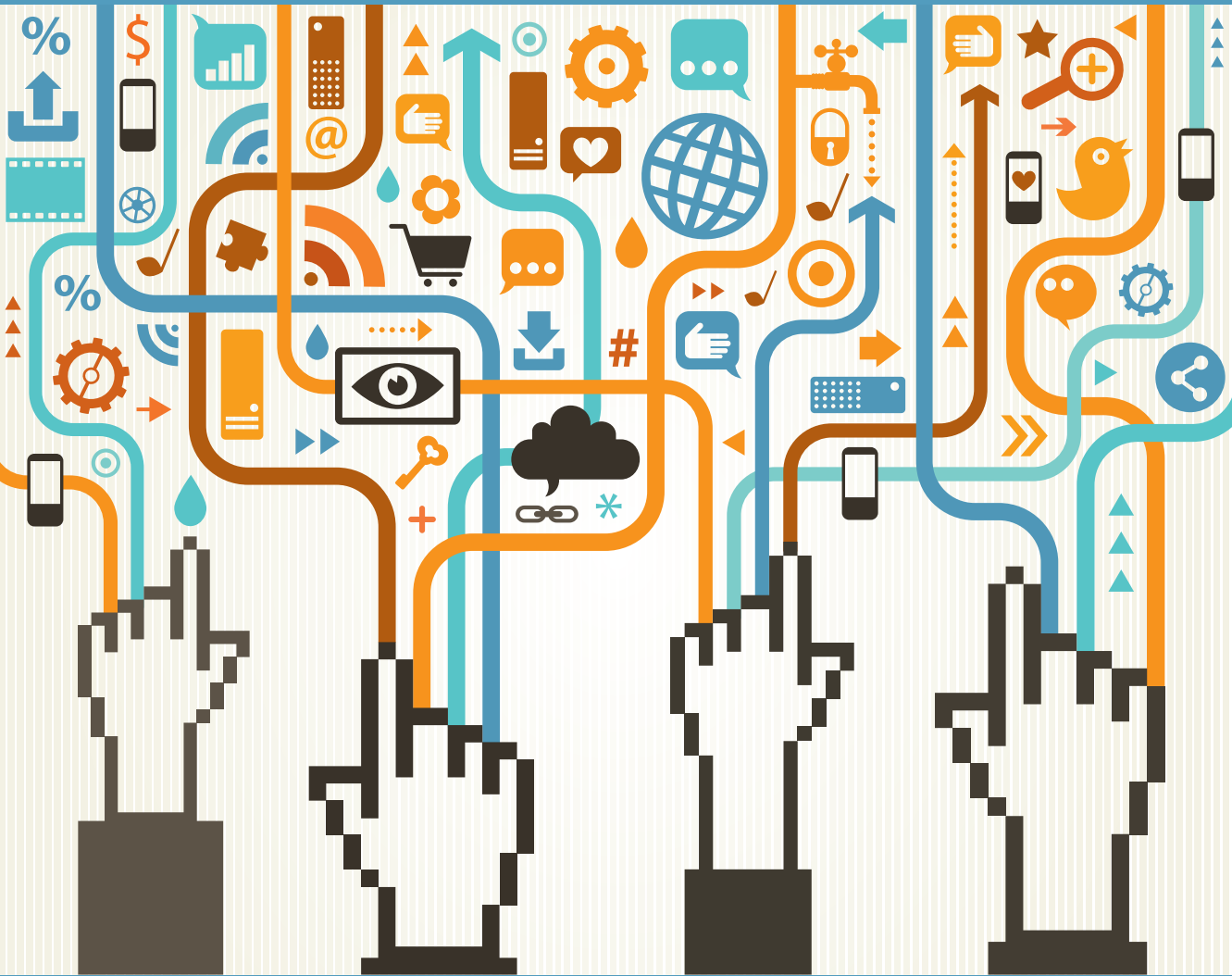
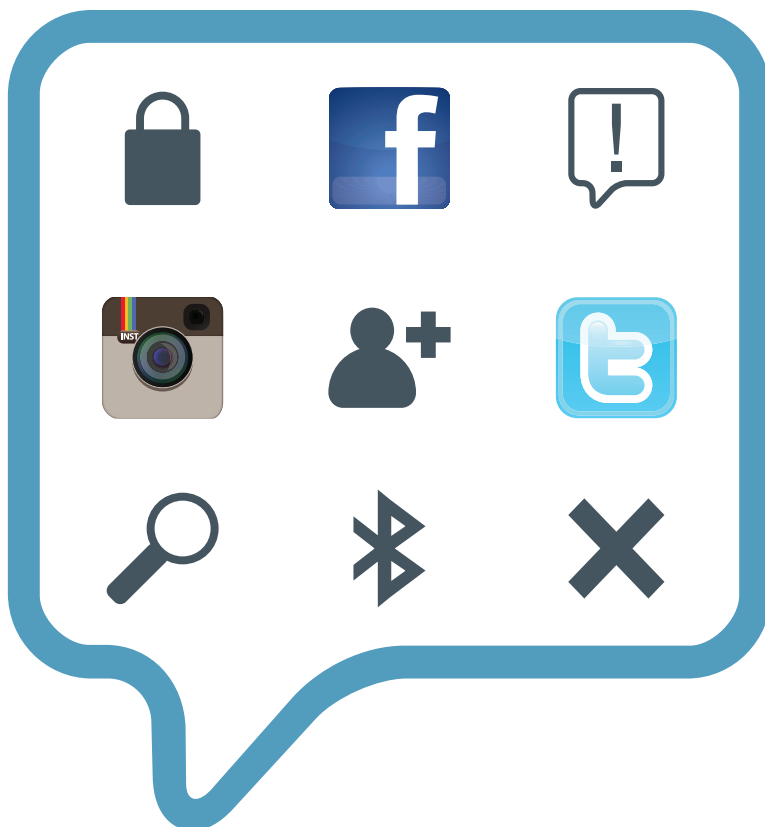


