Someone created an account pretending to be me or a friend', and 'This account impersonating you?'. The third option is selected.
- Is this account impersonating you?**: Radio buttons for 'Yes, I am the person being impersonated', 'No, but I'm the authorized representative of the person being impersonated (ex: parent or legal guardian)', and 'No, this account is impersonating my friend'. The first option is selected.
- Your full name:** Text input field.
- Your email address:** Text input field.
- Your Instagram username (if applicable):** Text input field with a note: 'To find your username, we suggest using the web browser version of our site (instagram.com/[username]).'
- Instagram username(s) of reported account(s):** Text input field.
- Please attach a clear picture of a government issued photo ID of the person being impersonated**: A note explaining the requirements for the ID photo.
- The ID you provide:**
 - Must be government issued (ex: passport, driver's license)
 - Must be in color
 - Must clearly show the individual's full name and photo
- Note:** We won't be able to process your request unless you submit an ID that meets these requirements.
- Upload an ID:** A section for uploading the ID photo, with a 'Browse' button.
- Please tell us how this account is impersonating you.**: A section for providing a detailed description of the impersonation, with a 'Description' text area.
- Note:** If you're having trouble uploading files from your phone, please visit the Instagram Help Center from a computer.
- Send** button at the bottom.

Managing your Snapchat account

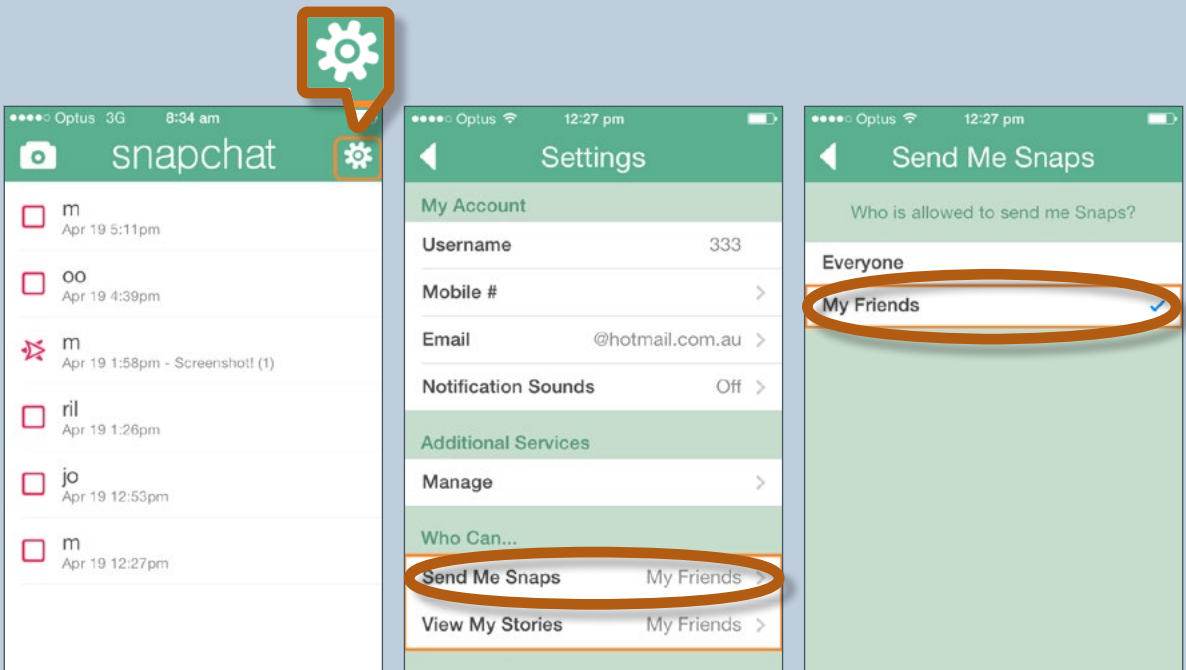
Does an image really delete on Snapchat?

There are many ways an image can be saved, even on Snapchat. iOS and Android devices have a feature which allow the device to take a photo of what is on the screen ('screenshot'). Snapchat notifies the sender if an image they have sent has been captured; however you are not always notified. There are also many other ways images can be saved without the sender being notified so it is important to think before you post. What does this image say about you? Will you regret posting it in 5, 10, 15 years' time? As soon as you post an image or video you have lost control. You don't know who will see that image or where it will end up.



Managing your privacy settings

Snapchat has very limited privacy settings. One privacy setting that is available is the ability to restrict who can send you snaps. This can be enabled by going into the 'Settings' menu, select 'Who can ...', 'Send Me Snaps', then select 'My Friends'. This will ensure that only users on your contact list can send you images.



Delete your account

To delete your Snapchat account go to www.snapchat.com/a/delete_account, enter your account username and password and press 'Delete My Account'.



Protecting your mobile devices



Disable geotagging for applications and cameras on your mobile device

iPhone

iOS 3: **Settings > General > Location Services.** This will turn off location services for ALL apps.

