

[safeonsocialmedia.com.au](http://safeonsocialmedia.com.au)

# 2017

## The Guide to being Safe on Social Media

# Facebook



Published by Safe on Social Media Pty Ltd

Text copyright – Kirrily Pendergast 2016

Graphics copyright – Funky Monkey Graphics 2016

Production Manager – Lachlan Pennefather

The moral right of the author has been asserted

No part of this guide or it's associated modules may be reproduced or transmitted by any person or entity in any form by any means, electronic or otherwise including photocopying, recording or scanning or by any information storage and retrieval system without prior permission from the publisher.

The publisher 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 social media use or any other activities described in this guide.

Whilst every attempt has been made to ensure that the information in this guide is accurate. It is the nature of Social Media to be constantly changing, therefore the author gives no guarantees to the completeness or accuracy of the contents of this guide.

# Contents

What is Facebook? .....	4
Why do people use Facebook? .....	4
What are the risks involved with using Facebook? .....	5
Bullying and harassment on Facebook .....	6
Passwords .....	7
Your Date of Birth .....	8
Friend Requests .....	9
Login Alerts and Approvals .....	11
App Passwords .....	15
Public Key .....	16
Trusted Contacts .....	17
Your Browsers and Apps .....	18
Legacy Contact .....	19
Privacy Settings – Who can see your stuff .....	20
Who can contact you and who can look you up? .....	22
Timeline and Tagging .....	23
Who can see things on your timeline? .....	24
How can you manage tags by others and tagging suggestions? .....	25
Followers .....	26
Apps .....	27
Payments .....	28
Facebook Scams .....	29
To Learn more about Facebook or to report an issue .....	33

# Your Guide to being Safe on Social

## Facebook

Home 5



### What is Facebook?

Facebook is the biggest Social Media Network in existence today. It was launched on 4th February 2004 by Mark Zuckerberg and some of his Harvard College friends. Originally built just for Harvard students it rapidly expanded to other colleges in Boston and the rest really is history.

Since 2006 anyone who is at least 13 years old has been allowed to become a registered user of Facebook.

On 1st February 2012, Facebook listed on the US Stock Exchange. The company was valued at \$104 billion US Dollars – the largest valuation to date for a newly listed public company.

- As of December 2015 Facebook now has 1.04 billion daily active users on average
- 934 million are accessing Facebook from a mobile device
- 83.6% of their active daily users are outside of the US and Canada.

A big part of Facebook's pitch to its advertising clients is that it has so much information about its users that it can more effectively target ads to those who will be responsive to them. So always remember when it comes to Facebook and the fact that you are using it for free, you are actually the product.

### Why do people use Facebook?

Facebook is used by different people for different things and no user experience will ever be the same. From participating in causes to sharing petitions about things that matter to you, promoting a business' product or service, entering competitions, validation and emotional support, and everything in between is just a small example of why people like to use Facebook.

Facebook is available in multiple languages across the globe (it also provides a translation service) and with over 1 billion active users it is referred to as the "heartbeat" of the internet.

Facebook is accessed most often through a smartphone; it is constantly with you; you can therefore be in constant communication with your network of friends and family.

The daily activity on Facebook is almost to the point of inconceivable; with over 1 billion active users, it is literally changing minute by minute, due to the information being shared.

There is very little you can't do on Facebook, and you are no doubt at some time contributing to the billions of pieces of content added on a daily basis through comments, weblinks, videos and even recommendations to your favourite restaurant.



## What are the risks involved with using Facebook?

There are many, and they are wide and varied, but here is a start:

- Facebook, like all social media, consumes an enormous amount of time and can become quite addictive. You need to monitor the amount of time you spend online so it doesn't interfere with productivity in your "offline" life;
- 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 and this can't be predicted – just like it can't be in the physical world;
- Because the privacy settings on Facebook are constantly changing, there is always a risk to your personal privacy.

Facebook provides custom safety and privacy settings and features, and has dedicated areas of the platform for education purposes. We recommend that as well as reading this guide you also visit the Facebook Safety Centre [www.facebook.com/safety](http://www.facebook.com/safety)

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. 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.

*The following is a list of risks that as a user of Facebook you should consider:*

- 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.

# Bullying and Harassment on Facebook

## What to do

If you are being bullied or harassed on Facebook here are the first steps of what to do:

- Take screen shots of the bullying or harassing comments. It is always good to have a record and make sure you share with someone you trust;
- Don't retaliate. Bullies are always looking for a reaction so 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);
- 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 The Children's e-Safety Commissioner here in Australia.

The Office provides Australians access to a complaints system to assist children who experience serious cyber-bullying.

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 .

If you want to talk to someone in confidence please contact:

**Beyond Blue - [www.beyondblue.org.au](http://www.beyondblue.org.au) - Phone: 1300 22 46 36**

**Lifeline - [www.lifeline.org.au](http://www.lifeline.org.au) - Phone: 13 11 14**

## Passwords

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

*Here are our top tips when it comes to passwords:*

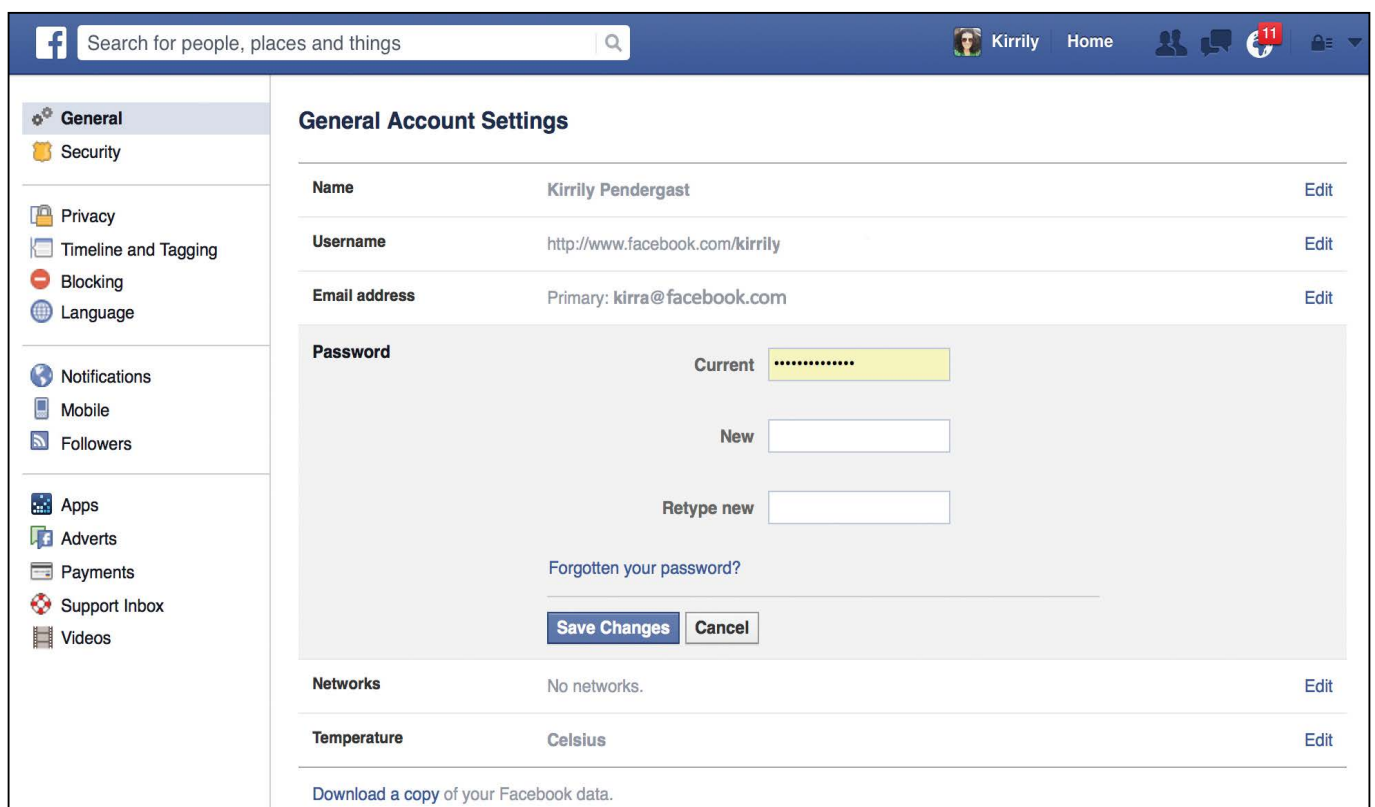
- Always use a strong alphanumeric password using upper and lower case letters and numbers for example: lI0v3D0g2 instead of ilovedogs
- Do not use the same password for your Facebook account as you use for your bank account.
- Never share your password with anyone.
- Change your password regularly and always change it immediately if one of your friends is hacked, as that makes you immediately vulnerable.

We recommend that you change your password right now!

Then, at least every three months from now on.

Simply follow these steps:

- Click on the 'Down' arrow on the far right of your profile.
- In the general account settings you will see 'Password'; it will tell you how long it has been since you changed your password.
- Click on 'Edit' and change it.



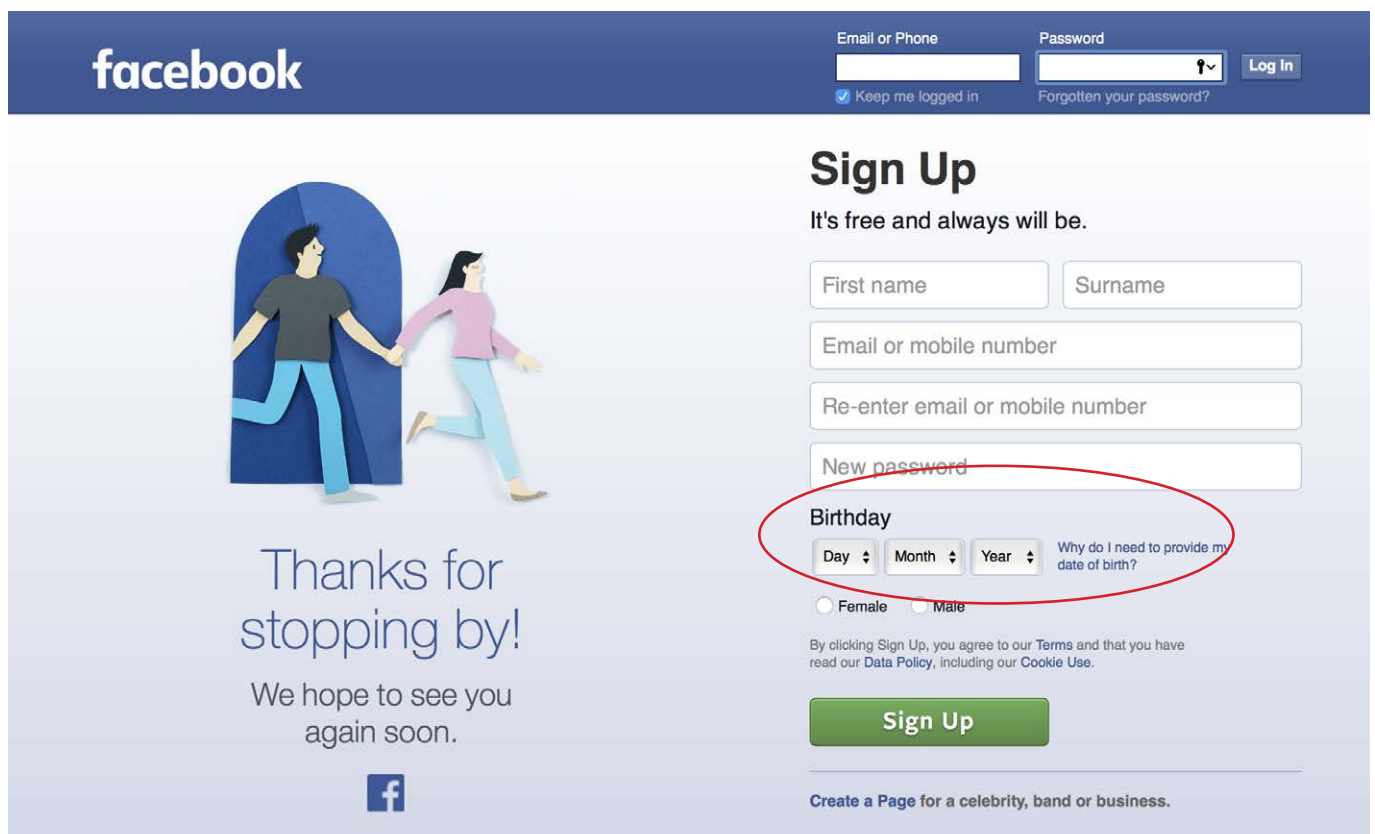
The screenshot shows the Facebook 'General Account Settings' page. On the left is a sidebar with various settings categories: General, Security, Privacy, Timeline and Tagging, Blocking, Language, Notifications, Mobile, Followers, Apps, Adverts, Payments, Support Inbox, and Videos. The 'General' category is selected. The main content area is titled 'General Account Settings' and contains several fields: Name (Kirrily Pendergast), Username (http://www.facebook.com/kirrily), and Email address (Primary: kirra@facebook.com). The 'Password' section is highlighted and contains fields for 'Current' (masked with dots), 'New', and 'Retype new'. Below these fields is a link for 'Forgotten your password?' and two buttons: 'Save Changes' and 'Cancel'. At the bottom of the settings area, there are sections for 'Networks' (No networks) and 'Temperature' (Celsius), each with an 'Edit' link. A link at the very bottom says 'Download a copy of your Facebook data.'

## Your Date of Birth

During set up of Facebook one of the first things you are asked to do is enter your full date of birth, including the year you were born. This is a key piece of information for any form of personal identification and should be treated with your personal security in mind.

This is the only time you are required to do this. Please do not lie about your age by entering a false date of birth. We strongly suggest that you do not lie about your age on Facebook. There are multiple legal reasons why Facebook restricts membership to people 13 and older. If you are aged between 13 and 18 years, Facebook has built in special protections just for you that comply with US Federal law and that of most countries.

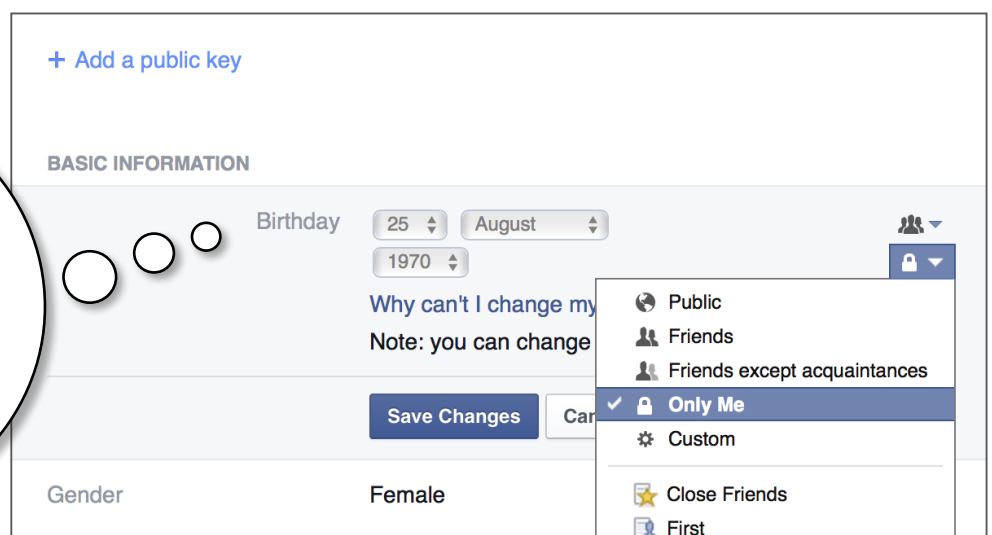
If you are a parent that has a child who is under the age of 13 using Facebook we strongly suggest that you cancel their account. There are a number of reasons for this, it is not just about who might be looking at what they post, but it is also to protect them from what they could be exposed to at an age too young to emotionally deal with what they may see or read.