SOCIAL MEDIA REPUTATION MANAGEMENT



AFP

AUSTRALIAN FEDERAL POLICE



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	10
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 Instagram account 16

Make sure your profile is set to private	16
Only accept friend requests from people you know and trust and learn to block offensive users	16
Report fake profiles	17

Protecting your mobile devices 18

Disable geotagging for applications and cameras on your mobile device	18
iPhone	18
Samsung Galaxy S Series	19

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.

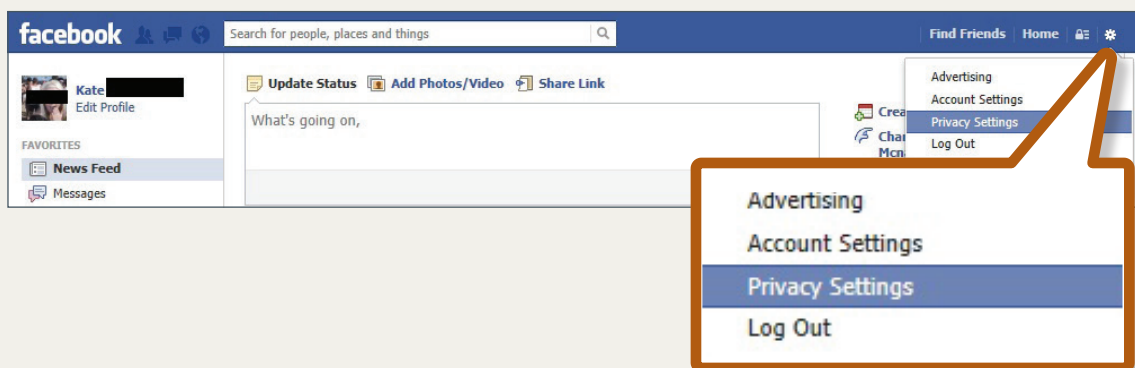
A conviction of child pornography-related offences can have serious long term consequences including being placed on a sex offenders' register and imprisonment.

