Safe on Social Guide to

Facebook 2019

Safe on Social

safeonsocial.com

Published by Safe on Social Media Pty Ltd

Copyright
Safe on Social Media Pty Ltd 2017

The moral right of the author has been asserted

No part of this e-book or its associated modules may be reproduced or transmitted by any person or entity in any for by any means, electronic or otherwise including photocopying, recording or scanning or by any information storage without prior permission other than the licensor who is licensed to use this information on their website, in newsletters and in print and has been granted permission from the publisher under an annual license.

The publisher, authors, licensee, licensor and their respective employees or agents will not accept responsibility for injuries or damage, physical or emotional occasioned to any person as a result of a social media use or any other activities described in this e-book.

Whilst every attempt has been made to ensure that the information in this e-book is accurate, it is the nature of social media to be constantly changing. Therefore, Safe on Social Media Pty Ltd gives no guarantees to the completeness or accuracy of the contents of this guide.

Contents

About Facebook....4
Advantages and disadvantages of Facebook....5
Safety Check....6
Problems and Preventions....7
Identity Theft....9
Facebook and Scams....10
Other Recent....10
Harming your professional reputation and future job prospects....12
Damage to mental health....12
Exposure to age inappropriate content....12
Bullying and harassment on Facebook....13
Blocking on Facebook and unfriending....14
Passwords....15
Facebook Security Features....17
Who can contact me....19
Blocking Someone....19
Report a problem....20
Advanced....20
Security and Login....22
Login Alerts and Approvals....25
Two factor authentication system....29
Encrypted email notifications....30
Privacy features....30
Limit last posts....31
Determine who can search for you....32
Blocking....32
Notifications....34
Mobile Notifications....37
Text message....37
Mobile Settings....38
Public Posts....38
Apps = Third-party apps....39
Disabling the apps....42
Ads....43
Support Inbox....44
Timeline and Tagging....44
Geo-Tagging....46
Turning off Location Services....46
Live Steaming....54
Issues....54
Live broadcast map....55
Concerns....55
Controlling your child's pictures – Scrapbook....56
Things to consider....56
Logging Into other sites using Facebook or Google....57
You are giving the website your personal information....57
You put yourself at risk of hacking....57
Your information is valuable....57
How much information are you authorizing Facebook to collect....57
Facebook and the online quiz....59
Directory....60

About Facebook

Facebook was initially developed by Mark Zuckerberg while attending Harvard University.

After creating in 2003 ,a site called facemash where he compared photographs of people to determine their attractiveness, he came to a realisation that the university students, despite protesting the use of their photographs, actually enjoyed using the internet and looking at pictures of their friends.

In January 2004, he registered the website thefacebook.com, and on February 4th 2004 launched The Facebook , only open to Harvard university students. In June 2004, he received his first private investment from Peter Thiel, co-founder of PayPal.

The newly incorporated name was Facebook.com.

The site added over a million users in a six-month period once it was expanded to students at other Ivy League universities, and on September 26th 2006, it became open to anyone over 13 years of age with a valid email address.

To emphasize the reach of Facebook listed below are some statistics recorded as of February 2017.

- Facebook has 2.07 billion users
- 1.28 billion users check in daily
- A smart phone user will check in an average of 14 times daily
- There are 83 million fake profiles on Facebook
- 30 million deceased individuals still have Facebook sites.
- The Facebook servers hold over 330 petabytes of data about its users
- Every day Facebook experiences roughly 60,000 hacking attempts on its servers
- Each day 160,000 accounts are hacked into
- Facebook's user base grows by eight people per second, or 7,246 people every 15 minutes
- Over 300 million photographs are uploaded per day

Registered users create customized profiles with information, photographs and videos of themselves. It is possible to view other people's profiles, make comments, play games, post articles and interact and connect with different groups of people.

Advantages and Disadvantages of Facebook Use

Some of the major **advantages** of Facebook are:

- Networking – you can use Facebook to connect with your family, friends, work colleagues, school friends, and meet new and like-minded people.

- Building your brand – whether a personal brand or for a business or an organization, a musician or an artist, what you put on Facebook creates the image of your brand and is an excellent way to reach a larger audience.

- Photo and video hosting – Facebook is a great place to store all your holiday snaps and videos (providing you know how to set your privacy settings securely), and share them with Friends.

- As a source of news and information – the size, reach of Facebook, and the fact that it is in real-time makes it a powerful reporting tool, and source of information. Recently, the plague of fake news reports has become an issue for the validity of information viewed on Facebook.

Some of the major **disadvantages** of Facebook are:

- Privacy - due to a lack of understanding of Facebook's ever-changing privacy functions, many people post things to their Facebook pages that are viewable publicly - under the mistaken impression they are only sharing with friends . Posting personal information online on sites like Facebook can have detrimental and far-reaching effects.

- Time consumption – because Facebook is fun and interesting, people are spending more and more time using it, and less time doing other things like real life socializing and activities. It is also having a vast effect on productivity in the workplace.

- Facebook will never be able to 100% guarantee your safety. As Facebook is "social" your safety will always rely in some way on the behaviour of others you are connected to. This can't be predicted – just like it can't be in the physical world. When you use Facebook, you are completely responsible for your own safety. What you do and what you share on Facebook will determine breaches of your personal safety and privacy. Facebook itself cannot be held accountable for any negative experiences. If you are a teacher or a parent and don't use Facebook, you also need to be informed and keep communication open with your child or student to understand if there is an issue (bullying trolling/ inappropriate posts) with what is being posted on Facebook.

Risks to always keep in mind:

- Posting information on Facebook about yourself that could disclose your physical location
- Posting information on Facebook that could be manipulated and used against you to cause psychological harm
- Identity theft from sharing too much personal information on Facebook through data such as your birthday, or photos of identification such as drivers' licenses, passports or plane tickets
- Posting information that could hurt your professional reputation and future job prospects
- Harassment, stalking and online bullying

- Spending too much time online
- Damage to your relationships
- Exposure to age inappropriate content, and if you are under 18yrs inappropriate contact with adults
- Posting compromising photos or videos that might be used against you
- Trolling
- Loss of productivity both in and out of school and your workplace
- Social isolation.

Safety Check

Facebook has installed a tool that is only activated in a time of disaster, or in the event of a terrorist attack. It is used to notify and connect with friends and loved ones during the event.

To date , Facebook has activated this feature 600 times, and it has been utilized by over 1 billion people. It is an excellent service for large scale disasters like earthquakes, or cyclones.

In addition to illustrating the wellbeing on those on your friends list, these other features are available:

- There is a Community Help section that will be available in crisis – locating for users where they may receive aid and additional assistance.

- Personal notes may be added through Safety check to appear on a Facebook profile page

- Information about the crisis is included with a feed directly from the Global Crisis reporting agency

- Fundraisers will be able to be run through the Safety check feature

Some negatives:

- The assumption can be made, that if a friend hasn't checked in to Facebook and marked themselves as being safe, that something may have happened to them, and this can cause unnecessary concern.

- The scale of the events is not marked well on the maps Facebook uses. For smaller disastrous events, large swathes of the map have been illustrated as areas effected when this is not the case.

- In 2016 users located in Bangkok were asked to mark if they were safe of not after footage was linked about an explosion that had taken place. This explosion had actually taken place a year previously - and unfortunately Facebooks intervention was incorrect. This lead to considerable angst and fear from relatives of those in the marked area - unnecessarily.

For more information

www.facebook.com/help/695378390556779

Problems and Preventions

Legacy Contact Details

It is now much easier to deal with a Facebook account once the owner of the profile has passed away.

This had been a concern for a number of years, causing considerable angst when relatives were unable to access or close down a deceased loved one's account.

It is called Legacy Contact.

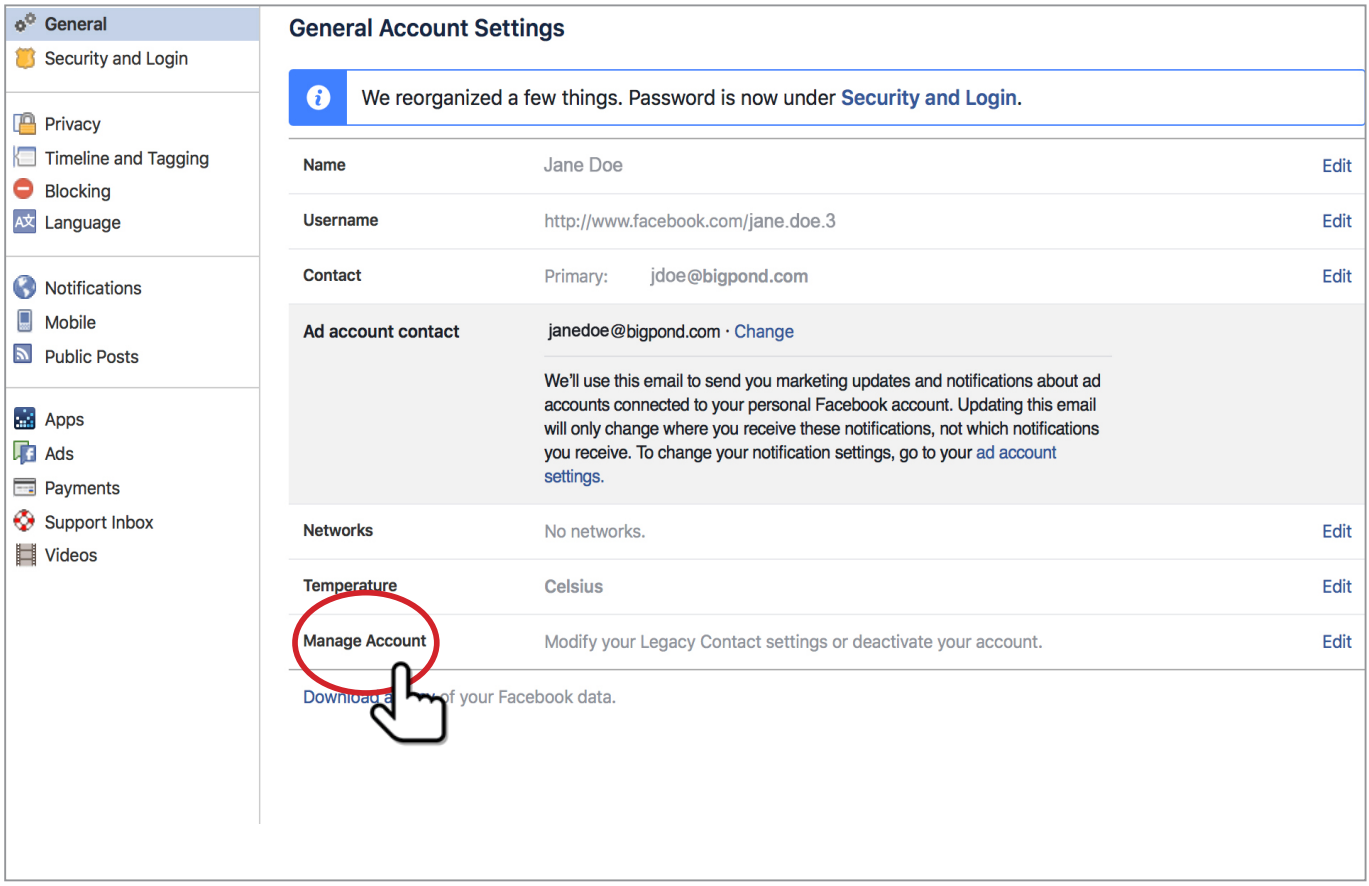
An account holder will be able to select someone from their friends list to essentially, act on their account.

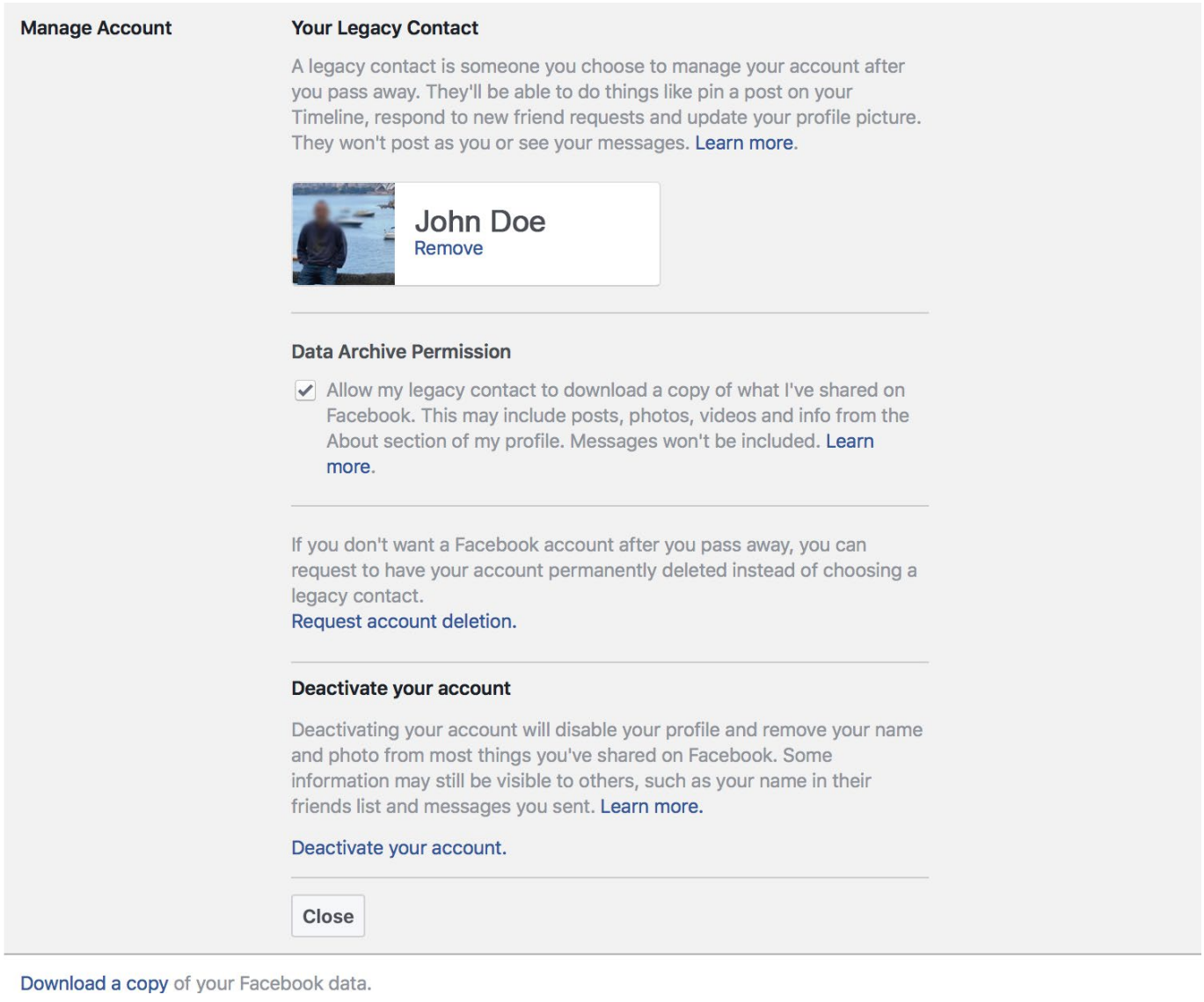
The person selected will be able to interact with the account – writing posts at the top of the timeline, change profile details etc.

Their posts will not appear as though they were from the page owner, and they cannot alter previous posts.

This person must agree to the responsibility, and you can choose whether to allow them the option of downloading your images, posts, and photographs.

Private messages will not be able to be downloaded or accessed.





NB-
Being named in a will, as a digital heir, will also mean the individual is considered a legacy contact by Facebook – though it is easier to use the legacy contact option.

Identity theft

The con artist who was the inspiration behind the movie Catch Me if You Can, Frank Abagnale has said "Never put your date of birth, and where you were born (on personal profiles) or you are saying – come and steal my identity"

Avoiding stating your specific age, avoid using passport style photographs on your page, and keep your privacy settings as tight as possible.

False profiles

One of the most common forms of identity theft that happens on an almost daily basis on Facebook is this duplicate account scam.

If your accounts friends list is not set to private, photos are stolen from your profile and set up in an account that looks exactly like yours. Your friends list is copied, with the hacker taking particular notice of your friends who also don't have their friends list set to private. You are blocked from this profile and the account starts sending friend requests to all of your friends that have unsecured friends lists.

When your friends accept this fake friend request it can do nothing for months but sooner or later a message will be sent saying that they are stuck somewhere and urgently need money, or something to that effect.

Facebook has put the security for this in a completely different area to the rest of your security settings.

So here is how to stop it.

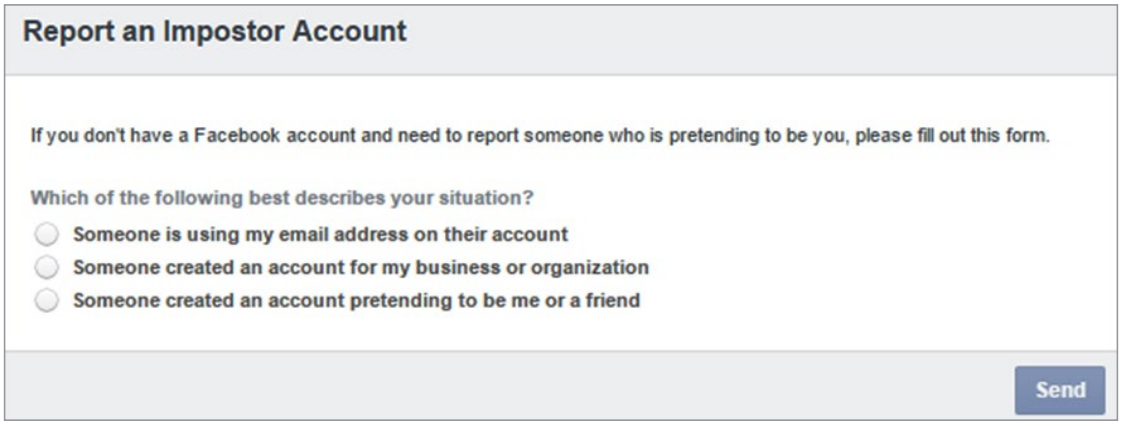
- Go to the little pen or down arrow icon immediately above where all the little thumbnail photos of your friends list is.

- Click on the icon and go to edit privacy

- Change this to "only me" that way only you can see who you are friends with and it makes you worthless to a scammer.

- While there, change who can follow you to only me as well.

- And report the false profile.



Facebook and Scams

There has been huge increase in the number of scams being reported to the Australian consumer watchdog. Many of these, are reported as taking place through Facebook.

The most common of these fall into the dating, romantic, or fake trader category.

Dating and romantic scams cost Australians close to $42 million dollars in 2016 alone.

Fake traders representing themselves as online stores were increasingly successful in persuading people to buy non-existent goods.

Sextortion is on an upward trend with blackmailers using compromising pictures of a victim that were often shared online to extort money.

While you use social media , it is important you remain alert.

Common warning signs that something is a scam and some things to think about:

- Spelling and grammar errors
- Inconsistencies in stories told
- Requests for personal information
- Asking for credit card details
- Requesting money be sent
- Requests for login details
- Requests for pin numbers
- Asking for address

Other recent

Phishing scams - A message will be sent that appears to be from a legitimate Facebook or Messenger account. This message will claim that the persons account will be disabled for a violation, unless that person follows a link to login and confirm their details. But the message never originated from Facebook, the page they are directed to is a fake, and is being used to collect their login details and information. The result is that the individuals Facebook page can now be accessed and used by another unknown person.

A similar version, is where a message window opens claiming to lead to a video sharing site, where a video including the account owner is supposed to feature. This again leads to a false page, asking for login details.

ALWAYS check the web address to make sure of the authenticity of the website, and enable the two-factor authentication protocol in Facebook settings.

Sponsored posts - these purport to utilize a legal loophole to facilitate you working from home while making large sums of money. A get rich quick scheme. Some of these are actually sponsored by Facebook but they are scams, no doubt about it.

Facebook Cloning – where a duplicate or clone account is set up. This will copy as much detail as possible from a profile page, then proceed to try and trick friends and followers into believing this account is that of the real account holder. Once a friend request is accepted, these usually lead to attempts to get your friends to send "you" money. (see False profiles mentioned earlier) HIDE your friend list, and limit the information on your profile page.

The "like and share to win" – Like the post, share the page and go into the draw win a prize. These scams are either a blatant attempt to collect email details so millions of spam emails can land in your inbox, or as an attempt to get money when you 'win' the prize and need to send money for shipping and handling fees.

By limiting the amount of data that is available about you, not providing your details to unverified pages and being cynical about seemingly great offers you should be able to avoid the bulk of these. Never send money to anyone who asks for it online!

And if it seems too good to be true, it will be.

Harming your professional reputation and future job prospects

Companies regularly check search engines to find out information on applicants. It's estimated that up 90 % of executive recruiters use online research to screen potential candidates, and only 27% give these candidates the opportunity to discuss the online search results.

It is just as important for a job candidate to think about their online persona, as well as their interview outfit. Your social media presence is now part of your resume.

You are able to screen your online presence.

Here's how:

1. Check your online identity. Run various searches for your name on major search engines and social media sites.

2. Put your best foot forward. Show the positive things you do like sport or charity work.

3. Limit negative content. For example, showing your support online for a distasteful political group is something you should think carefully about.

4. Use a different spelling of your name, or determine a way to differentiate yourself , so you cannot be found in a search.

There is a line between work and your private life. There are personal and professional risks to using Facebook.

Damage to mental health

Too much time spent on Facebook can affect mental health and wellbeing in the following ways:

- It can make you feel like your life isn't as cool as everyone else's.
- It can lead you to envy your friends' successes.
- It can lead to a sense of false reality, where your world view is distorted.
- It can keep you in touch with people you'd really rather forget.
- It can make you jealous of your current partner.
- It can become addictive.

Limiting the amount of time spent on social media is vital.

Exposure to age inappropriate content

Facebook has age restrictions.

The recommended age stated in its terms and condition is 13+. It is worthwhile respecting this.

Even if a child is old enough to open a Facebook account, be advised that the sheer volume of content Facebook must moderate is almost beyond the company itself. It has recently employed an additional 4,000 moderators.

Nudity, hate speech, fake news, violent news clips and bad language are unfortunately fairly commonplace within Facebook.

The linking option within the app to other sites can lead to involuntary exposure to more to very inappropriate content.

Bullying and harassment on Facebook

What to do:

If you are being bullied or harassed on Facebook here are the steps to take:

- Take screen shots of the bullying or harassing comments. It is always good to have a record and make sure you share these with someone you trust and make sure they are dated and the time is noted.
- Don't retaliate. Bullies are always looking for a reaction - don't give them the satisfaction. Always remember that one of the most proven, effective ways to defeat a bully is to deprive them of your reaction.
- Unfriend and block the person (you will see tips on how to do this in the next section).
- Report the behaviour to Facebook. If you experience difficulty getting a post removed, contact the Office of the eSafety Commissioner for assistance at **www.esafety.gov.au**
- Make sure you tell a trusted friend, parent, family member, teacher or someone else that can help you.
- If you feel that you are in immediate physical danger, call the Police.

Bullying on Facebook may be a crime under Australian Law when it involves using the internet in a threatening or harassing way, stalking, encouraging suicide, or encouraging violence.

If the victim of bullying and harassment is a child:

We are fortunate to have The Office of eSafety Commissioner here in Australia. The Office provides Australians access to a complaints system designed to assist children who experience serious cyber-bullying. They can also help intercede with various social media platforms should the content fail to be removed promptly. You will find more information and their contact details at the back of this guide.

If the victim of bullying and harassment is an adult:

If someone is threatening you, stalking, intimidating, or harassing you, you may be able to apply to your local court for an intervention order to keep them from contacting you any further.