The image shows the Facebook Sign Up page. At the top, there's a blue header with the Facebook logo on the left and login fields on the right. The login fields include 'Email or Phone' and 'Password' with a 'Log In' button. Below the login fields are links for 'Keep me logged in' and 'Forgotten your password?'. The main content area has a large illustration of a man and a woman running towards the viewer, with the text 'Thanks for stopping by! We hope to see you again soon.' and the Facebook logo below it. To the right of the illustration is the 'Sign Up' section. It starts with the text 'It's free and always will be.' followed by input fields for 'First name', 'Surname', 'Email or mobile number', and 'Re-enter email or mobile number'. Below these is a 'New password' field. The 'Birthday' section is circled in red and contains dropdown menus for 'Day', 'Month', and 'Year', along with a link 'Why do I need to provide my date of birth?'. Below the birthday fields are radio buttons for 'Female' and 'Male'. At the bottom of the sign-up section is a green 'Sign Up' button. Below the button is a link 'Create a Page for a celebrity, band or business.'

### SAFETY TIP

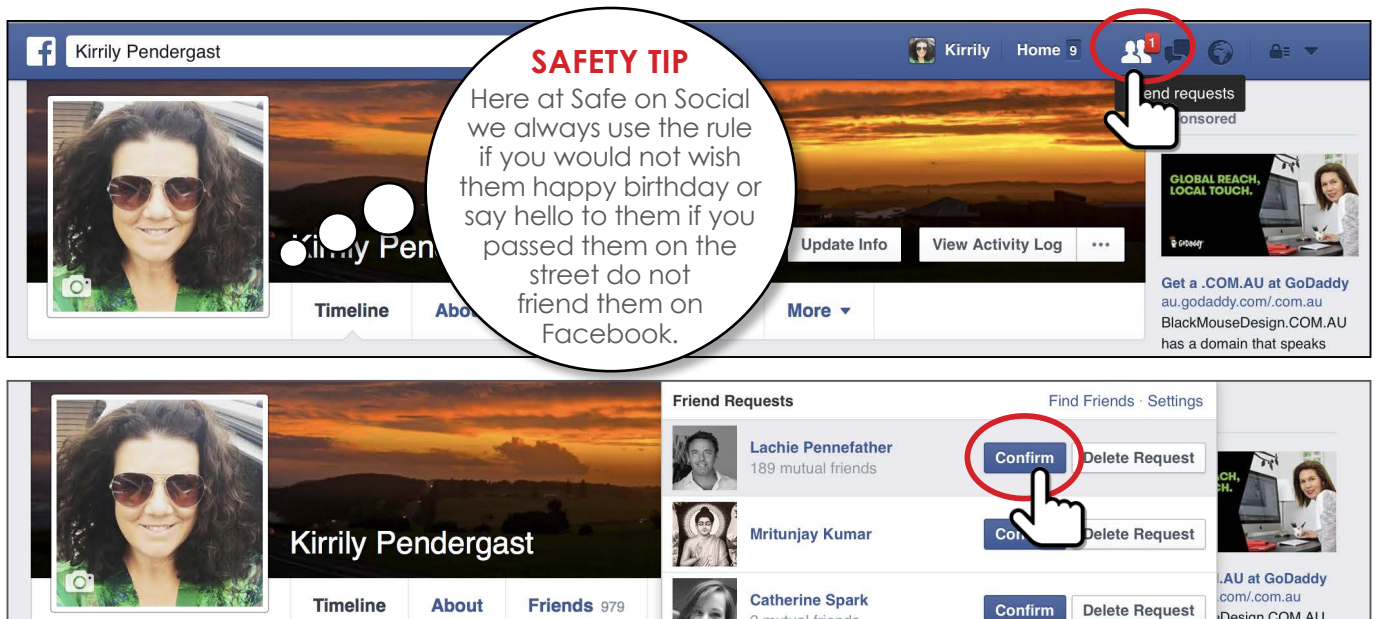
Birthdays are fine and can be left displayed on your profile so your friends remember to wish you a happy birthday! However, we recommend that you hide the year. Your friends usually know how old you are and this protects you from identity theft.



The image shows the 'BASIC INFORMATION' section of a Facebook profile. At the top is a link '+ Add a public key'. Below it, the 'Birthday' field is shown with dropdown menus for 'Day' (25), 'Month' (August), and 'Year' (1970). To the right of the birthday field is a privacy icon (a lock) and a dropdown menu. Below the birthday field is a link 'Why can't I change my birthday?' and a note 'Note: you can change your birthday once every 60 days'. Below the birthday field is a 'Save Changes' button. Below the 'Save Changes' button is the 'Gender' field, which is set to 'Female'. To the right of the gender field is a privacy icon (a lock) and a dropdown menu. The dropdown menu is open, showing options: 'Public', 'Friends', 'Friends except acquaintances', 'Only Me' (selected), 'Custom', 'Close Friends', and 'First'.

## Friend Requests

If a friend request comes from someone that you are genuinely friends with offline and they are someone that you want to stay in touch with, go ahead and click "confirm". If not, you can just ignore their request or click "delete request". Don't worry they do not get a message saying that you have chosen to ignore their friend request.



## How to remove friends and block people

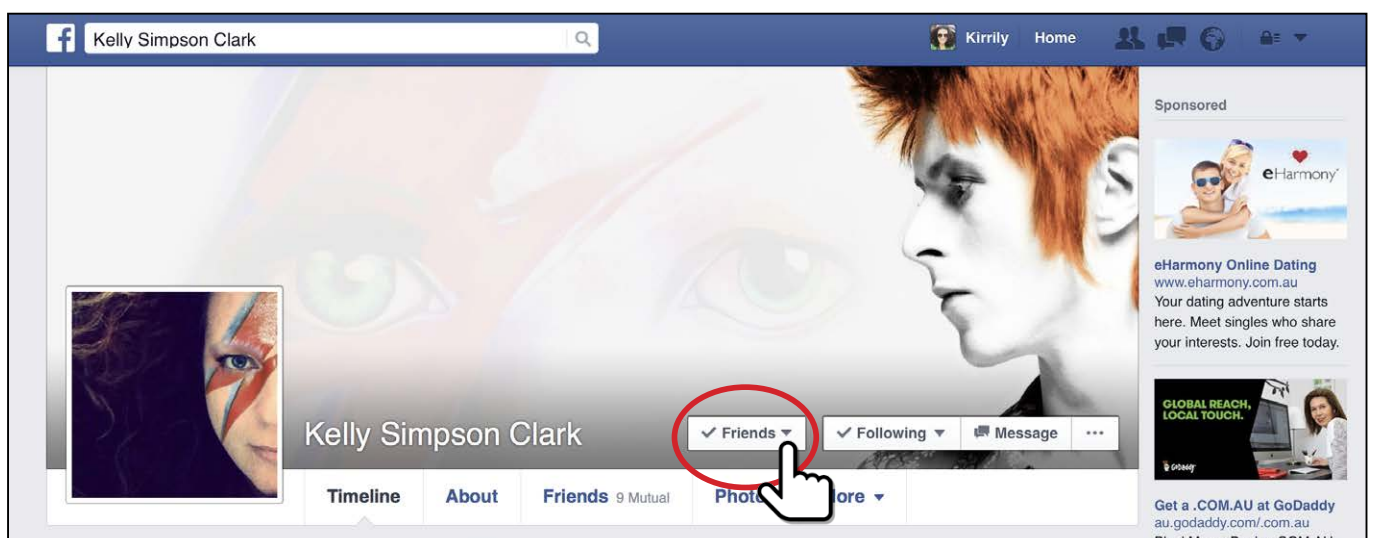
Friends come and go and you may not always get along well with someone. Just as easily as you can add friends on Facebook you can unfriend them. They will not get a message saying that you have unfriended them.

We often see online bullying behavior escalate in nastiness due to retaliation. Online bullies and their victims often switch roles. By reacting rather than ignoring the bullying behaviour things can rapidly get worse.

Being kind online or ignoring someone isn't just a good idea, it can also be a great way to protect yourself.

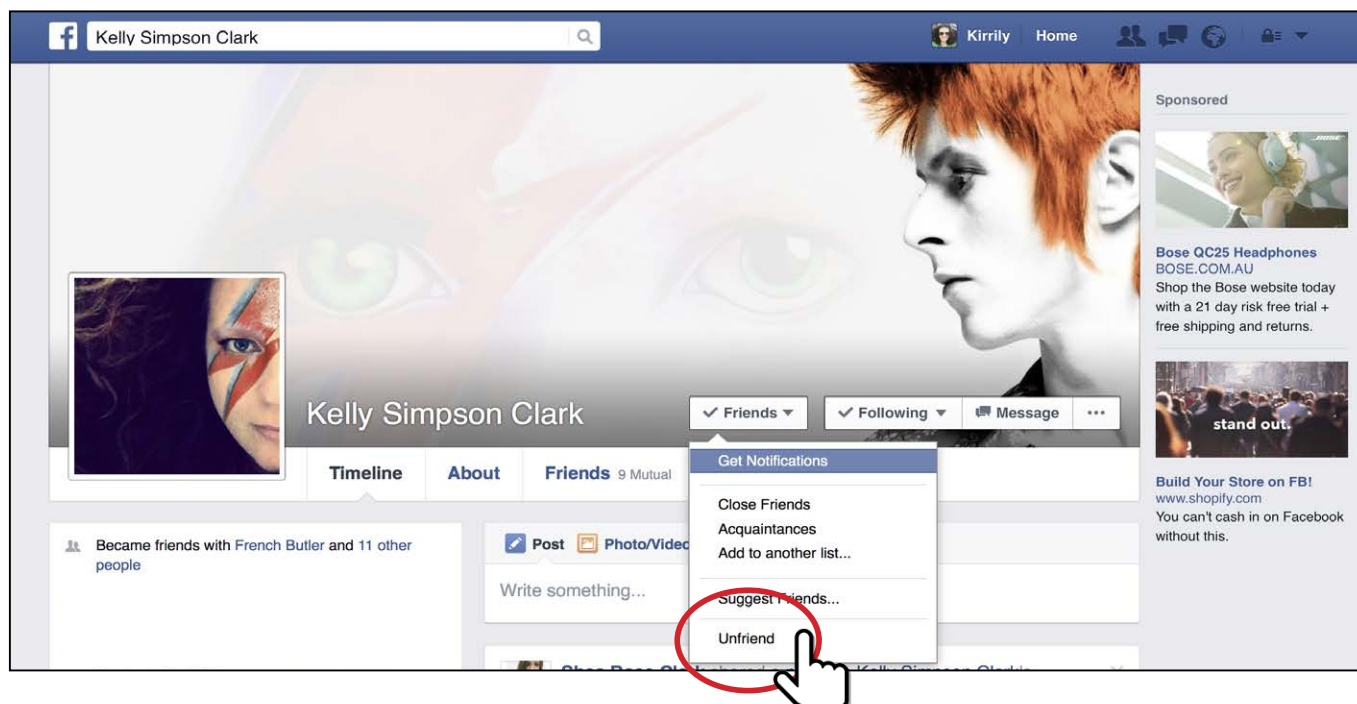
If you want to "unfriend" someone or "block" them here is how you do it:

### 1. Go to their profile page and click on the down arrow on the friend's box





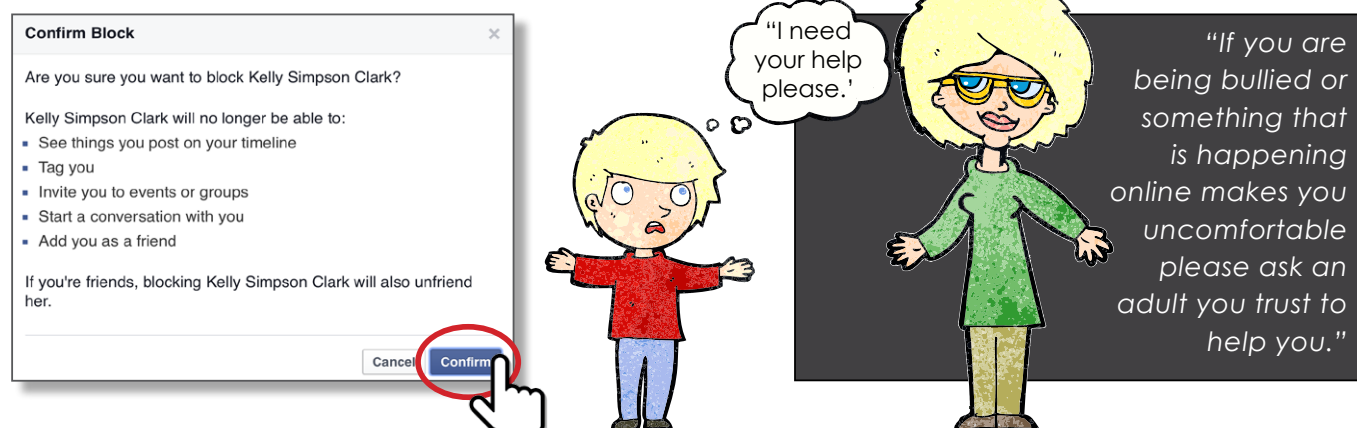
## 2. Click Unfriend



If you would like to block them, simply go to the three dots next to the message box. When you click on this you will see the bottom option is "Block".

