





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 form or 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
9bWfmd hY X`Ya UJ`bc h UWU h c bg`.....	\$
Privacy features	30
Limit last posts	31
Determine who can search for you.....	32
Blocking	32
B ch UWU h c bg`.....	(
A c V]Y`B ch UWU h c bg`.....	+
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

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. sefe socializingy.

- Spending too much time online
- Damage to your relationships
-

Problems and Preventions

Legacy Contact Details

My friend's account was deleted after he 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.

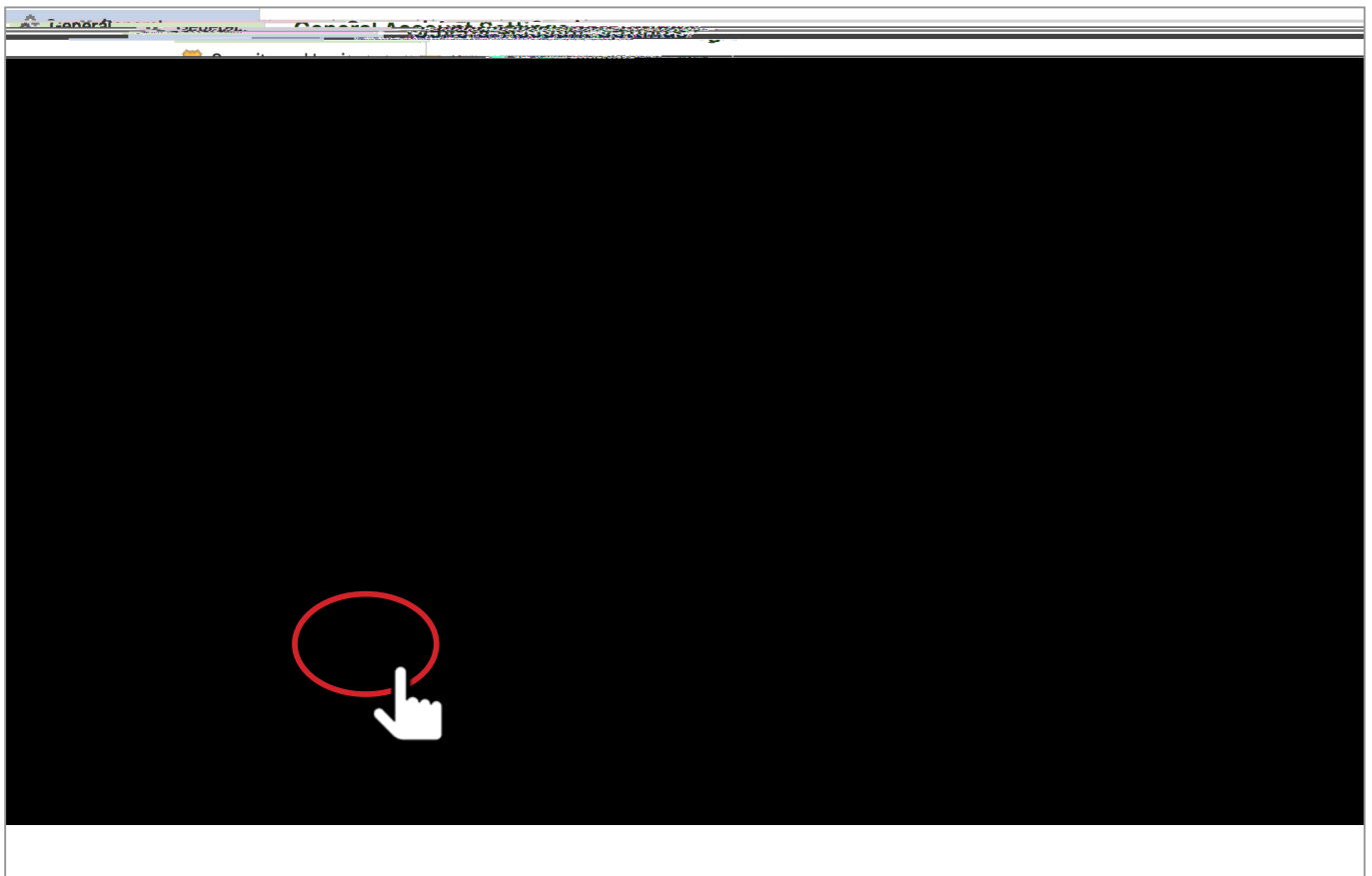
An account holder will be able to select someone from their friends list to essentially, act on their account.

The person selected will be able to interact with the account – writing posts at the top of the page.

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.



Your Legacy Contact

A legacy contact is someone 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, update your profile picture. They won't post as you or see your messages. [Learn more](#)



Data and History

- Allow my legacy contact to download a copy of my data from Facebook. This may include posts, photos, videos and info from the About section. [Learn more](#)

If you don't want a Facebook account after you pass away, you can deactivate your account. [Learn more](#)

Deactivate your account

Deactivating your account will disable your profile and remove your name and photo from most things you've shared on Facebook. Some information may still be visible to you, such as your name in their friends list and messages you sent. [Learn more](#)

[Deactivate your account.](#)



[Download a copy of your Facebook data](#)

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 \UgđJX ĨBYj Yfđi hmc i fXUH'cZV]fhžUbX'k \YfY'mci' k YfY'Vc fb'fb'bdYfgc bU'dfc ŪYđ'c'f'mci' 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.

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

Zmci fUWŁci bhgZ]YbXg'gh]gbchgyhlc'dfj UHžd\c hcgŪfY'đc'Yb'Zca'mci f'dfc ŪY'UbX'gYhi d' 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 V'cW_YX'Zca'h]gd'fc ŪY'UbX'h\Y'UWŁci bhgUfřgYbX]b[Z]YbX'fYe i Yđg'hc'U'c'Zmci f Z]YbXg'h Uh have unsecured friends lists.

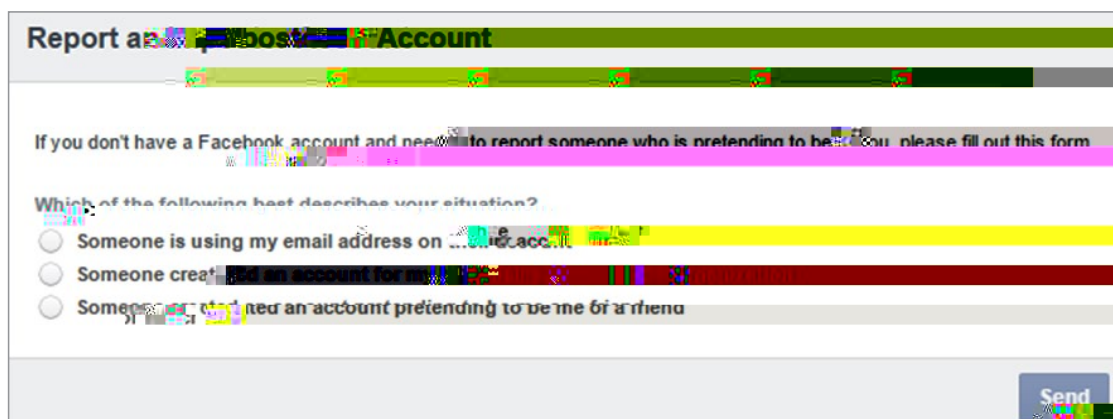
When your friends accept this fake friend request it can do nothing for months but sooner or later a message will be sent saying that they are stuck somewhere and urgently need money, or something to that effect.

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.

!''''5bX'fYd'c'fh'h\Y'Z]gY'd'fc ŪY''



The image shows a screenshot of a Facebook report form titled "Report an Account". The form asks the user to describe their situation. The options are:

- Someone is using my email address on ... acc. it.
- Someone creat...
- Someone ... created an account pretending to be me or a friend.

A "Send" button is visible at the bottom right of the form.

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.

Facebook Cloning – where a duplicate or clone account is set up. This will copy as much detail as possible from the real account. Once a friend request is accepted, these usually copy all the details of the real account holder. Once a friend request is accepted, these usually copy all the details of the real account holder. Once a friend request is accepted, these usually copy all the details of the real account holder.

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 others, you can help protect your privacy and security.

Harming your professional reputation and future job prospects

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

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

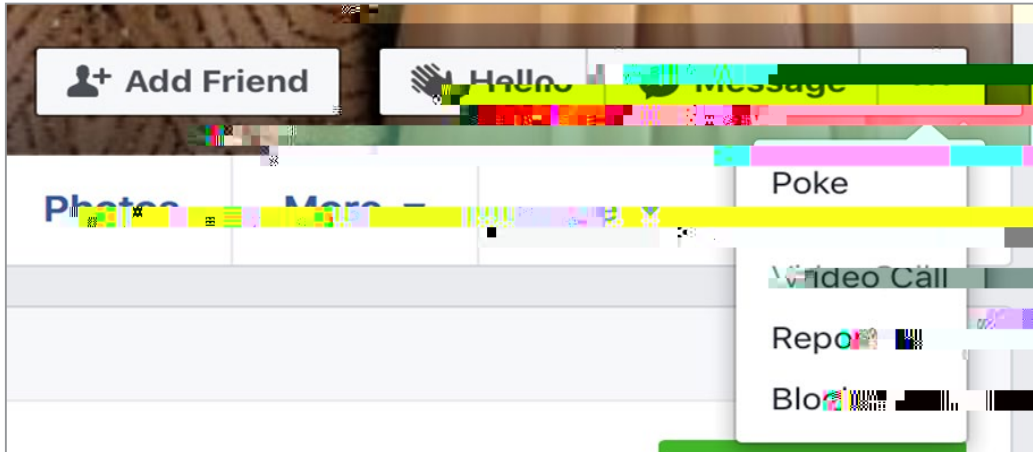


Blocking on Facebook and unfriending.

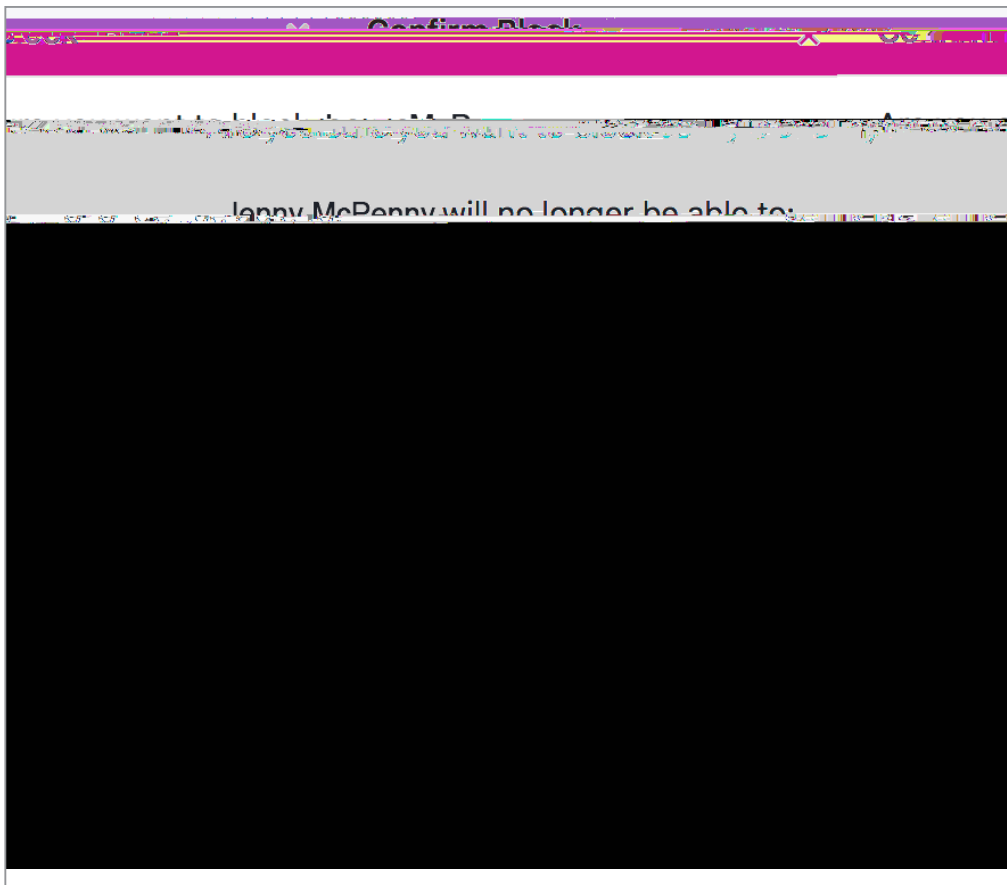
Users can both unfriend and block people on Facebook. This can shut out persistent bullies and stop them viewing a private account.