Managing your Facebook account



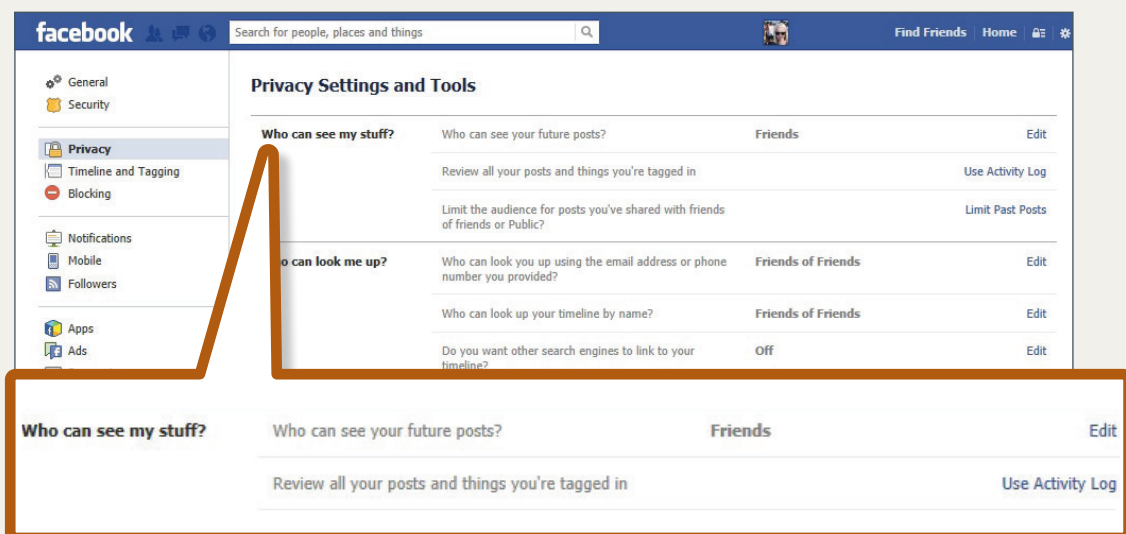
Make sure your profile is set to private

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'**.

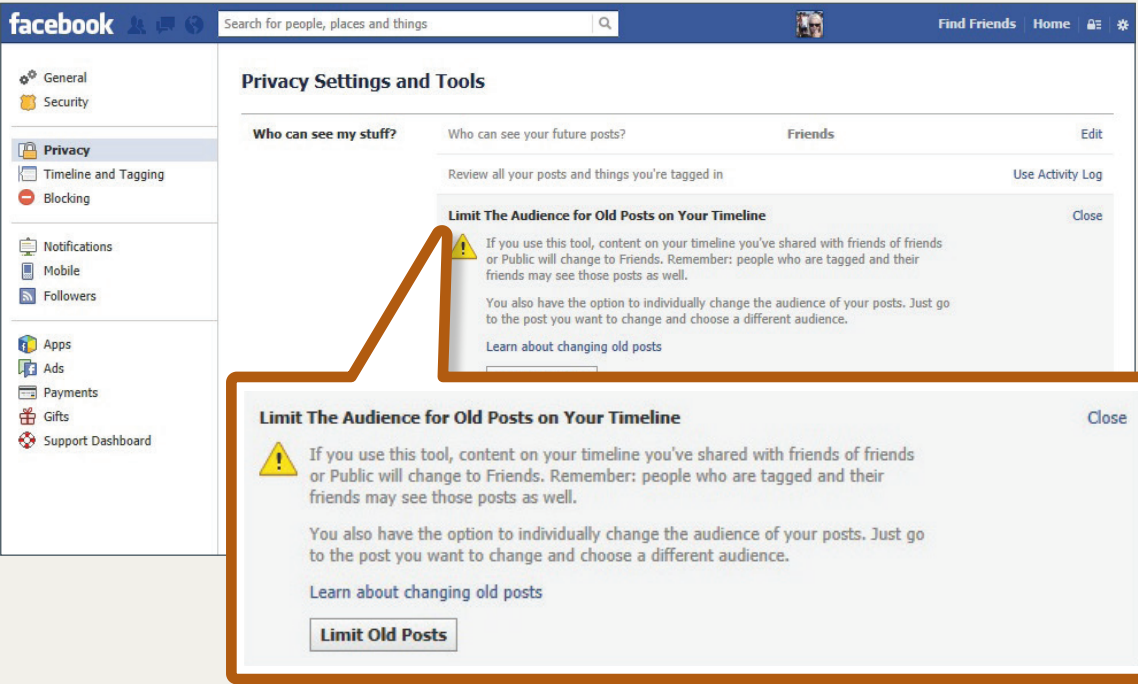


Under the **'Who can see my stuff?'** section, you can manage who is able to access your timeline.

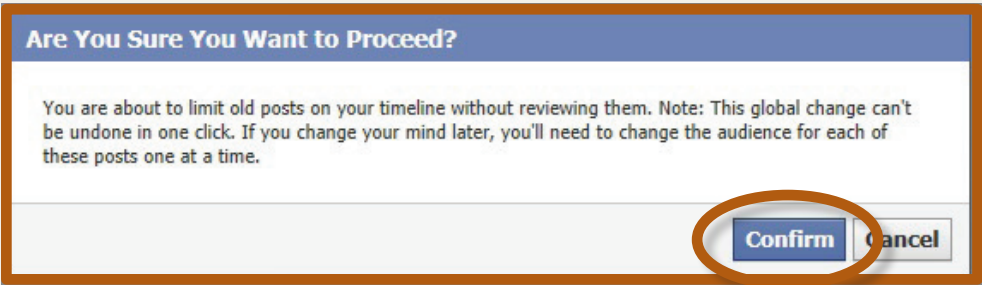
Next to **'Who can see your future posts?'**, click on **'Edit'** to ensure that **'Friends'** is selected.