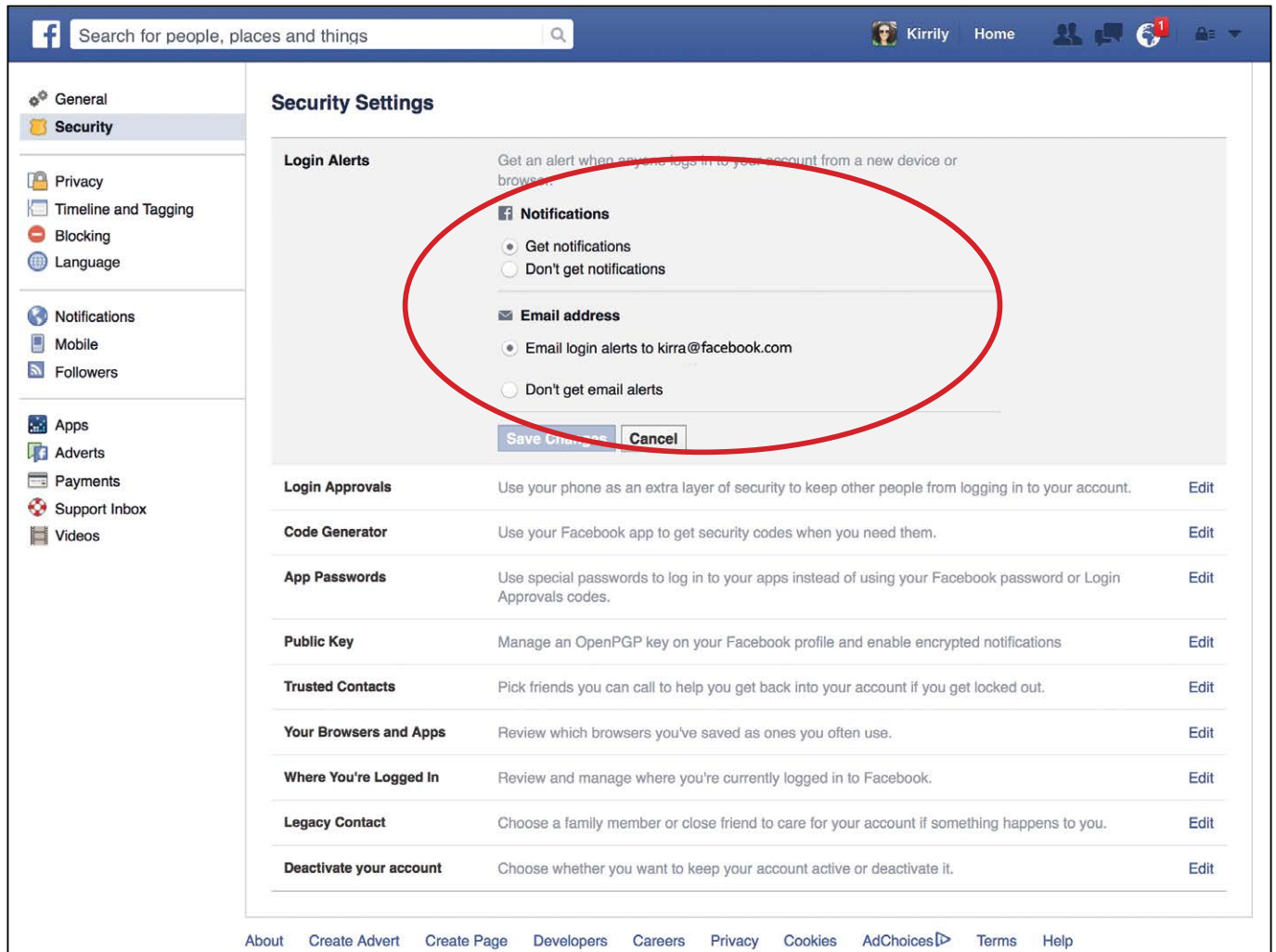


When you click "Block" you will see a new box pop up. This will look like the box below and ask you to click confirm.



## Login Alerts and Approvals

Facebook “Login alerts email alerts to you so you are notified via email or SMS message whenever there is suspicious use of 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's security, Facebook launched “Login Approvals”. This feature uses what is known as Two-Factor Authentication, meaning: something you have (a device) and something you know (a password or code).

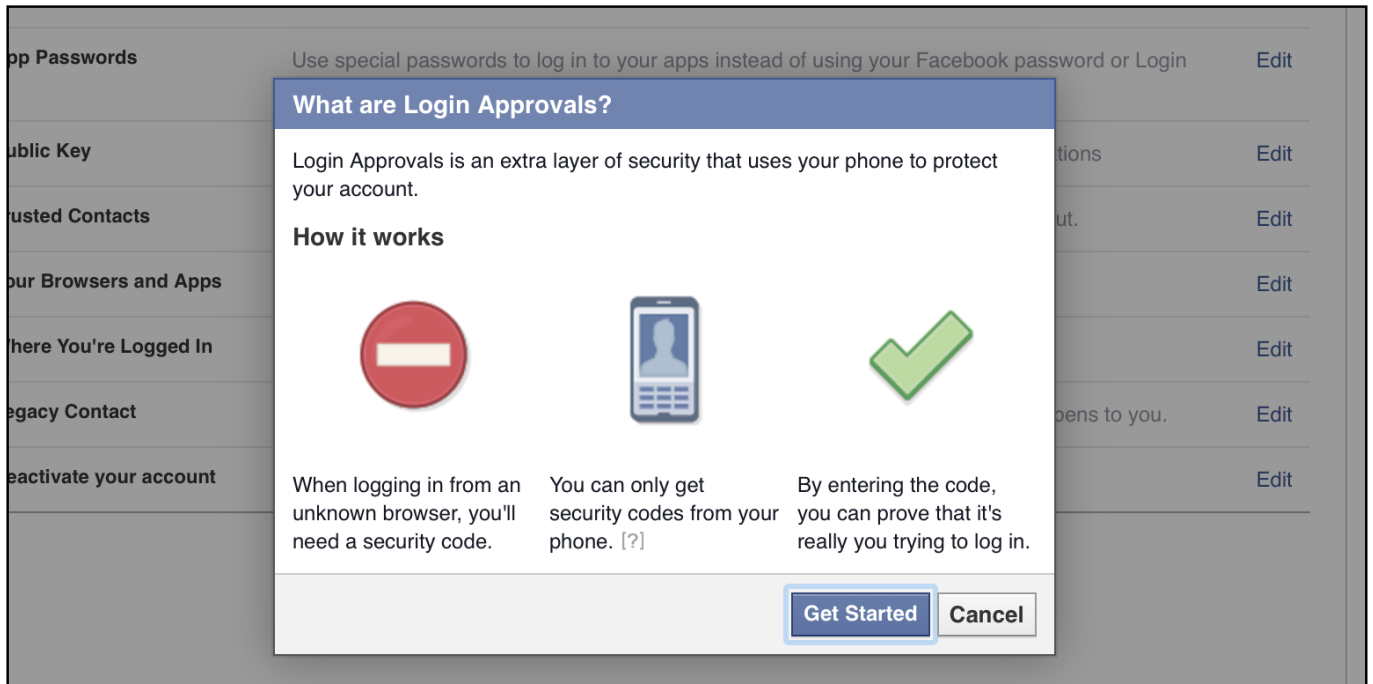
Facebook two-factor authentication or “code generator” uses your mobile device with your Facebook account and authenticates the login by sending a verification code to your mobile phone.

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

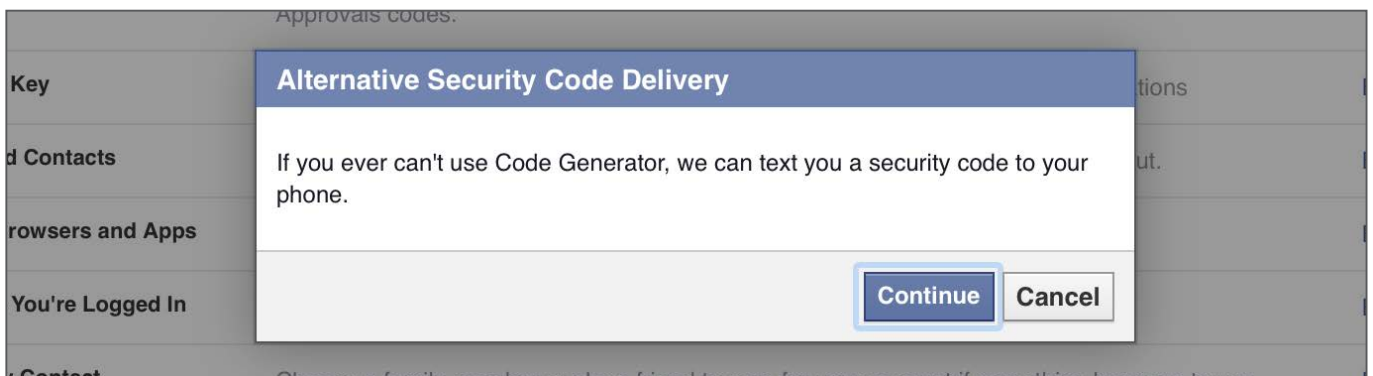
**To set up login approvals without using the “code generator” option for your Facebook account simply follow these steps:**

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.

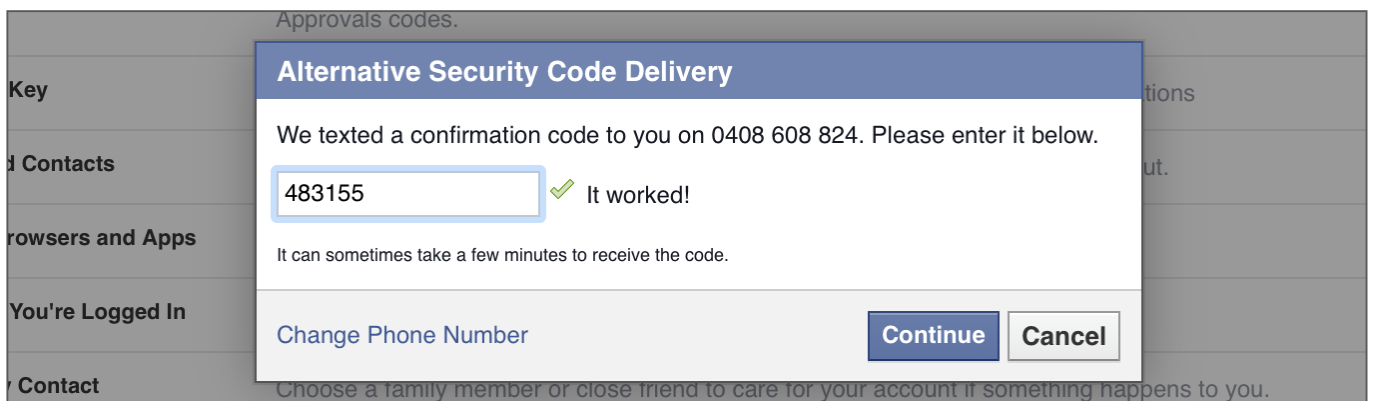
3. The second down the list is 'Login Approvals'; click 'Edit'.
4. Click the box that says "require a security code to access my account from unknown browsers". You will be presented with a box and an option to click "Get Started"



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

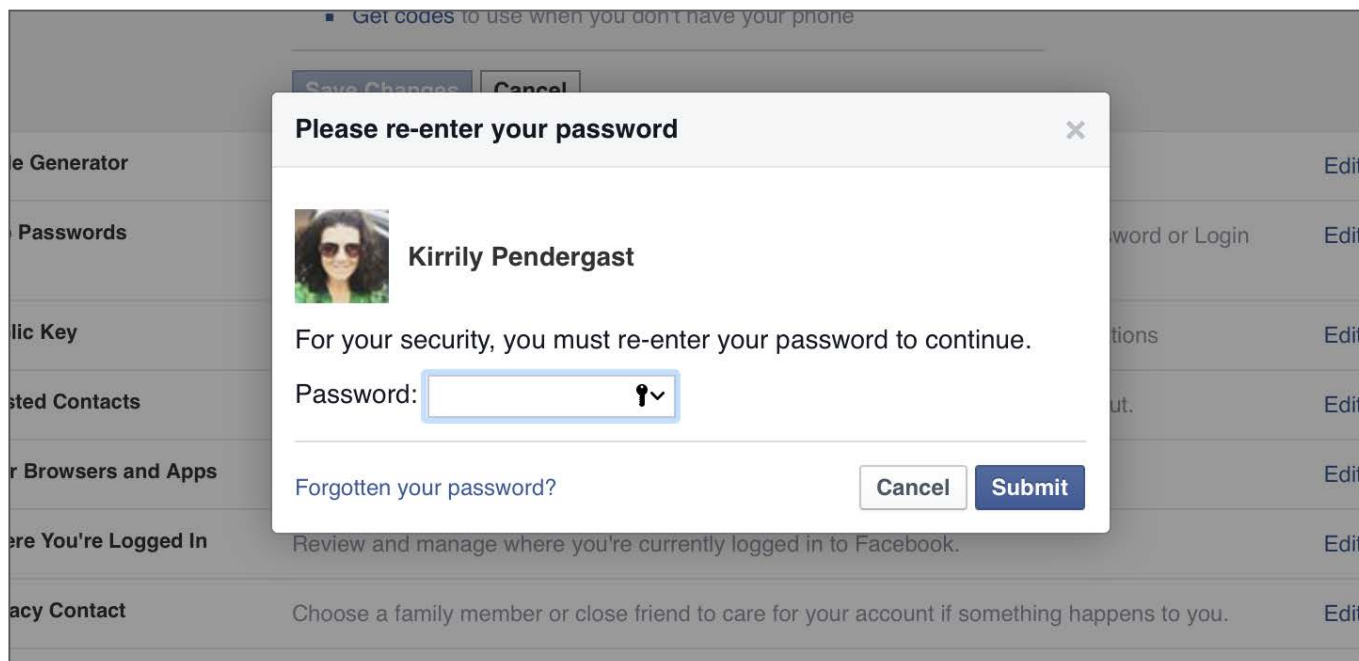


5. You will then see "set up security code delivery". Enter your phone number and click 'Continue'. Shortly after you will receive a text message on your phone with a confirmation code. Enter the confirmation code in the box provided and click 'Continue'.



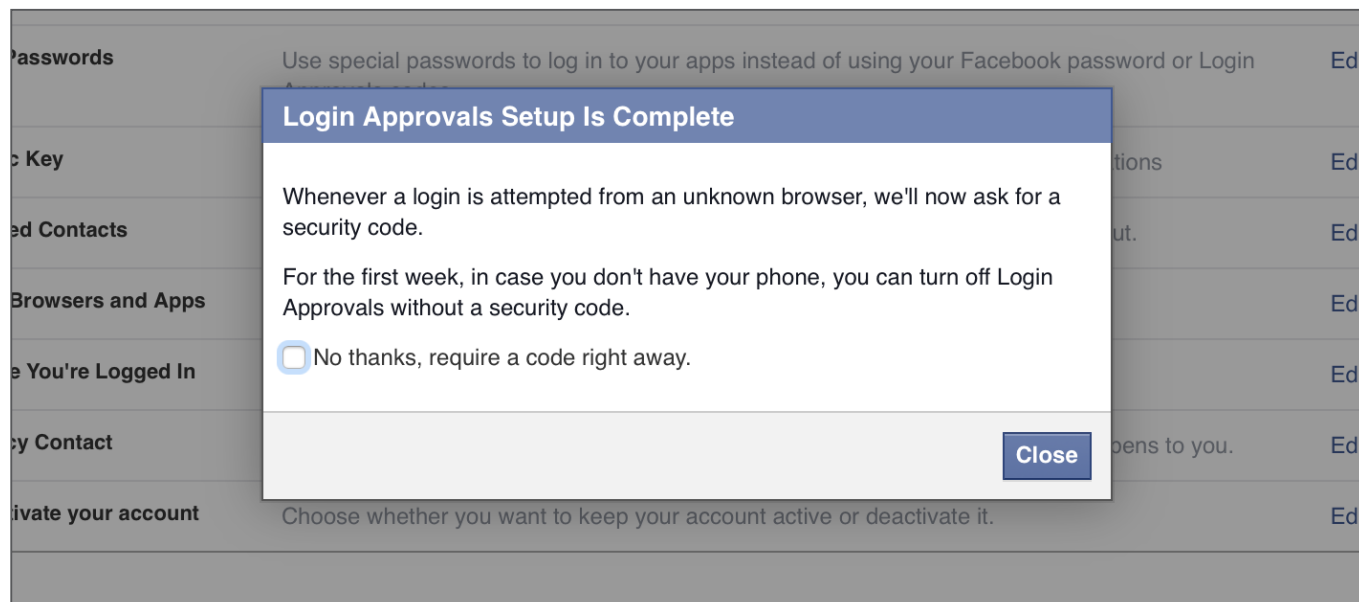


- Facebook will then ask you to re-enter your Facebook password.



A screenshot of a Facebook interface showing a modal dialog box titled "Please re-enter your password". The dialog box features a profile picture of a woman and the name "Kirrily Pendergast". Below the name, it says "For your security, you must re-enter your password to continue." There is a password input field with a "Show/Hide" icon (an eye with a checkmark). At the bottom of the dialog, there is a link "Forgotten your password?" and two buttons: "Cancel" and "Submit". The background shows a blurred view of the Facebook settings page.