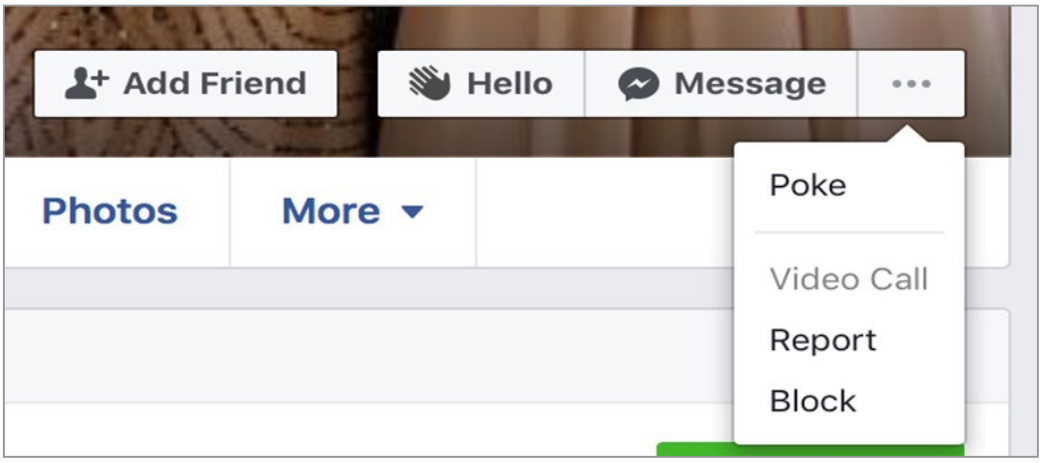
You may also contact the Office of The eSafety Commissioner for assistance in getting content removed and individuals blocked. You will find more information and their contact details at the back of this guide.

Blocking on Facebook and unfriending.

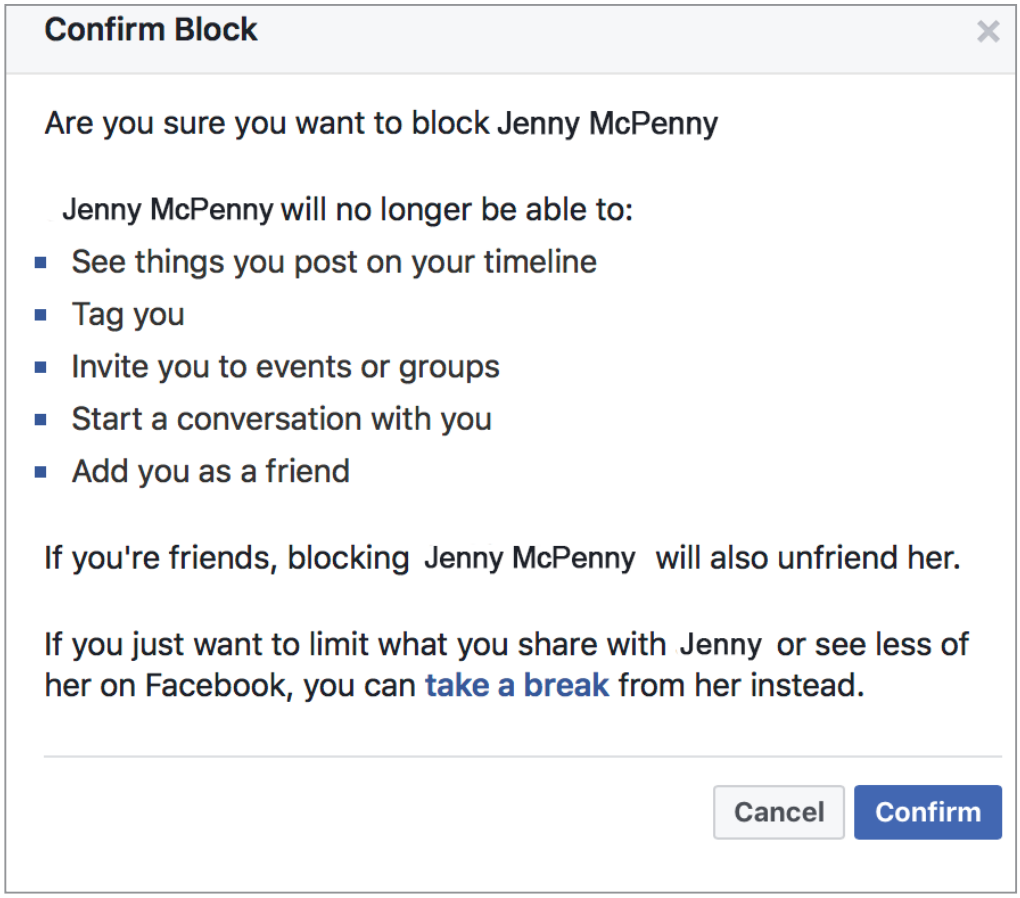
Users can both unfriend and block people on Facebook. This can shut out persistent bullies and stop them viewing a private account.

The basic method:

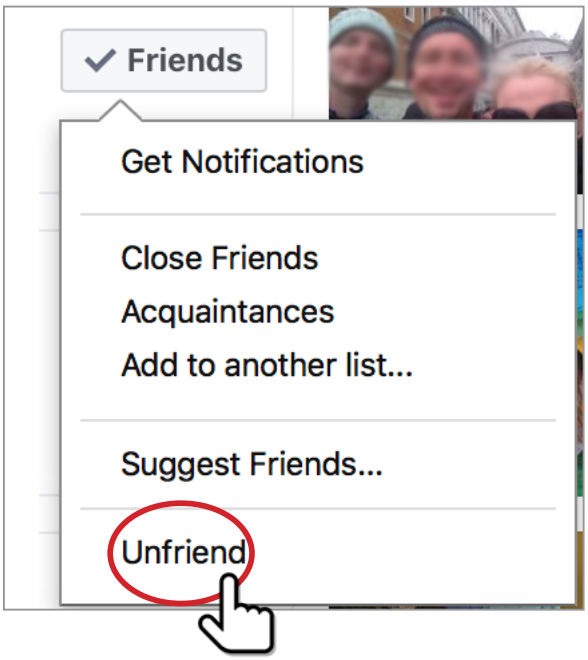
- To block someone: select "report/block this person" from the dropdown menu on their profile.



By clicking on the Block feature, a window will appear asking you to confirm your decision and defining what effect that action will have.



- To unfriend someone: go to your friends list, and bring up the menu below. You can unfriend someone from here.



Passwords

Always keep strong passwords, containing both upper and lowercase letters with at least one numeric symbol. Change these regularly. Always use different passwords for your different social media accounts.

Setting a strong password on your Facebook profile is the very first thing you should do. You are the first line of defence when it comes to securing your online life and strong passwords are your best friend.

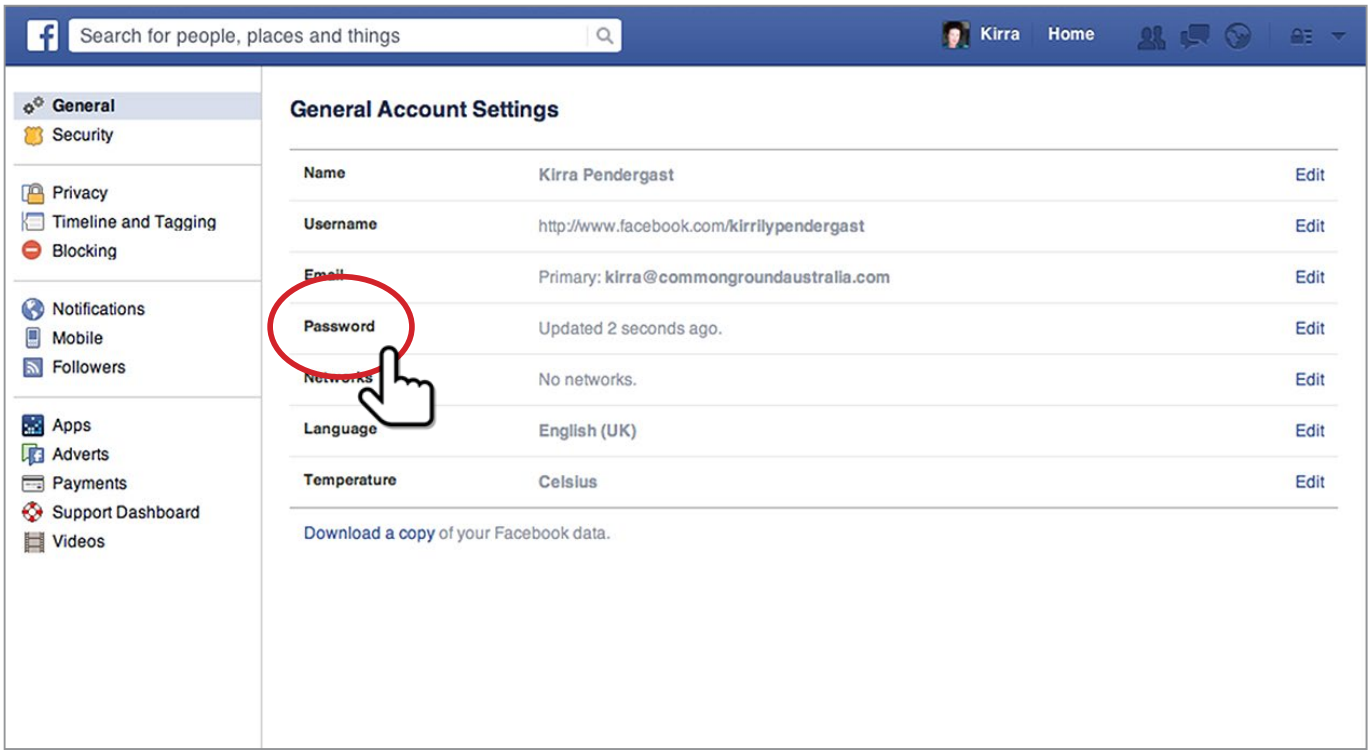
Here are our top tips for passwords:

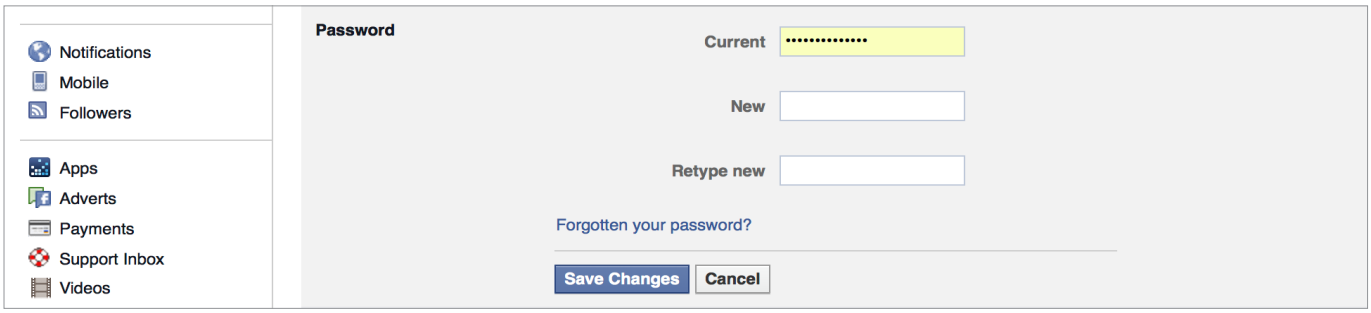
- Always use a strong alphanumeric password using upper and lower case letters and numbers for example: Il0v3D0g2 instead of ilovedogs.
- Do not use the same password for your Facebook account as you use for you bank account.
- Never share your password with anyone.
- Change your passwords regularly and always change it immediately if one of your friends is hacked, as this makes you immediately vulnerable.

We recommend that you change your password right now!

And every thirty days from now on.

The screen shot below shows the link to click on to alter your password.



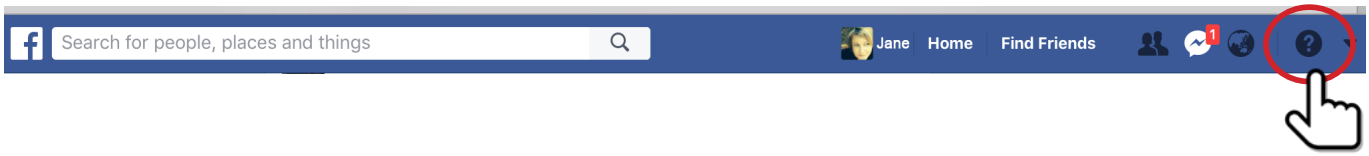


Facebook Security Features

Spend half an hour familiarizing yourself with Facebooks security settings. **Basics** details the simpler version of controls, use this if you don't immediately have the time to go through the lengthier options. **Advanced** expands to look at the full spectrum of security settings Facebook has made available.

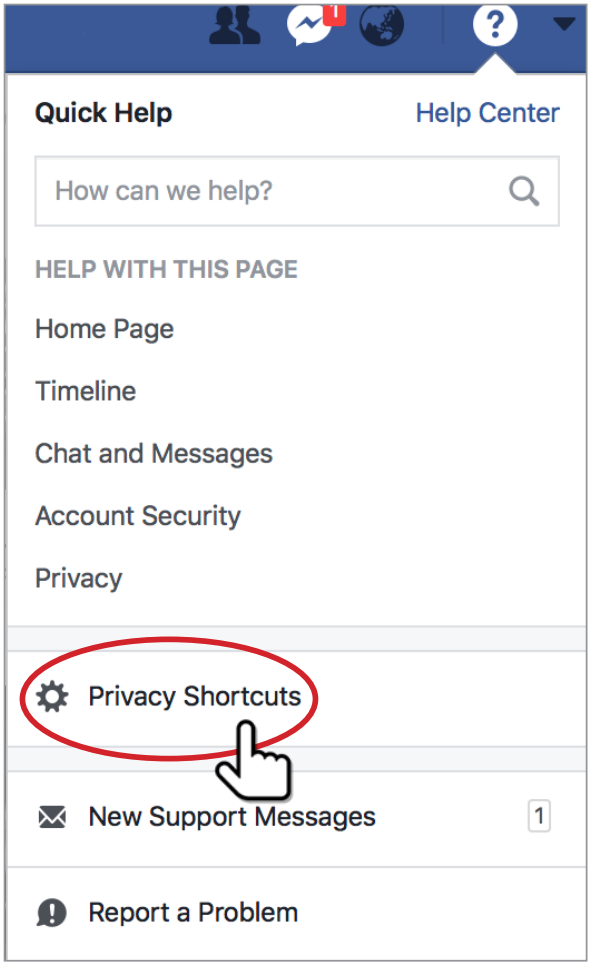
Basics

This is the beginners guide to Facebook privacy, that will take you to the most essential controls.



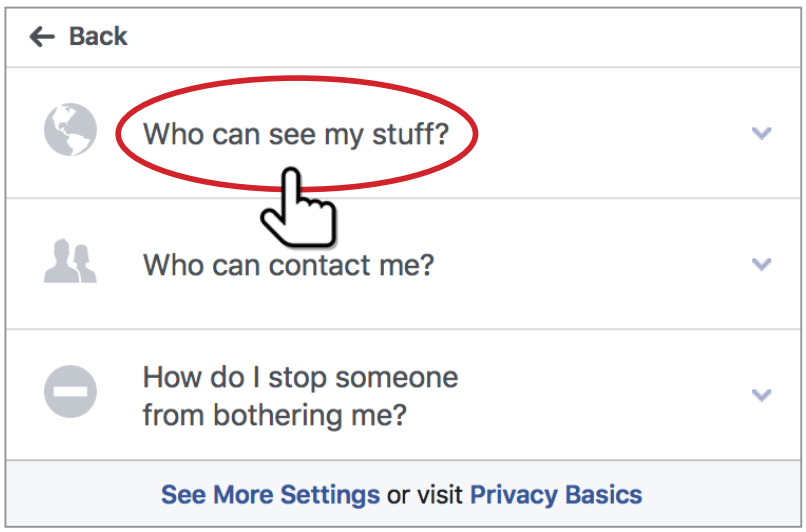
The question mark in the top right corner will bring up a drop down menu.

There are options to assist in using a Facebook account to navigate through but most importantly this menu contains vital Security and Privacy information.

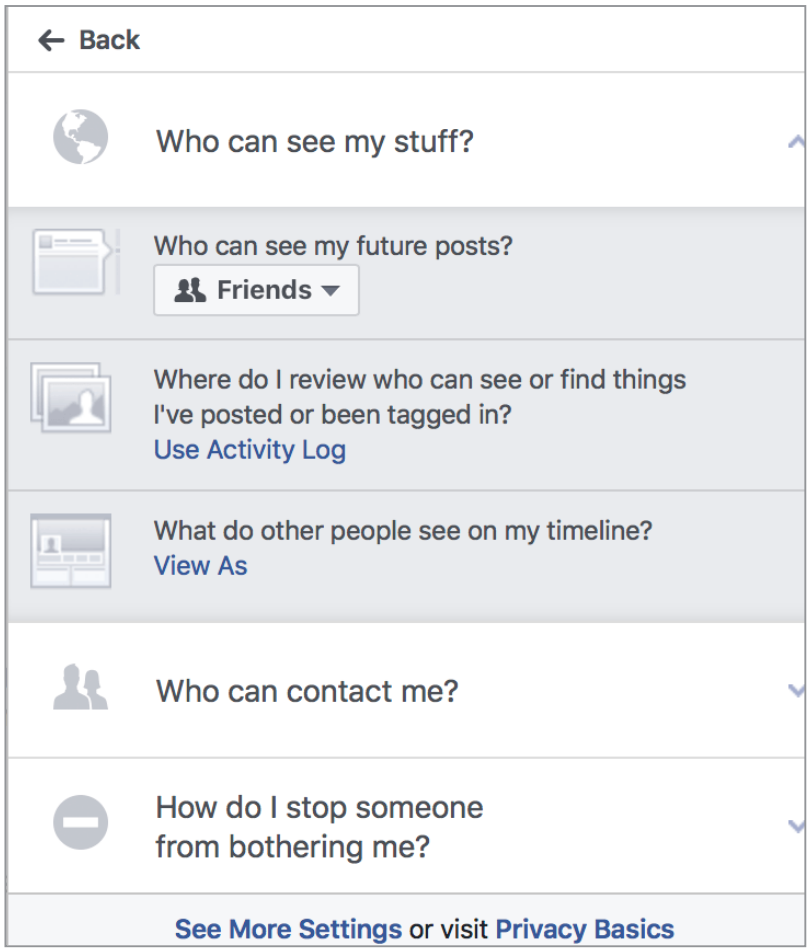


Choose the **Privacy Shortcuts** option.

These are the choices given:



Who can see my stuff will take you to:



The **future post** option allows you to choose between:

- Friends - private account to a limited audience you control (recommended
- Friends of Friends - semi- private account, but no control over who your friends, friends ar
- Everyone - public account with your information viewable for anyone

The **Activity log** option leads you to a section where all your recent comments, likes and photos - essentially all your interactions on Facebook.

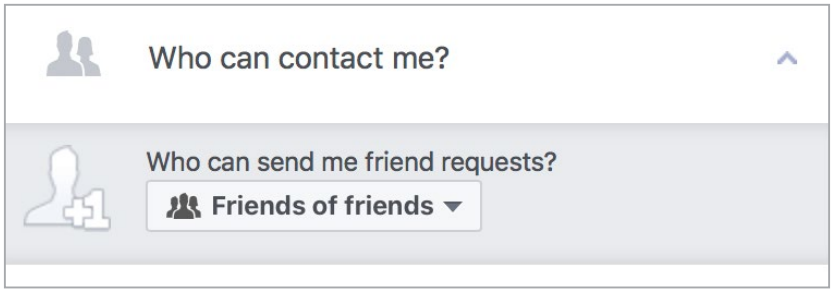
It gives you the ability to edit these in one place.

In the top right of each post there are two icons:

- The two heads will show you who can view that particular post- your friends, another's etc
- The pencil is the Edit feature and allows you to remove your interaction with that particular post

Lastly, the **View as** option shows you your Facebook profile as it appears. This illustrates effectively what effect your privacy features, or lack of them will show to the world.

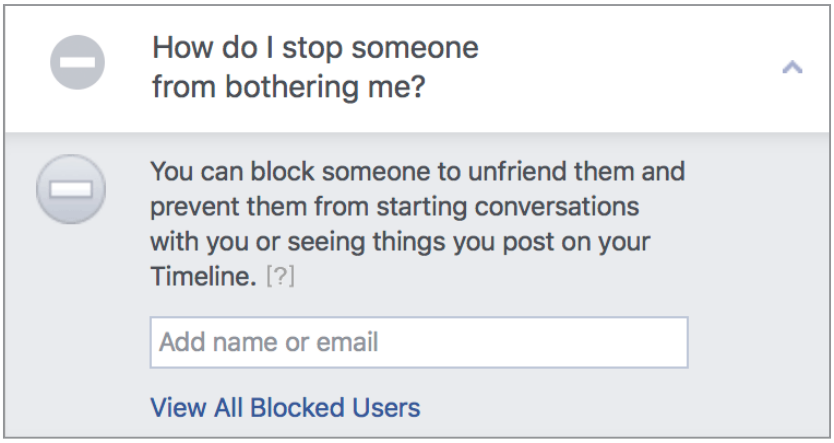
Who can contact me



Limits your receipt of random friend requests.

There are two choices of Friends of Friends and Everyone.

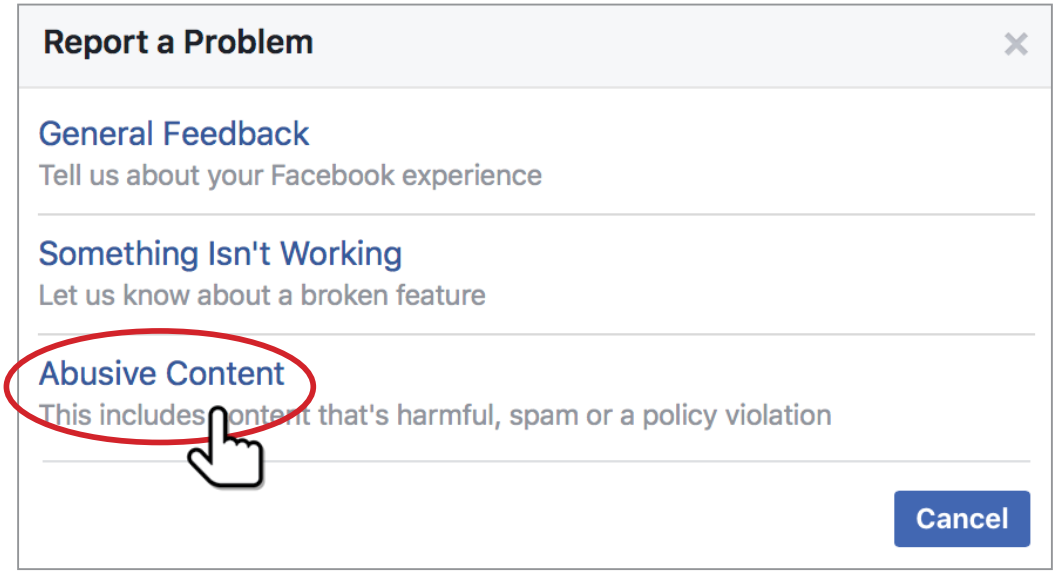
Blocking Someone



The option shown above is the quickest way to eliminate bullies, stalkers and the like from seeing your account, and stop them interacting with you.

Report a problem

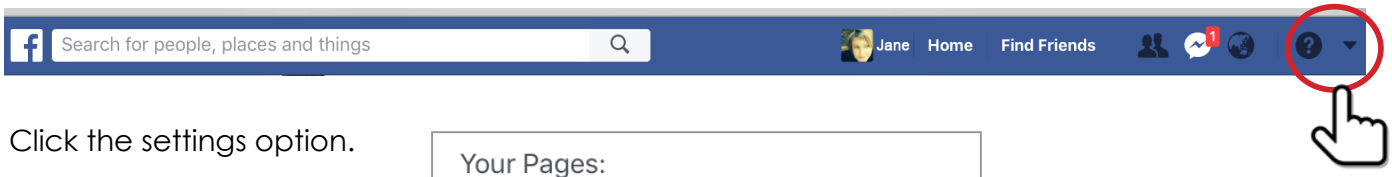
This is the quick contact link to Facebook for reporting problems including abusive behaviours online.