The basic method:

!''''''Hb 'V'cW_gca YcbY. :g'YWhi fYdcfh#V'cW_hjgdYfgc bI 'Zca 'hY'XfcdXck b'a Ybi 'cb'hYj]f dfcUY"



6mW]W_b['cb'hY'6'cW_ZYUhi fYžU'k]bXck 'k]'UddYUfUg_b['mci 'hc'Wc bUfa 'mci fXYW]gc b'UbX' XYUb_b['k \UhYZZYWhhUhUWh]cb'k]'\Uj Y"



- 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.

GYhb['U'gfcbl 'dUgg cfx'cb'mci f: UWVcc_dfcUY 'jghY'j YfmUfgh]b['mci 'g\ci 'X'Xc"Mc i 'UFY hY 'Ufgh]bY 'cZXYZYbW' k \Yb 'jWc a Yghc 'gYW f]b['mci f'cb]bY 'ZY 'UbX 'gfcbl 'dUgg cfxgUFY 'mci f best friend.

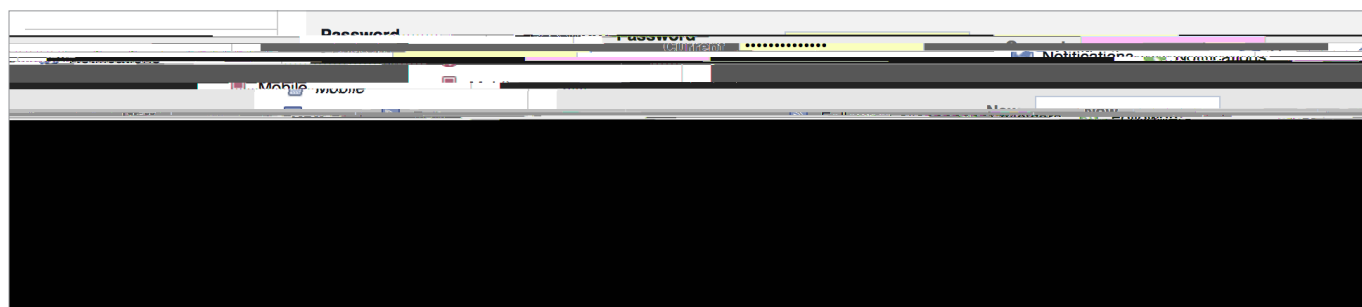
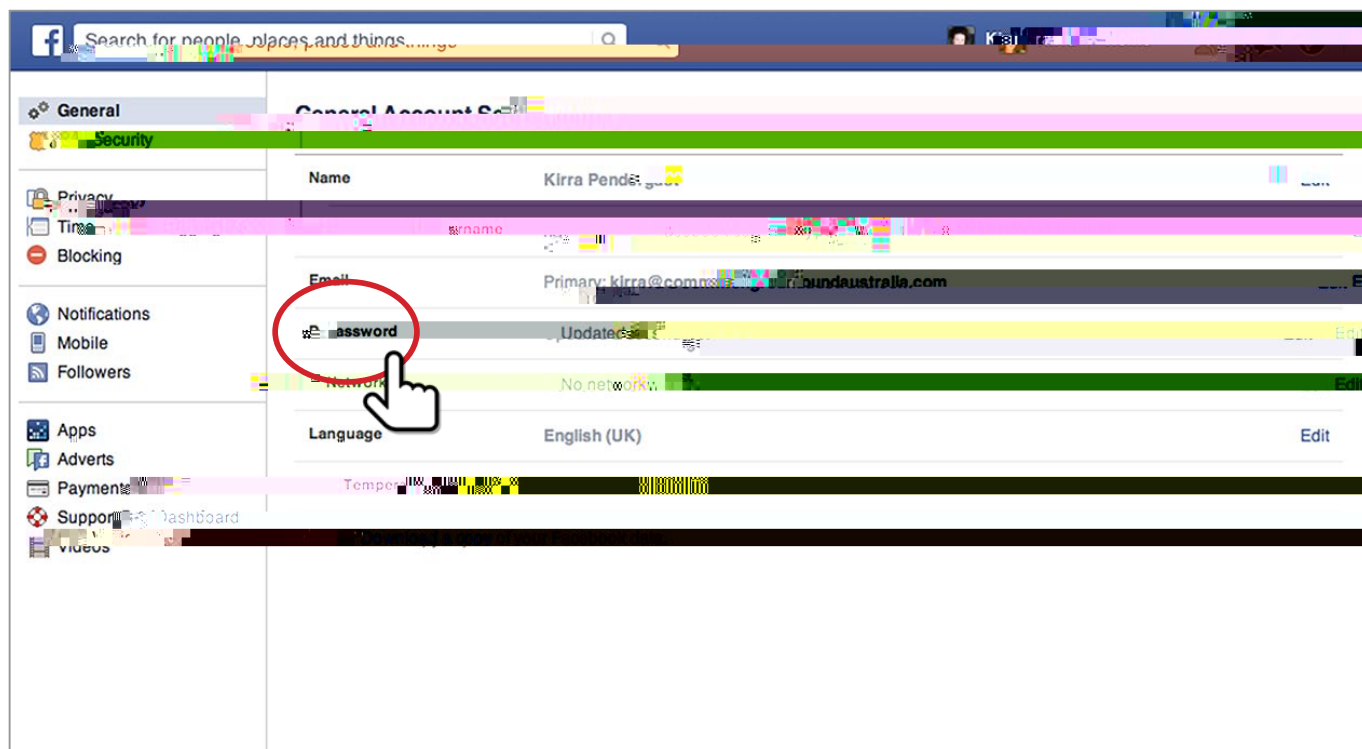
Here are our top tips for passwords:

- Always use a strong alphanumeric password using upper and lower case letters and numbers for example: lI0v3D0g2 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 Facebook's 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.

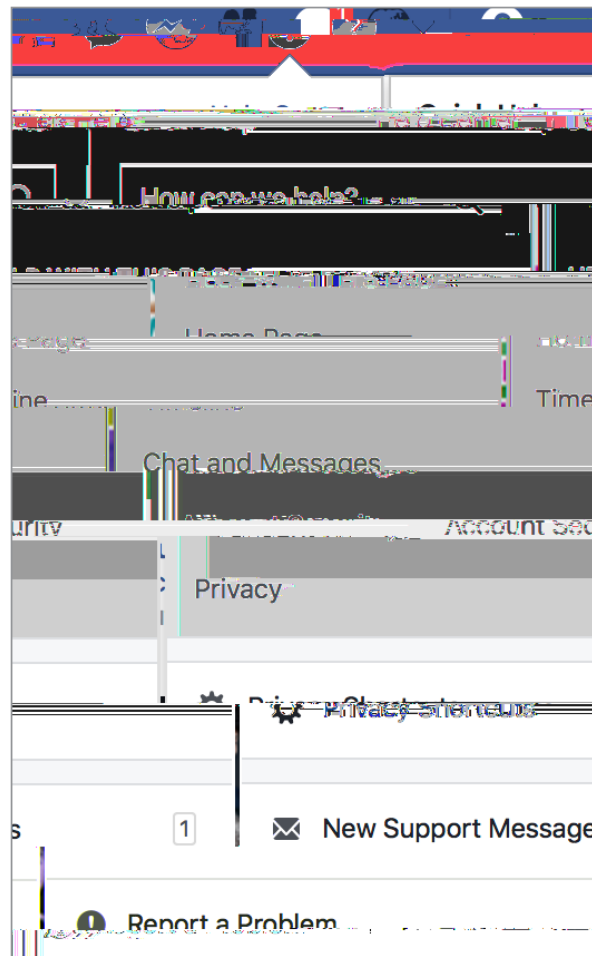
Basics

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

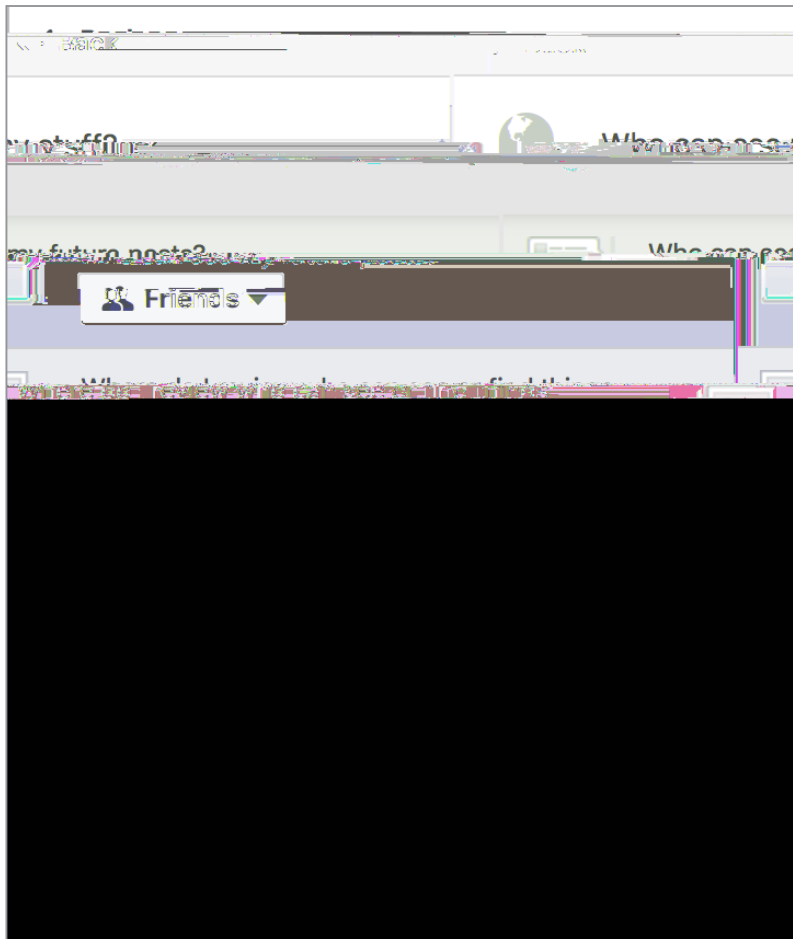


The question mark in the top right corner will bring up a drop down menu.

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.

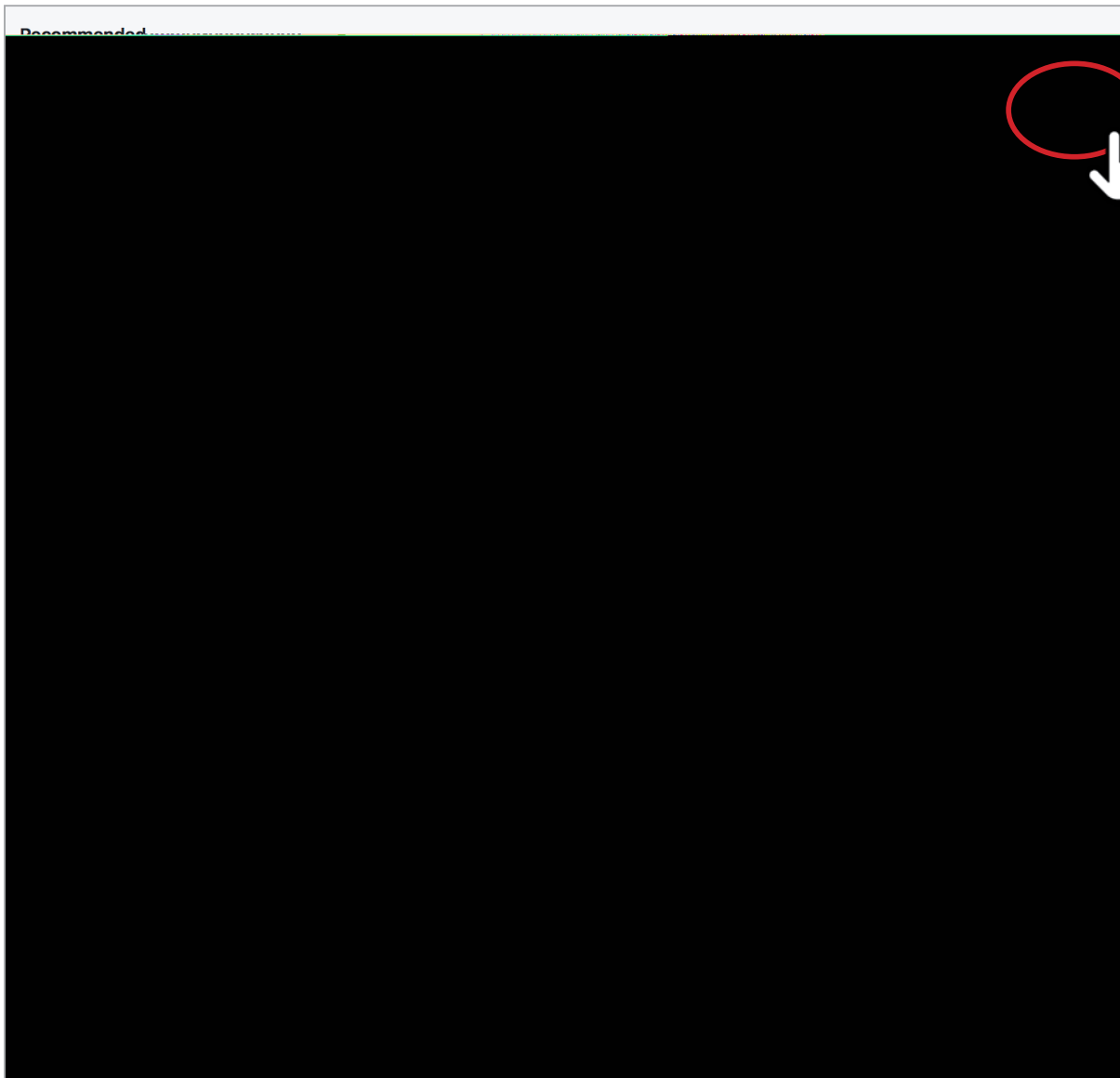


The **Activity log** option leads you to a section where all your recent comments, likes and photos - essentially all your interactions on Facebook.