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



A screenshot of a Facebook interface showing a modal dialog box titled "Login Approvals Setup Is Complete". The dialog box contains the following text: "Whenever a login is attempted from an unknown browser, we'll now ask for a security code." and "For the first week, in case you don't have your phone, you can turn off Login Approvals without a security code." Below this text, there is a checkbox labeled "No thanks, require a code right away." which is currently unchecked. At the bottom right of the dialog, there is a "Close" button. The background shows a blurred view of the Facebook settings page.

### 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, even when you aren't connected to the internet in case you can't receive your login approval code via SMS.

You will use that code in addition to your password to log into Facebook. You can also use Code Generator if you ever need to reset your password.

By using Login Approvals Code Generator you will have an extra security layer that will make it harder for someone to hack your Facebook account.

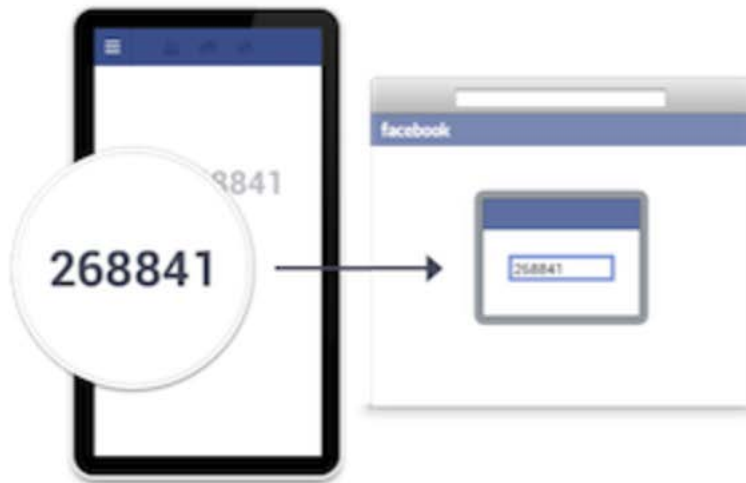
Not only do they need to hack your password, they also need to either get hold of your mobile phone to receive the security code or hack that code to access your account.

The code is needed to access Facebook from a device that wasn't previously authorised.

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

- Get codes to use when you don't have your phone

### Test Code Generator



To test Code Generator, enter the security code that appears on your phone.

Close

Back

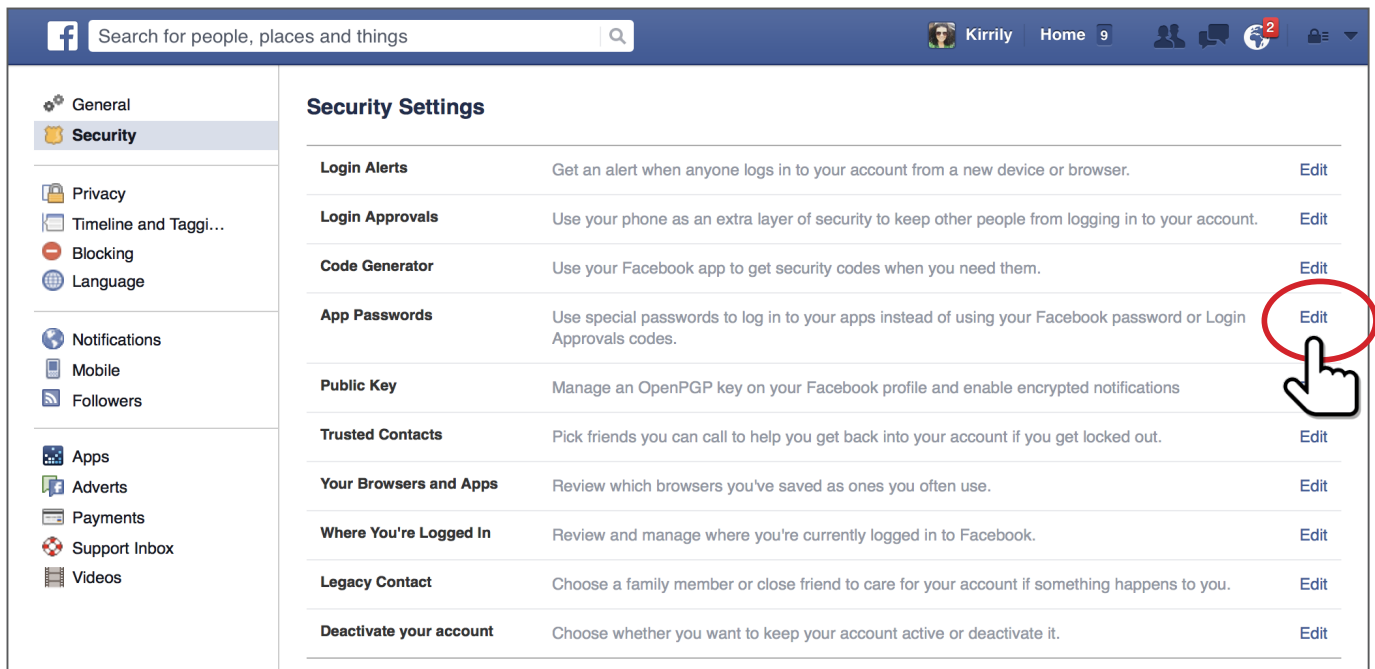
Choose whether you want to keep your account active or deactivate it.

## App Passwords

Under the code generator in your security settings you will see App Passwords. This has replaced "secure browsing".

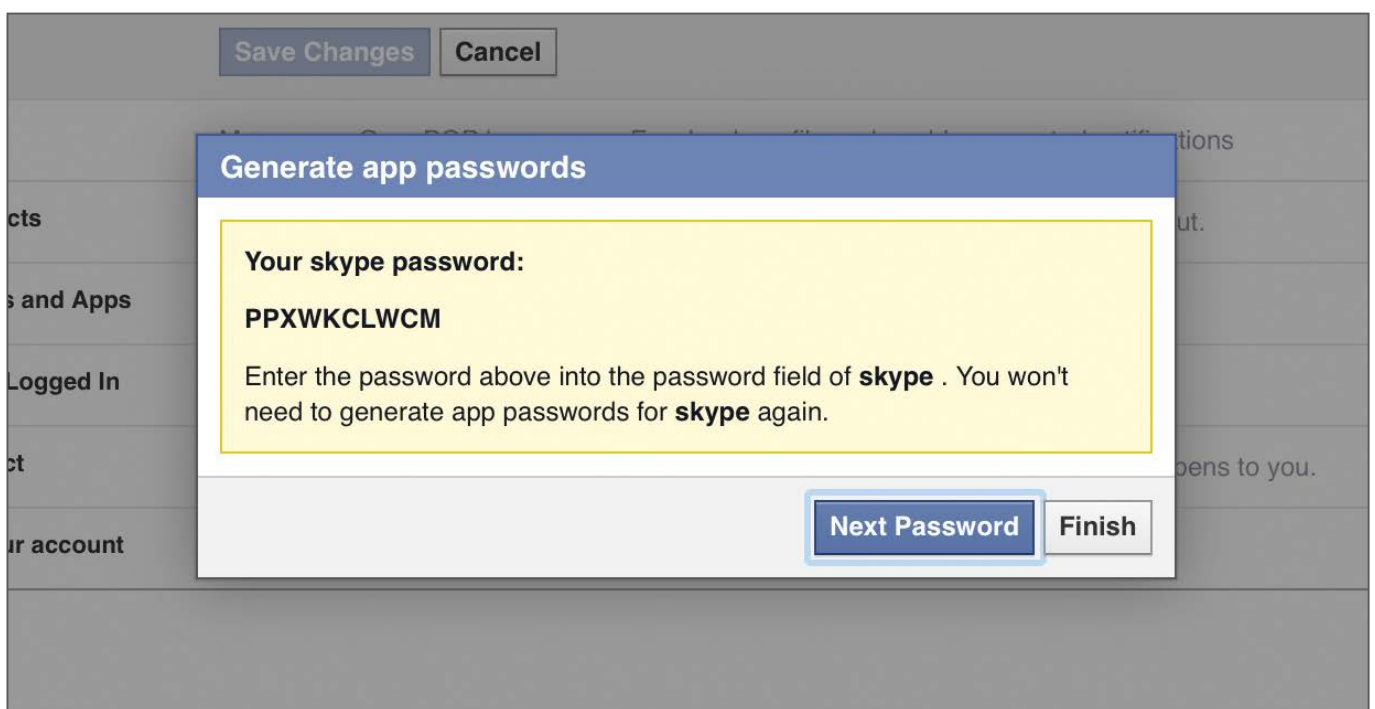
By doing this, you automatically limit all external applications that are integrated with Facebook from sharing or taking your personal information without your knowledge or approval.

To start securing your account, click "Edit" in the Apps Passwords section.



When you follow the prompts you will be able to set up use of an apps password instead of using your Facebook password to log in to third party apps.

You only need to enter your app password once.



## Public Key

The latest update to Facebook's security tools is the "Public Key". This allows you to add strong encryption keys and chose to have notification emails sent to you in an encrypted format.

'Strong Encryption' refers to data that are coded so that they cannot be read or understood by anyone who does not have the correct key to decrypt them.

Public keys are how people communicate with most popular encryption products. Every user has a public and a private key, the public key is shared freely, while the private is kept secret.

Anyone can encrypt a message using someone else's public key, which can then only be decrypted by the owner of that public key using their private key.

Encryption technology is complex and can be used the wrong way. We believe that this approach can be quite dangerous and that any "back door" in encryption products could make you vulnerable.

The other security settings in Facebook are enough for the everyday user, so this is not compulsory for a secure account.

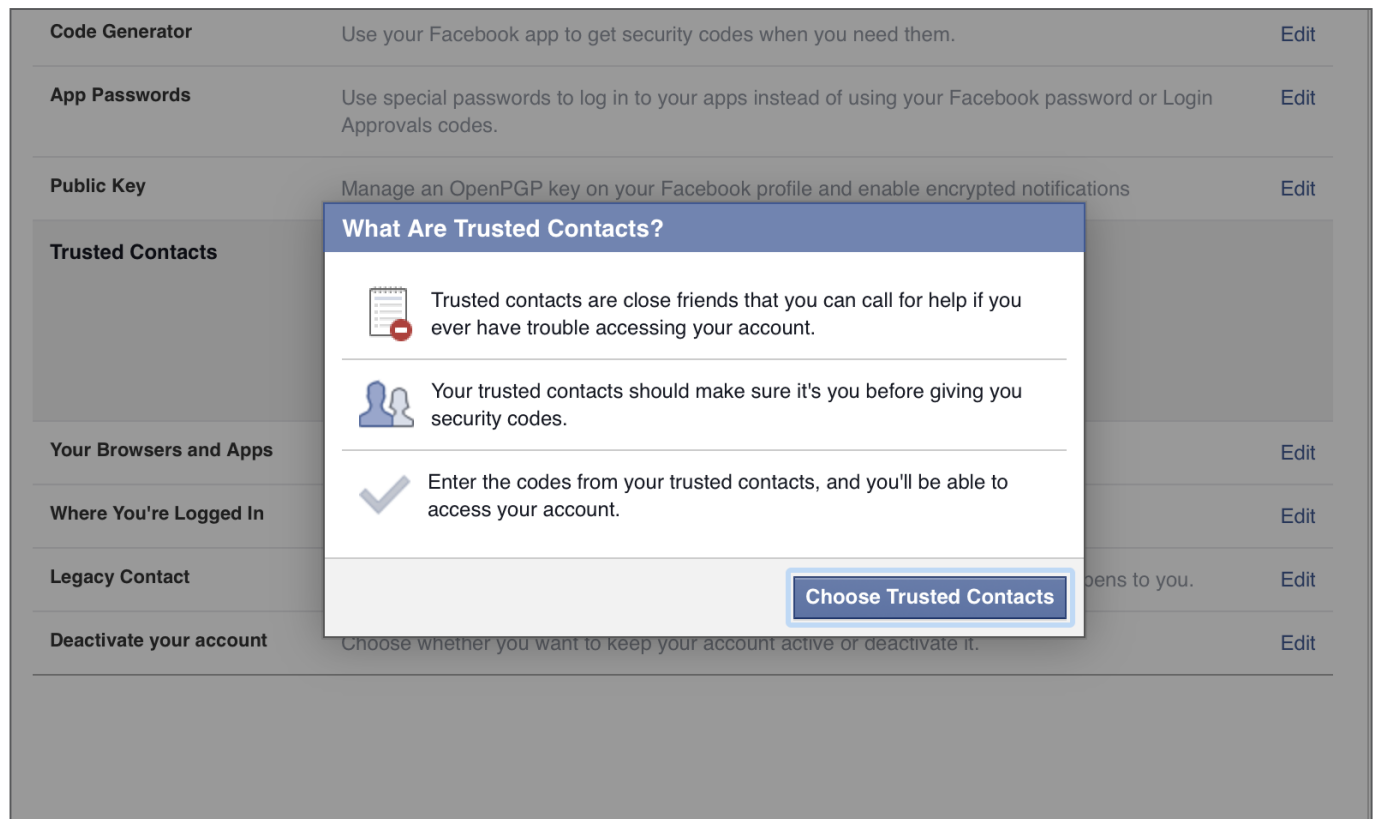


## Trusted Contacts

This is another area of Facebook's security settings that can be very dangerous, the use of which is advised against.

This is not required when there are other security options such as Login Approvals.




By making someone a 'Trusted Contact' you are effectively giving them access to your account and that is never a good idea.



The screenshot shows the Facebook security settings interface. A modal titled "What Are Trusted Contacts?" is open, explaining the feature. The background settings list includes:

- Code Generator**: Use your Facebook app to get security codes when you need them. [Edit](#)
- App Passwords**: Use special passwords to log in to your apps instead of using your Facebook password or Login Approvals codes. [Edit](#)
- Public Key**: Manage an OpenPGP key on your Facebook profile and enable encrypted notifications. [Edit](#)
- Trusted Contacts**: (Selected)
- Your Browsers and Apps**: [Edit](#)
- Where You're Logged In**: [Edit](#)
- Legacy Contact**: [Edit](#)
- Deactivate your account**: Choose whether you want to keep your account active or deactivate it. [Edit](#)

The modal "What Are Trusted Contacts?" contains the following information:

-  Trusted contacts are close friends that you can call for help if you ever have trouble accessing your account.
-  Your trusted contacts should make sure it's you before giving you security codes.
-  Enter the codes from your trusted contacts, and you'll be able to access your account.

A button labeled "Choose Trusted Contacts" is located at the bottom right of the modal.

## Your Browsers and Apps

This is an area in Facebook Security Settings that lists every device you have ever logged in from – these can be removed if you choose.

### Where you are logged in?

There has been a little hysteria about this area of Facebook circulating. The actual log-in location can be misleading. The log in details that are listed are actually the location of the DNS Server of the network you're logged in through, which can be a very long way from your actual physical location.

It can be especially confusing if you're logging in through a mobile device and therefore through the cellular network.

If you have login alerts set up like we recommended above, you will be notified of someone actually attempting to login to your account rather than where you have logged in.

To stay on the safe side, we recommend that you check this every now and then and simply "end activity" on the places that you have not visited recently.

Apps

Adverts

Payments

Support Inbox

Videos

Trusted Contacts

Pick friends you can call to help you get back into your account if you get locked out.

Edit

Your Browsers and Apps

Review which browsers you've saved as ones you often use.