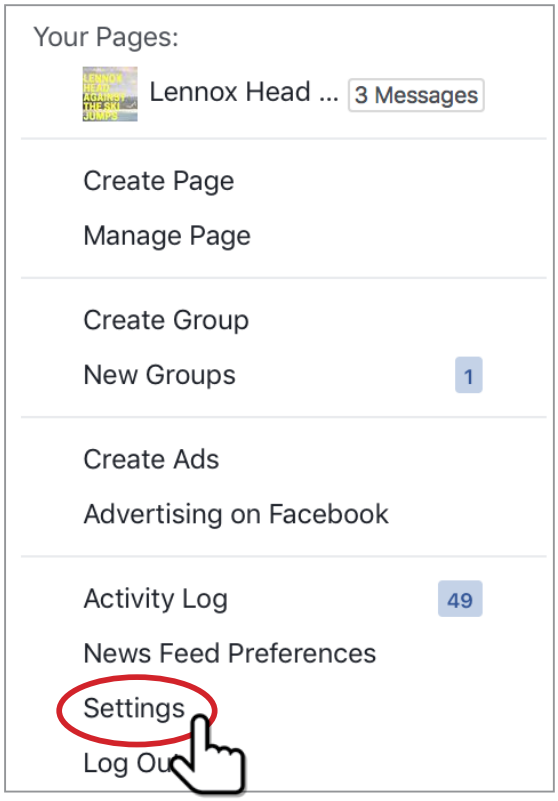
Clicking the **Abusive Contact** button will link to the Facebook help Centre where you are able to follow the choices to make your report.

Advanced

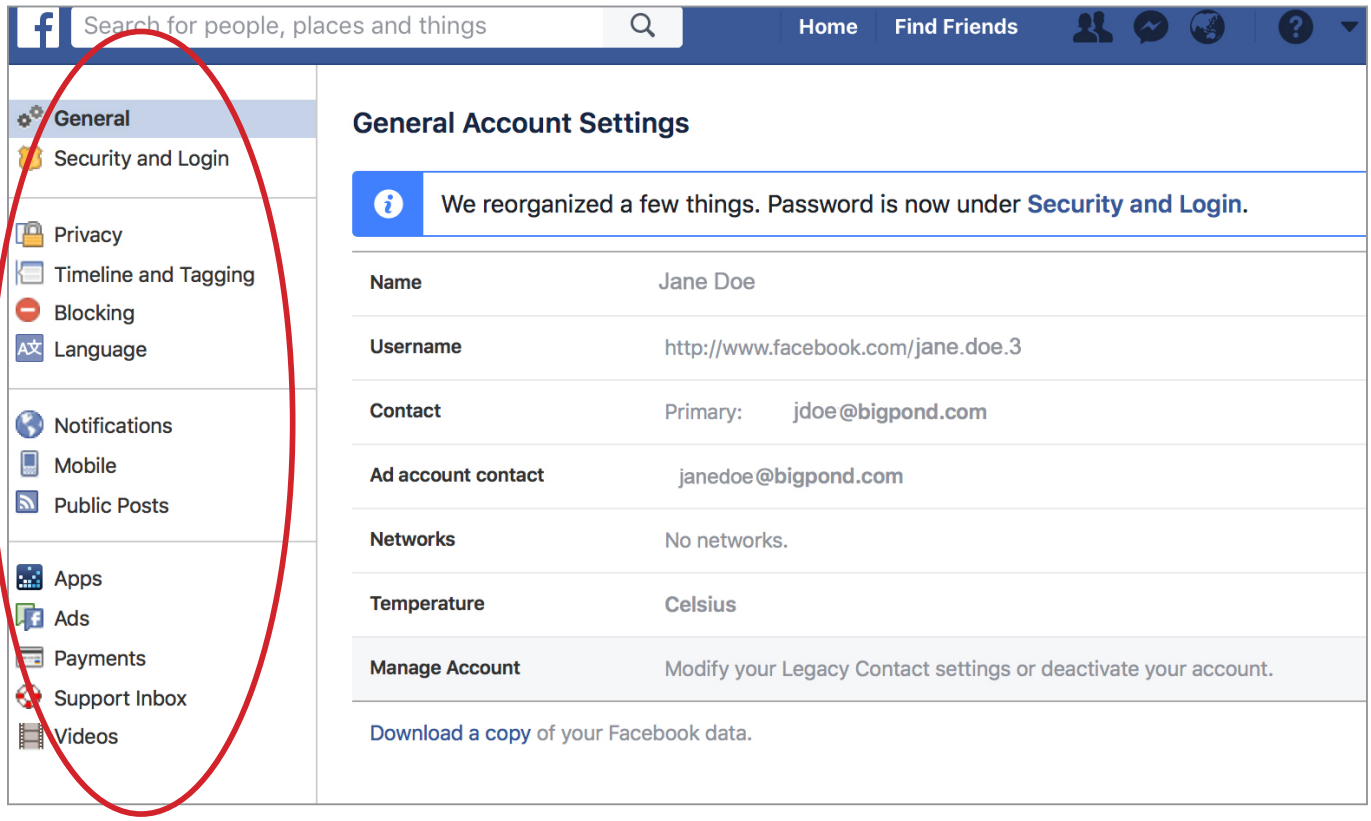
Start with the downward arrow at the top right of your Facebook page. This will bring up the drop-down menu.



Click the settings option.



The options on the left allow you to work through and lock down your account in a variety of ways.



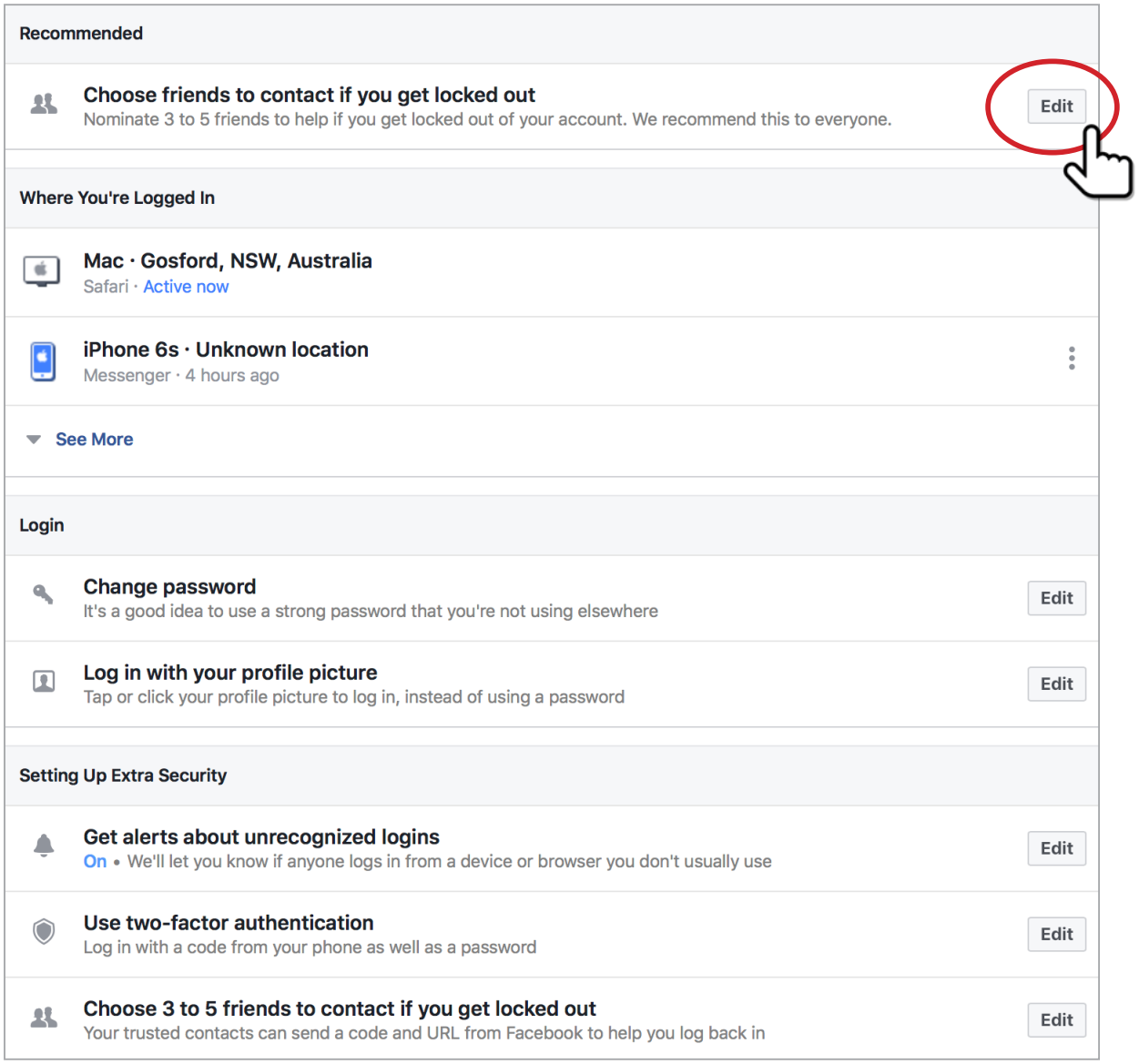
Each of the selections on the left has features that will control your account and the information you post.

All actions taken on Facebook have privacy and security concerns and familiarizing yourself with these will make your Facebook experience a safe and secure one.

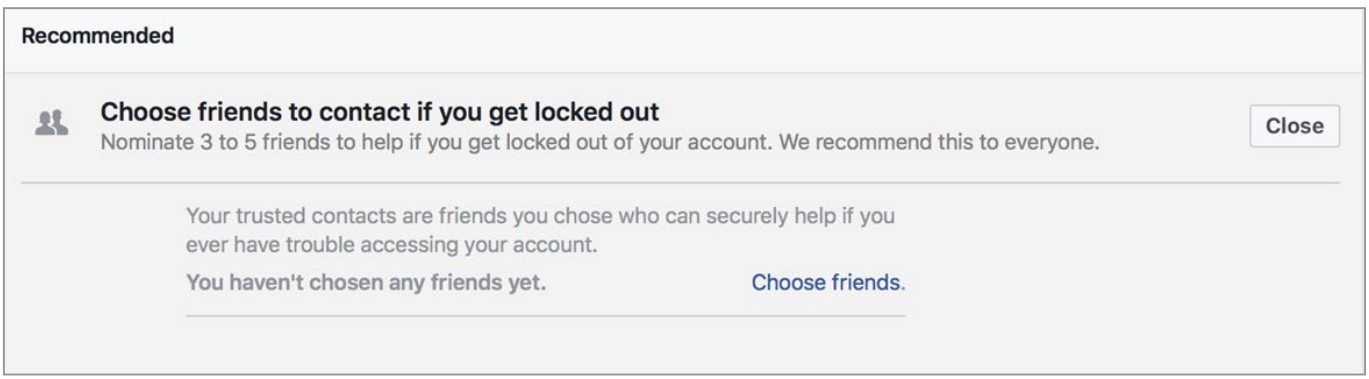
Spending time going through the controls with the family, and explaining the reasons why these are necessary is a pro-active way to have a discussion about internet safety and security.

Security and Login

This section contains several options that allows you to provide extra security for your account.

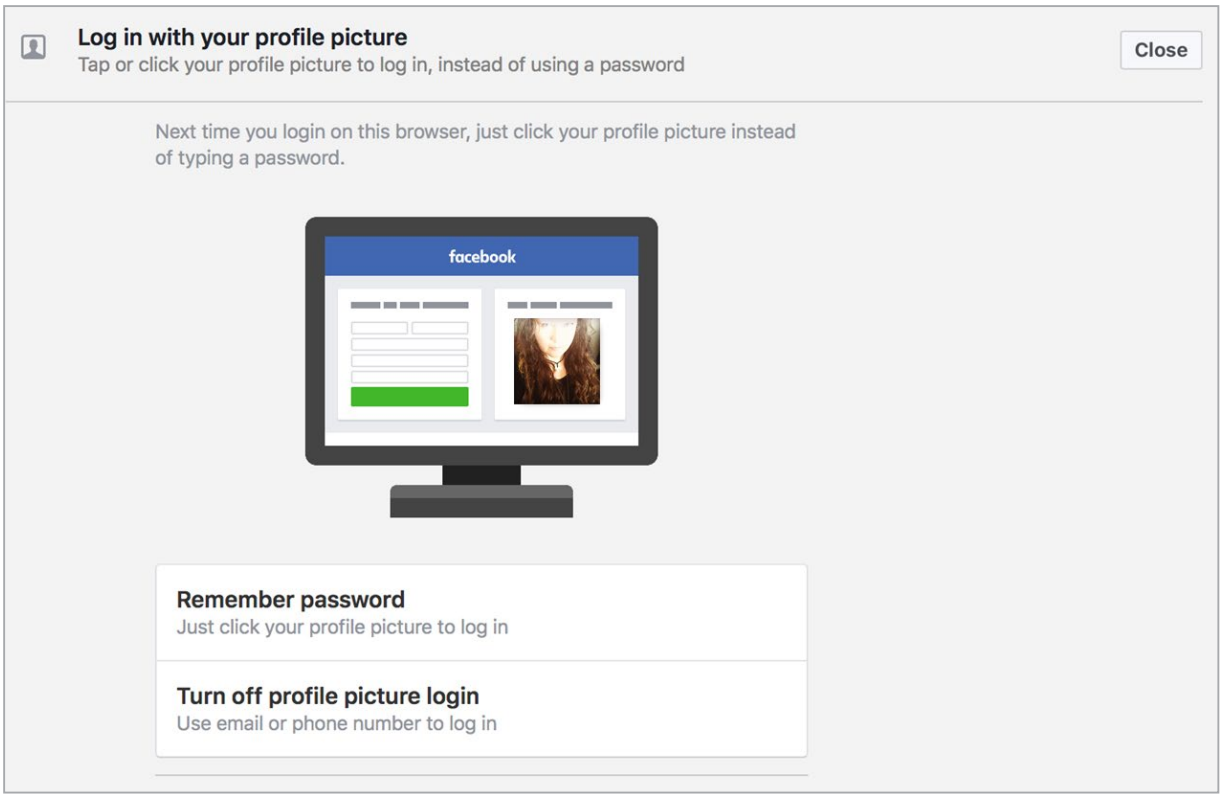


- There is a choice to select a number of trusted friends, should you become locked out of your account.



- The old "Where you're logged-in" function provides you with a list of the locations where your more recent logins have taken place. Should you have a concern that another person has been using your account, this is a useful tool.

- **Login with your profile picture**. This function is more for ease of use, than it is a valid security feature. It is meant to assist when account is either uninstalled or logged out of, and make it easy to return. Facebook needs to be given permission for it to work. Once enabled, you can log-in to Facebook by tapping on your profile photo. There is an extra requirement that can be added at this stage, to add a four-digit passcode to this method of login-in. To secure this feature, the passcode is a good idea.

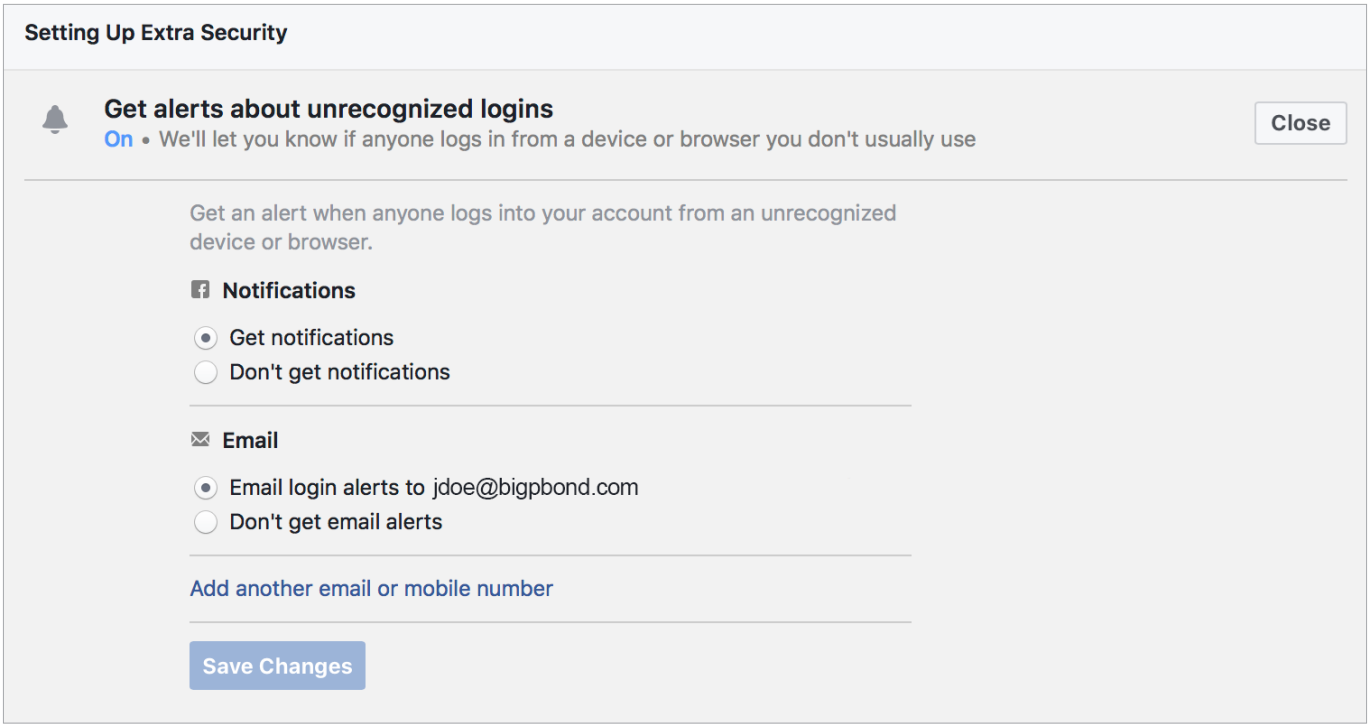


It's simple to turn off if you have enabled it; by using the lowest button in the screen shot above, and following the prompts.

Setting up extra security. These are the sections essential essential to really secure your Facebook account.

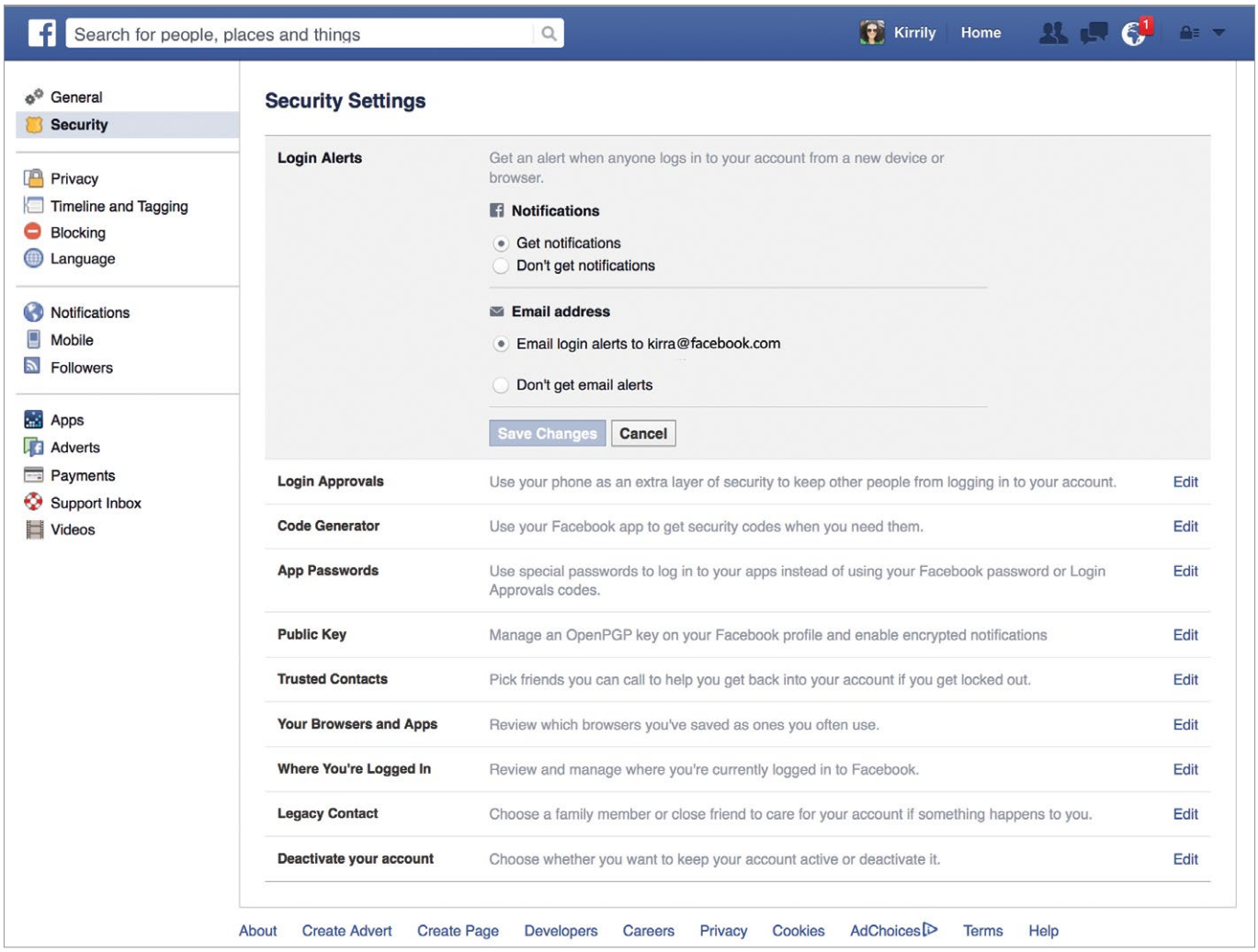
Alerts from unrecognized logins.

While this can often be the account holder logging in from a different device, this is not always the case. Using this system to receive notifications when an account is accessed from a new device, will warn you of activity on your account, independent of your own use. Once a new device is authorized the notification will not appear when the device is used again.



Login Alerts and Approvals

Facebook sends emails or SMS messages when there is suspicious activity on your Facebook account from a different location. You can determine if you want to receive these alerts and control how you receive them in your **security settings**. We highly recommend that you use this feature.



To further ensure your account security, Facebook launched "Login Approvals". This feature uses a Two-Factor Authentication Two-factor refers to: something you have (a device) and something you know (a password or code).

Facebook two-factor authentication or "code generator" uses your mobile device with your Facebook account and authenticates the login by sending a verification code to your mobile phone.

You can set up Android, iPhone, smart phones or any simple mobile phone to receive the verification code. Once you set up the secondary device for the Login Approvals, make sure that you never lose this device; or, you will be unable to use your Facebook account.