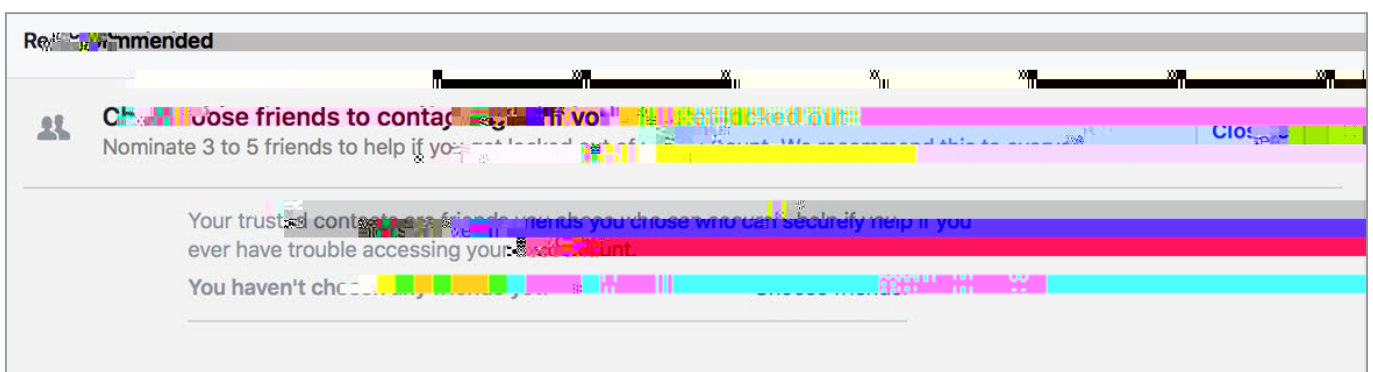
It gives you the ability to edit these in one place.

Security and Login

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

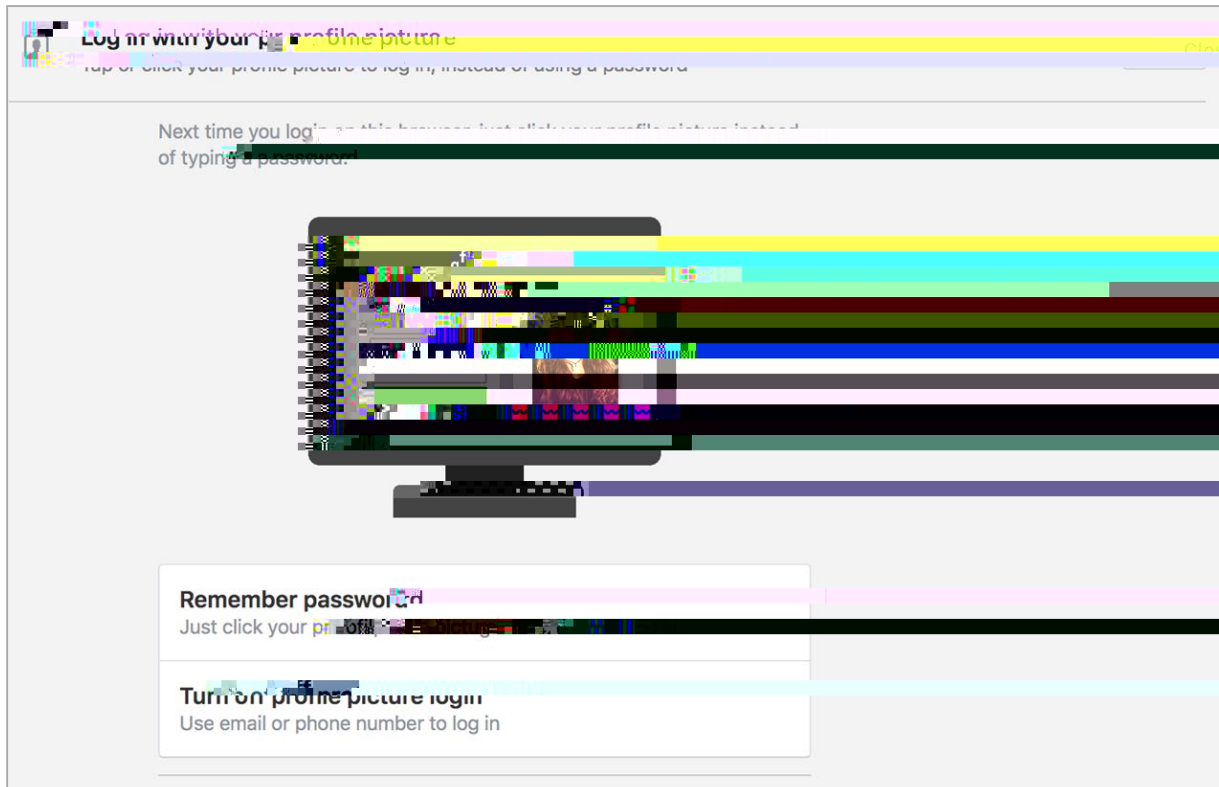


- There is a choice to select a number of trusted friends, should you become locked out of your account.



- 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.

- **L** . 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. 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.

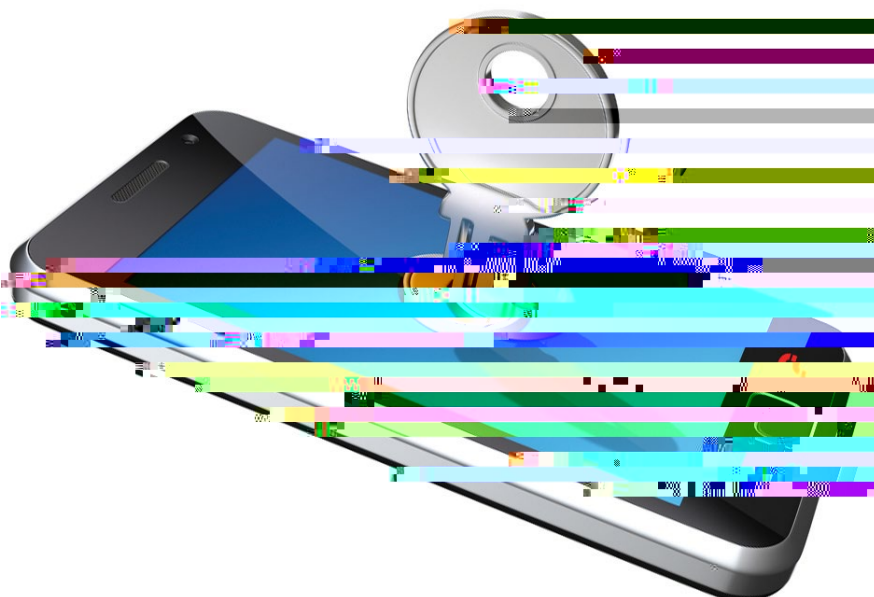
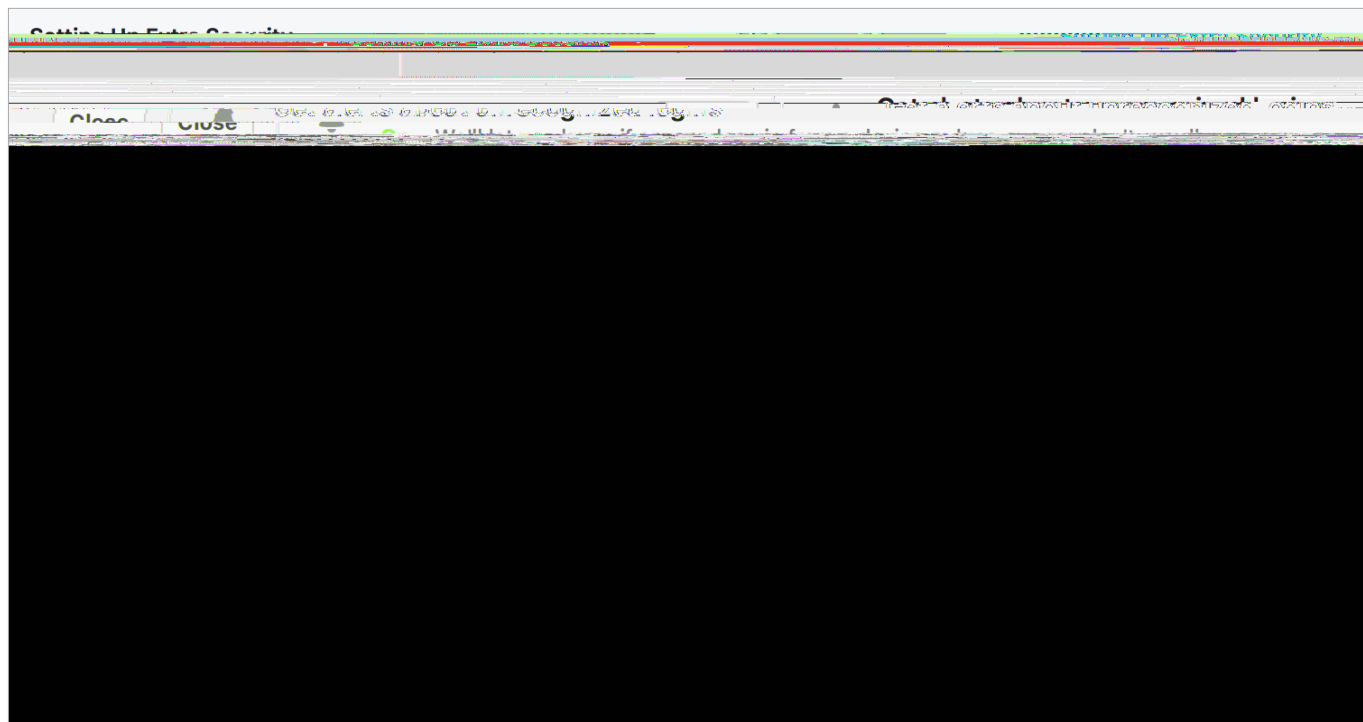


It's simple to turn off if you have enabled it; by using the lowest button in the screen shot above, and following the prompts.