Edit

Where You're Logged In

Current session

End All Activity

Device nameSafari on Mac OS X

LocationSydney, NSW, Australia (Approximate)

Device TypeSafari on Mac OS X 10.11

If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Desktop (6) ▾

Last accessedYesterday at 19:02

Device nameChrome on Mac OS X

LocationUnknown

Device TypeChrome on Mac OS X 10.10

End activity

Last accessedYesterday at 18:27

Device nameSafari on Mac OS X

LocationUnknown

Device TypeSafari on Mac OS X 10.10

End activity

Last accessed29 January at 21:11

LocationUnknown

Device TypeMobile Safari on iOS 7

End activity

Last accessed22 December 2015 at 18:39

Device nameSafari on Mac OS X

LocationUnknown

Device TypeSafari on Mac OS X 10.10

End activity

Last accessed19 December 2015 at 18:31

Device nameChrome on Mac OS X

LocationUnknown

Device TypeChrome on Mac OS X 10.8

End activity

Last accessed24 November 2015 at 10:52

Device nameSafari on Mac OS X

LocationSydney, NSW, Australia (Approximate)

Device TypeSafari on Mac OS X 10.8

End activity

## Legacy Contact

Death is always a hard subject to discuss, but this is effectively your 'Facebook will'. Just as you would nominate someone to take care of your possessions after you die, you can nominate someone to take care of your Facebook account.


The legacy contact feature allows you to nominate who you would like to take care of your account when you die.

Don't worry - they won't have full control of the account or be able to see your personal messages but they will be able to choose whether to keep your profile online or not, change your profile picture, make some tribute posts to notify people of your death, continue to accept friend requests, and administer your online memorial.

**Legacy Contact**

**My Legacy Contact**

A legacy contact is someone who you choose to manage your account after you pass away. They'll be able to do things like pin a post on your Timeline, respond to new friend requests and update your profile picture. They won't post as you or see your messages. [Learn more.](#)

**Lachie Pennefather**

Account has been memorialised, the account will be removed straight away.

---

**Account Deletion**

☐ If you don't want a Facebook account after you pass away, you can request to have your account permanently deleted.

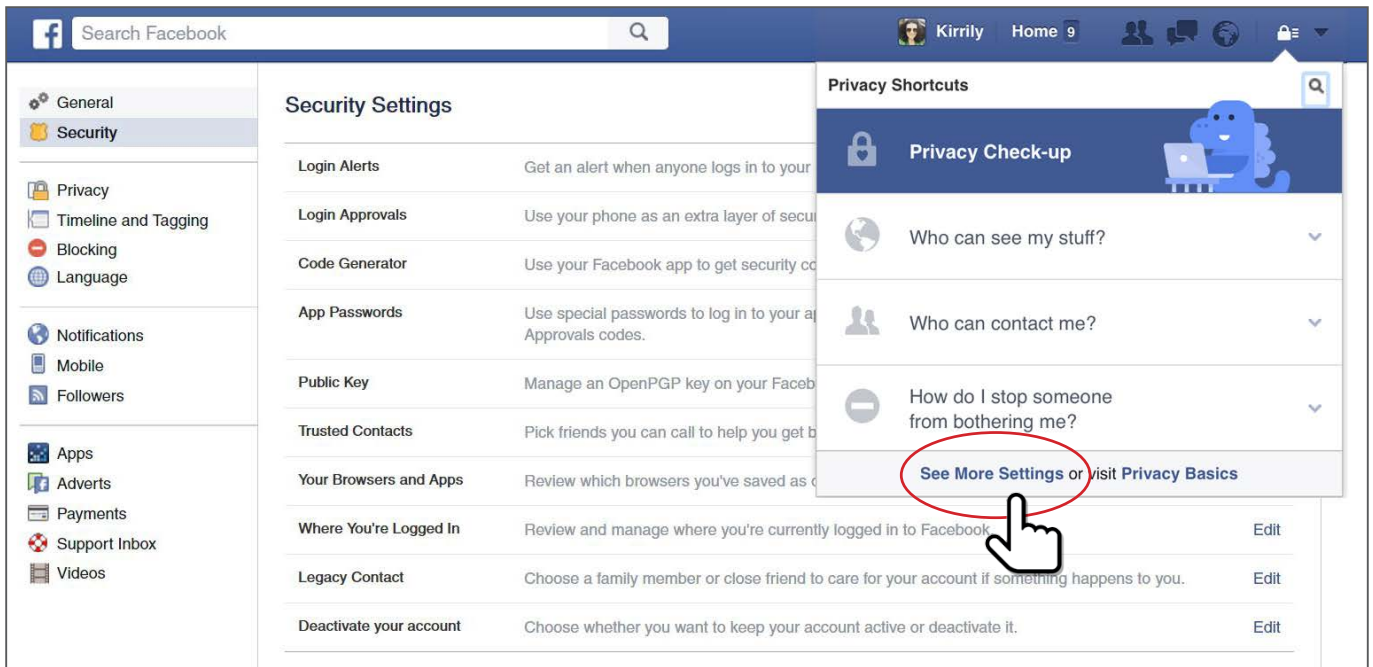
---



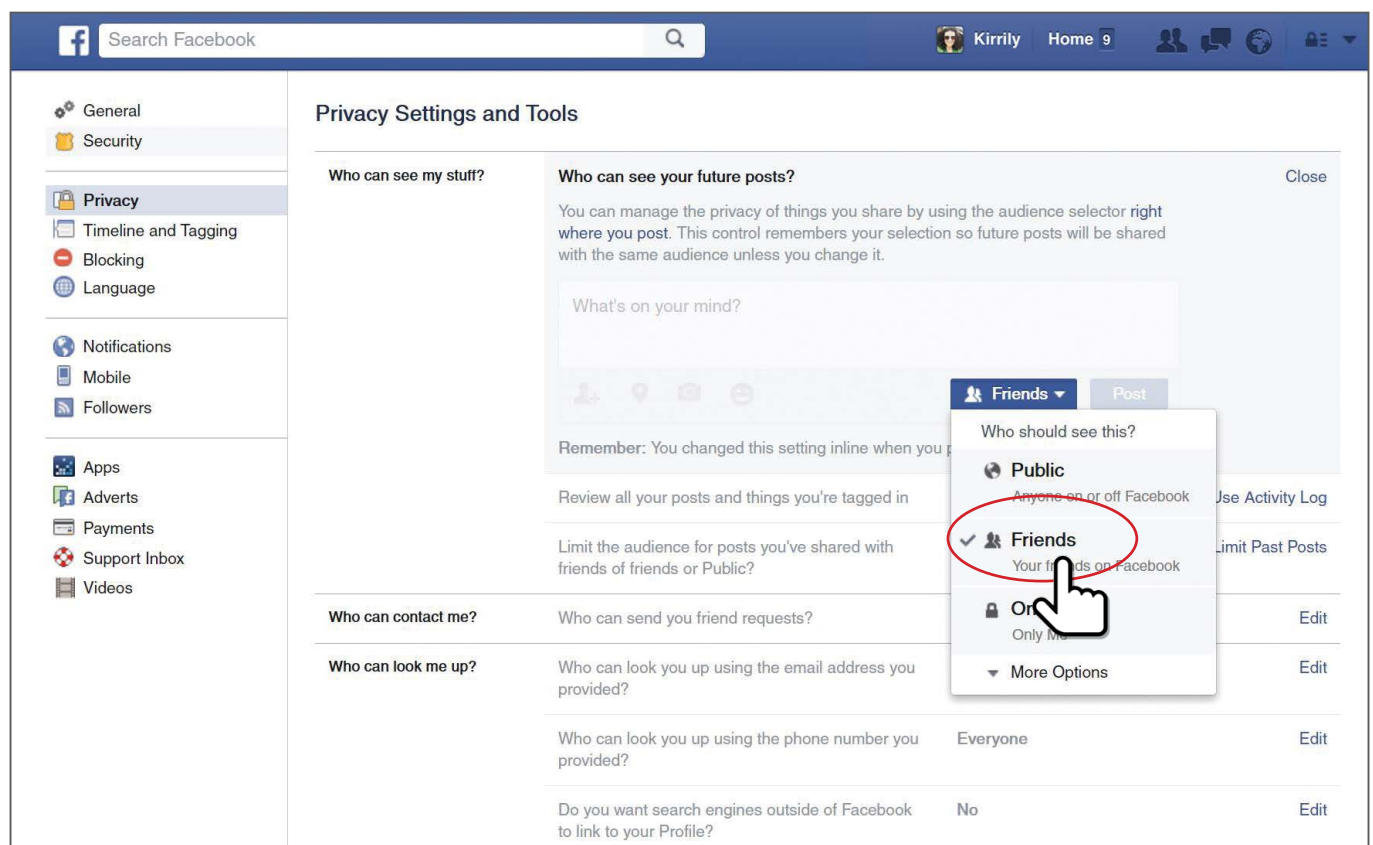
## Privacy Settings – Who can see your stuff

We recommend that you periodically check your privacy settings, as sometimes they change during major upgrades to Facebook.

There is a quick link where you are hosted by a little blue dragon that you can access by clicking on the padlock icon in the top right hand corner of your profile page. We recommend that you immediately click on “see more settings”



The first thing we recommend is to ensure that your “who can see my stuff” settings are changed to ‘Friends only’.





We also suggest that you set the option to review and approve any posts or multi-media (photos, videos etc) you are tagged in, in the activity log.

This ensures you will be notified every time someone tags you in a post and you have the option to approve or deny whether it is displayed on your timeline.

Again we strongly suggest that you limit past posts so that things you forgot to make private from a few years back are retrieved from being public to private, so only your friends can see what you posted before you knew all about privacy settings.

The screenshot shows the Facebook 'Privacy Settings and Tools' page. On the left is a navigation menu with options: General, Security, Privacy (selected), Timeline and Tagging, Blocking, Language, Notifications, Mobile, Followers, Apps, Adverts, Payments, Support Inbox, and Videos. The main content area is titled 'Privacy Settings and Tools' and contains several sections:

- Who can see my stuff?**
  - Who can see your future posts? **Friends** [Edit](#)
  - Review all your posts and things you're tagged in [Use Activity Log](#)
  - Limit the audience for posts you've shared with friends of friends or Public? [Limit Past Posts](#)
- Who can contact me?**
  - Who can send you friend requests? **Everyone** [Edit](#)
- Who can look me up?**
  - Who can look you up using the email address you provided? **Friends** [Edit](#)
  - Who can look you up using the phone number you provided? **Friends** [Edit](#)
  - Do you want search engines outside of Facebook to link to your Profile? **No** [Edit](#)

A red circle highlights the 'Use Activity Log' and 'Limit Past Posts' links, with a hand cursor pointing at them.

At the bottom of the page are links: About, Create Advert, Create Page, Developers, Careers, Privacy, Cookies, AdChoices, Terms, and Help.

## Who can contact you and who can look you up?

Always ensure that the “who can contact me” setting is set to whatever you are comfortable with – by clicking edit you have a two options.

For those of you under 18 years of age it will automatically restrict you to friends of friends only.

Adults have two options: friends of friends, or everyone.

The screenshot shows the Facebook Privacy Settings and Tools page. The left sidebar contains navigation links: General, Security, Privacy (selected), Timeline and Tagging, Blocking, Language, Notifications, Mobile, Followers, Apps, Adverts, Payments, Support Inbox, and Videos. The main content area is titled "Privacy Settings and Tools". It contains several sections for privacy control:

- Who can see my stuff?** (Current setting: Friends, Edit link)
- Who can see your future posts?** (Current setting: Friends, Edit link)
- Review all your posts and things you're tagged in** (Link: Use Activity Log)
- Limit the audience for posts you've shared with friends of friends or Public?** (Link: Limit Past Posts)
- Who can contact me?** (Current setting: Everyone, Edit link)
- Who can send you friend requests?** (Current setting: Everyone, Edit link)
- Who can look me up?** (Current setting: Everyone, Edit link)
- Who can look you up using the email address you provided?** (Link: Close)
- Who can look you up using the phone number you provided?** (Current setting: Everyone, Edit link)

The "Who can look me up?" section is expanded, showing a dropdown menu for "Who can look you up using the email address you provided?". The dropdown menu is currently set to "Friends" and is circled in red. A hand cursor is pointing at the "Friends" option. Below the dropdown menu, there is a note: "This applies to people who can't already see your email address."

It is safer if you set “Who can look me up” to “friends only” or “no one” as this may give access to your email address. You should follow the same advice for the section about your phone number.

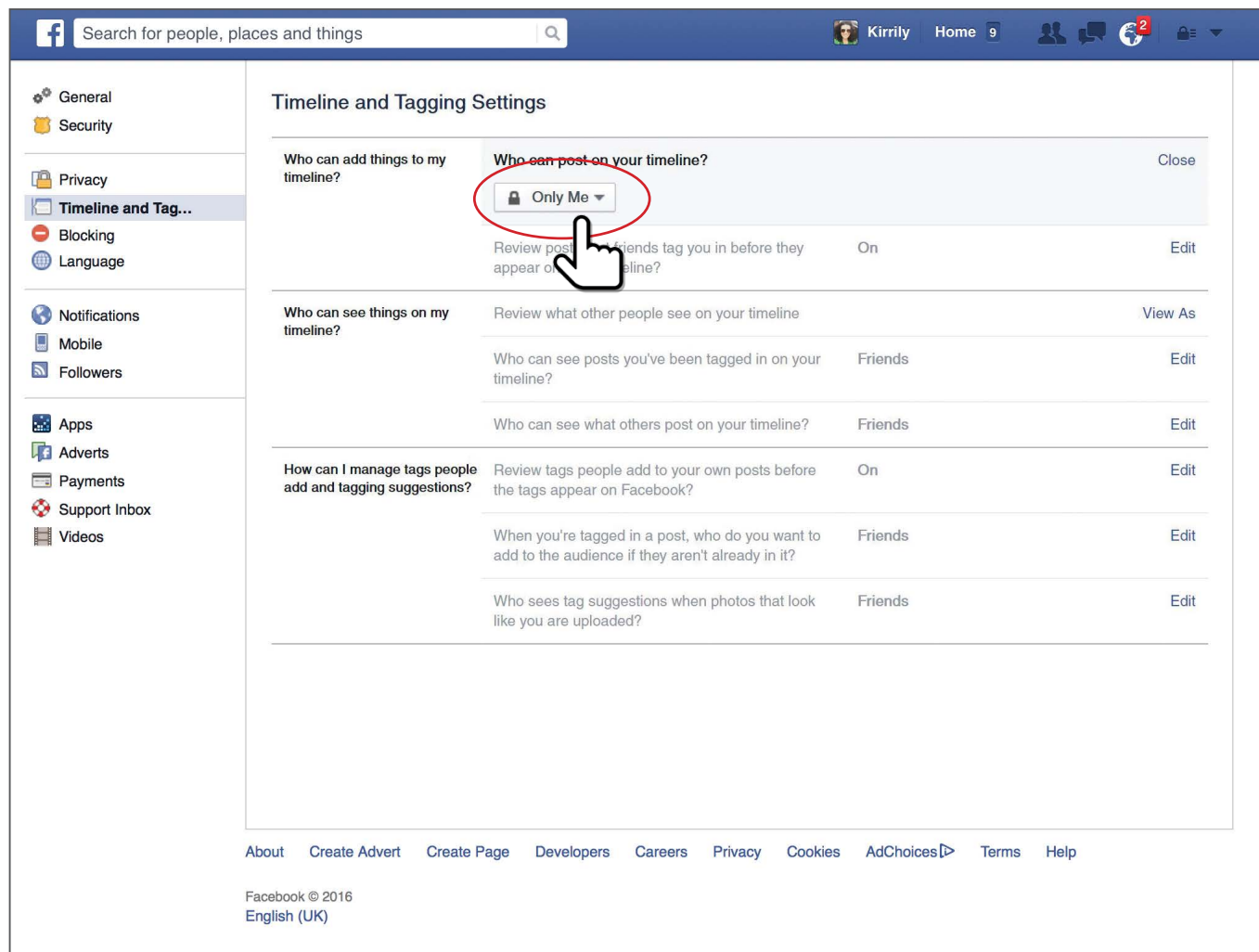
Definitely click “no” for search engines linking to your timeline or everything you post will come up on Google if someone searches your name!