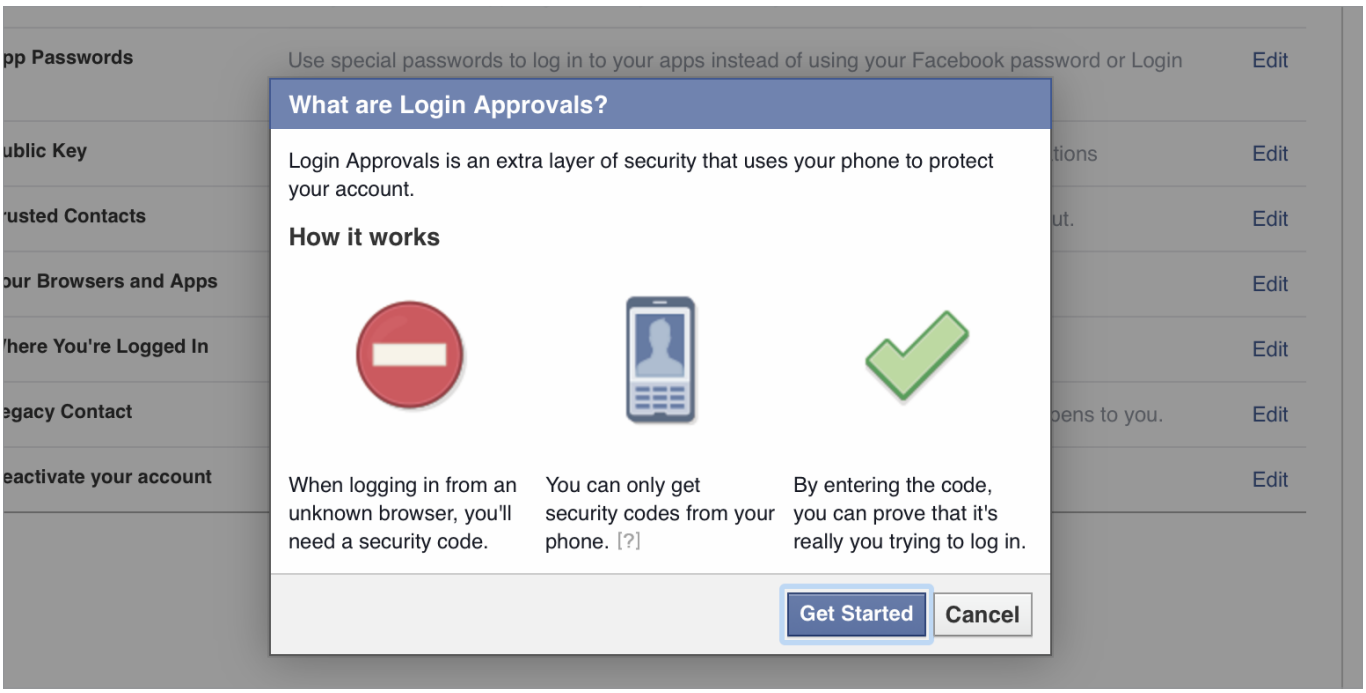
To set up login approvals without using the "code generator" option for your Facebook account simply follow these steps:

1. Click on the 'down' arrow on the top right corner of your profile page. This will take you to the general settings area by default.

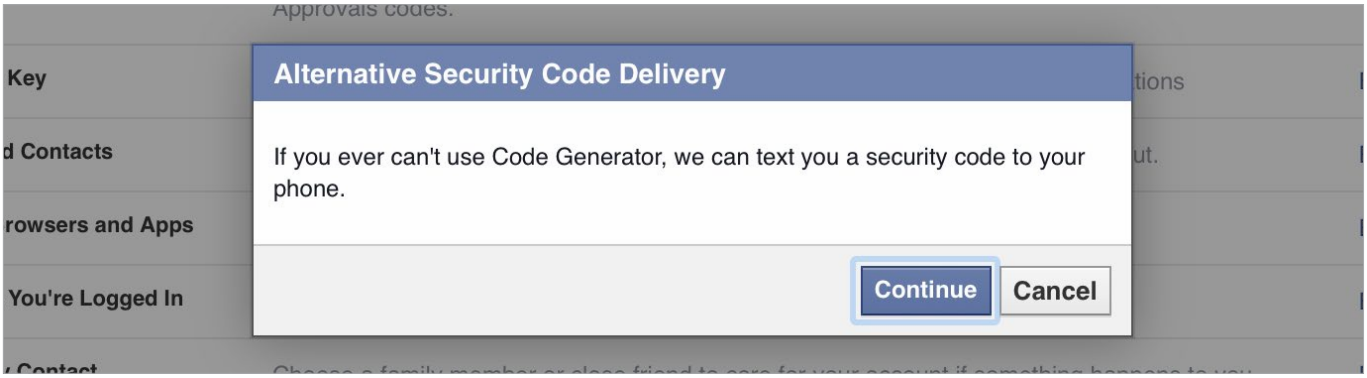
2. On the far left of the page directly under the word '**General**' you will see security. Click on this and it will take you to the security settings area.

3. The second down the list is '**Login Approvals**'; click '**Edit**'.

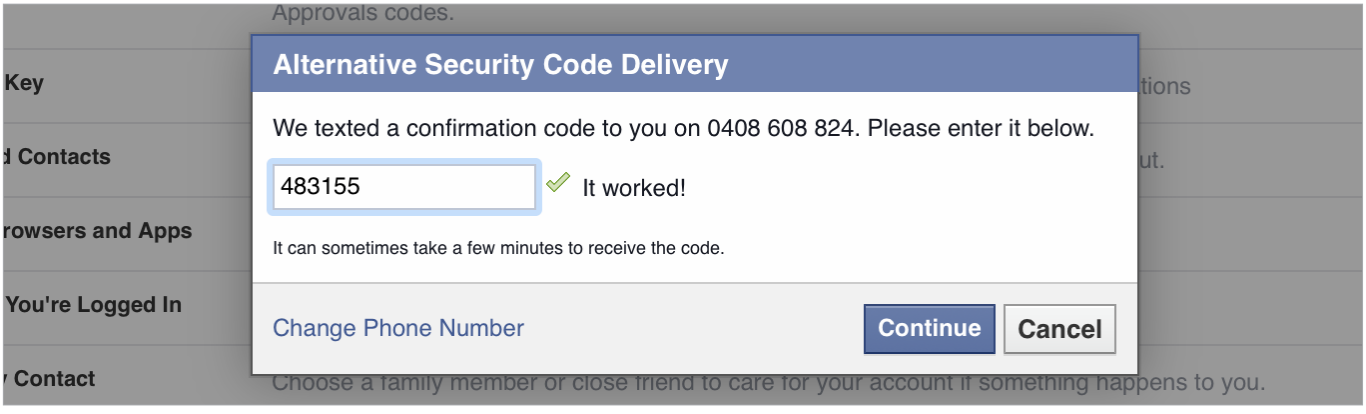
4. Click the box that says "require a security code to access my account from unknown browsers". You will be presented with a box and an option to click "Get Started"



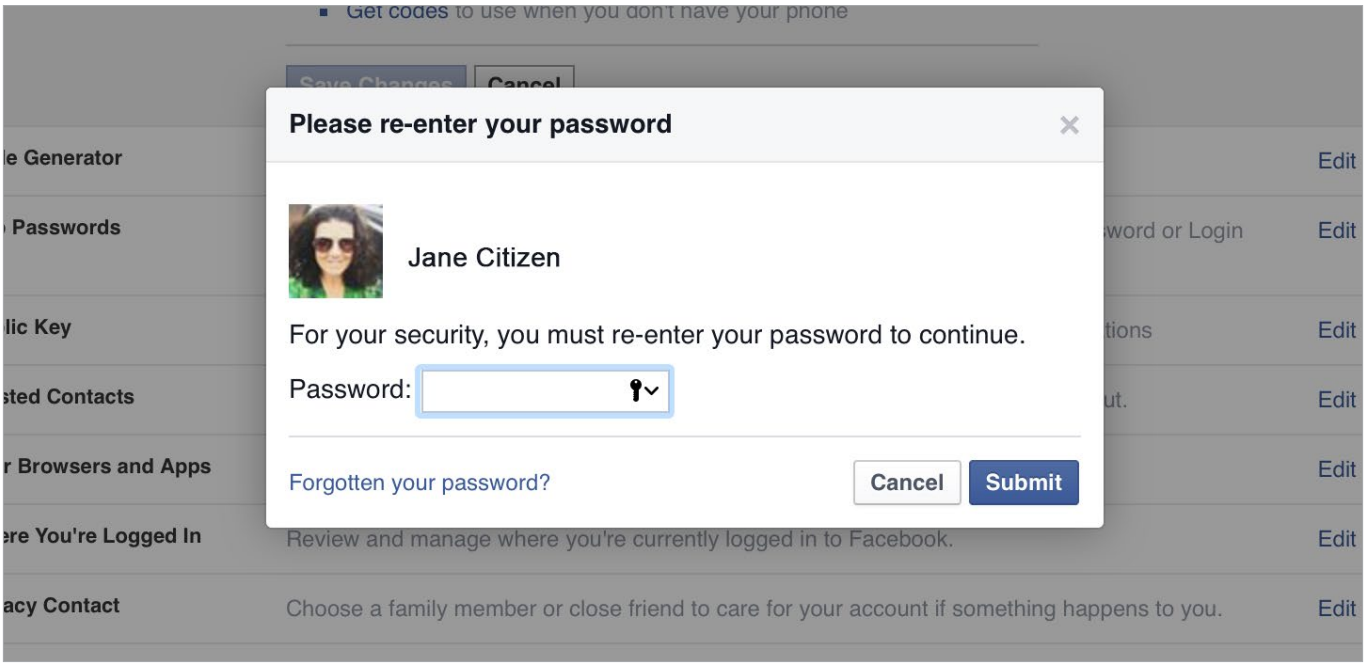
This will be followed by another window that tells you that if you can't use Code Generator, Facebook will text you a security code to your phone. Click 'Continue'.



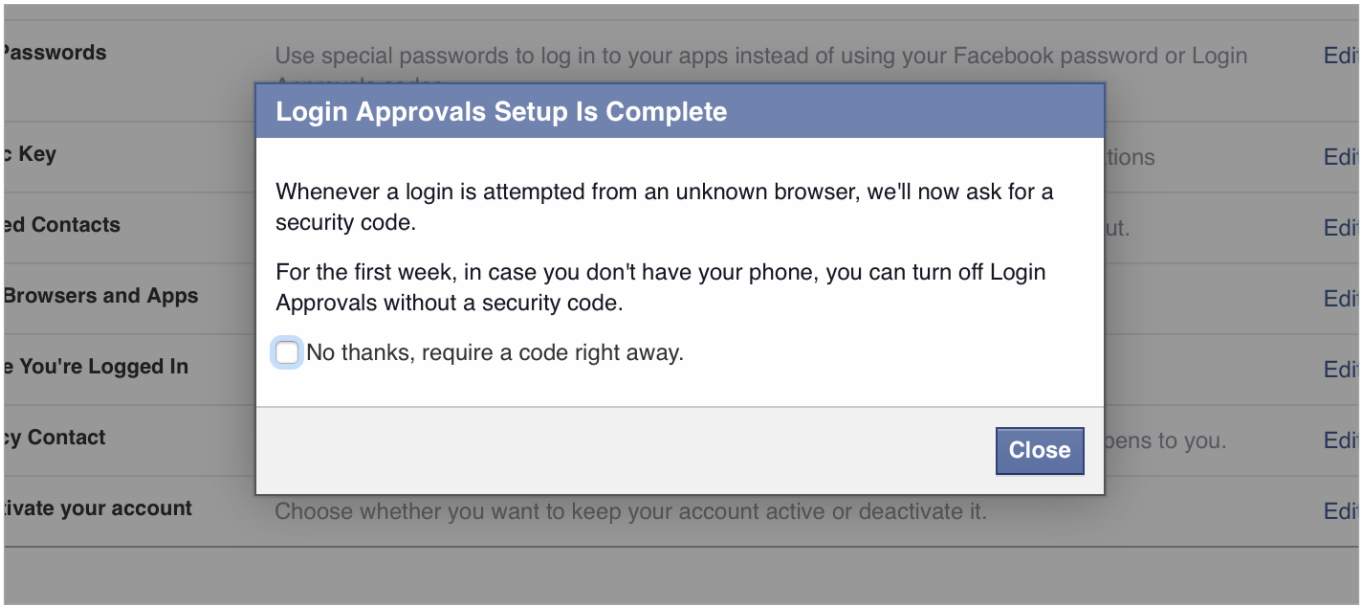
5. You will then see "set up security code delivery". Enter your phone number and click 'Continue'. Shortly after you will receive a text message on your phone with a confirmation code. Enter the confirmation code in the box provided and click 'Continue'.



6. Facebook will then ask you to re-enter your Facebook password.



7. After you have re-entered your password you will see the following, make sure you click the box specifying that you require a code right away. click '**Close**'.



To set up login approvals using "code generator"

Code Generator is a part of the Facebook app and creates a security code every 30 seconds. This occurs even when you are off-line, and this feature can send necessary codes via SMS.

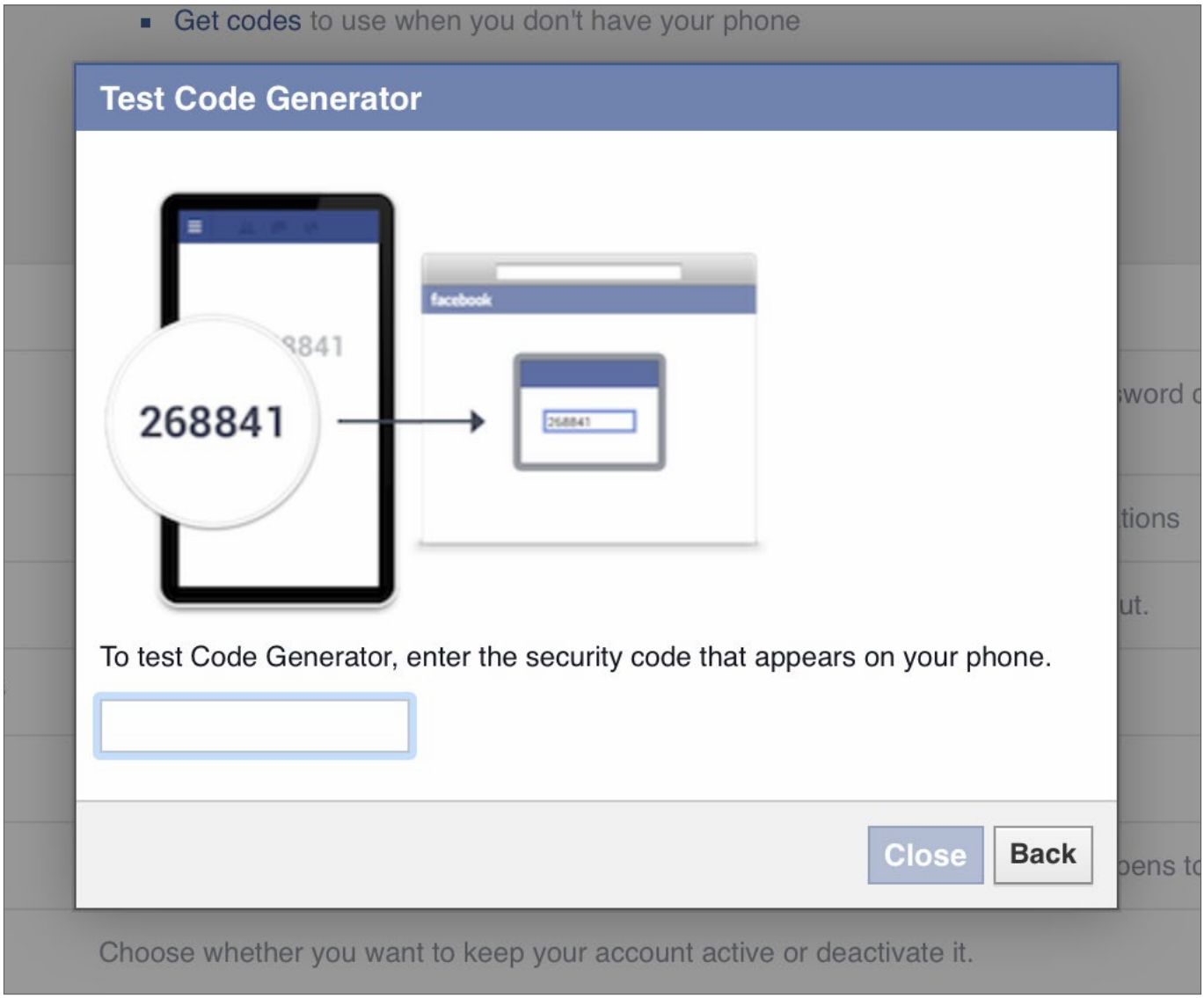
This code, and your password will be used to log into your Facebook account.

Using Login Approvals and the Code Generator" feature will give you an extra layer of security, and make it more difficult for your Facebook account to be hacked.

Not only do they need to hack your password, they also need to either get hold of your mobile phone to receive the security code or hack that code to access your account.

The code is needed to access Facebook from a device not previously authorised.

Once set up, an attempt to log into your account from another computer, a security code is sent to your mobile to notify you.



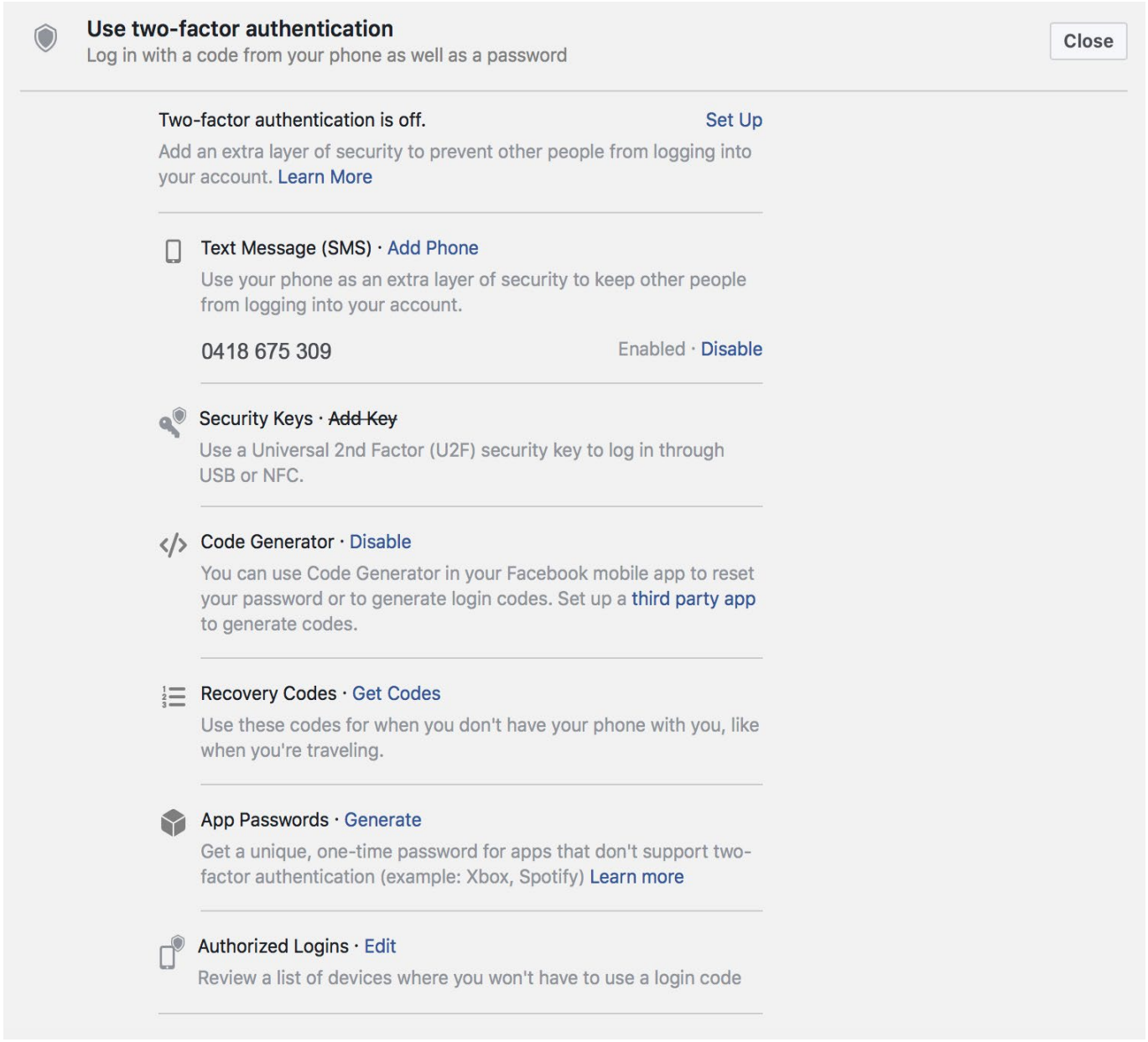
Two factor authentication system

This is step two, after a secure password on your account.

When Facebook doesn't recognize the computer or device an account is either logged in from, or there is an attempt to access from a strange device, a special security code or confirmation will be required.

You are able to select how you receive alerts . The options are :

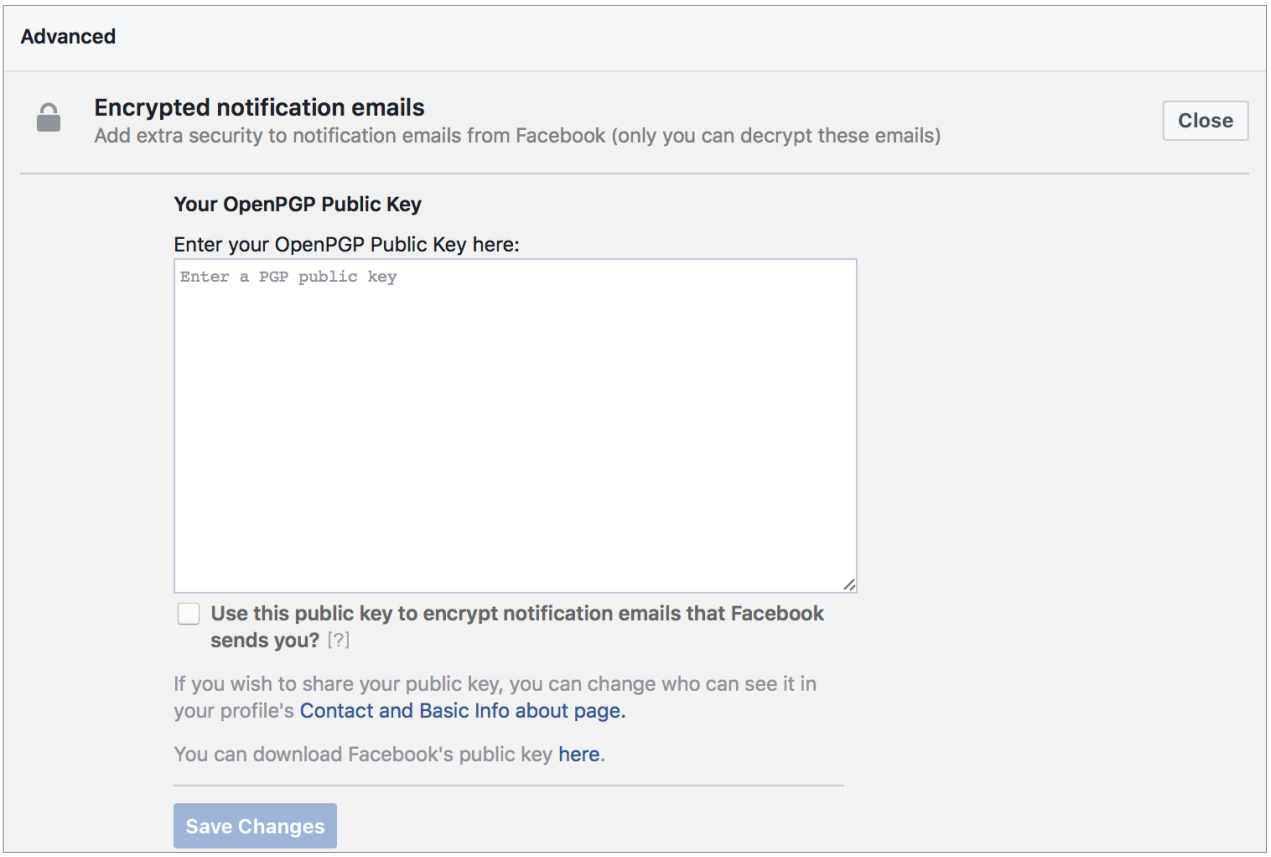
Receive a text message
Receive a security code from the Code Generator
Tap your security code on another device
Approve the login from a recognized device
Use a printed recovery code
Use security codes from a third-party app.