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 or phone number 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 contains navigation links: General, Security, Privacy (highlighted), Timeline and Tagging, Blocking, Notifications, Mobile, Followers, Apps, Ads, Payments, Gifts, and Support. The main content area is titled 'Privacy Settings and Tools' and contains several settings sections. A large orange callout box highlights the 'Who can look me up?' section, which includes the following settings:

- Who can look you up using the email address or phone number you provided?** (This applies to people who can't already see your email address or phone number.)
 - Friends (selected)
- Who can look up your timeline by name?**
 - Friends of Friends
- Do you want other search engines to link to your timeline?**
 - Off

Click on **'Edit'** next to **'Who can look up your timeline by name?'** 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 cog wheel on the upper right-hand side of the page and selecting '**Privacy Settings**'.

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



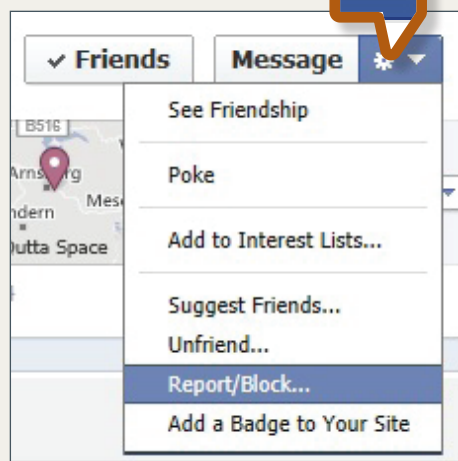
Alternatively, you can block people through the Privacy Shortcuts menu by clicking on the padlock icon on the upper right-hand side of the page.

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

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

 A screenshot of the 'Report and/or Block This Person' dialog box. It shows three main options: 'Unfollow from' (with a sub-option 'You will no longer see updates from [name] in your News Feed'), 'Unfriend' (with a sub-option 'will not be able to post on your timeline'), and 'Block' (with a sub-option 'Blocking means you won't be able to see or contact each other on Facebook'). There is also a 'Submit a Report' section with sub-options 'Report [name] account' and 'Report content shared by [name]'. At the bottom, there is a checkbox 'Is this your intellectual property?' and 'Confirm' and 'Cancel' buttons.

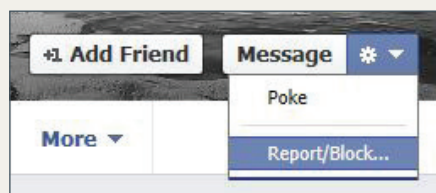
Blocking someone who is not a friend

 A screenshot of the 'Report and/or block this person' dialog box. It shows three main options: 'Block' (with a sub-option 'Blocking means you won't be able to see or contact each other on Facebook'), 'Submit a Report' (with a sub-option 'Let us know about abuse on Facebook' and further options 'Report content shared by [name]' and 'Report [name] account'), and 'This is my old Profile' (with sub-options 'Recover this account, it's hacked' and 'Close this account'). At the bottom, there is a checkbox 'Is this your intellectual property?' and 'Confirm' and 'Cancel' buttons.


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'**.



 A screenshot of the 'Report and/or block this person' dialog box. It shows three main options: 'Block' (with a sub-option 'Blocking means you won't be able to see or contact each other on Facebook'), 'Submit a Report' (with a sub-option 'Let us know about abuse on Facebook' and further options 'Report content shared by [name]' and 'Report [name] account'), and 'This is my old Profile' (with sub-options 'Recover this account, it's hacked' and 'Close this account'). At the bottom, there is a checkbox 'Is this your intellectual property?' and 'Confirm' and 'Cancel' buttons.

In the corresponding dialog box, select **'This person is impersonating someone'** 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 cog wheel on the right-hand side of your timeline. You can recover your account if you later change your mind.



The screenshot shows the Facebook interface with the 'Security Settings' page open. The left sidebar contains various settings categories, with 'Security' highlighted. The main content area lists several security features like 'Security Question', 'Secure Browsing', 'Login Notifications', 'Login Approvals', 'App Passwords', 'Recognized Devices', 'Active Sessions', and 'Deactivate your account.' The 'Deactivate your account.' link is highlighted with an orange arrow.