# Timeline and Tagging

## Who can add things to your timeline?

In this section, first and foremost click “Only Me” or “Friends” in who can add things to your timeline.

Allowing anyone to post to your timeline invites endless amounts of spam, including offensive content, which can have a harmful affect on your public persona, and upset unwitting witnesses to this material, and in this case it is your family, friends, and in some cases colleagues, so it is advisable to protect your timeline from this violation.



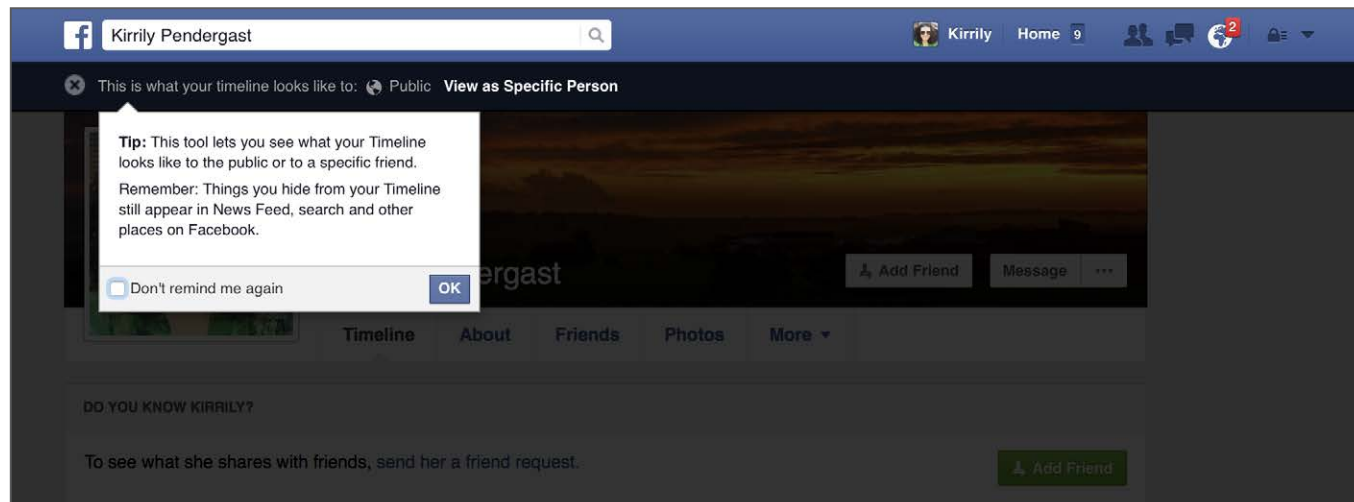
The screenshot shows the Facebook 'Timeline and Tagging Settings' page. On the left is a sidebar with navigation links: General, Security, Privacy, Timeline and Tagging (highlighted), Blocking, Language, Notifications, Mobile, Followers, Apps, Adverts, Payments, Support Inbox, and Videos. The main content area is titled 'Timeline and Tagging Settings' and contains several settings sections. The first section, 'Who can add things to my timeline?', has a sub-section 'Who can post on your timeline?' where the 'Only Me' option is selected and circled in red with a hand cursor icon pointing to it. Below this is a setting for 'Review posts that friends tag you in before they appear on your timeline?' set to 'On'. The second section, 'Who can see things on my timeline?', includes 'Review what other people see on your timeline' (with a 'View As' link), 'Who can see posts you've been tagged in on your timeline?' set to 'Friends', and 'Who can see what others post on your timeline?' set to 'Friends'. The third section, 'How can I manage tags people add and tagging suggestions?', includes 'Review tags people add to your own posts before the tags appear on Facebook?' set to 'On', 'When you're tagged in a post, who do you want to add to the audience if they aren't already in it?' set to 'Friends', and 'Who sees tag suggestions when photos that look like you are uploaded?' set to 'Friends'. Each setting has an 'Edit' link. At the bottom of the page are links for About, Create Advert, Create Page, Developers, Careers, Privacy, Cookies, AdChoices, Terms, and Help, followed by 'Facebook © 2016' and 'English (UK)'.

Setting	Value	Action
Who can add things to my timeline?		
Who can post on your timeline?	Only Me	Close
Review posts that friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?		
Review what other people see on your timeline		View As
Who can see posts you've been tagged in on your timeline?	Friends	Edit
Who can see what others post on your timeline?	Friends	Edit
How can I manage tags people add and tagging suggestions?		
Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
Who sees tag suggestions when photos that look like you are uploaded?	Friends	Edit

## Who can see things on your timeline?

You can set the two options in this section to whatever you are most comfortable with, as the risk is reasonably well controlled through other settings we have already covered.

There is a great tool that you can use periodically to see what your page looks like to others. "Review what other people see on your timeline"; clicking on this will allow you to see what your profile looks like to the public.

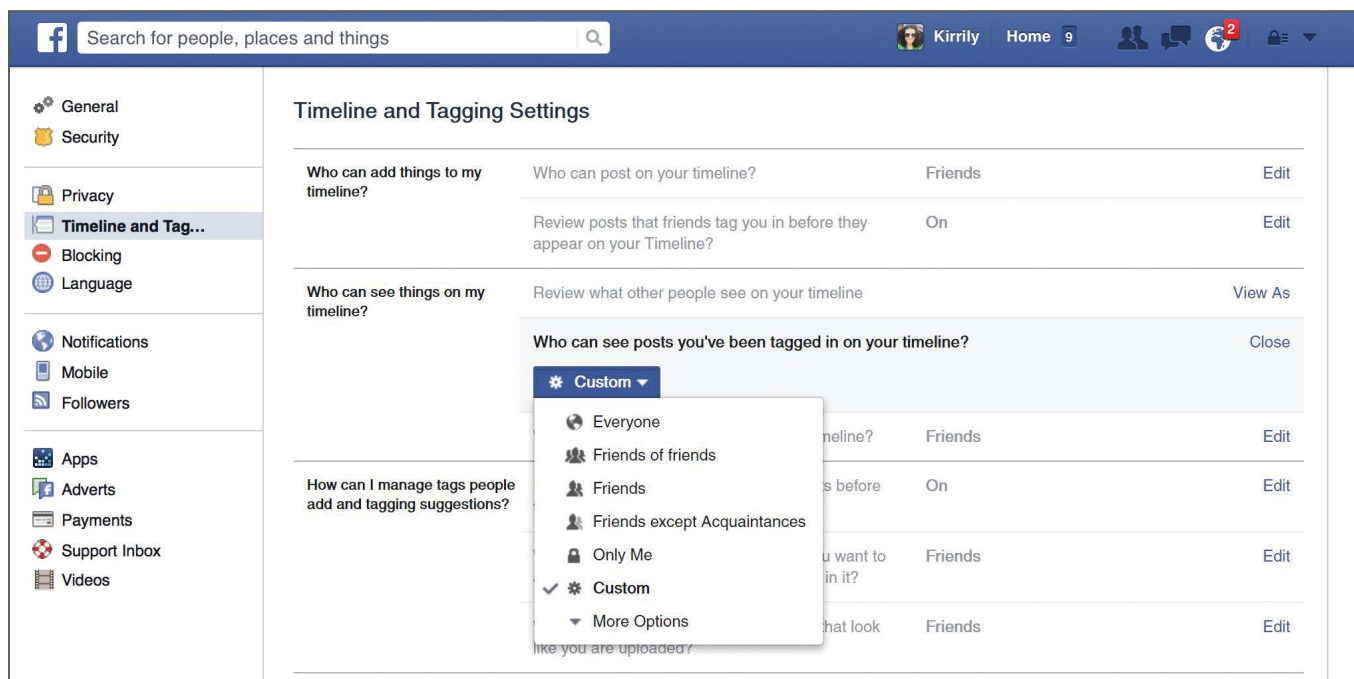


In the "who can see what others post on your timeline" section you are able to make the same selections that are available on every post you make.

If you go back to one of the posts on your timeline, you will see directly under your name on the post, a couple of little icons – one tells you how long ago the post was made, then next to that there is a little people icon and a 'Down' arrow. Click that arrow to amend the post to who you want to see it. This is good if others have asked your permission to share a post of yours publicly, like a picture of your missing dog.

In the main privacy settings, you can choose an overall default position. You might like to customise this to make sure that certain people cannot see things you post.

We advise that you choose either 'Custom' or 'Friends'. Do not click 'Everyone' or the whole world will see everything you post.

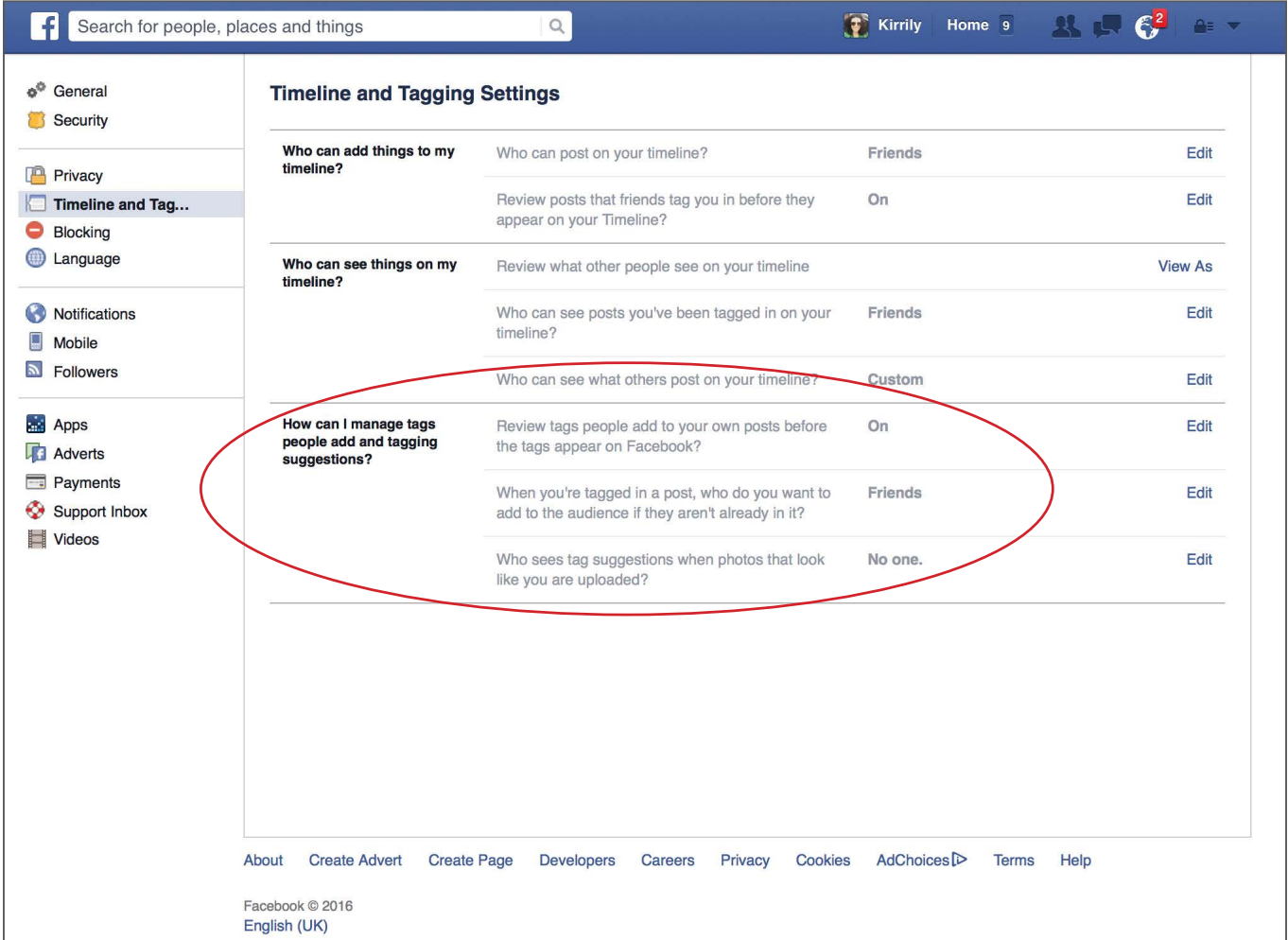


## How can you manage tags by others and tagging suggestions?

Tags and tagging can be your worst nightmare. We strongly recommend that the “review tags people add to your own posts before the tags appear on facebook” is on so that you have control over who is tagging themselves in your photos.

You can also choose who sees what posts you are tagged in. We suggest that this is always set to ‘Friends’ or ‘Only me’.

Who sees tag suggestions on photos that have been uploaded that look like you should always be set to ‘No one’.