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

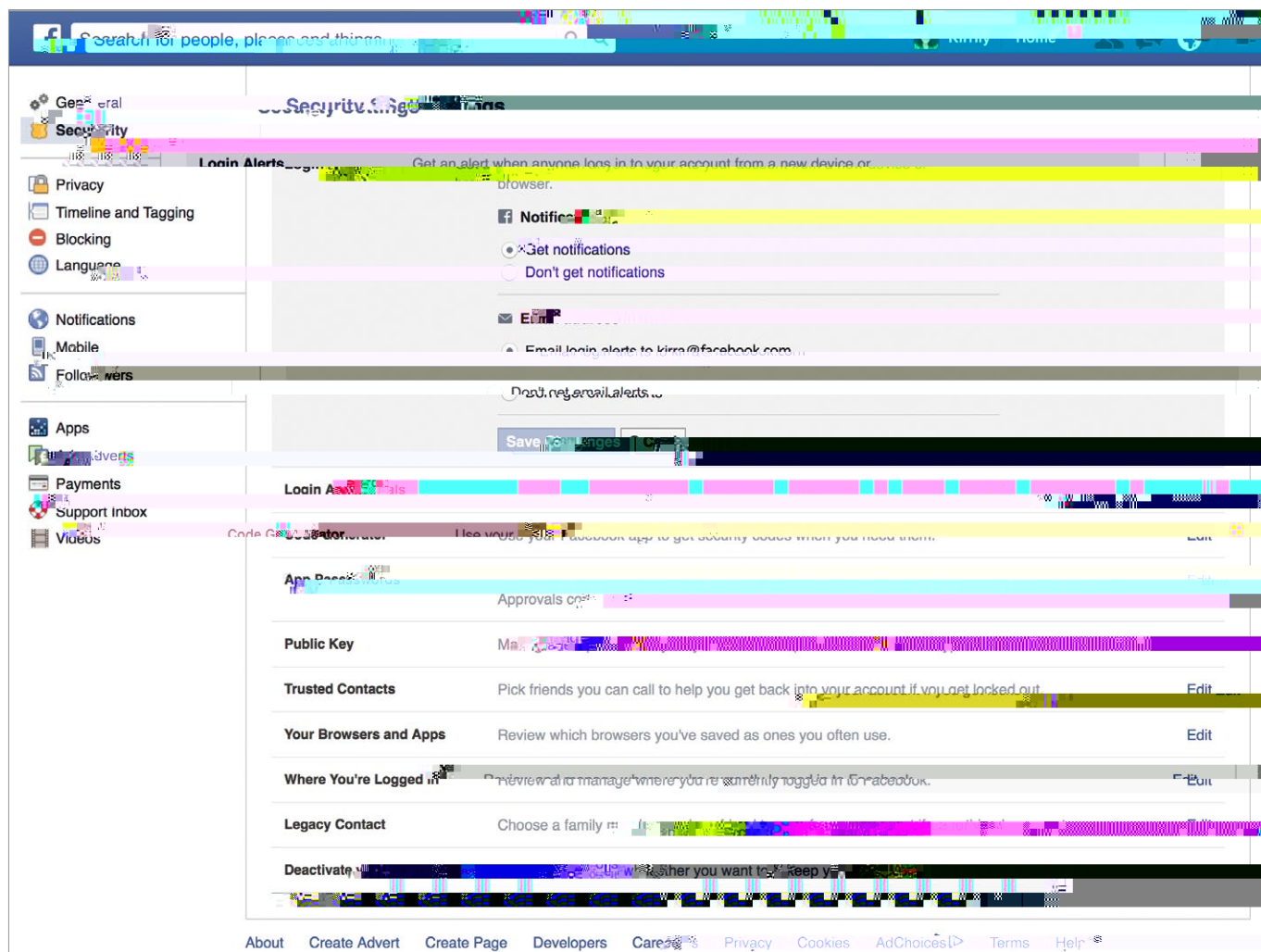
Alerts from unrecognized logins.

While this can often be the account holder logging in from a different device, this is not always the case. A notification from an unrecognized device, will warn you of activity on your account, independent of your own use. Once a new device is used to log in to your account, you will receive a notification from Facebook. This notification will inform you of the device used to log in, the location, and the time. You can then choose to log out of that device or not. This is a good security measure to have in place, as it can help you identify if someone else is using your account.



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).

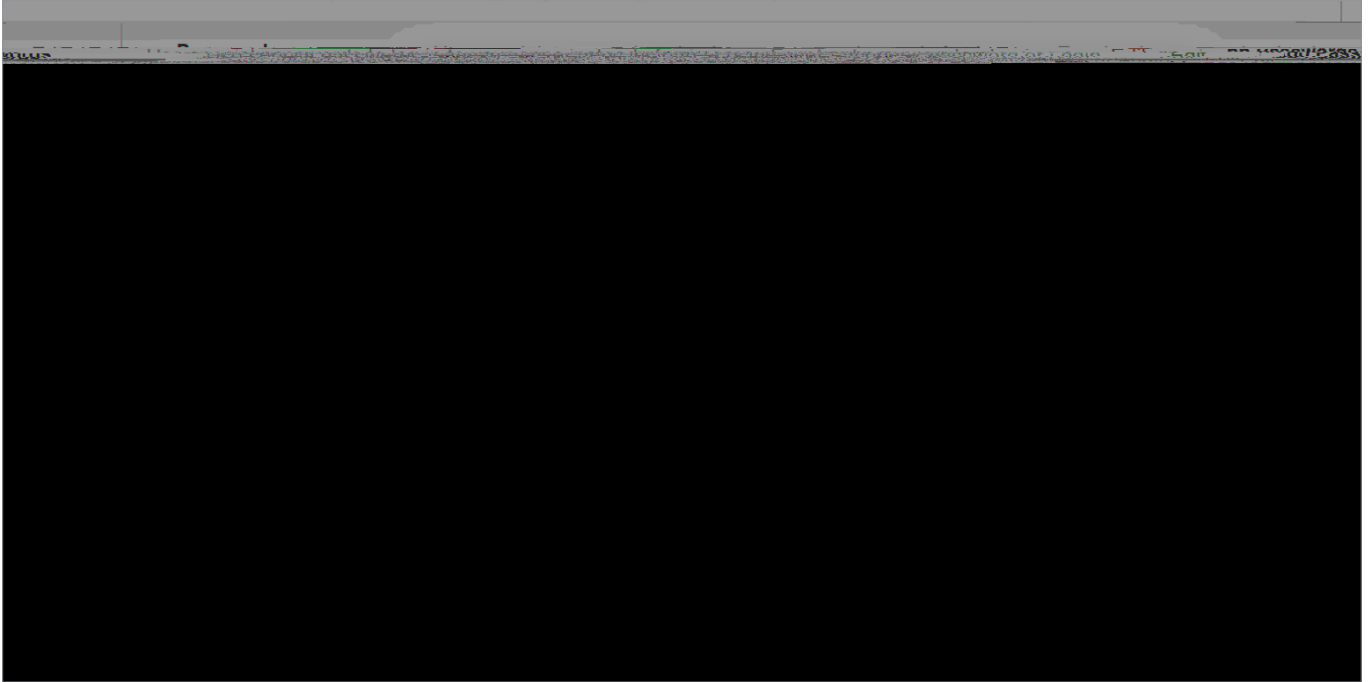
Facebook two-factor authentication or "code generator" uses your mobile device with your phone.

You can set up Android, iPhone, smart phones or any simple mobile phone to receive the that you never lose this device; or, you will be unable to use your Facebook account.

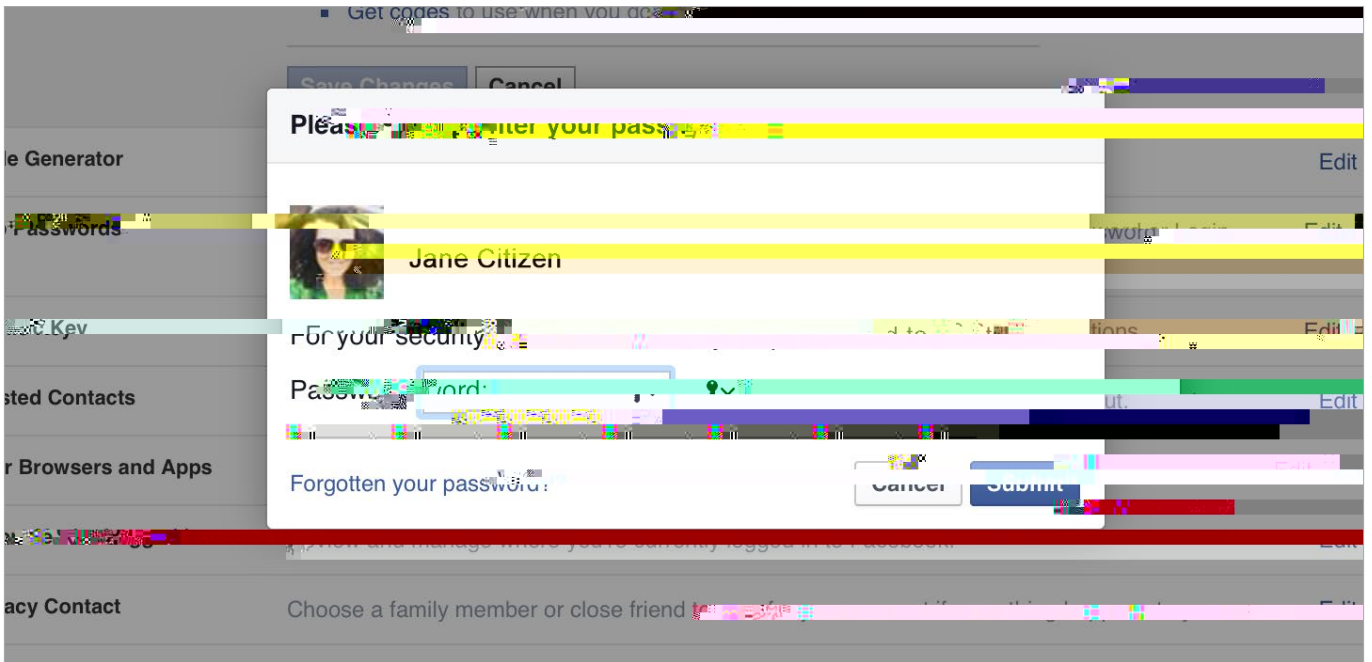
To set up login approvals without using the "code generator" option for your Facebook account simply follow these steps:

1. 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.

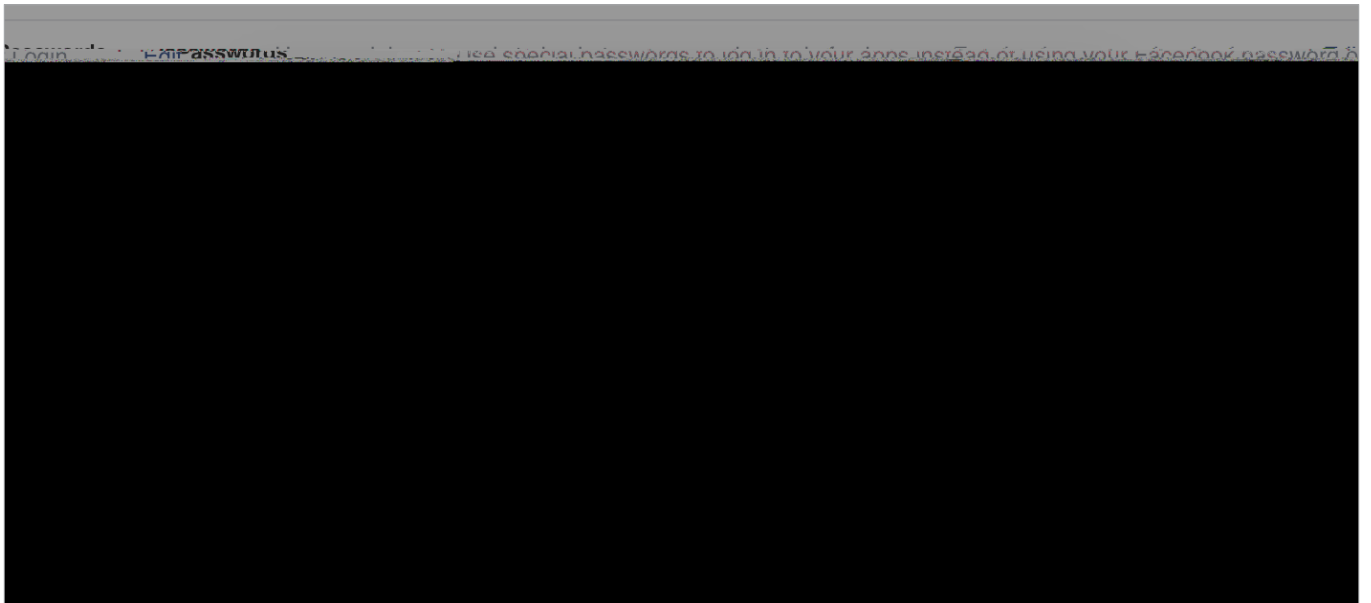
3. The second down the list is '**Login Approvals**'; click '**Edit**'.
4. Click the box that says "require a security code to access my account from unknown browsers". You will be presented with a box and an option to click "Get Started"



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"