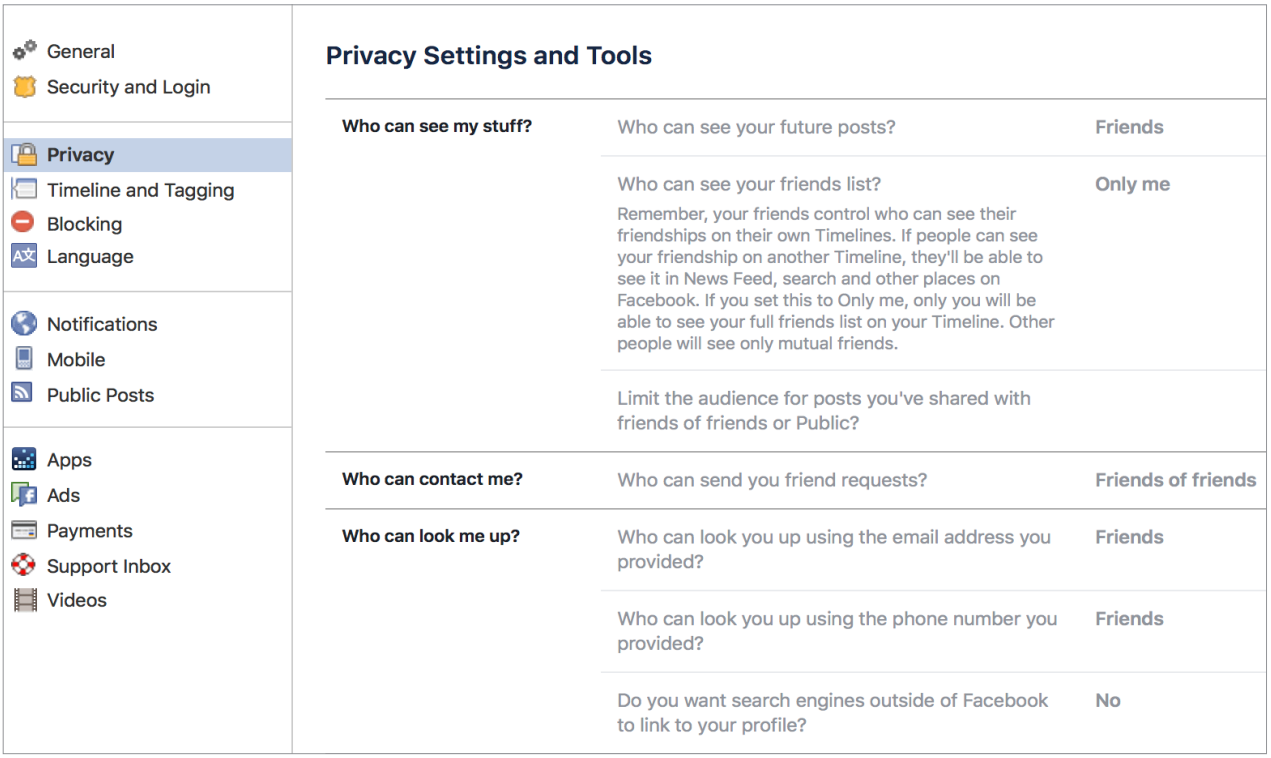
Encrypted email notifications

One of the more complex settings available, this has a use for sensitive accounts and content. Emails are hidden from from servers that scan users in-boxes, are fraudulent or used for marketing purposes.

Where this feature becomes very useful is in conjunction with Facebook Tor site. Combined together these systems hides the account holder's identity completely, maintaining anonymity.

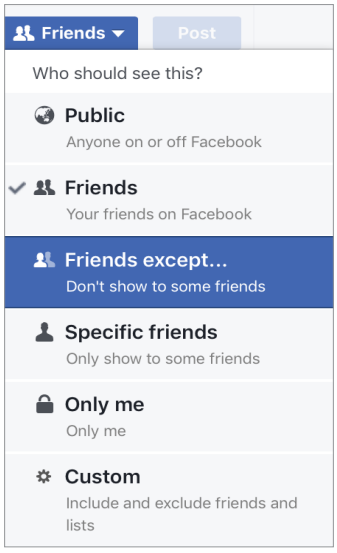


Privacy features



Here you may add further controls to those already set up on the **Privacy Shortcuts**.

- You can control who sees your future posts, choosing from the drop down-menu from



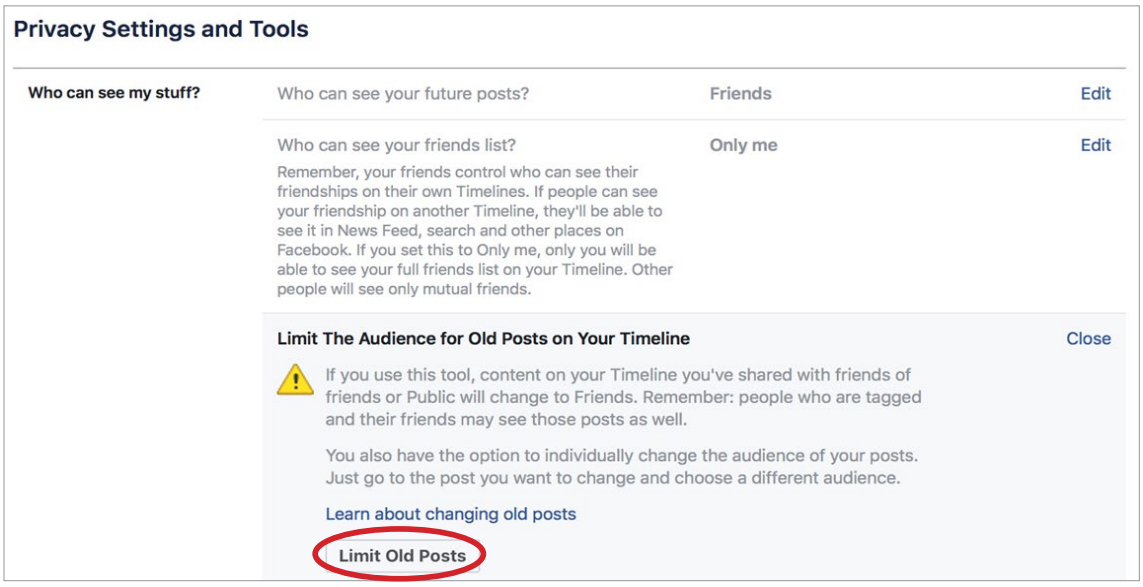
- Limit viewing of your friend list to:
    - Friends
    - Friends of Friends
    - Everyone
    - Only Me
- Limit last posts, allows to you to re-gig your privacy settings retrospectively (see below)

Limit last posts

To keep strangers from poring through every single detail of your Facebook history, you'll want to turn any post that's either **Public** or visible to **Friends of Friends** into strictly Friends only posts. To effect this change, click on the **Privacy Shortcuts** icon in the top right to bring down the following menu.

At the beginning of 2013, Facebook made old posts searchable. The Facebook Graph Search allows searches across every last check-in, status update, note, and comment you've ever posted throughout your entire Facebook membership.

The main concern with Facebook's new search system was whether each of your hundreds of past posts, now required its own, unique privacy setting. Facebook will let you you change your entire past en masse…... sort of.



Determine who can search for you.

- **Who can look me up** will curtail access to the e-mail address and phone number you provided to Facebook when you first installed an account.
  Again, the settings offer you the choice of Friends.

    - Friends of Friends
    - Everyone

It is recommended these choices be set to **Friends** only.

- If you want to prevent your Facebook profile appearing in Google search for your name, choose the "no" option when asked if you wish for search engines outside Facebook to link to your profile.

Blocking

This section has expanded considerably. You can have extensive control over the kinds of posts, messages, users, invitations, pages and apps that contact you.

Features include:

- **Restricted list**. If you place one of your friends on the restricted list, they will never know or see any of your posts you normally choose to show to only your friends. They will be able to view those set to everyone and to friends of friends, but for more casual acquaintances your more private memories and interactions can be limited.

- **Block Users**. Completely shut down a stalker, a bully or generally unpleasant person. With the exception of games you may both play on Facebook, they are unable to see you and your activity.

- **Block messages**. This affects the messenger app as well, and stops a bully or stalker being able to comment or message you.

- **Block app invites**. No more Farmville, or Candy Crush notifications with this turned on. It's essentially a spam from friends blocker. Once turned on , it will block all further invitations originating from that particular friend.

- **Block event invites**. For the friend who is constantly having parties, events etc. and inviting all and sundry. Once turned on, all event invitations from the friend will be blocked.

- **Block apps**. This is a handy one to limit the private information apps can access about you through Facebook. Turned on both blocks the app from contacting you, and stops it gathering information from your account.

- **Block pages**. This blocks a page from contacting and commenting on your posts. This function will also unfollow and unlike the page in question.

Manage Blocking

Restricted List

When you add a friend to your Restricted List, they won't see posts on Facebook that you share only to Friends. They may still see things you share to Public or on a mutual friend's Timeline, and posts they're tagged in. Facebook doesn't notify your friends when you add them to your Restricted List. Learn more.

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 Add name or email Block

- Luke Stephen Richardson Unblock

Block messages

If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app either. Unless you block someone's profile, they may be able to post on your Timeline, tag you, and comment on your posts or comments. Learn more.

Block messages from Type the name of a friend...

- Byron Bay Secrets 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 Type the name of a friend...

Block event invites

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

Block invites from Type the name of a friend...

- Graeme Chapple Unblock
- Justin Stewart Unblock

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 Type the name of an app...

- 21 questions Unblock

Block Pages

Once you block a Page, that Page can no longer interact with your posts or like or reply to your comments. You'll be unable to post to the Page's Timeline or message the Page. If you currently like the Page, blocking it will also unlike and unfollow it.

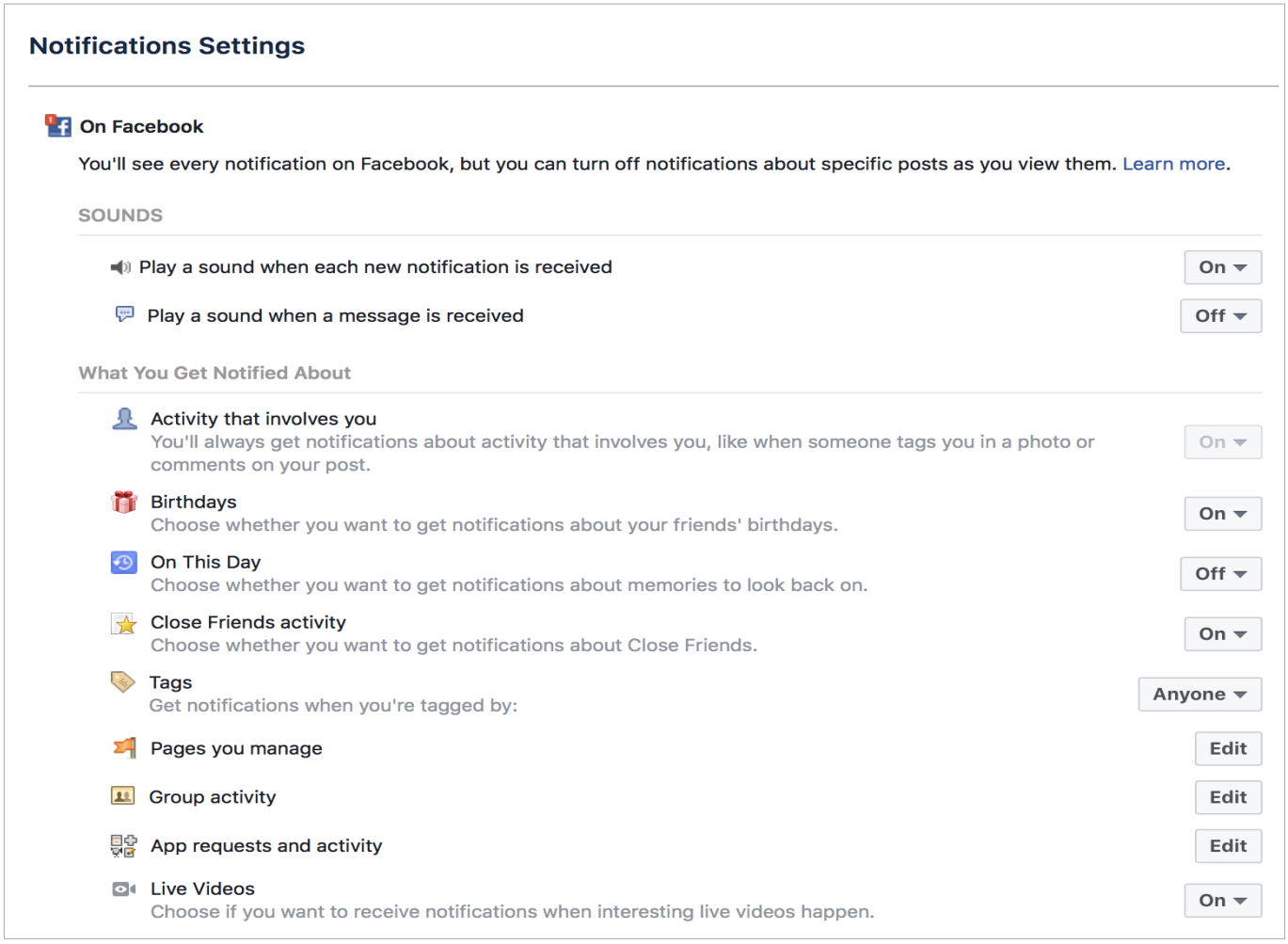
Block Pages Type the name of a Page...

Notifications

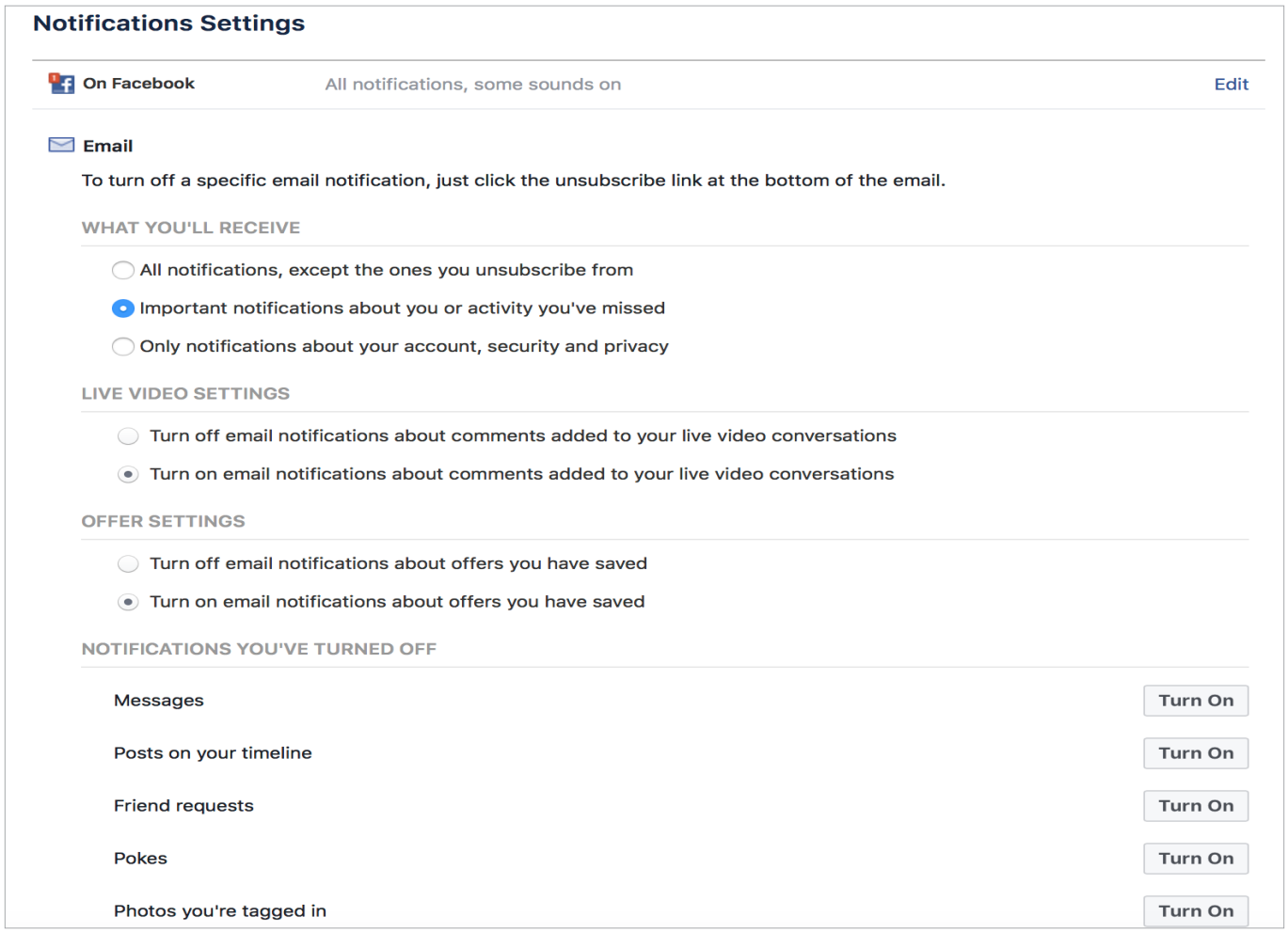
This is a very large section about controlling what notification messages you choose to receive on your devices.

Allowing all notifications can be chaotic with a constant stream of notifications being delivered by text and email.

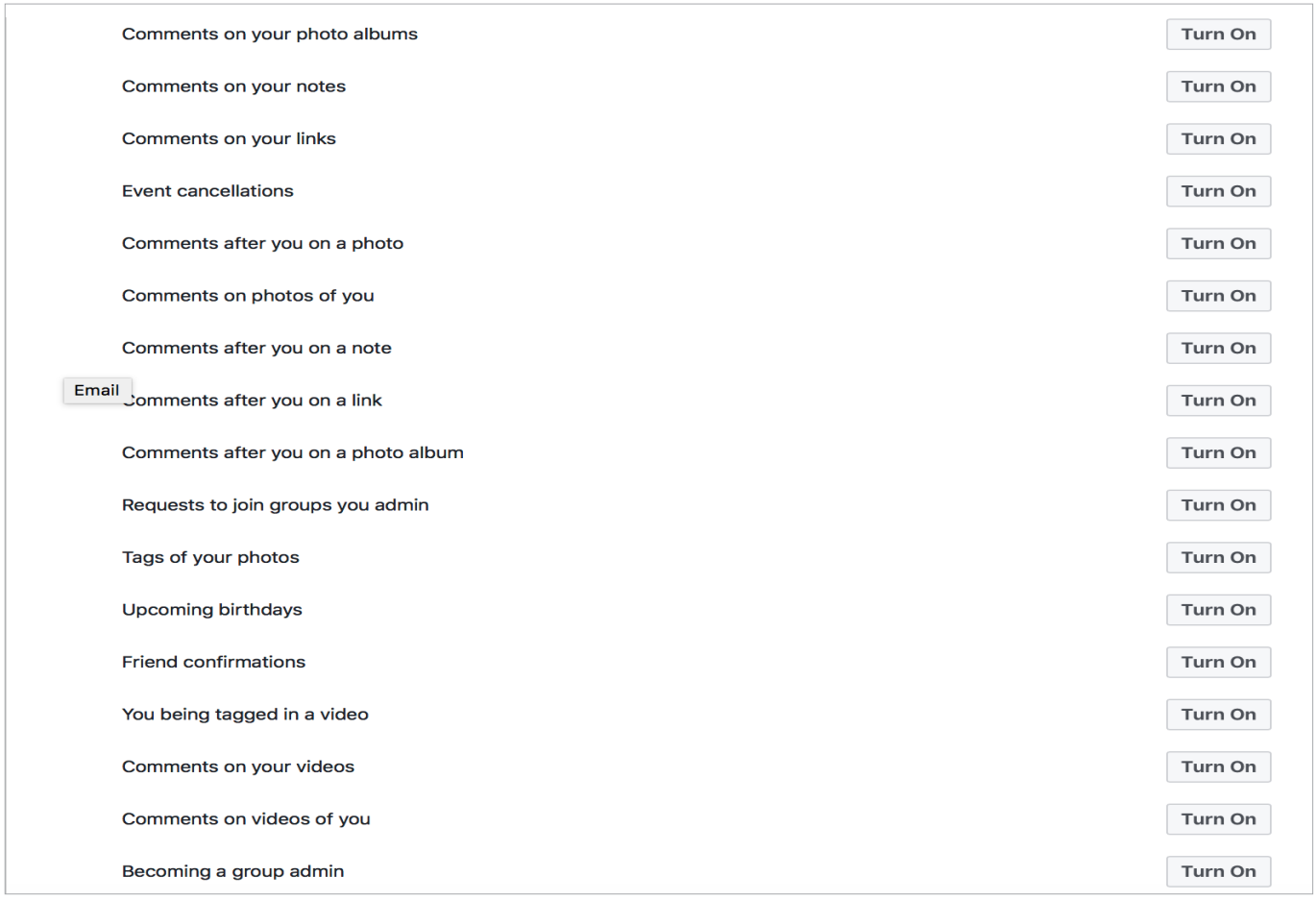
You can tailor this section nicely, so you are only reminded about important calendar events and not be constantly spammed each time there is an interaction with one of your activities on Facebook.



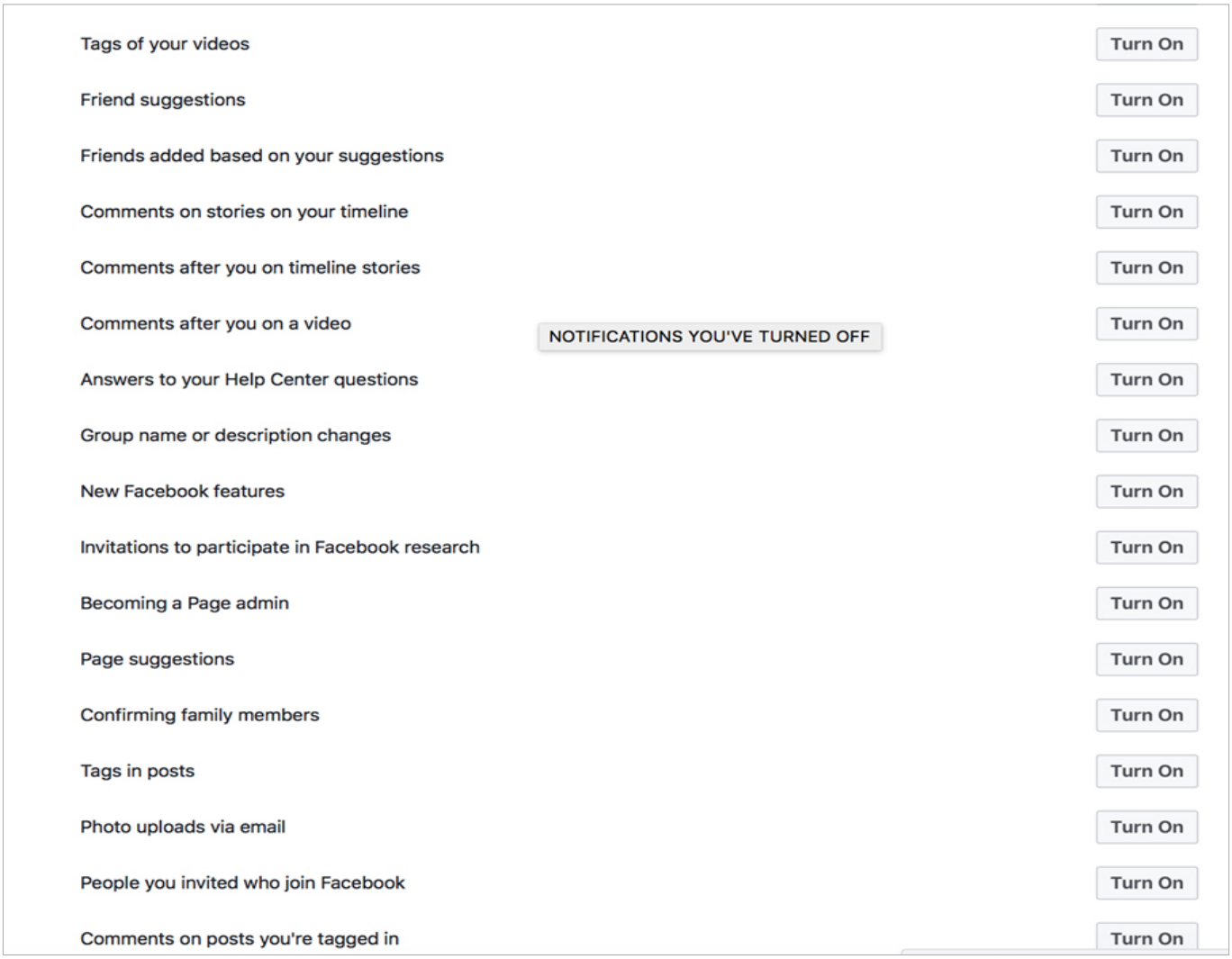
The sheer number of notifications you can turn off in the email section is daunting.