The screenshot shows the Facebook 'Timeline and Tagging Settings' page. A red circle highlights the section titled 'How can I manage tags people add and tagging suggestions?'. This section contains three settings:

Setting	Current Value	Action
Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
Who sees tag suggestions when photos that look like you are uploaded?	No one.	Edit

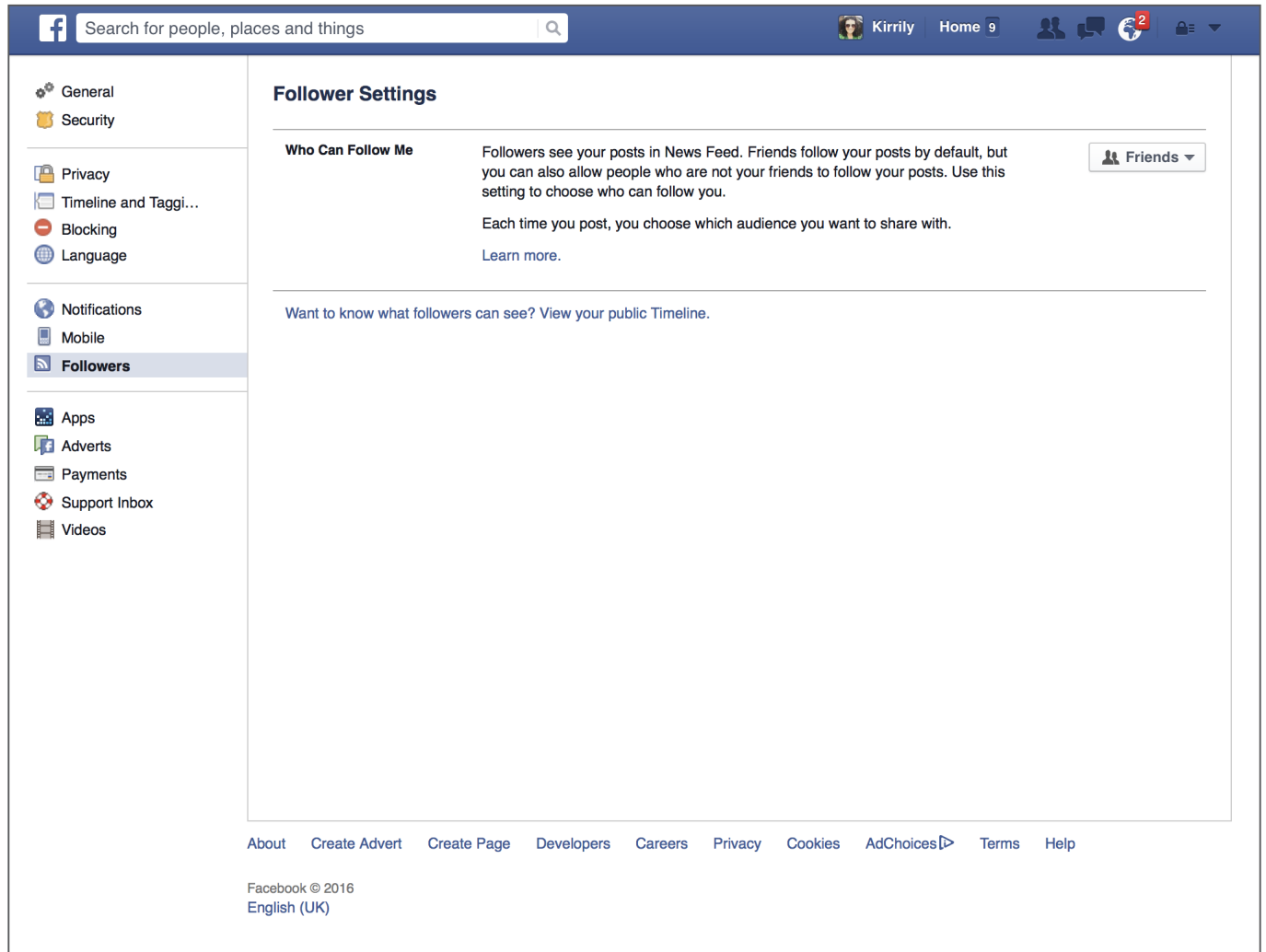
The left sidebar shows navigation options: General, Security, Privacy, Timeline and Tagging (selected), Blocking, Language, Notifications, Mobile, Followers, Apps, Adverts, Payments, Support Inbox, and Videos. The top navigation bar includes the search bar, user profile (Kirrily), Home, and notification icons. The footer contains links for About, Create Advert, Create Page, Developers, Careers, Privacy, Cookies, AdChoices, Terms, and Help, along with copyright information for Facebook © 2016 and English (UK).

## Followers

'Followers' setting is located on the left hand column, a few tabs under the General, Security and Privacy Settings areas.

This should always be set to 'Friends'.

If it is set to 'Public' this will allow people you don't know to see everything you post, but will not allow them to comment.



The screenshot shows the Facebook interface with the 'Followers' settings page open. The left sidebar contains navigation links: General, Security, Privacy, Timeline and Tagging, Blocking, Language, Notifications, Mobile, Followers (highlighted), Apps, Adverts, Payments, Support Inbox, and Videos. The main content area is titled 'Follower Settings' and includes a section 'Who Can Follow Me'. This section explains that followers see posts in the News Feed and that friends follow by default, but users can choose to allow non-friends to follow. A dropdown menu is set to 'Friends'. Below this, it states that the user chooses the audience for each post. A link to 'Learn more' is provided. At the bottom of the main area, there is a link to 'View your public Timeline'. The footer contains links for About, Create Advert, Create Page, Developers, Careers, Privacy, Cookies, AdChoices, Terms, and Help, along with copyright information for Facebook © 2016 and the language setting 'English (UK)'.

Search for people, places and things

Kirily Home 9

General  
Security  
Privacy  
Timeline and Taggi...  
Blocking  
Language  
Notifications  
Mobile  
**Followers**  
Apps  
Adverts  
Payments  
Support Inbox  
Videos

### Follower Settings

**Who Can Follow Me**

Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your posts. Use this setting to choose who can follow you.

Each time you post, you choose which audience you want to share with.

[Learn more.](#)

Friends ▾

Want to know what followers can see? [View your public Timeline.](#)

About Create Advert Create Page Developers Careers Privacy Cookies AdChoices Terms Help

Facebook © 2016  
English (UK)

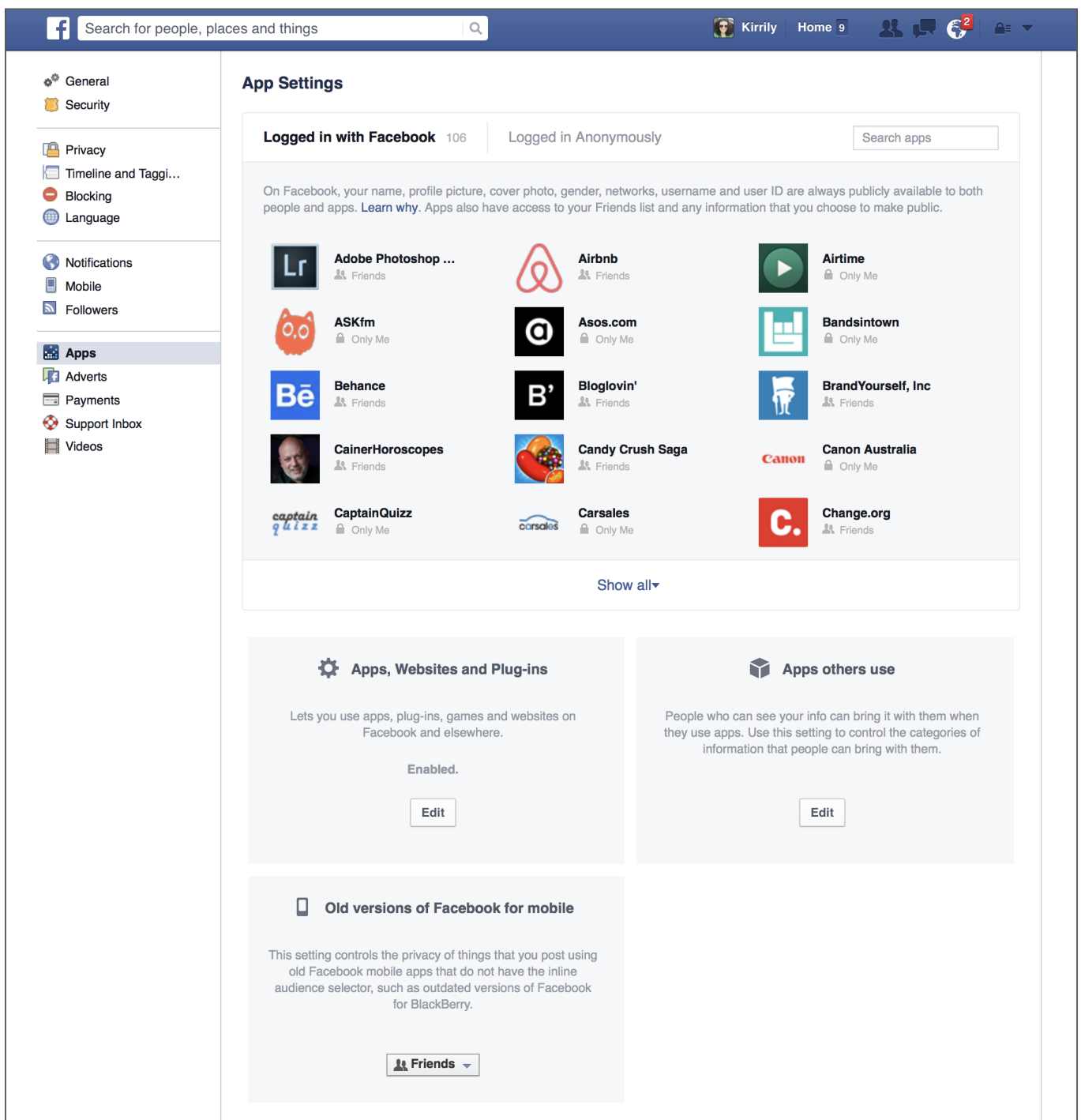
## Apps

By clicking on the Apps icon in the left hand column you can easily see what apps you have logged into using Facebook. You can go back and change the settings to 'Only me' so that your interaction with these apps is not posted to your Facebook page.

It is quite common to see people who think that their security and privacy settings are up to scratch only to have a random app posting to their page publicly.

In most cases this is ok, but if you have a false name on KiK or Ask.Fm, for example, it can be sharing the details of that false name on the front page of your Facebook page without you even knowing.

This may allow people you don't know to follow you on other apps after you have either blocked them from following you on Facebook or are not friends with them, but they can still see aspects of your public profile.



The screenshot shows the Facebook 'App Settings' page for a user named Kirrily. The page is divided into three main sections. The top section, 'Logged in with Facebook', shows a list of 106 apps. The middle section, 'Apps, Websites and Plug-ins', shows that this setting is 'Enabled'. The bottom section, 'Old versions of Facebook for mobile', shows that this setting is set to 'Friends'.

**App Settings**

Logged in with Facebook 106 | Logged in Anonymously | Search apps

On Facebook, your name, profile picture, cover photo, gender, networks, username and user ID are always publicly available to both people and apps. [Learn why](#). Apps also have access to your Friends list and any information that you choose to make public.

App Icon	App Name	Privacy Setting
	Adobe Photoshop ...	Friends
	Airbnb	Friends
	Airtime	Only Me
	ASKfm	Only Me
	Asos.com	Only Me
	Bandsintown	Only Me
	Behance	Friends
	Bloglovin'	Friends
	BrandYourself, Inc	Friends
	CainerHoroscopes	Friends
	Candy Crush Saga	Friends
	Canon Australia	Only Me
	CaptainQuizz	Only Me
	Carsales	Only Me
	Change.org	Friends

Show all ▾

**Apps, Websites and Plug-ins**

Lets you use apps, plug-ins, games and websites on Facebook and elsewhere.

Enabled.

Edit

**Apps others use**

People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information that people can bring with them.

Edit

**Old versions of Facebook for mobile**

This setting controls the privacy of things that you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.

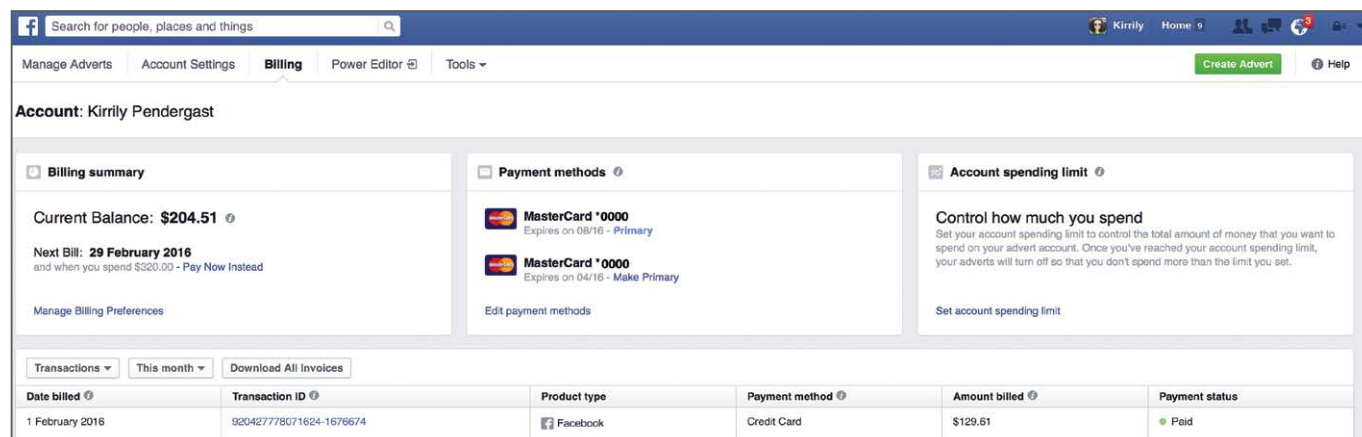
Friends ▾

## Payments

This is where your credit card details are saved if you have used your card on Facebook. Unless you are using your card regularly to pay for Facebook advertising, regularly check that either no card numbers are stored in this section. If there are you can simply click 'Remove'.



This area also stores all receipts of purchases that you have made with Facebook in the billing summary section in case you need to access them for accounting purposes.

You can also set limits for your spending with Facebook advertising here.





**Account: Kirrily Pendergast**

**Billing summary**  
Current Balance: **\$204.51**  
Next Bill: **29 February 2016**  
and when you spend \$320.00 - [Pay Now Instead](#)  
[Manage Billing Preferences](#)

**Payment methods**  
 **MasterCard \*0000**  
Expires on 08/16 - [Primary](#)  
 **MasterCard \*0000**  
Expires on 04/16 - [Make Primary](#)  
[Edit payment methods](#)

**Account spending limit**  
**Control how much you spend**  
Set your account spending limit to control the total amount of money that you want to spend on your advert account. Once you've reached your account spending limit, your adverts will turn off so that you don't spend more than the limit you set.  
[Set account spending limit](#)

Transactions ▾ This month ▾ [Download All Invoices](#)

Date billed	Transaction ID	Product type	Payment method	Amount billed	Payment status
1 February 2016	920427778071624-1676674	 Facebook	Credit Card	\$129.61	 Paid



## Facebook Scams

If you spend time on Facebook you may have already fallen victim to a scam or know someone who has. Scammers love a crowd and the biggest crowd online is Facebook.

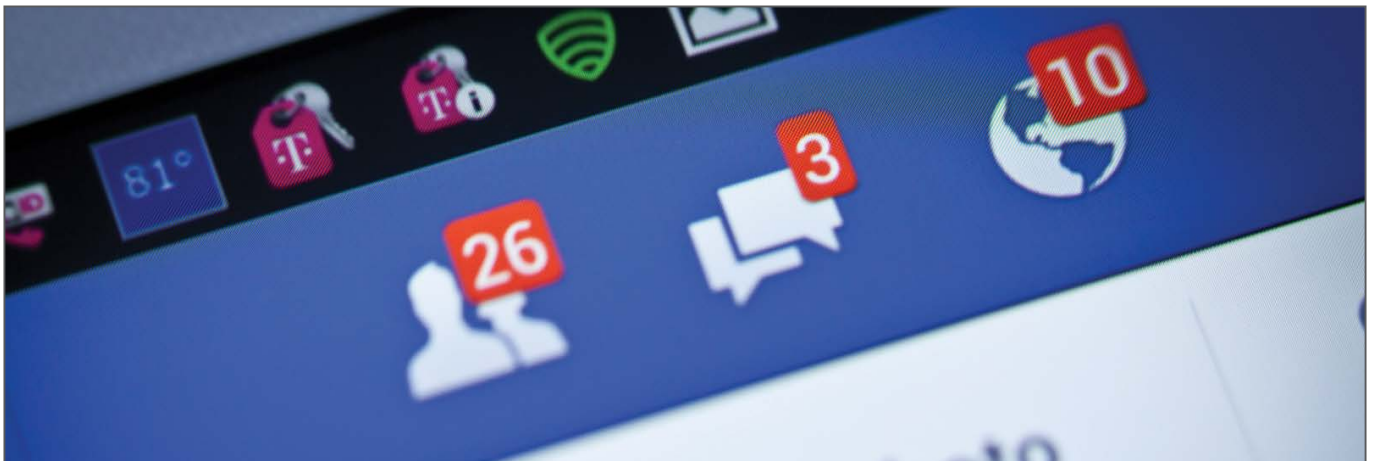
Most of the scams you will encounter online are phishing based scams that are trying to obtain your username and password. Other scams you have or will see are surveys or fake offers for free stuff, or to win things. Most of these will spread Malware and viruses, so it is very important that you have a good anti-virus application installed and keep it up to date.