The only way to change settings for individual apps is to reset the location warnings on your phone. You can access this through **Settings > General > Reset > Reset Location Warnings > Reset Warnings.** When you open up an app after the reset, you will be asked if that app can use your current location and then select **'Don't Allow'**.

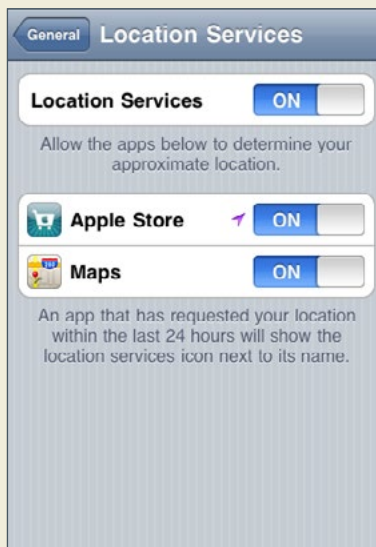
iOS 4 and 5: **Settings > Location Services.** Ensure that the **'Off'** option is selected next to **'Camera'** and any other app you do not wish to know your current location.

iOS 6: **Settings > Privacy > Location Services.** Ensure that the **'Off'** option is selected next to **'Camera'** and any other app you do not wish to know your current location.

iOS 7: **Settings > Privacy > Location Services.** Ensure that the **'Off'** option is selected next to **'Camera'** and any app you do not wish to know your current location.



iOS3



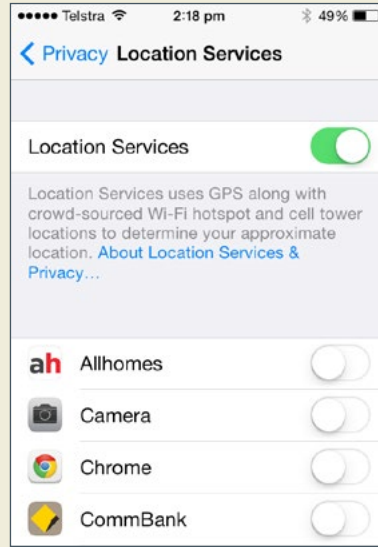
iOS4



iOS5



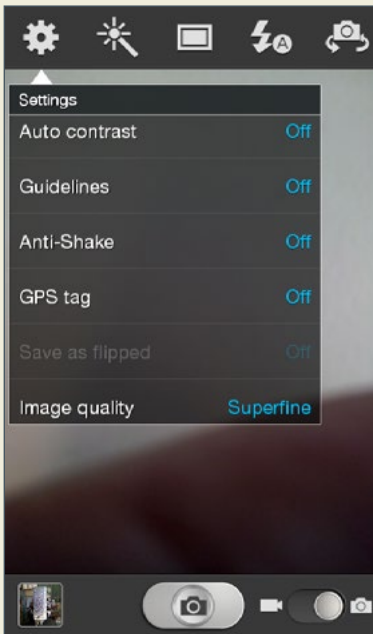
iOS6



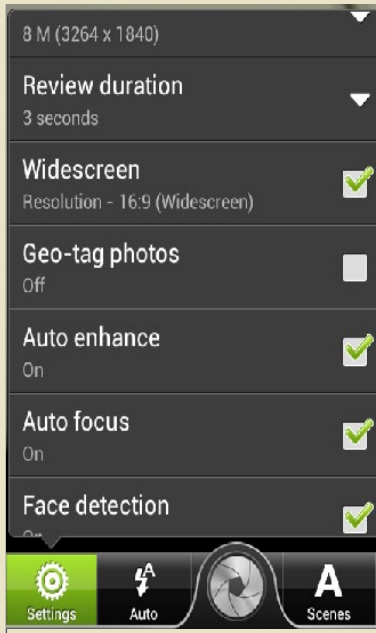
iOS7

Samsung Galaxy S Series

Open the 'Camera' app > Settings > GPS Tag > Off

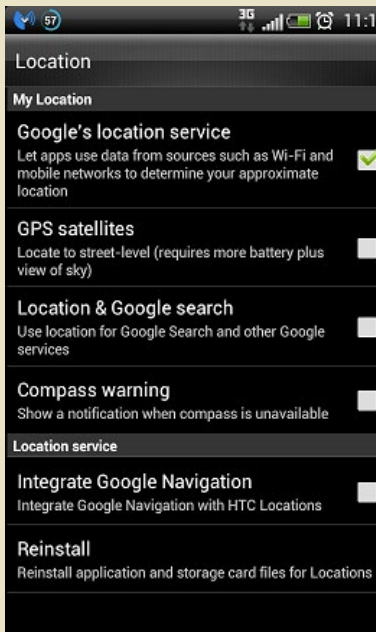


To turn off Geo-tagging on Android phones



Open your default camera app. Open the **Settings** menu, and click the **Geo-tag** box to disable the Geo-tagging function.

To turn off GPS functionality on Android phones



Select **Settings > Location** and disable the GPS satellites box.