But there are more...



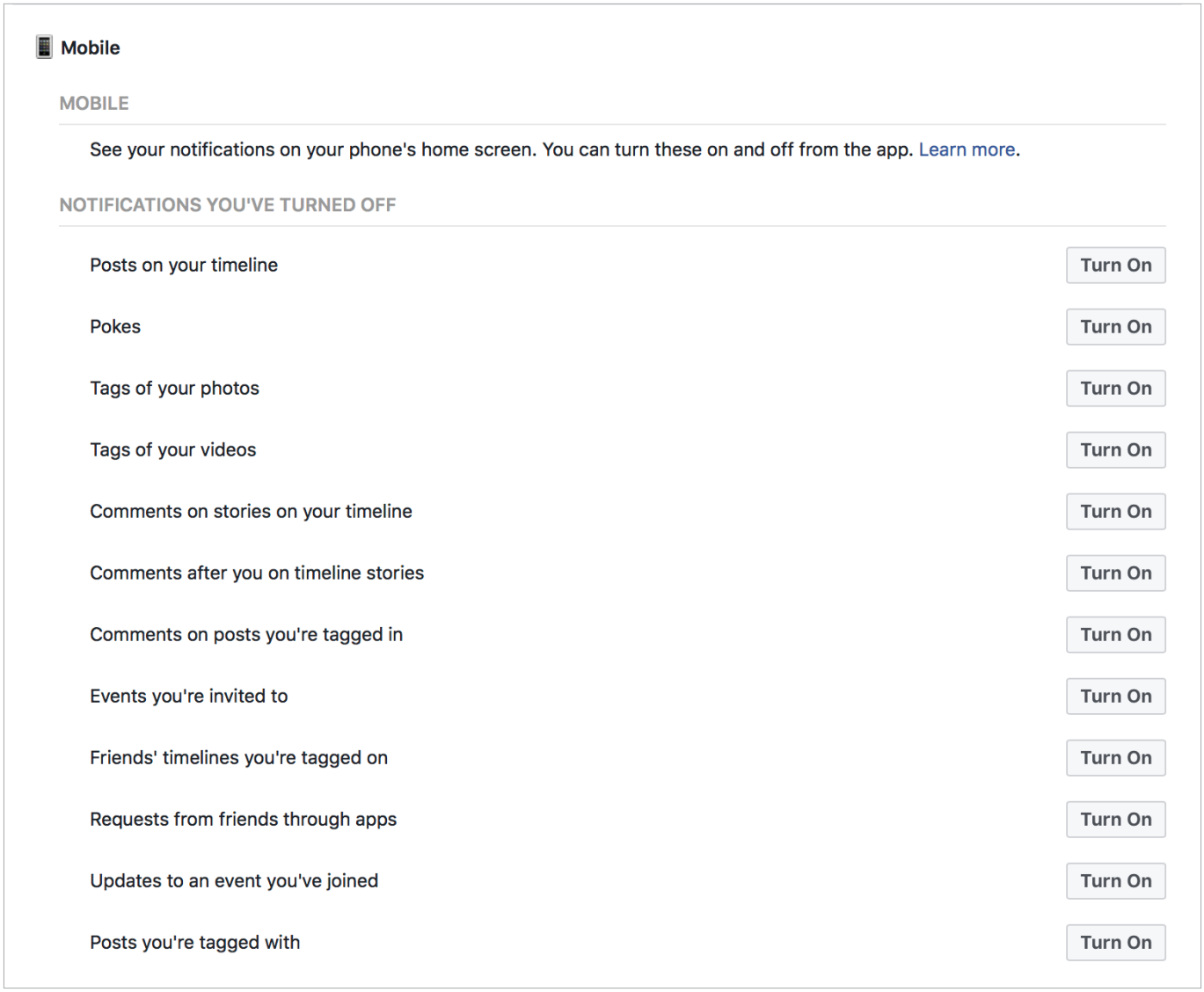
and still more...



Choose to remove the notifications that have no use to you, and will clutter up your inbox unnecessarily.

Mobile Notifications

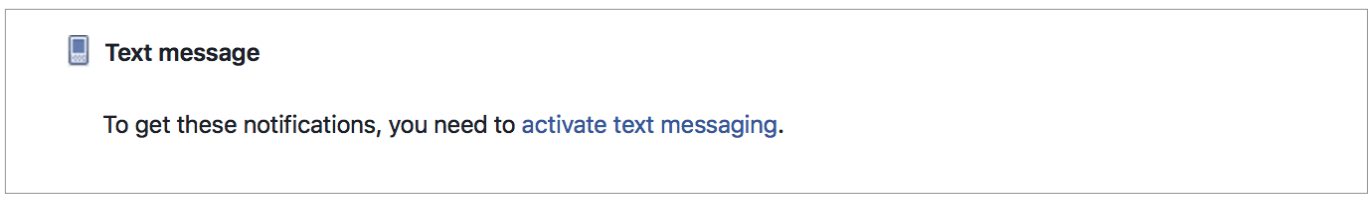
Select the notifications you wish to come through to your mobile devices



Make the same considerations as you would for your email notifications.

Text message

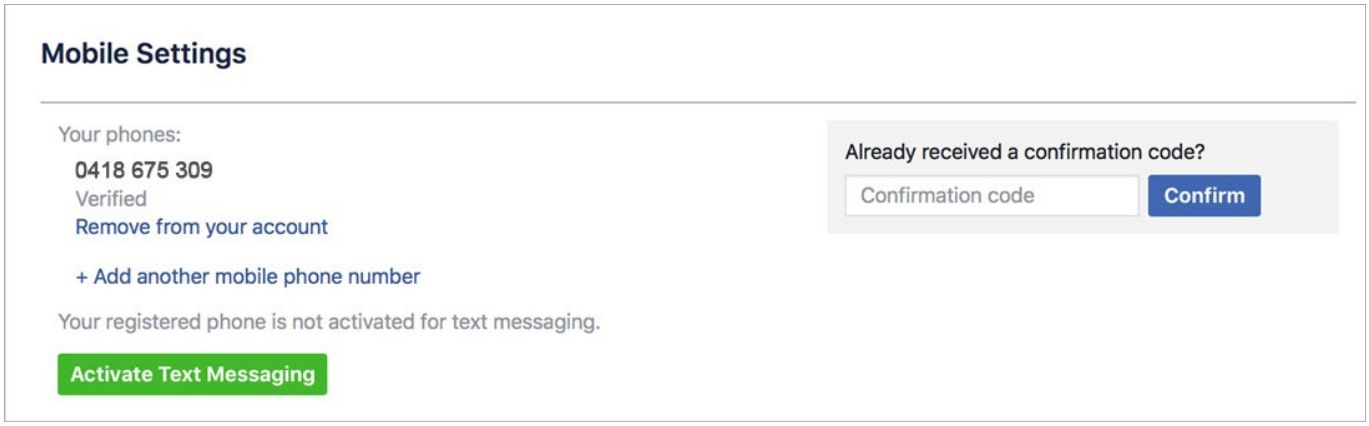
- Make a choice whether you want to receive text messages to your phone, when there are responses to your Facebook activity.



Notifications may be turned on and off very simply, should you wish to follow responses to a particular thread you are commenting on etc.

Mobile Settings

This is the location to change your mobile contact details, set confirmation codes and choose whether or not to activate the text messaging service.

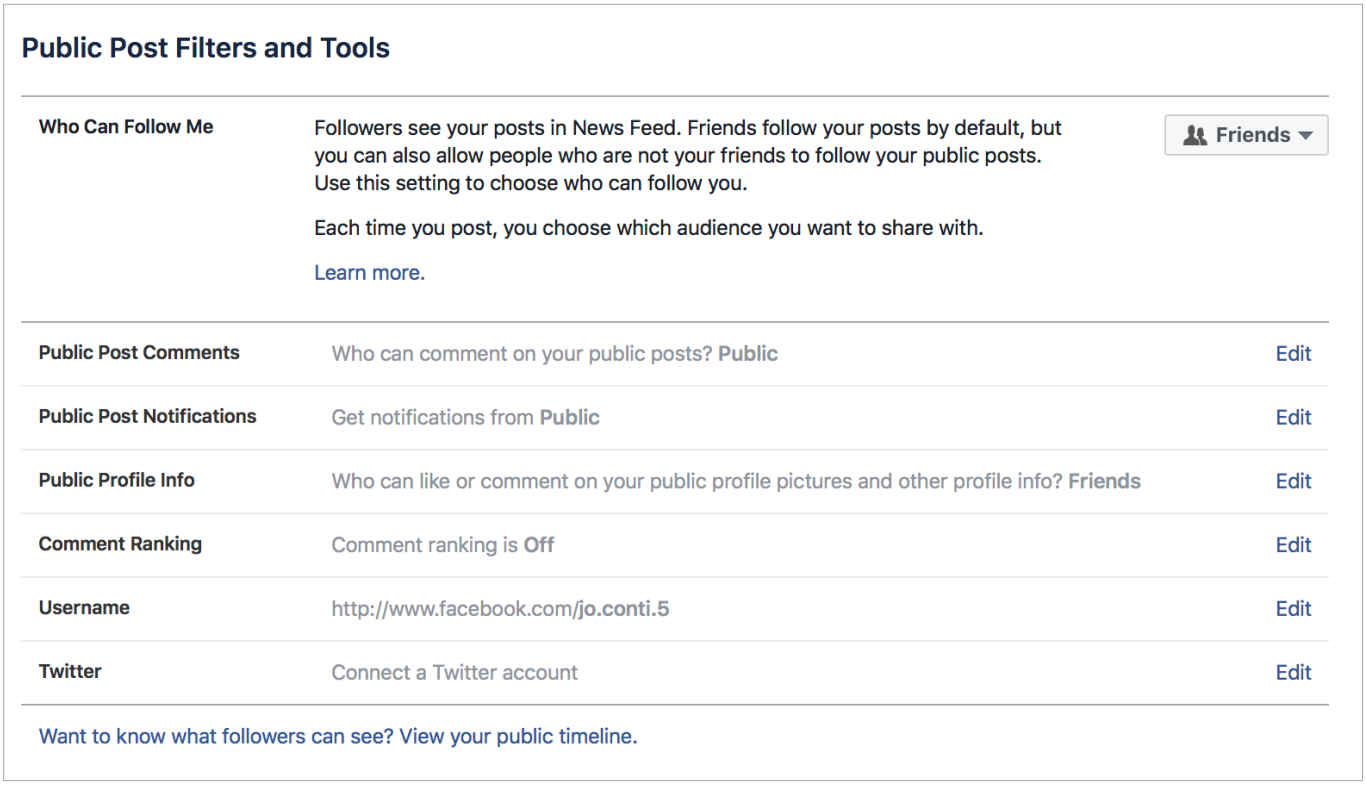


Public Posts

Here you are able to control the comments on public posts you make. Public posts may be viewed by anyone, and this tool allows you to moderate the activity that takes place on your post, and determine whether or not members of the public can engage with your profile.

Public posts are able to be searched in online search engines. This applies to both previous and new posts /pictures/videos made with the settings on public. If you have changed the public settings for future posts, it is worth reviewing the **Limit past posts** option mentioned above.

NB – if your last post was a public one, this will become the default for any newer posts. Remember to turn your privacy settings back to their normal levels the next time you wish to post.



Apps = Third-party apps

What they are

The word 'app' is an abbreviation of 'application'. In this instance is a software application, or a software program. These programs are typically found on a smart phone or a mobile device.

In context, an app can be defined as a software program for use online or on a smart device, via a browser. In early March, Google removed from its Android Market more than 60 applications carrying malicious software. Some of this malware was designed to reveal the users private information to a third party, replicate itself on other devices, destroy user data and even impersonate the devices owner.

It is important to ensure that apps are only downloaded from trusted websites and app privacy is maintained. Always read user reviews of an app when downloading and throw out apps you are even remotely suspicious about.

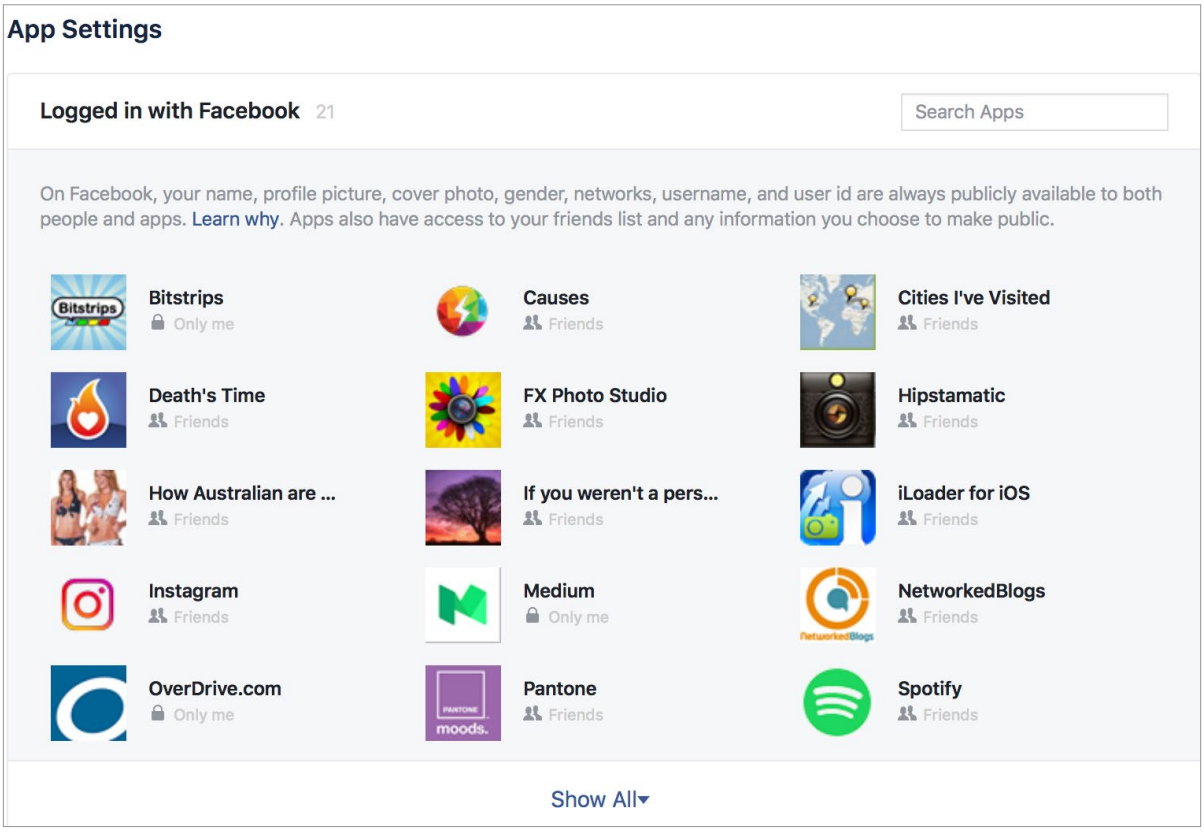
Keep an anti-virus system on your phone or device that runs apps updated and runs scheduled checks.

Use trusted security measures to store personal data and be very wary about sharing personal information. Always control app privacy. This is guaranteed to let you have the best of the social media world without compromising your security.

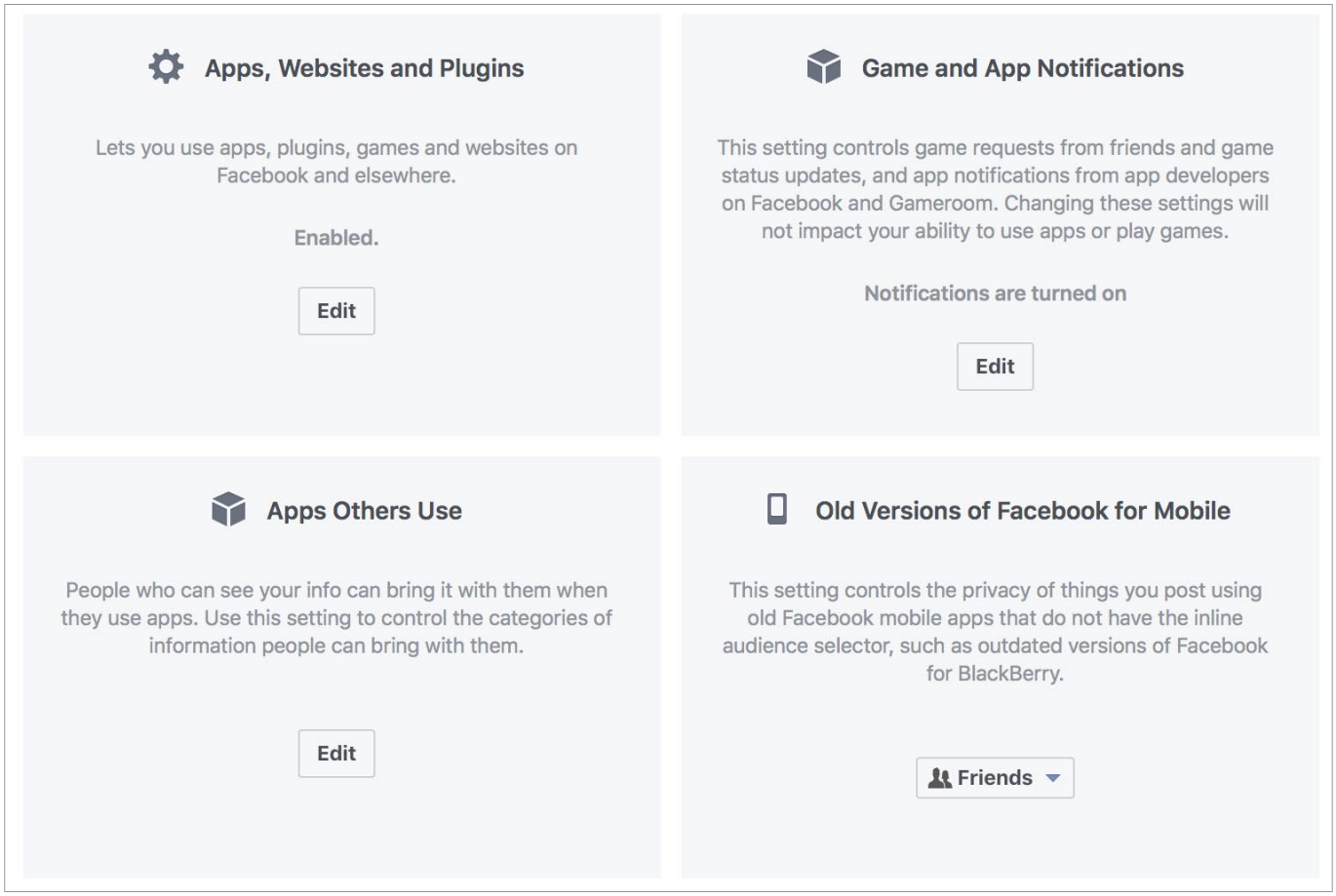
NB ;- It is a good idea to check what apps you have logged into using Facebook from time to time. Make sure you recognize all of the apps. This is where viruses tend to lurk. It is a good idea to clean it up every few months.

Manage Apps

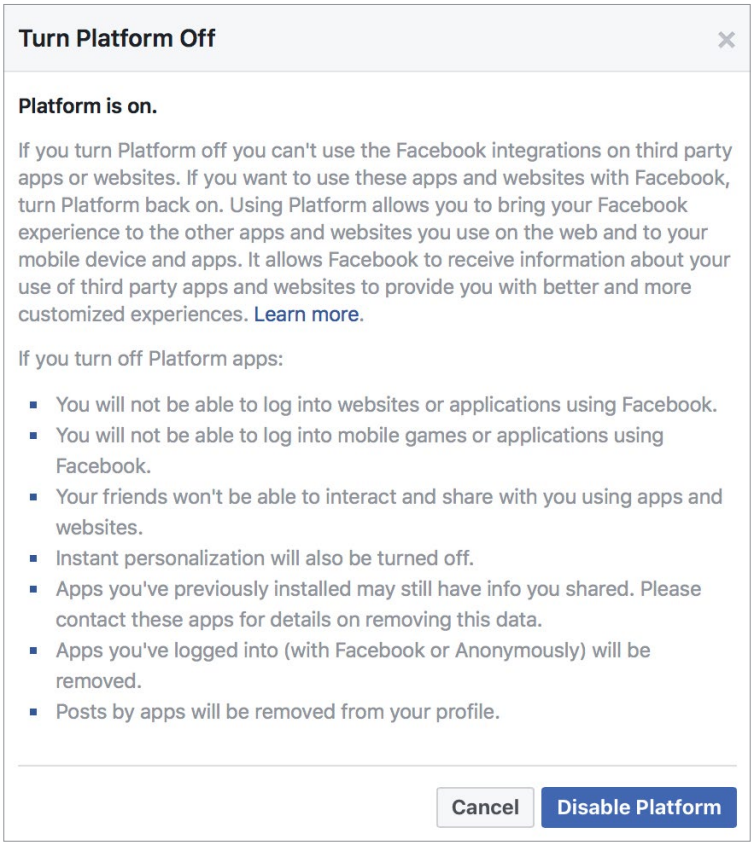
Review what apps you have allowed to access your personal information.



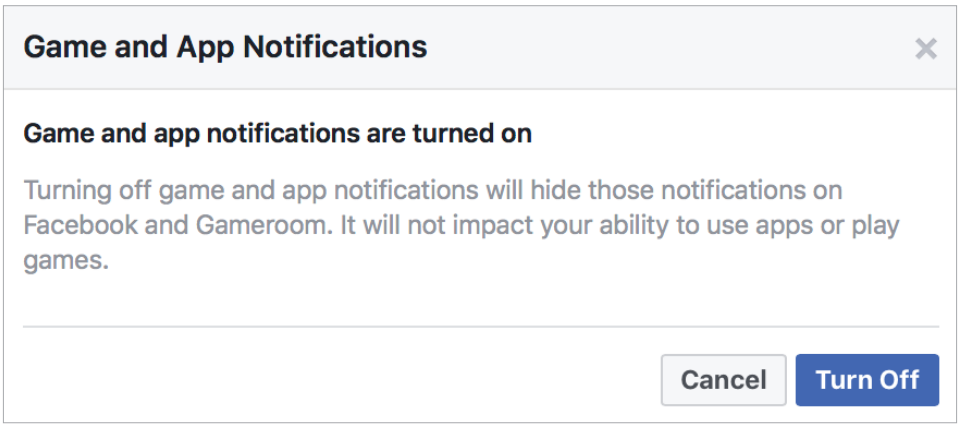
The settings in the next screenshot allow detailed control over the interaction these apps have with the information belonging to you and your friends.