### Do you know who your friends really are?

One of the main reasons that we join Facebook is to connect with friends. Through accepting "friend requests" you are letting someone into your life. They will be able to see all of your photos, videos and the written text that you post on a daily basis.

There is always the temptation to connect with friends of friends, or in some cases complete strangers that look interesting and you may have one or two friends in common so that makes it ok right? Wrong.

Daily, millions of scammers send friend requests. By accepting friend requests from people that you do not know, you put yourself and your friends at risk. Do not rely on having friends in common as a way to validate that someone is ok; you must protect your friends' and your own safety in the Facebook environment as you would in the real world, and this means applying some healthy cynicism toward strangers approaching you.



It is common for Facebook users to receive a friend request from time to time from friends that you are already friends with. This is a scam that is doing the rounds and is even more insidious than most. By making virtual copies of real Facebook accounts, scammers use your friends' photos and information from their real account's "About" page to create a fake one. They then block your friend for the fake account they have set up so they cannot see it. They then send friend requests to the friends listed on their real account.

Once the scammer has most or all of the original account holder's friends onboard, there are countless ways those friends can be scammed because, we tend to trust our friends, right?

One of the most common scams committed after a fake account has been created is messaging you asking for money to help get them through some sort of crisis. They usually include the fact that your friend is in trouble and urgently needs your help with medical or travel expenses.

While this scam can be dangerous it is also easy to avoid. If you receive a friend request from someone you are already friends with, search your friend list to see if you are still friends with that person. If you are, you have just received a friend request from a duplicate (and probably fake) Facebook account.

Some people open duplicate accounts for whatever reason so there is always a chance that the friend request really came from your friend and not a scammer. Find out by messaging your friend from the account they are already friends with and ask if the friend request is legit. Even better, call them on the phone and ask.

If the new account turns out to be fake, report it to Facebook.

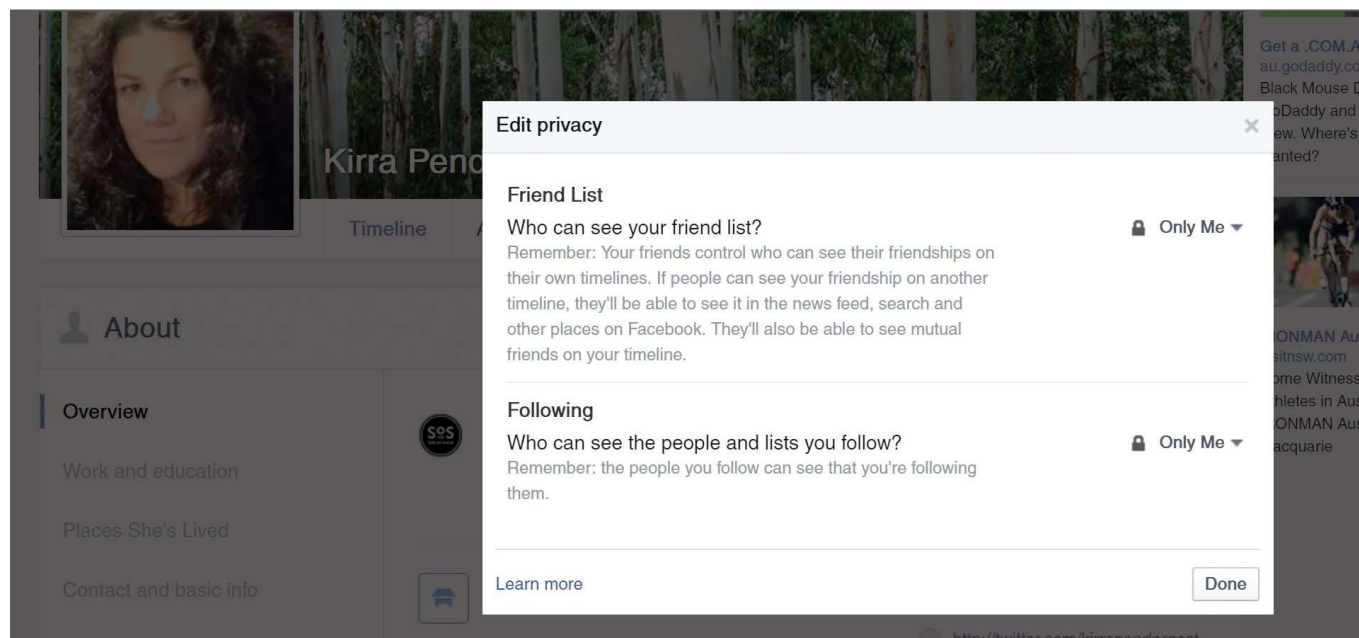
*Here is how to report it:*

1. Go to the timeline page of the fake Facebook account
2. Hover your mouse over the button labeled with 3 dots (it's located beside the Message button), then click 'Report'
3. Click 'Report this account'
4. Select 'Report XXXXX's account'
5. Click the 'Continue' button.

Facebook will take action against the user of the fake account as a result of reporting. Action is faster if several people report the account instead of just one person. We recommend that you tell the friend who had his/her account copied so he/she can report the fake account too. Also, ask all of your friend's friends to do the same. If Facebook receives several reports about the same fake account, they usually investigate and promptly shut it down.

There is really no need to share who you are friends with on Facebook. So to protect yourself from these kind of scams and therefore protect your friends as well here is what you can do:

If you go to the box that on the right hand side of your Facebook profile that has all your friends listed in it you can click on the down arrow or the little pencil and the following box will pop-up. Make sure you change both options to only me.



This will protect you and your friends, as, if a scammer can't see who you are friends with when they are searching for accounts to copy, they are less likely to copy your account.

If one of your friends has had their account copied or hacked, change your password immediately, as there is a good chance the scammer is already looking at ways to get into your account.

To do this, click on the down facing arrow across from your name and the messages icon at the very top right of your Facebook profile page. Scroll down and click on 'Settings' and you will be shown where you can change your password.

## Who is looking at your profile and who has blocked you?

These scams promise to show you who has been looking at your profile or who has blocked you from seeing their profile. None of these apps actually do anything except steal information about you. Facebook does not allow access to the type of data required to create these kinds of apps.

## Free gift cards

Bunnings, Woolworths, Coles and others do not give out cash vouchers, Virgin Airlines or QANTAS do not give away first class flights, and Range Rover does not give away cars. Every week we see a new "if you like and share" post that you will go in the draw to win. Before you click like on the page have a little look around: is there a full stop after the name on the top of the profile page? A small spelling mistake in the name? Do they only have a few thousand followers and one or two photos? This is a clear indication you're looking at a scam page, as usually big brands (as the aforementioned brands) will have hundreds of thousands of followers.

The old saying "if it seems too good to be true it probably is" definitely rings true in these cases.

## Scam page

**SAFETY TIP**  
Scam pages don't have many followers or photos when compared to the real page.

**SAFETY TIP**  
Fake pages often have a full stop or period directly after the name.

**SAFETY TIP**  
7,731 people like this

**SAFETY TIP**  
14 hrs · @

Today is an incredible day at Virgin Airlines as we are officially celebrating seating over 150 million passengers since 2014!! To celebrate we are giving away 500 FREE first class flights for the entire year to a few of our lucky fans!!

Want to win? You must Share this picture and like the page! then Comment Thank You below.

Winners will be decided on August 8 2015

Remember to Like our page to see who won.

**UPPER CLASS**

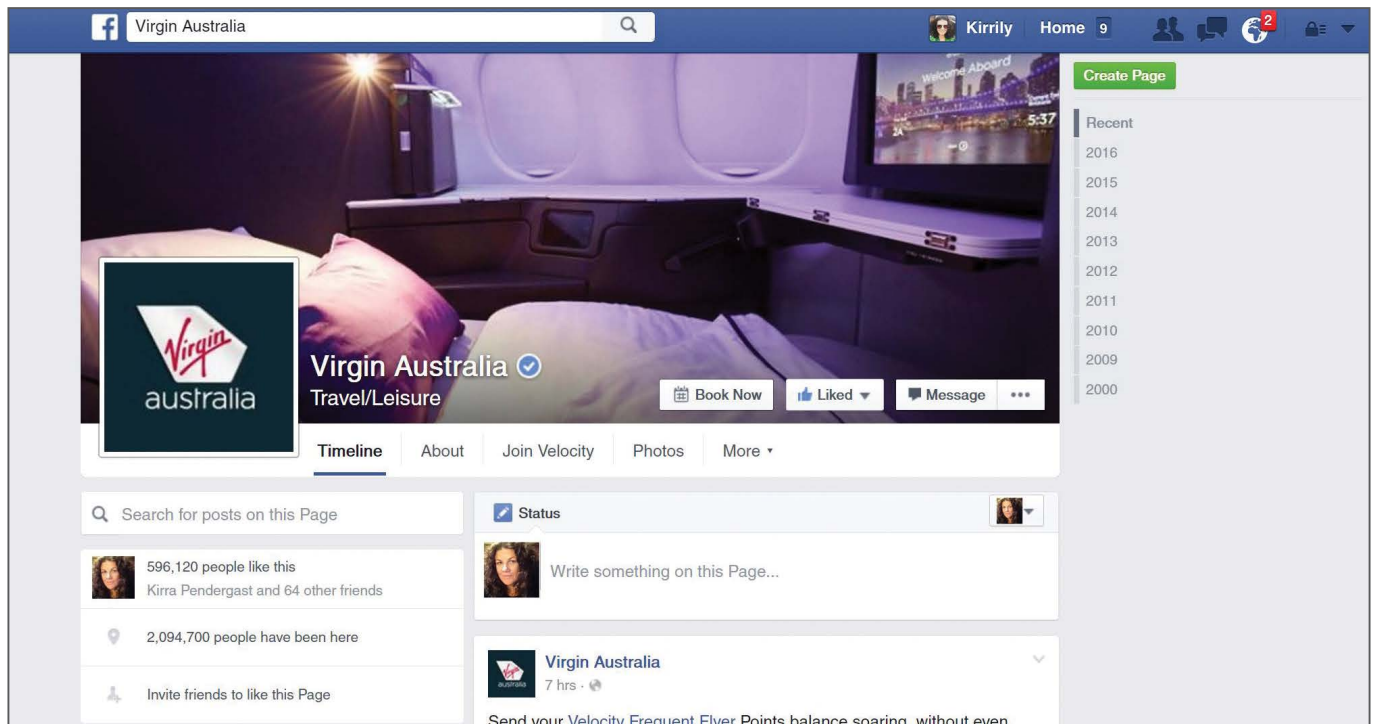
virgin atlantic

Passenger Name: FIRST / LAST NAME  
From: YOUR LOCATION To: YOUR DESTINATION  
Depart Time: 19:25 Boarding Time: 18:55 Depart Date: 59 Seat No: 7E Ticket: ETKT  
Flight No: VS 603 Cabin: UPPER CLASS Seq: 08.A  
REF 13-1842154010

virgin atlantic  
**BOARDING PASS**  
Passenger Name: FIRST / LAST NAME  
From: YOUR LOCATION To: YOUR DESTINATION  
Depart Time: 19:25 Boarding Time: 18:55 Depart Date: 59 Seat No: 7E Ticket: ETKT  
Flight No: VS 603 Cabin: UPPER CLASS Seq: 08.A  
REF 13-1842154010  
VS 603 UPPER CLASS  
2 0 0  
TATA



## Real page



### Free lifetime Pass to your favourite fast food outlet

A recent scam that flooded Facebook pages is a series of posts that say you can get a free lifetime pass to popular fast food outlets. The post asks you to click a link and follow the instructions to claim your lifetime pass. So far, we have seen these posts referring to big chains like McDonalds and KFC.

These posts are in no way associated with these fast food outlets and are a typical Facebook survey scam that is attempting to trick you into promoting these false claims to your Facebook friends; by default you are divulging all sorts of personal information in the process.

By clicking on the post link you will be taken to a fake page that has been designed to look like it is a part of Facebook. The page instructs you to share the link with your Facebook friends and with 5 Facebook groups that you are a member of to be able to claim your prize.

Once you share the post, as instructed, you will see a pop-up that claims you must complete a survey before receiving your prize. This pop-up includes a list of links.

These links open survey websites that offer the chance of winning further prizes in exchange for completing surveys and, of course, you need to supply your name, home address, email, phone numbers, etc.

The fine print actually states that by filling in these surveys you are giving permission for your personal information to be shared with sponsors and third party groups.


This means soon after you will receive a lot of spam email and unwanted marketing phone calls!

The scammers earn their money by selling your information and through affiliate marketing programs.




To Learn more about Facebook or to report an issue visit

<https://www.facebook.com/help>

 Help Centre

Go to News Feed



Search

Desktop Help

English (UK)

Login & Password

Get Started on Facebook

Manage Your Account

Privacy

Security

News Feed

Sharing

Messaging

Connecting


Pages

Ads


Facebook Mobile

Popular Features


Popular topics




Manage Your Password




Get Help Using Facebook on Your Phone or Tablet




Report an Issue




Build Your Facebook Page



Create Facebook Ads



Manage Your Ad Campaigns

 Australian Government  
Office of the Children's eSafety Commissioner

### Quick guide to the Office of the Children's eSafety Commissioner

#### What we do

At the Office of the Children's eSafety Commissioner (the Office) we:

- deal with complaints about serious cyberbullying material affecting Australian children (under the age of 18)
- investigate offensive or illegal online content, such as child sexual abuse material
- provide online safety education and training, and undertake research.

#### How we handle complaints

The Office works with social media services to quickly remove serious cyberbullying material.

The material generally needs to have been reported to the social media service first. The social media service has 48 hours to remove the material. If the material is not removed, it can be reported to the Office.

We also work with schools, parents and others (such as police and the person responsible for the material) to address the underlying behaviour and any ongoing bullying.

#### What type of complaints can we act on

The Office can act on complaints about cyberbullying material that seriously threatens, intimidates, harasses or humiliates an Australian child.

We assess seriousness by looking at the circumstances of the child and the material itself.

We take into account any vulnerabilities of the child, and their relationship with the person posting the material.

We also look at the language used, the number of potential views and the sensitivity of the material.

#### What types of complaints have we acted on

- Serious name calling and nasty comments—for example, comments that incite suicide, outing, or sexually threatening language.
- Fake accounts or impersonations.
- Offensive or upsetting pictures or videos.
- Hacking of social media accounts (potentially due to password sharing).
- Hate pages.

#### Who can complain

Complaints can be made by a child, their parent or another responsible person the child has authorised to make the complaint for them.

#### How to report cyberbullying material

- Report the cyberbullying material to the social media service
- Collect evidence—copy URLs or take screenshots of the material  
If the content is not removed within 48 hours...
- Report it to [www.esafety.gov.au/cyberbullying-complaint](http://www.esafety.gov.au/cyberbullying-complaint)
- Block the person and talk to someone you trust

If you are in immediate danger, call Triple Zero (000).  
If you need to talk to someone, visit Kids Helpline online or call them on 1800 55 1800, 24 hours a day, seven days a week.

A cyberbullying complaint can be made at [www.esafety.gov.au/reportcyberbullying](http://www.esafety.gov.au/reportcyberbullying)


## Australia's 24/7 Youth Counselling service.

### Need support?

**For ages 5 - 25**

[www.kidshelpline.com.au](http://www.kidshelpline.com.au)

#KidsHelplineAU



## Kids Helpline

# 1800 55 1800

Kids Helpline is a service of BoysTown.

Page 33



[www.safeonsocialmedia.com.au](http://www.safeonsocialmedia.com.au)