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.

Delete My Account

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. If you would still like your account deleted, click "Delete My Account".

Delete My Account
Cancel

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'**.



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'.

Help Center

English
Sign in

Report an account for impersonation.

Fill out the form below to request help.

What is your issue?

- ☒ 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.

Not what you need help with? [Choose another topic](#)

Help Center

English

Sign in

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

Legal alias

Common nickname

Your Email address

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)

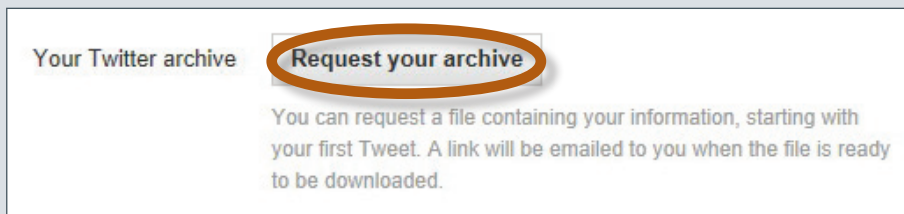
Security reminder: Do not include private information (address, home phone) in this request. Never include your password.

Not what you need help with? [Choose another topic](#)

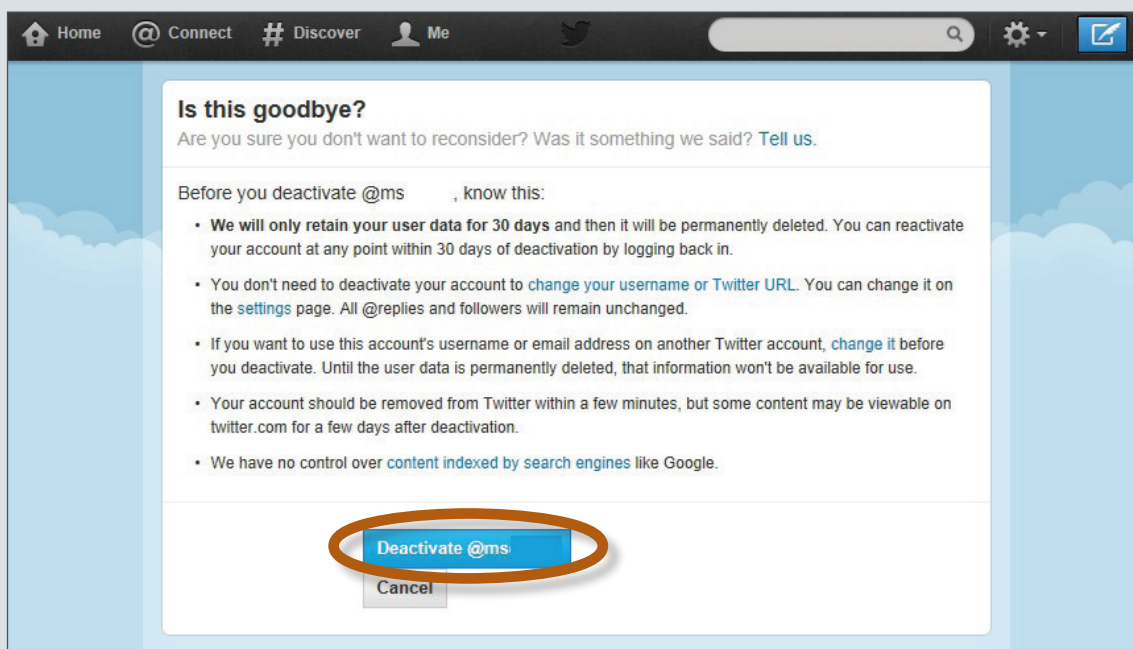
Select the **'A user is pretending to be me or someone I know'** option and then select the option which corresponds with whom you are reporting on behalf of. Complete the form with the information requested. You do not need a Twitter account to report a fake profile.

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 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.

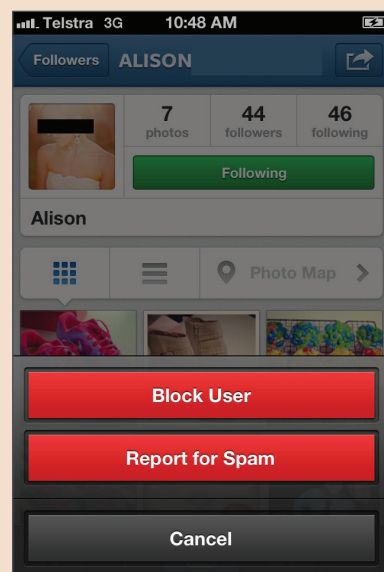
This can be done via the Instagram app on your mobile device. First select the **'Profile'** option on the lower right-hand side of the screen.