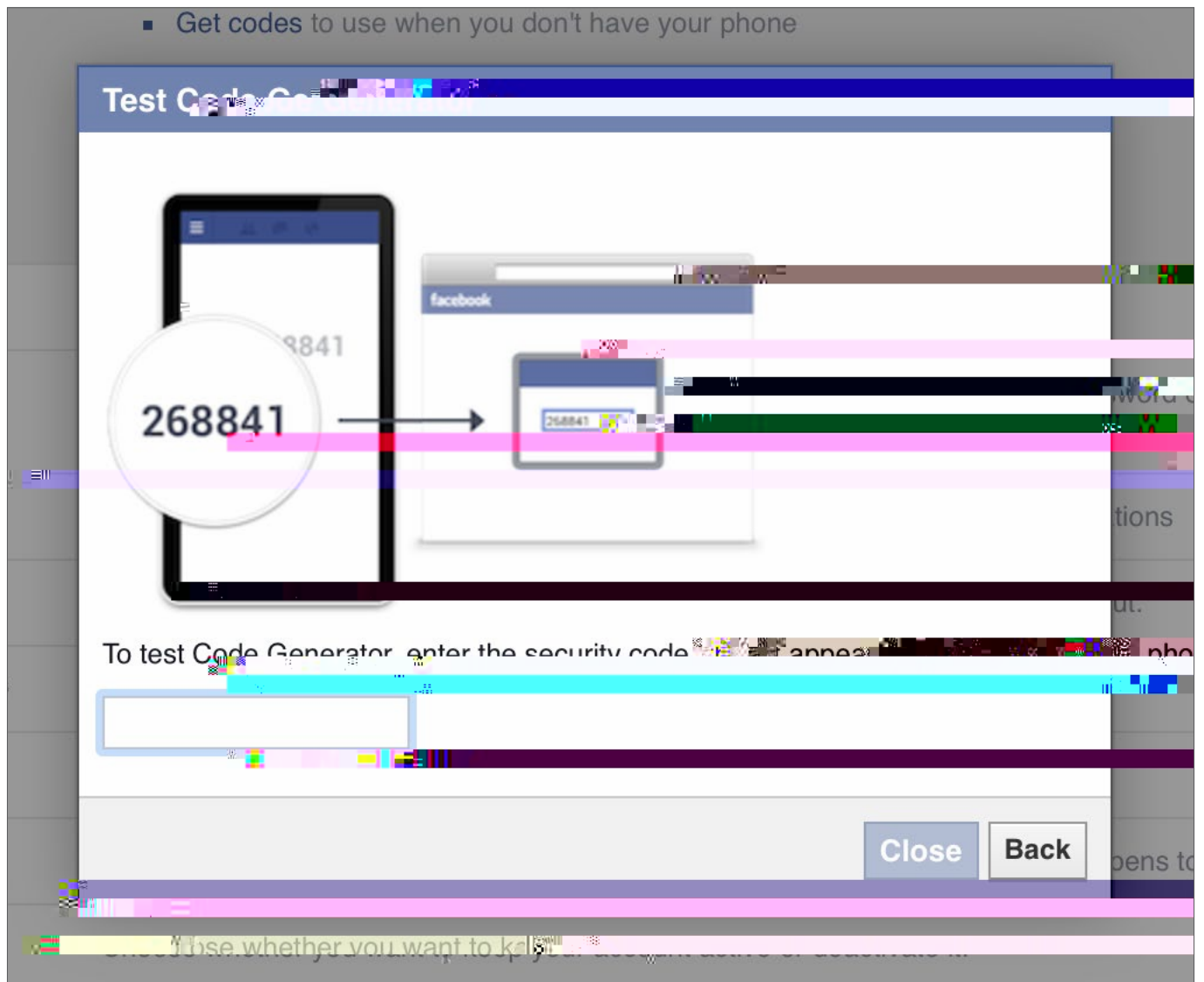
Code Generator is a part of the Facebook app and creates a security code every 30 seconds. This occurs even when you are off-line, and this feature can send necessary codes via SMS.

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,

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.



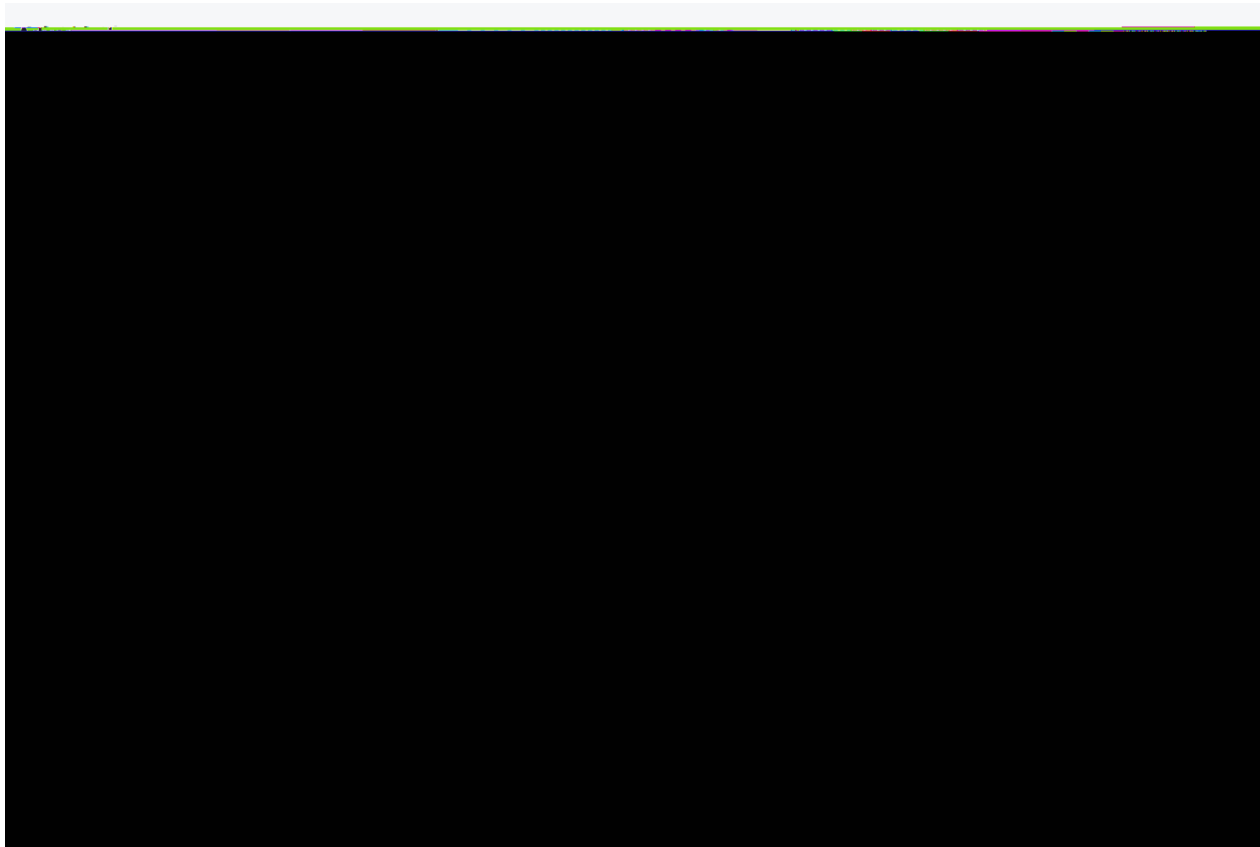
Two factor authentication system

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,

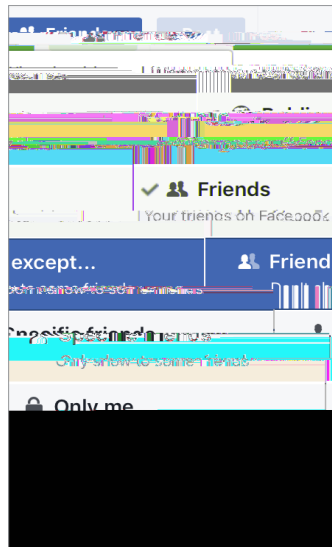
One of the more complex settings available, this has a use for sensitive accounts and content. Emails are hidden from from servers that scan users in-boxes, are fraudulent or used for marketing purposes.

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.



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



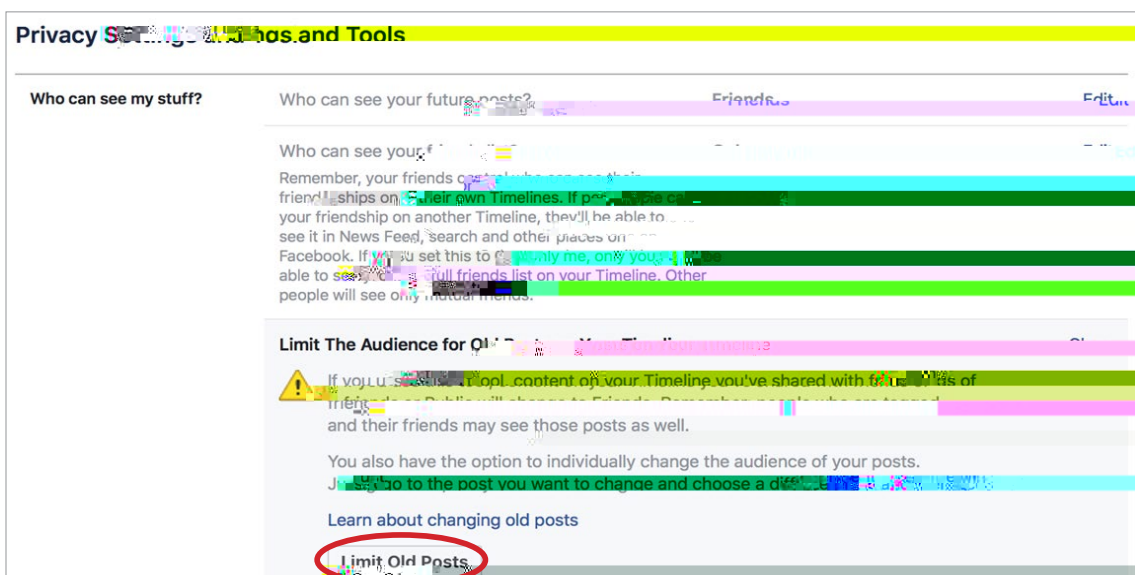
- Limit viewing of your friend list to:
 - Friends
 - Friends of Friends
 - Everyone
 - Only Me
- Limit last posts, allows to you to re-gig your privacy settings retrospectively (see below)

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 have listed. Again, the settings offer you the choice of Friends.

- Friends of Friends
- Everyone

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

- 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** essentially a spam from friends blocker. Once turned on, it will block all further invitations originating from that particular friend.
- **Block event invites**

Manage Blocking

Restricted List

When you add a friend to your Restricted List, you can still see their posts and share photos to friends. They may not see things you share publicly or on your friends' Timeline, and posts they're tagged in. Facebook doesn't notify your friends when you add you to your Restricted List. Learn more.

Block users

Once you block someone, they can no longer see things you post on your timeline, tag you in 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 participate in.

Block users

- Luke S...

Block messages

If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app. Even if they use a phone number, they may be able to post on you, you, and comment on your posts or comments. Learn more.

Block messages from

- Byron O...
- Secrets O...

Block invites

Once you block invites from someone, you'll no longer receive any requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request.

Block invites from

Block event invites

Once you block event invites from someone, you'll no longer receive any requests from that friend.