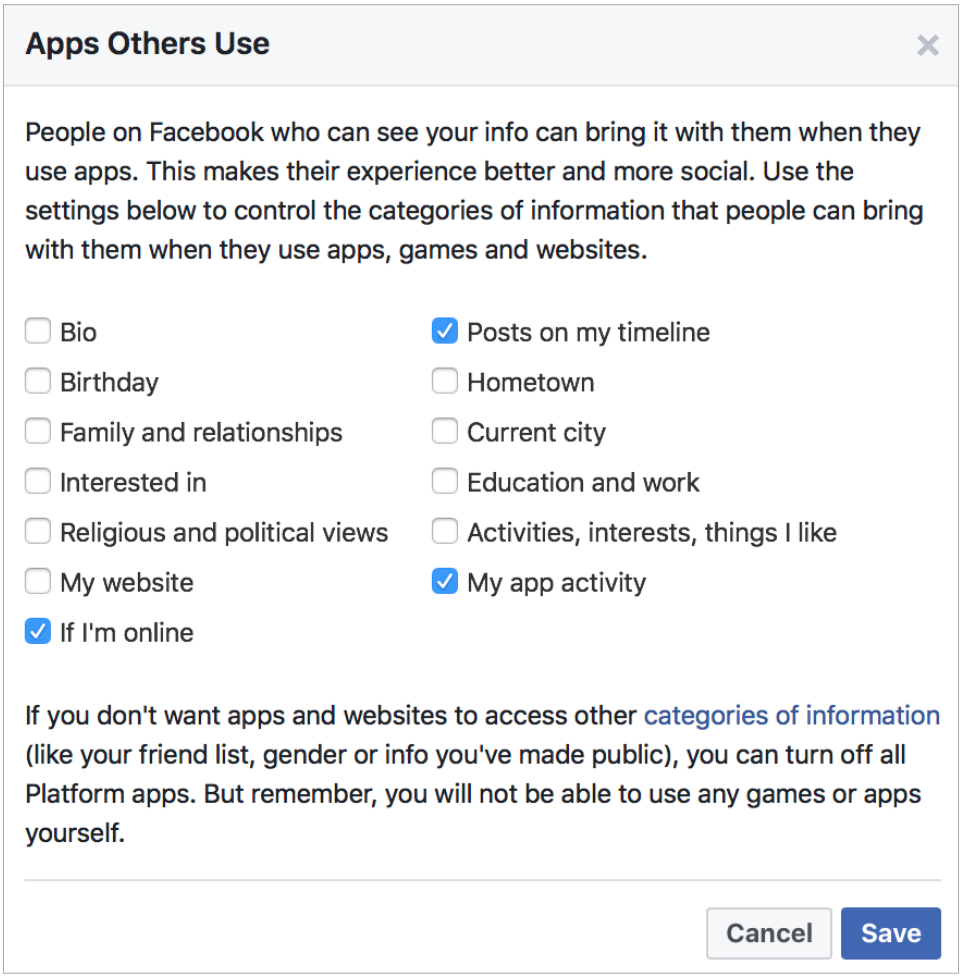
Apps, websites and Plugins offers this menu choice, and outlines how enabling this feature will work with your account.



Game and Apps Notifications will hide notifications from these apps.



Apps other use limits the sharing of your information with apps your friends are utilizing.



Disabling the apps

Android

For Android 4.3 onwards, the OS has a feature called "**App Ops**". Lets you selectively disable some permissions for your apps.

Under **Settings**, you will find "**App Ops**".

Depending on your phone, apps and the permissions they use, this is categorized into 4 tabs-

- **Location**
- **Personal**
- **Messaging**
- **Device**

It's easy to see what app uses the permissions you're concerned about.

On the right is a timestamp for when the app last used the permission. On picking an app, you'll get a screen with easy on/off buttons for each permission. This does not affect the working of the app but only those permissions about broadcasting your personal information and whereabouts that you have chosen to withdraw.

If not **App Ops** (depending on your update), there will be a variations of this under *Settings – Apps- (select App) - Permissions under App Info -Details.*

iPhone

Privacy settings for apps can be modified through following the path **Settings - Privacy.**

You can select a type of data from the list that pops up on your screen thereafter to see which apps have asked for permission to use that data.

Unlike in Android, the information is data set wise and not app wise.

An app won't appear on the list until it asks permission to use your data. You can add or remove permission from any app that has asked for access to data. An app can use your data only if you have given it your permission.

Windows

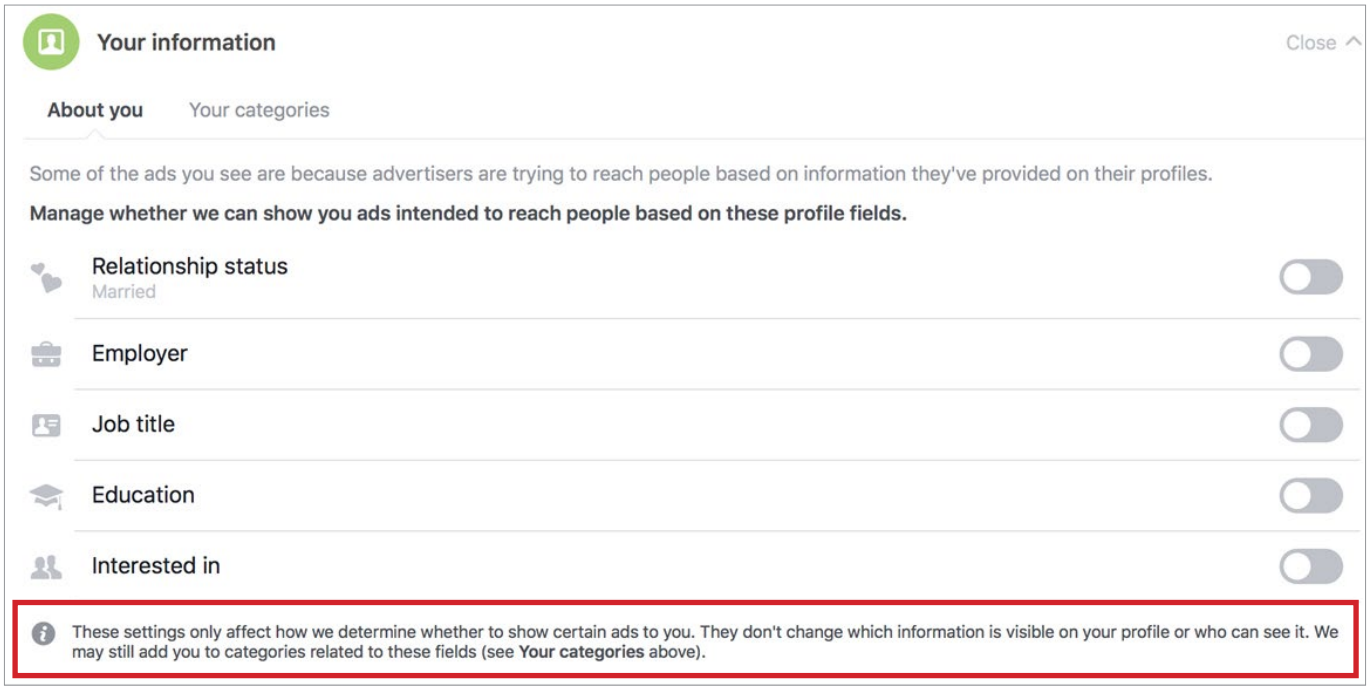
Click to open **Settings** on your device. Select "**Change PC Settings**" and the select **Privacy** on the left.

From here you can prevent applications from accessing personal data, using your advertising ID, and block websites from providing targeted content by using your language list.
The **Location** section lets you choose which apps (if any) can use your location as well.

Ads

Reaping revenue in the billions, Facebook has a lot to gain from advertising. This feature allows you to select advertising, tailored to you as an individual - derived from your personal details in your profile.

This section allows you choice over the advertising content you receive, whether or not you interact with advertisers, and importantly – let Facebook know if you are interested in being shown ads based on your personal information.

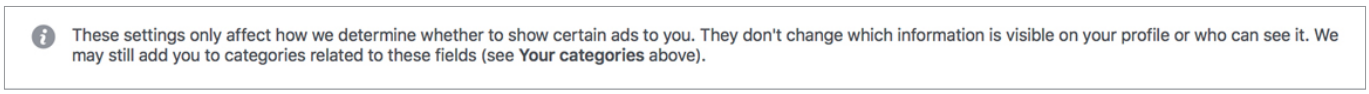


NB- note Facebook may disregard this, as mentioned in the bottom line.

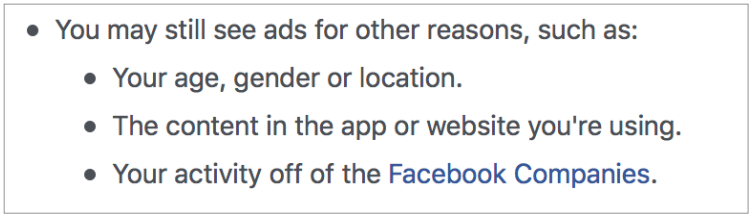
For now, you can stop these targeted ads appearing on your timeline, and stop sharing any interactions with advertising you have made.

Some of your activity with advertorial content can be quite revealing. Targeted ads can be disconcerting when Facebook uses the information they have about you to select your preferences, giving the companies they sell space to the opportunity to increase their revenue.

Essentially this function is useless, peppered with disclaimers that state examples like:



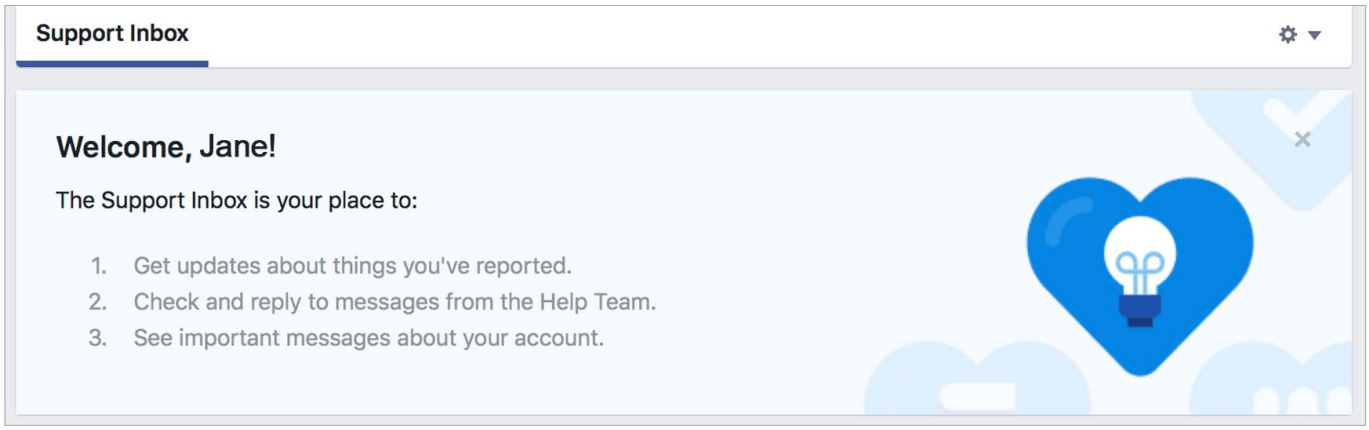
or



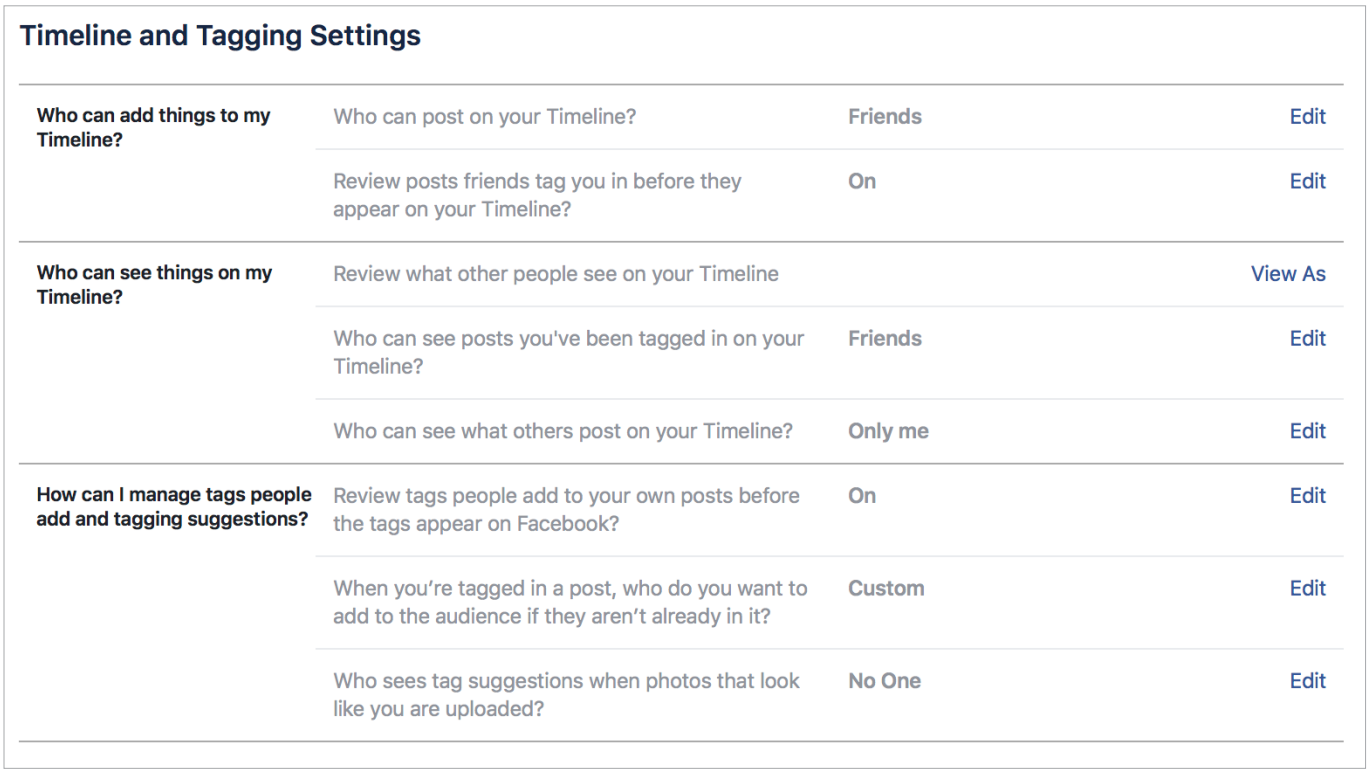
It is unavoidable. Facebook is going to show you ads, this feature lets you pick what kind.

Support Inbox

The screen shot sums up this function. Here you will find responses from the Facebook moderators about accounts, images and comments you have reported. And the moderations decisions, and recommended courses of action.



Timeline and Tagging

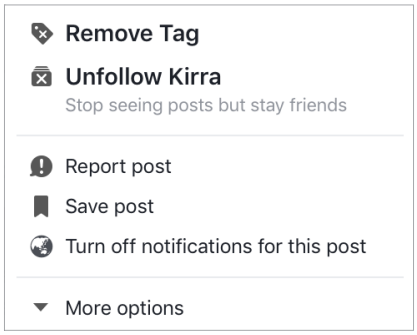


This is where you customize your timeline, allow who can post on it and review tags that people may add to your posts.

The default setting allows your friends to post to your timeline, the only other choice is to limit it to yourself.

These settings concentrate on what is on YOUR timeline only. You may be tagged in other posts etc. that will appear publicly and be searchable. You must manually remove the tag in this situation.

Place your cursor over the particular post and in the top right corner the drop-down menu arrow will give you the options below -



What about the tags others add and tagging suggestions?

You are always notified if a person not on your friend list tags you in a photo.

The face-matching technology Facebook uses is what leads to tags being suggested when photos are posted.

This are derived from the posters friend list.

To stop yourself being a suggestion choose the **no one option** listed.

Geo-Tagging

Social media location geo-tags are pieces of information that can be attached to a tweet, status or photo on a social networking site that show the physical location of where something has been posted. These tags can be exceptionally specific, identifying both your home and your workplace. Facebook also collects your data tracking the places you have been.

The solutions :

- Remove these from your pictures before you upload them to Facebook , or opt out of tagging your locations

- Turn off the location services in your devices camera app. There are also specific apps that scrub this information - (deGeo for iPhone or Photo Privacy Editor for Android)

- Disable Location Services for Facebook on your Mobile Phone / Device

- Revoke permission using your phones settings.

Locations

Turning off Location Services

Yes, your mobile device tracks your location.

This can be handy for features like Weather, Traffic, Find My i-phone and maps but most of the apps you use for entertainment purposes track you as well.

The information gathered by these varies from sales and marketing purposes, to declaring your exact posting location on social media.

If you are not comfortable with this, it is easy to opt out, and just turn on location services when you need to.

Location history - this serves to show exactly where you have been throughout the day.

"Frequent locations" and "significant locations" pin point your patterns of movement.

This information is easily available on Apple devices or as part of googles location data on an android device.

Here's how to opt out:

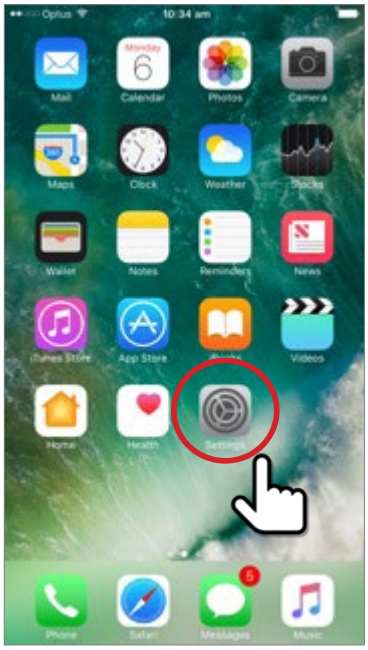
When setting up a new device, or you are installing an app on your iOS device there will be a prompt to share any location data.

A "Yes "or an "Allow" will feed your information to a database. Convenient apps that tailor information specific to you and your movements (weather etc.) also carry similar databases holding swathes of information about a variety of individuals.

Apple devices

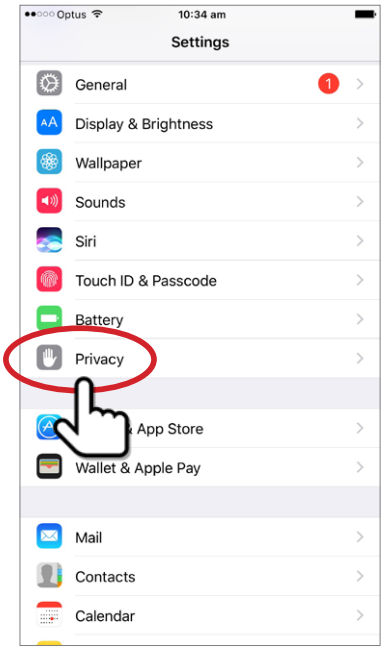
Disabling services for your iPhone and iPad in iOS

Step one



Select the grey settings wheel from the home screen of your device

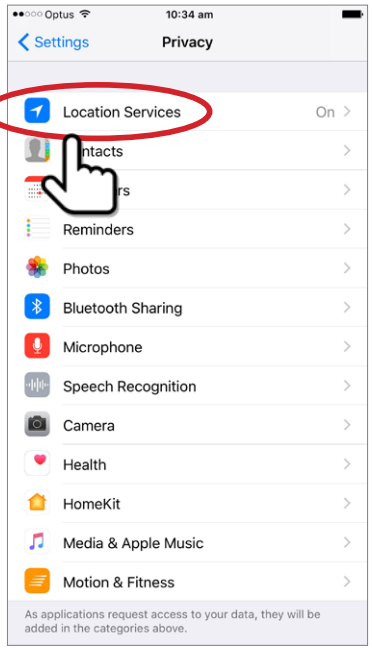
Step 2 A new menu will open up



Tap on the privacy option

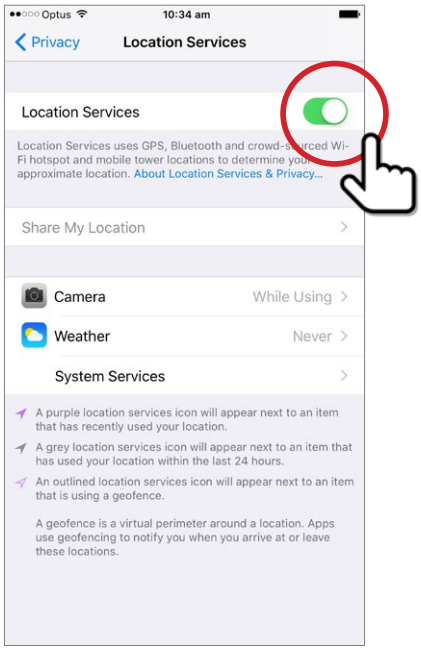
Step 3

From this menu, chose Location services



Step 4

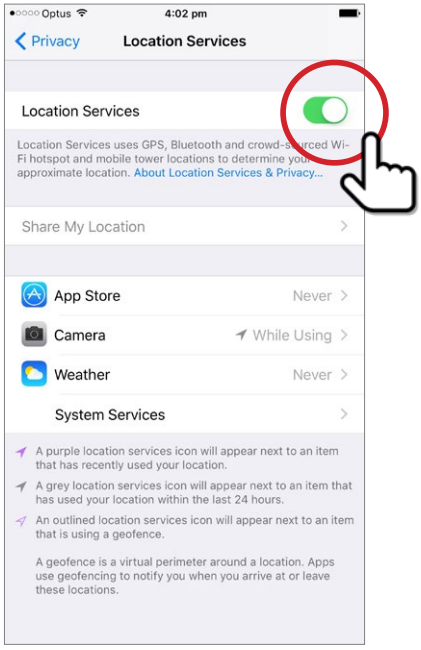
The next menu allows you to switch off Location services using the green switch. It also provides you with a choice to how you wish to control the other location based services. Consider how you wish to use your device, and use these accordingly.



Toggle the green switch to the off position

Step 5

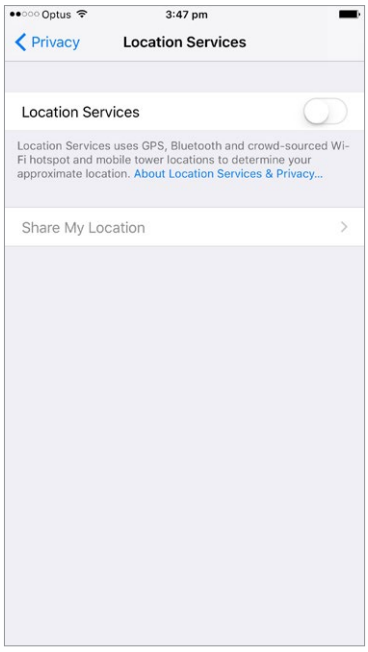
You should see a screen like the one below:



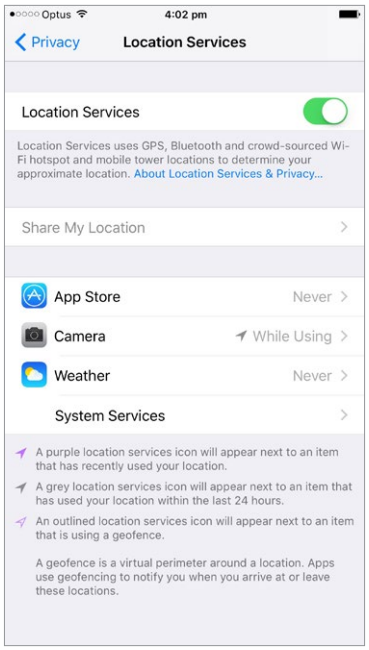
Press the Turn off option.

Step 6

Your screen should show this image. Your job is done.
(insert iphone step 6 here)



Note



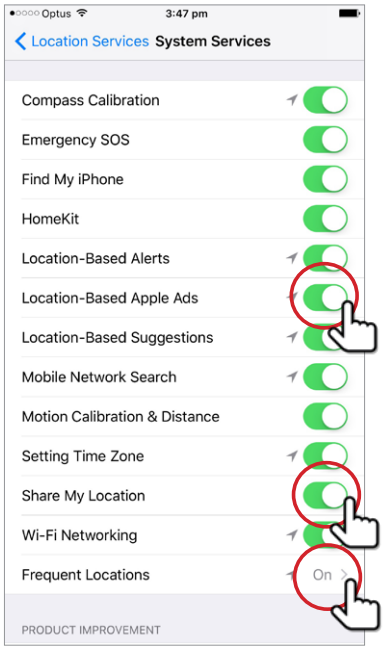
In this image there are several other options.

App Store - has been turned off completely through the store, and will be authorised on a purchase by purchase basis

Camera - choose when you wish the camera to record your location

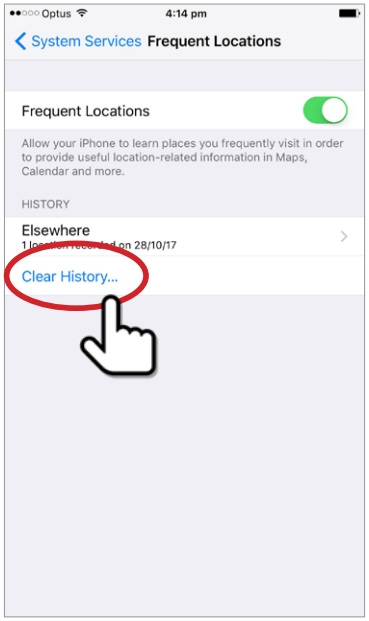
Weather - optional, depending on your usage

System Services - where the more detailed tracking systems lie.