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

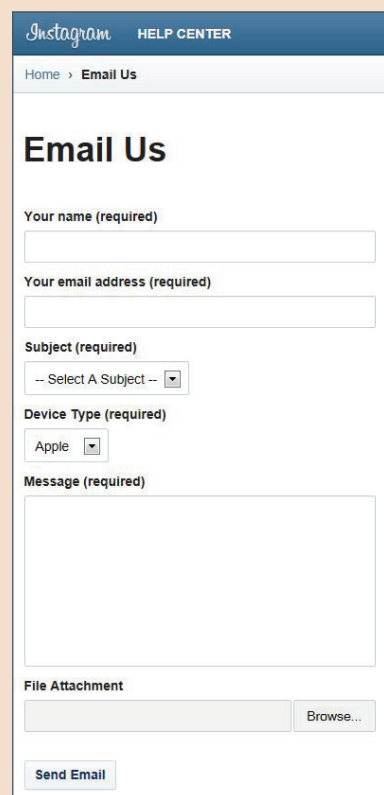
You can block users via the Instagram app on your mobile device. Open the profile page of the offensive user and select the **'Further Options'** icon on the upper right-hand side of the screen. Select the **'Block User'** option and when prompted by the dialog box, select **'Yes, I'm sure'**.



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.



Instagram HELP CENTER

Home > Email Us

Email Us

Your name (required)

Your email address (required)

Subject (required)

-- Select A Subject -- ▾

Device Type (required)

Apple ▾

Message (required)

File Attachment

Browse...

Send Email

Protecting your mobile devices



Disable geotagging for applications and cameras on your mobile device

iPhone

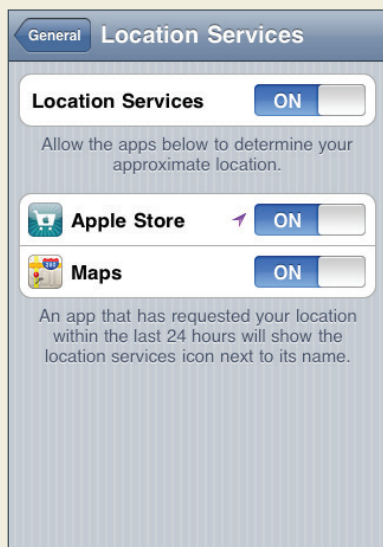
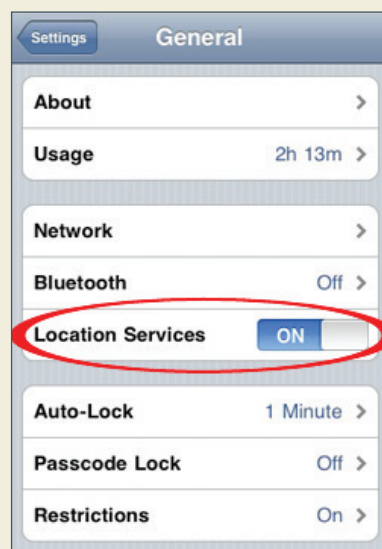
iOS 3: Settings > General > Location Services. This will turn off location services for ALL apps.

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.

iOS3



iOS4



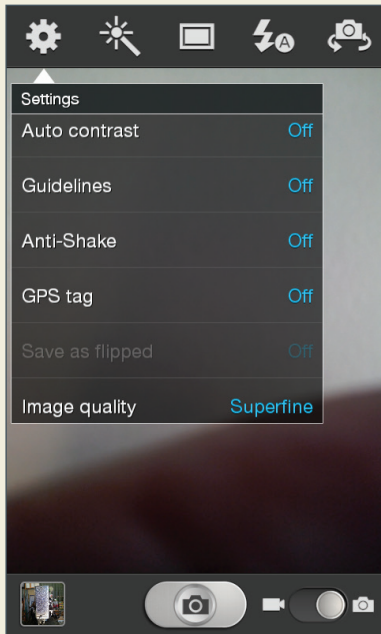
iOS5



iOS6

Samsung Galaxy S Series

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



Notes

[illegible]