Block invites from

- Graeme Chapple Unblock
- Justin Stewart Unblock

Block apps

Facebook

Block apps

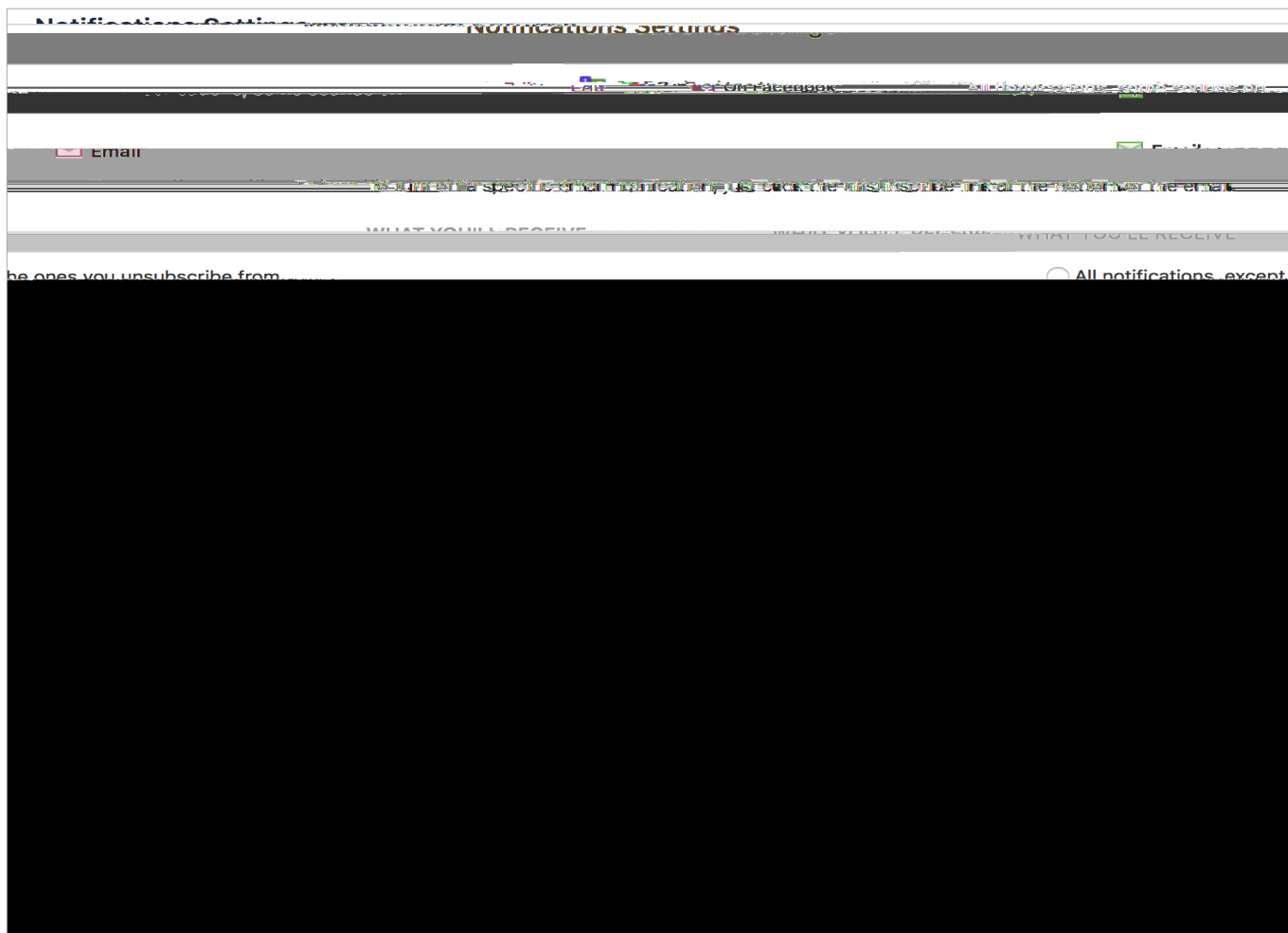
- 21 questions Unblock

Block pages

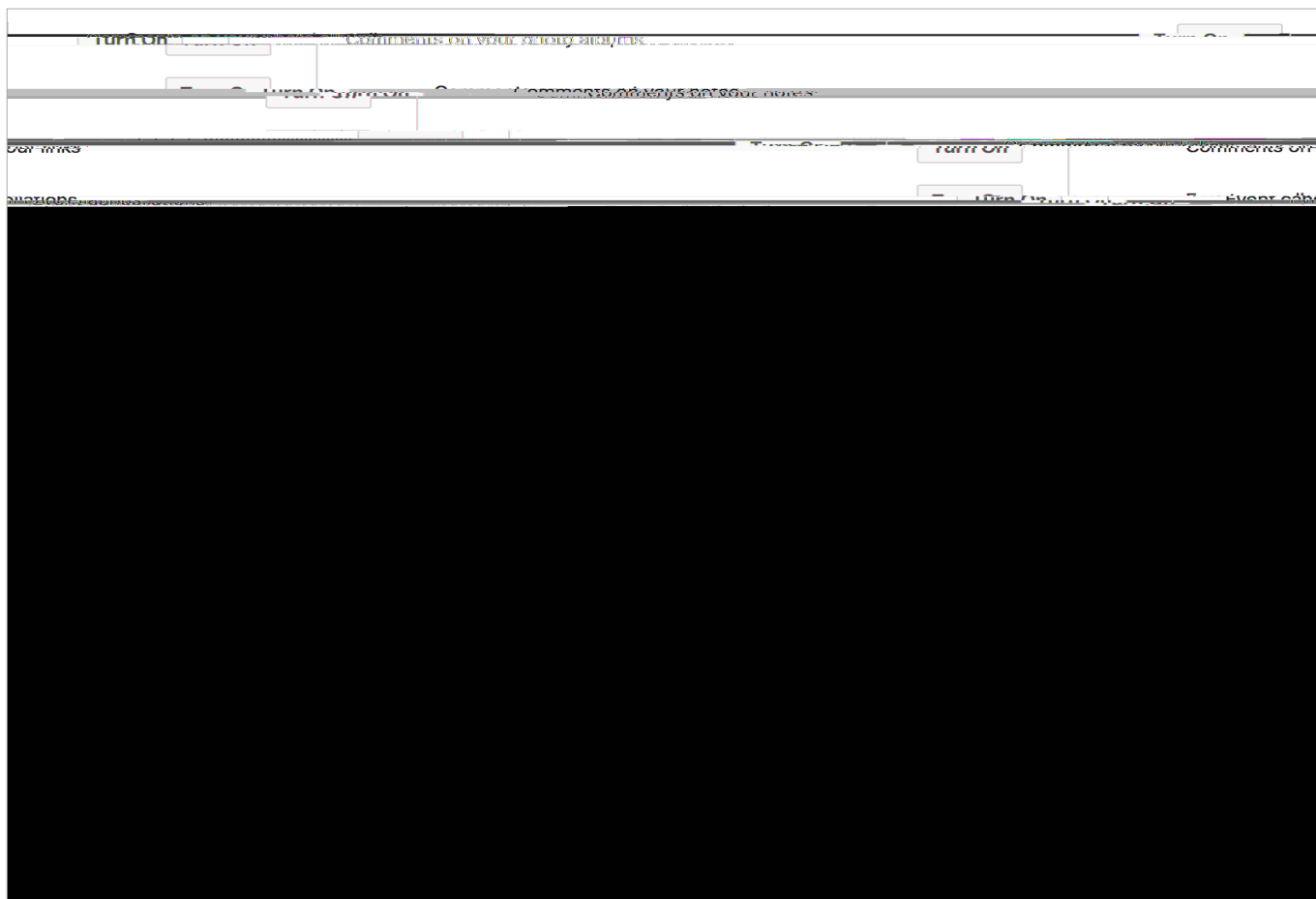
Once you block a page, that page can't see your profile or post to it. You can't see the page's Timeline, Page, and posts. You'll be unable to post to the page's Timeline, Page, and posts. If you're on the Page, blocking it will also unlike and unfollow it.

Block pages

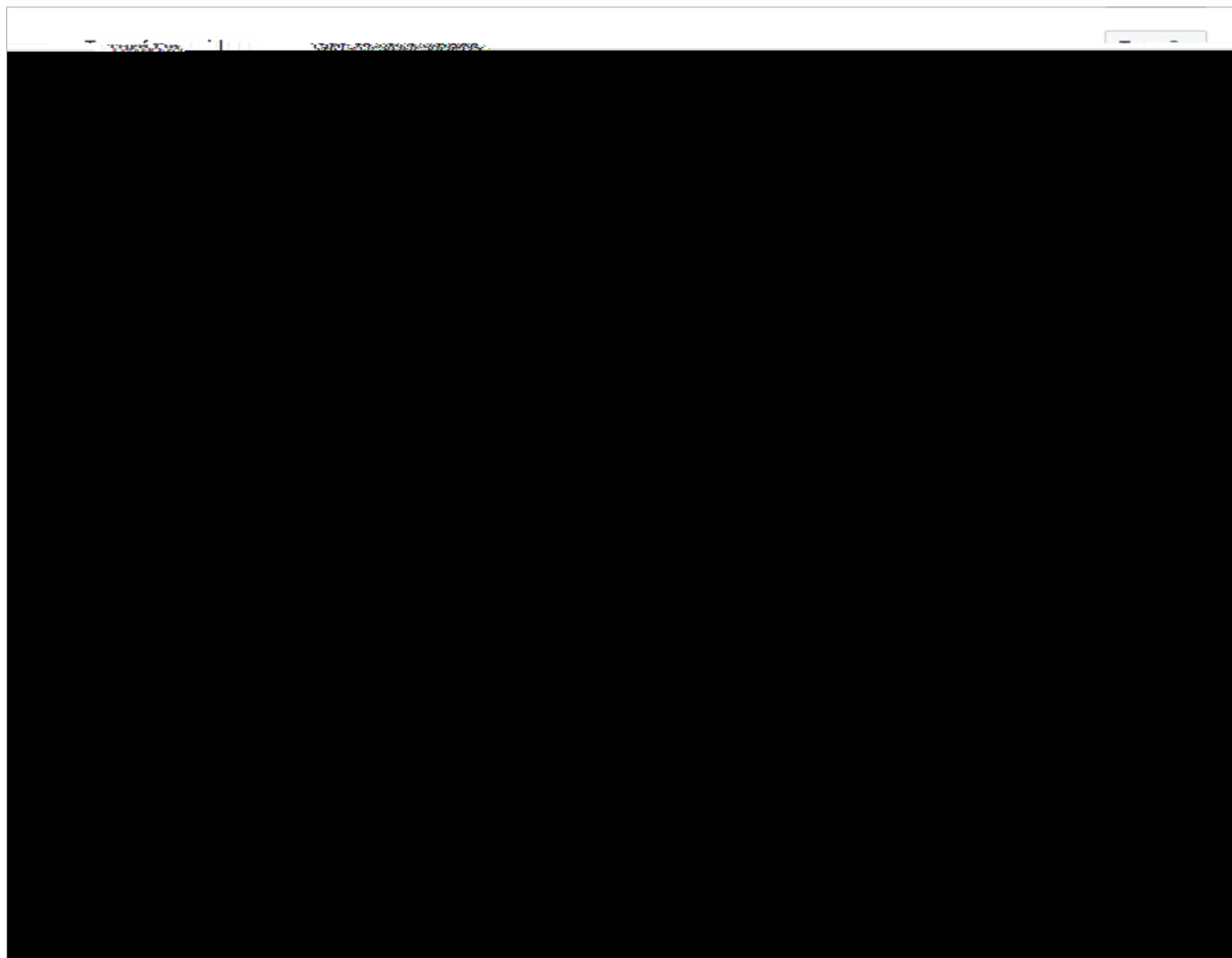
HY'g\YYf'bi a VYf'cZbch[UWU]cbgimci 'Wub'hi fb'cZZ]b'kY'Ya U]'gYWh'cb'lgXUi bh'b["



But there are more...

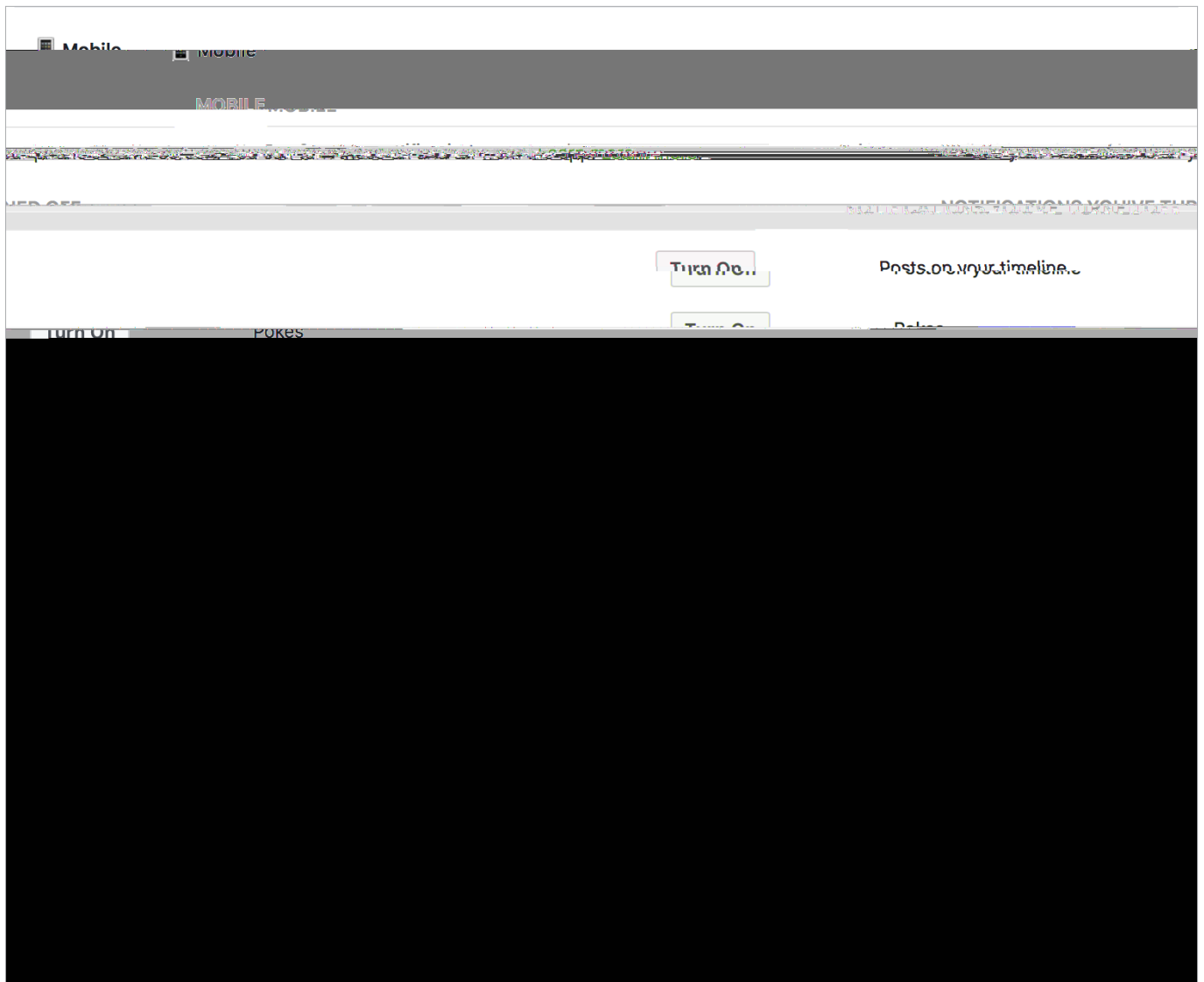


and still more...