Turn these off, to limit the information available about you.

You will now be prompted should your location be necessary or they will not work at all.



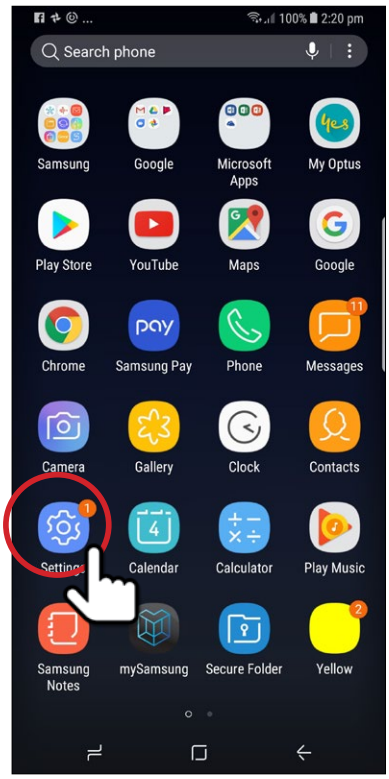
NB - tapping on the frequent locations button provides you with the window necessary to remove all your location data from the device.

Select Clear History should you wish to do this.

On an android device

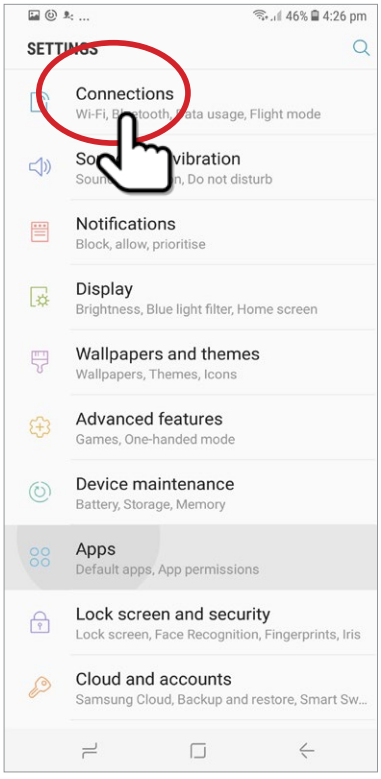
Step 1

Select the purple setting button on your home screen.



Step 2

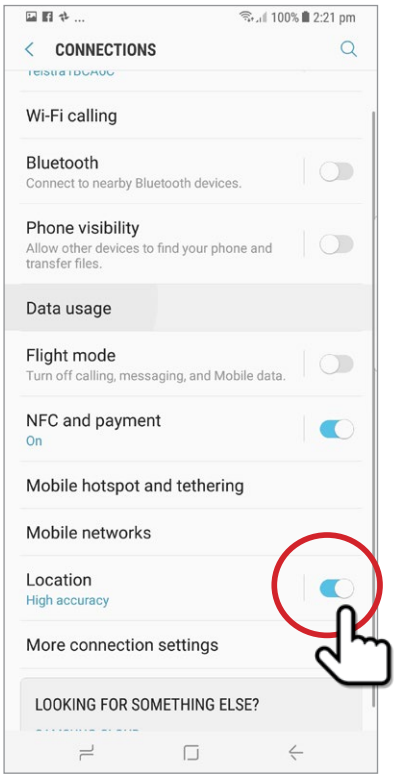
The following menu will appear:
(insert step 1.5 android and circle connections)



Choose the connections option

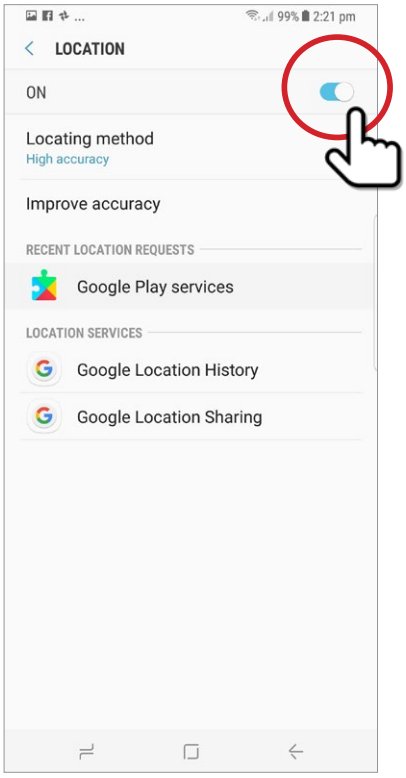
Step 3

Beside the Location tab is a blue button, toggle this to the off position.



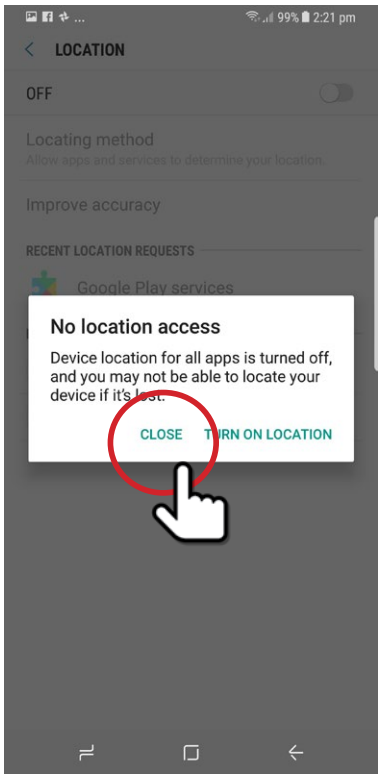
Step 4

The location window will show you several things including recent requests for location information. The blue button beside the ON words is what we after. Toggle this into an off position.



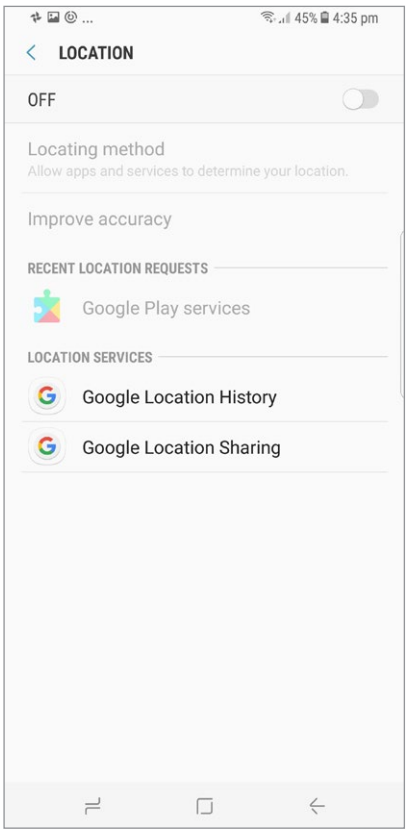
Step 5

A pop up window provided you with some information on what an off choice may entail. Pressing close will shut down location.



Step 6

Your screen now shows the following.



NB- the features shown in the location page of Google sharing history, and Google Location Sharing are worthwhile investigating further if you are inclined.

Google Location history may be turned on or off, and Google Location allows to share or not, the location in real-time of contacts etc.

Let's be clear

Location services are really useful, and drive a lot of our favourite apps.

Before you disable those features, make sure you're not relying on them.

Consider whether or not the apps and services you use are valuable enough that the information you are giving is an acceptable trade. If they are, leave those features on.

Live Steaming

From mobile devices and by the desktop, this is an option for real time video streamed via your Facebook account.

This feature is now accessible by your web cam, and can be linked through your status bar on Facebook.

Issues

Violent content

With the advent of Live streaming Facebook has run into some issues.

There has been a spike in the number of people filming illegal acts, (some quite brutal in nature) and then streaming them on Facebook. Rapes, murders, violent confrontations, suicides, torture and to drug use have all made their way past Facebook moderators.

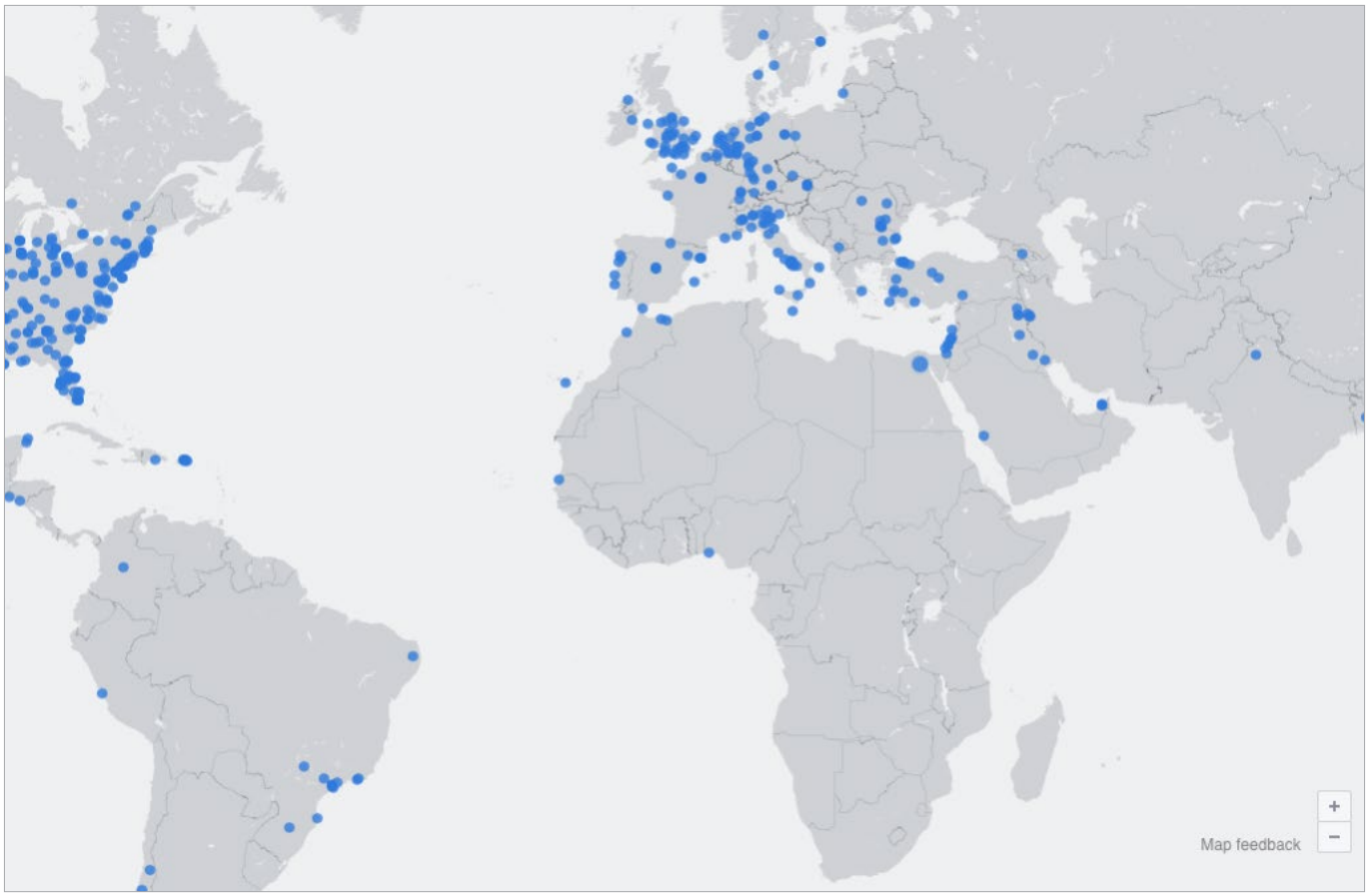
Facebook has recently responded by employing an additional 3,000 people to monitor the live streaming feature and take responsibility for the content the app is sharing.

This is quite a step, considering the number of moderators for all other posted content equates to a mere 4,500 for the millions of weekly posts.

As an example, two murders were left on the site for over 24 hours- one in Thailand involving a baby, and an accidental shooting of an American man. Facebook has recognized it bears some responsibility.

Users may report a live stream but this takes time while the stream remains active. As yet, Facebook doesn't have a method of automatically determining whether a streams content is acceptable for broadcast.

Live broadcast map



Each of the blue dots shown represents an area where a live stream is being broadcast. With a few clicks, a user can be viewing the stream wherever it is.

The map is located under the Explore options and via the live stream option.

Concerns

- This is an avenue for viewing some really nasty material. Many of the blue dots on the map may be harmless, some are not.
- Stalking - it is very easy to determine who is live streaming near your location. A private account eliminates being pinpointed.
- Privacy - Facebook privacy controls have become increasingly complicated. Many users have unsecured accounts, without adequate protections. This leads to them to inadvertently sharing much more than they intended.
- Identity theft – live streaming reveals considerable information about the average user. It is likely that these streams are monitored by people looking for users without adequate security settings, consider carefully the information you are sharing.

The same concerns that surround public posts and photos apply to live streaming. To protect yourself, use the Facebook security and Privacy settings previously addressed.

Controlling your child's pictures – Scrapbook

This is a feature that allows a parent an element of control over the images of their children that they post online.

A scrapbook may only be created for the users own child, and is only viewable by the parent or guardian who compiled it. A partner maybe allowed to contribute pictures and tags with the permission of the scrapbooks creator.

Children are listed as family members and tagged with their names.

The scrapbook may be shared with other individuals or groups or even publicly- depending on the settings chosen. The people sent the scrapbook do have the option of sharing but a parent will receive a notification if this happens, giving them the option to request the tag be removed, the photo taken down or limit the people they share it with.

Things to consider

- Review the photos posted of your child. You might think it is cute to show your child naked in a bath, they might not be so appreciative later. It is a parents' responsibility to protect their child's digital footprint till they are old enough to do this for themselves.

- Identity theft. Always minimize the information you share online about your child. A child is an ideal target for identity theft, as it may be years before this theft discovered.

- It is better to allow your child to determine how public they will wish their lives to be. Lead by example if you wish your kids to grow up protecting their online privacy, and protect them by respecting their privacy.

It is increasingly, a very normal thing to do – posting picture of your children on your Facebook feed. And if you have activated all the security settings available, and are running a private account there are limited concerns.

Consider the Scrapbook feature Facebook has introduced to curate and control who can view what you share.

When a parents account is public, so are all the images of their children. Pictures in school uniform, outside the front of the school or your home, pictures of your child holding their school award with the full name of the child and the school displayed become a problem.

Location tags combined with the details freely provided, make a child very easy to locate. Tagging the child, and other friends in public photo posts offers further information.

A parent who fits into this category has provided to the world - where their child attends school, the area they live in, the sports they play. All these things are useful for stalkers or predators who wish to establish a relationship with a child online.

Be smart. Only share images of your children through a private Facebook account. Ask your family not to tag you or your children in photos they post. Open a Facebook Scrapbook for your family to exchange pictures.

It is important to protect the privacy of your children while they are young.

Logging Into other sites using Facebook or Google

This is a fairly common request that you have probably seen before. A notification will appear asking you to log in with Facebook or perhaps Google. At least 60% of Facebook participate in this social media log on.

It's an option frequently used on news sites, streaming services and a lot of apps and games. While it seems fairly harmless and may often be more convenient, there are a few reasons why it is not recommended.

You are giving the website your personal information

Some social media sites, particularly Facebook and LinkedIn carry a large amount of personal data – simple examples are names, birthdays, email lists for yourself and your friends. You are consenting to your data being provided to a third-party company whose terms of use may be unknown.

You put yourself at risk of hacking

The more times this option is used, the more you expose yourself to hacking. Not all the websites that are harvesting and storing your data are secure. Signing into several sites with the same log-in leaves you vulnerable. If the security settings on the account you are logging in from are not what they should be, you are at risk of being hacked and compromising all you other accounts (Daisy-chain account).

Your information is valuable

Your information has value. Repeatedly providing personal data to a variety of websites allows a very detailed marketing profile to be built up about your preferences. This allows advertising to be targeted specifically to you. Facebook turns over $16 billion dollars a year in advertising revenue. Google tracks your data using your search preferences and builds demographics which it then sells. Google made over 5 billion dollars last year from advertising.

How much information are you authorizing Facebook to collect

By signing up for a Facebook account, you have agreed to Facebook to using your data as it sees fit. A read of the privacy policy reveals this in detail. And yes, Facebook uses this for financial gain - 62 billion dollars of gain a year.

As an example, when you like a page about soccer or dancing, you will find yourself viewing advertisements relating to these topics. You have shown an interest, you might buy something as a result, this results in links to relevant advertisers.

Facebook reach and data about you:

- Facebooks algorithm will continue to profile you, using all the interactions you take with your Facebook account. Even the amount of time you spend on your Facebook account can be used reveal your relationship status.

- Link your other social media apps, and logging into these accounts using Facebook and you offer up further information, that is funneled to what Facebooks algorithm has determined are relevant advertisers.

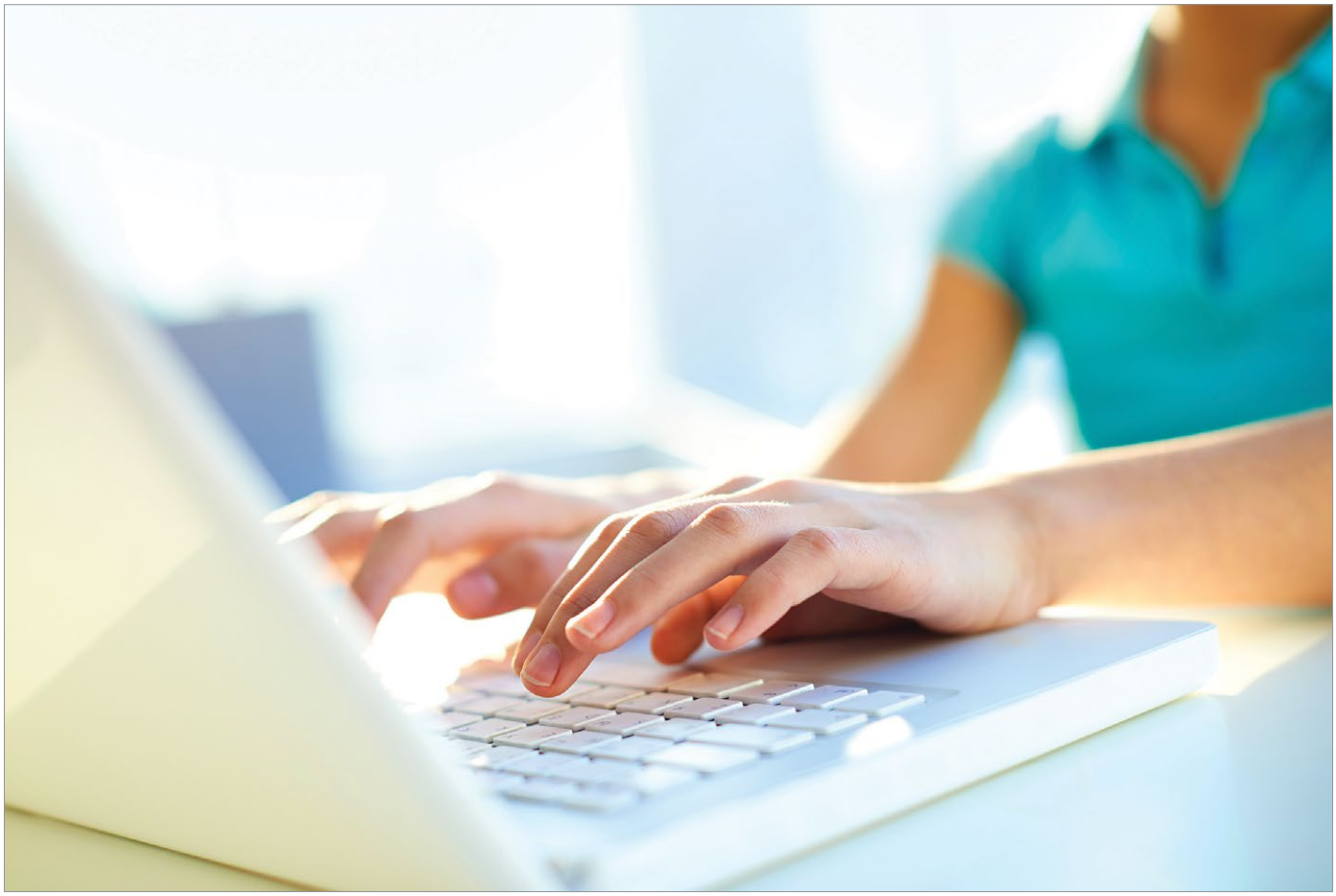
- The facial recognition software the platform uses allows it to see you in untagged photographs posted by friends. Facebook took this program too far when it began tagging individuals automatically in 2016, providing users with no method of opting out. Data protection bodies in Canada and the EU protested this feature, and Facebook decided to halt this tagging process. Be assured though, this is still all data being filed away about you and your movements.

- If you have a mobile version of Facebook and you haven't switched off the location services on the Facebook app and your device, Facebook follows you around digitally – tracking you as you go from store to store, or place to place

- When you type a hasty, angry post then delete it. Facebook records both your decision to delete and your original opinion.

- Should you choose to shop on Facebook, or purchase items through likes provided on the platform, a view of your financial situation can be revealed. This kind of information can also be determined by what posts you like and the images you post, and the travel you record.

The reach is remarkable, and emphasizes the fact that all information posted on any social media is public.



Facebook and the online quiz

What kind of personality are you? What kind of leader are you? What does you star sign reveal about your love life?

The online quiz is a great temporary distraction, but when you are asked to provide more information to find out all the details this random app has determined about you, stop and think.

Be especially wary of any app that wants details such as full name, date of birth, postal code or email before revealing any results.

Think about it logically, how can you really gain any insightful information about you? And what information from Facebook are you handing over to some of these quiz companies?

Here's a list of what you are revealing about yourself.

- All your publicly listed information
- All your posts. Ever
- All your photos
- Your friends list
- All your likes. Ever
- Your IP address
- Information about your device

And what do these third-party companies do with your information?

Do they store it? What is it used for? And are they selling this on to other companies - even further distant from the original permissions you gave to Facebook.

The answers all led to the fact that this is how the companies behind the quiz apps make money - they use your data to tailor advertising and yes, they on sell your information because you agreed, in a privacy agreement you probably never saw.

If you are fine with this information being handed over, pay no attention to any of the above.

Your privacy is important.

Directory

Australian Government | Office of the eSafety Commissioner

The Office of the eSafety Commissioner is committed to empowering all Australians to have safer, more positive experiences online. The Office was established in 2015 with a mandate to coordinate and lead the online safety efforts across government, industry and the not-for profit community.
www.esafety.gov.au

---

kidshelpline Anytime | Any Reason **1800 55 1800**

Kids Helpline is Australia's only free, private and confidential 24/7 phone and online counselling service for young people aged 5 to 25.
www.kidshelpline.com.au

Welcome to LAWSTUFF, the website dedicated to providing legal information to children and young people in Australia.
www.lawstuff.org.au

Bullying. No Way! provides information and ideas for students, parents and teachers. If you want to talk to someone in person or online click here to get contact details for helplines.
www.bullyingnoway.gov.au

ACORN
Australian Cybercrime Online Reporting Network

Cybercrime is an issue which affects many Australians. As Australia's reliance on technology grows, the cost and incidence of cybercrime is expected to increase. The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of the Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime. It will also provide advice to help people recognise and avoid common types of cybercrime.
www.acorn.gov.au

Think you know what young people see, say and do online?

ThinkUKnow was started in the United Kingdom by the Child Exploitation and Online Protection Centre (CEOP) and was developed for Australian audiences by the AFP in 2009. The program is a partnership between the Australian Federal Police (AFP), Microsoft Australia, Datacom and the Commonwealth Bank, and is delivered in collaboration with New South Wales Police Force, Northern Territory Police, Queensland Police Service, South Australia Police, Tasmania Police, Western Australia Police and Victoria Police as well as Neighbourhood Watch Australia. It is Australia's first (and only) nationally delivered crime prevention program.

www.thinkuknow.org.au

www.safeonsocial.com