7 \ccg' 'lc' fYa cj Y' hY' bc hUW hcbg' hUh \Uj Y' bc' i gY' 'lc' 'mc i ž U

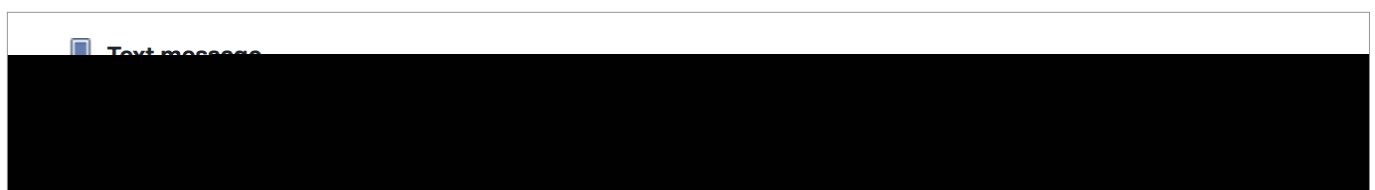
GY'YWhhY'bc hUW hcbg'mci 'k]g\ 'hc 'Wca Y'h'fci [\ 'hc 'mci fa cV]Y'XYj]W'g



A U_Y'h\Y'gJa Y'Wc bg]XYfU hcbg'Ug'mci 'k ci 'X'Zc'f'mci f'Ya U]'bc hUW hcbg'

Text message

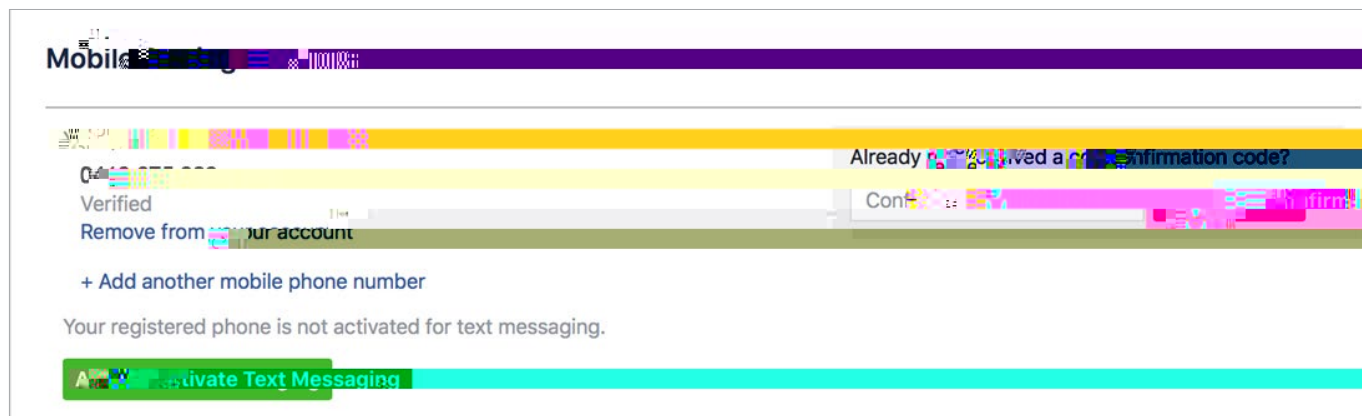
- Make a choice whether you want to receive text messages to your phone, when there are responses to your Facebook activity.



BchUW hcbg'a UmVY'hi fbYX'cb'UbX'cZZj Yfm]ga d'nž g\ci 'X'mci 'k]g\ 'hc 'Zc'ck' fYgdcbg'g'hc'U' particular thread you are commenting on etc.

Mobile Settings

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

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.

On 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.

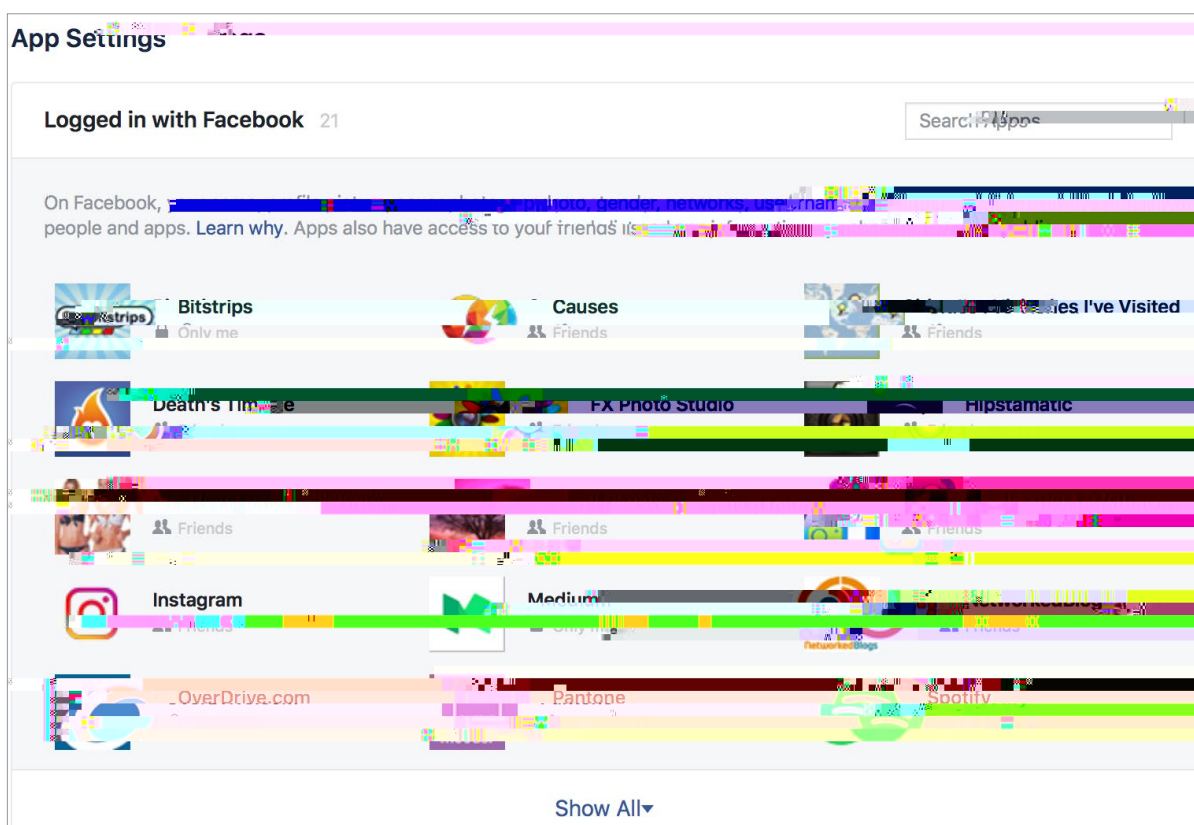
Keep an anti-virus system on your phone or device that runs apps updated and runs scheduled checks.

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

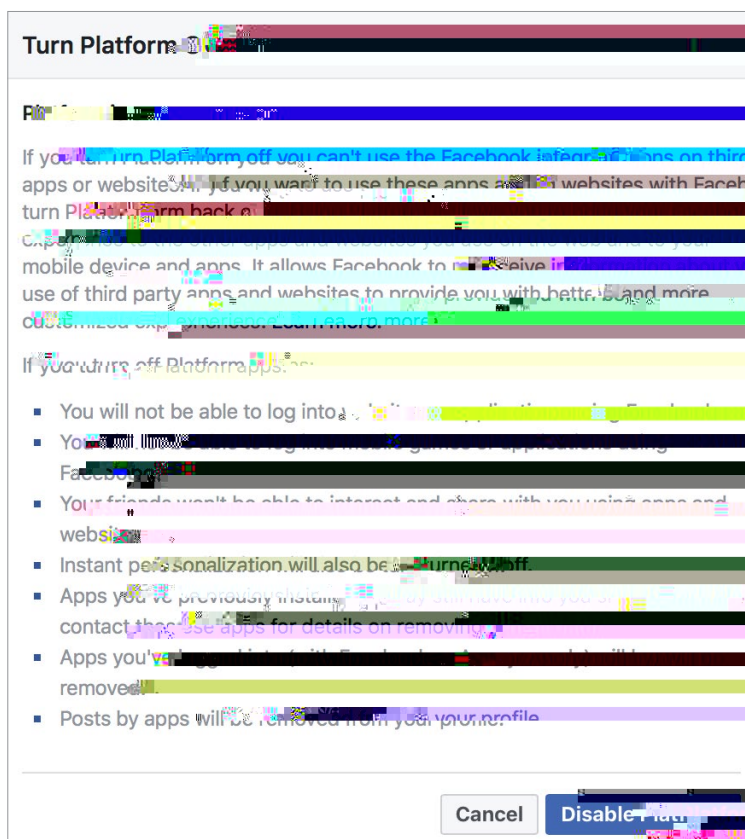
Review what apps you have allowed to access your personal information.



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.



k]` \XY`bchUWhcbgZca`hYgY`Uddg'

Disabling the apps

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

Support Inbox

Here you can see all the reports you've made about accounts, images and comments you have reported. And the moderations decisions, and

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?

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 was taken. 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
- Use 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.

Many 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.

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 their services to you are holding swaths of information about a variety of individuals.

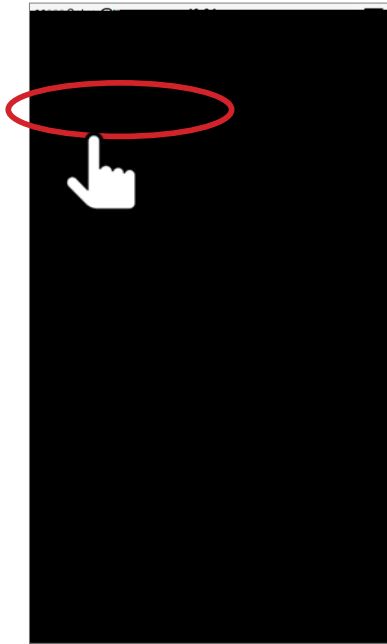
Apple devices

Disabling services for your iPhone and iPad in iOS

Step one

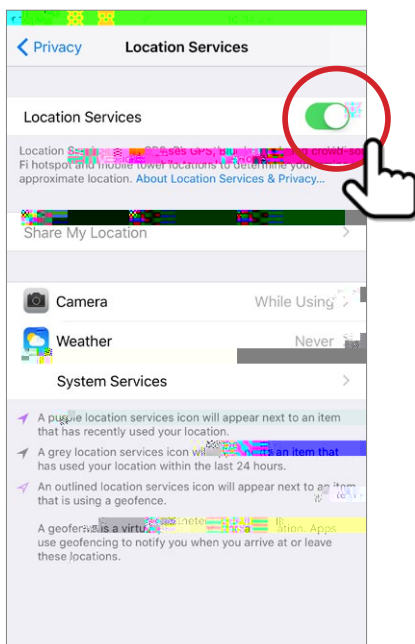
Step 3

From this menu, chose Location services



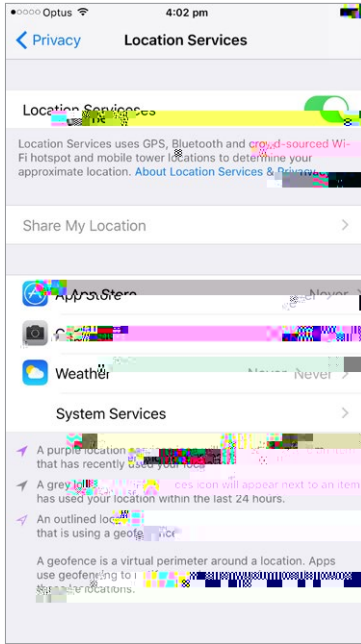
Step 4

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

Note

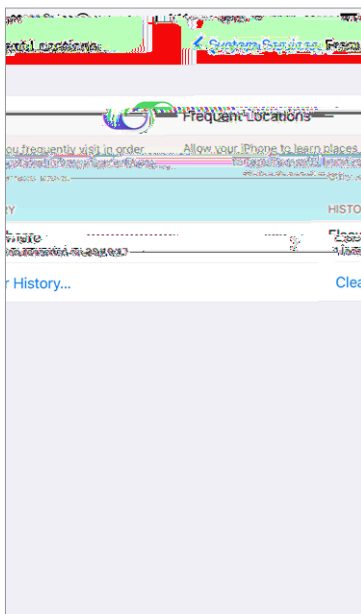
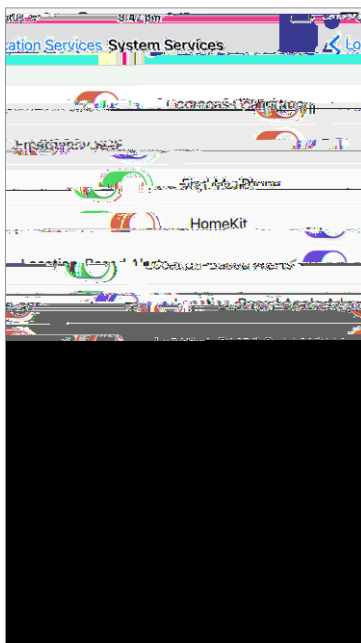


In this image there are several other options.

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

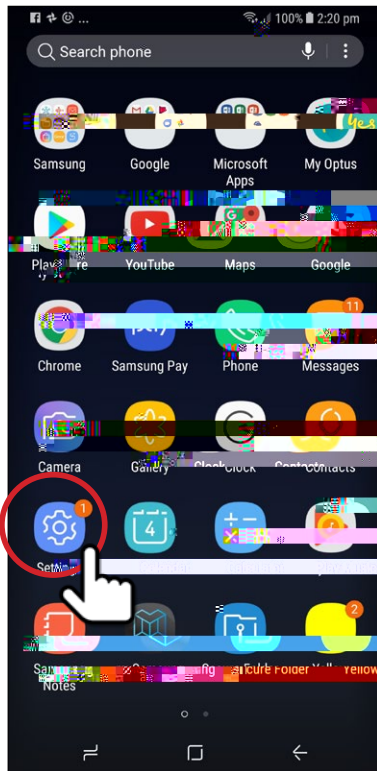
Weather - optional, depending on your usage



On an android device

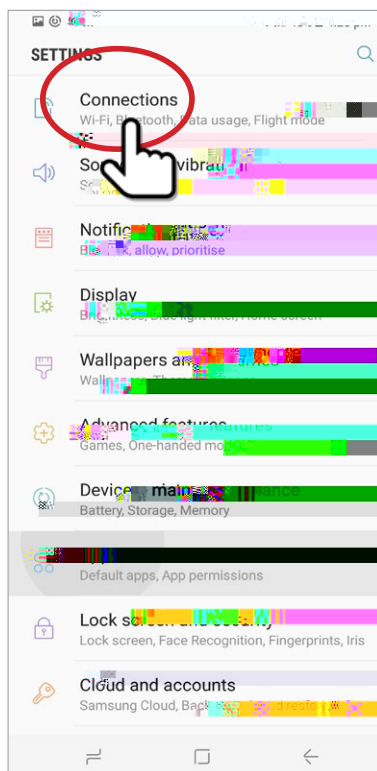
Step 1

Select the purple setting button on your home screen.



Step 2

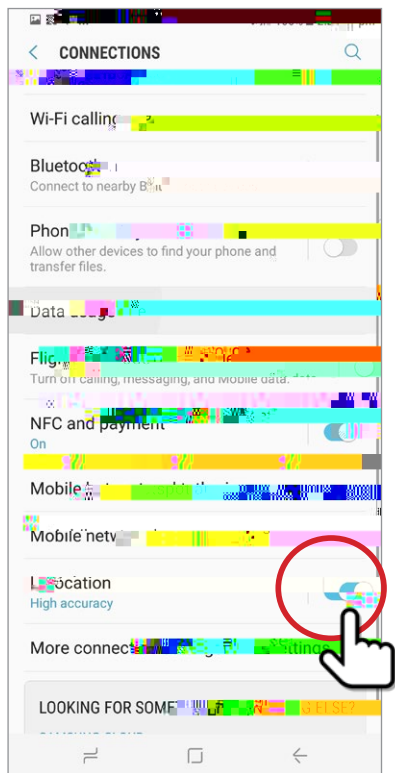
The following menu will appear:
(insert step 1.5 android and circle connections)



Choose the connections option

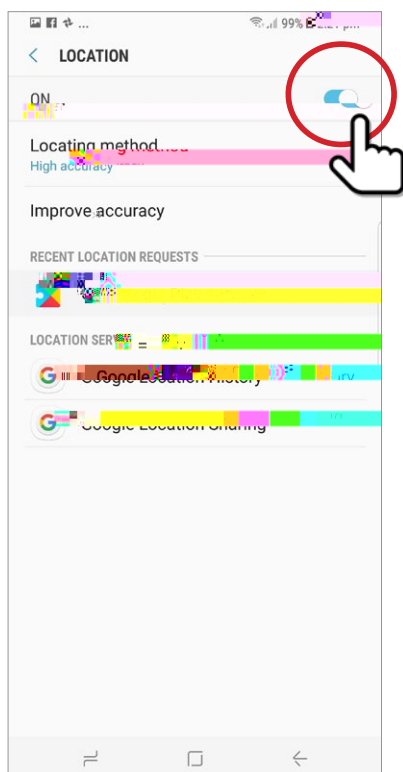
Step 3

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



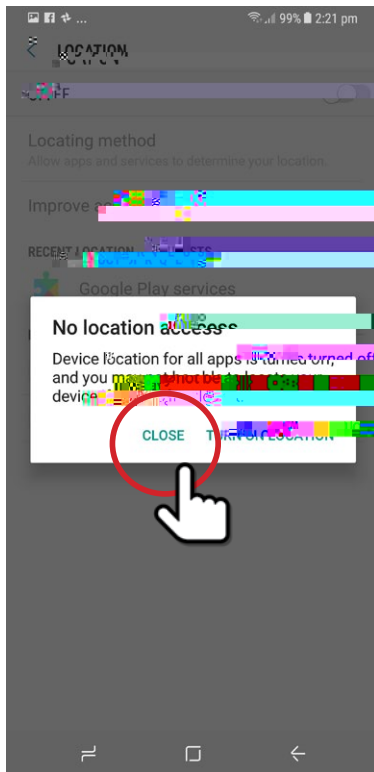
Step 4

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.



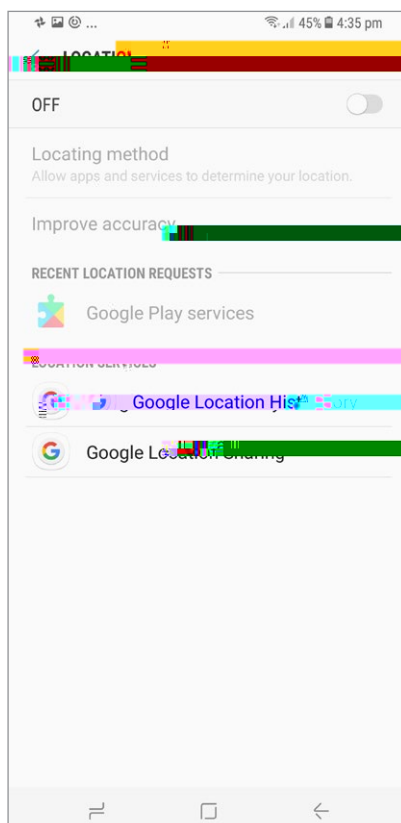
Step 5

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.



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.

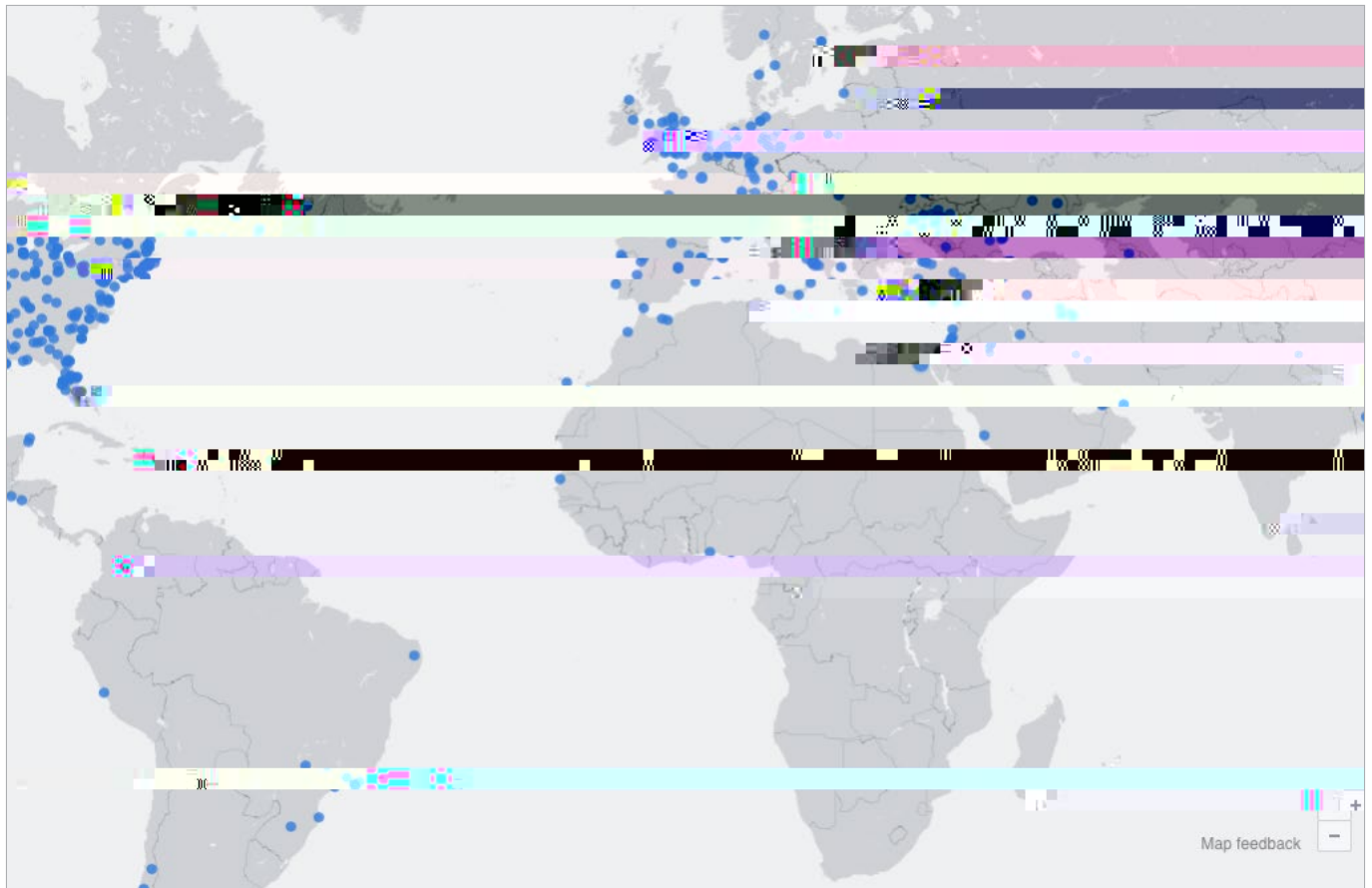
Issues

Violent content

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

and then streaming them on Facebook. Rapes, murders, violent confrontations, suicides, torture

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

Logging Into other sites using Facebook or Google

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.

- Link your other social media apps, and logging into these accounts using Facebook and you offer up further information, that is funneled to what Facebook's 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 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 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 your star sign reveal about your love life?

The online quiz is a great temporary distraction, but when you are asked to provide more

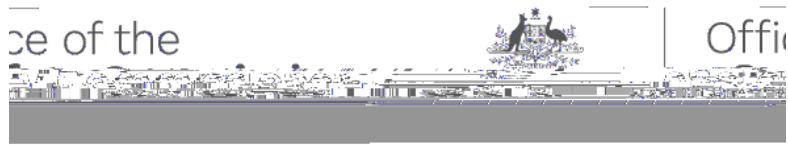
Be especially wary of any app that wants details such as full name, date of birth, postal code or email before revealing any results.

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?

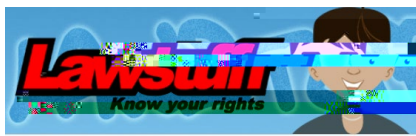
Here's a list of what you are revealing about yourself.

-

Directory



Department of the Environment and Water Resources
Office of the Environment Minister
www.esafety.gov.au



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

www.lawstuff.org.au

Bullying. 1 N0.581 w q 1 0 0 1 42.51e2po Way!ation
www.lawstuff.org.u



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 other law enforcement agencies across Australia.

www.thinkuknow.org.au
