THE CYBER SAFETY Lady

STEP - BY - STEP SAFETY & PRIVACY
SETTINGS FOR INTERNET SAFETY

KEEPING YOU SAFE ONLINE

ONLINE SAFETY & PRIVACY FOR STUDENTS 13Yrs+

BY LEONIE SMITH

www.thecybersafetylady.com.au

Author Leonie G. Smith

This book expresses the views and opinions of the author. The author will not be held responsible or liable for any damages caused or alleged to be caused either directly or indirectly by this book. The content within the book is provided without warranties. The views and opinions expressed in this book by the author are in no way representative of the author's current or previous employers.

Contact Details

Leonie Smith

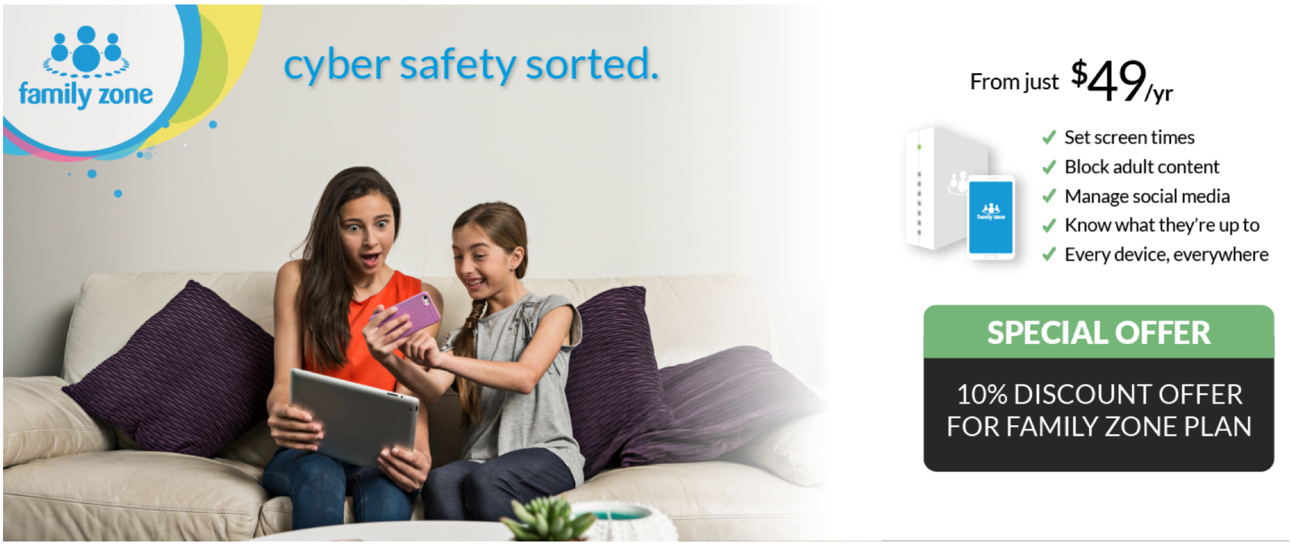
Website www.thecybersafetylady.com.au

First Edition May 2011

Latest Revision Oct 2018.

Note: If you see one of these QR codes (image left) through this manual, you can use a QR scanning app on your smart phone to go directly to the link on your phone. Some phones have a scanner built into the camera on the phone. Just open the camera and hold it up to the Code. Or go to your app store to download a QR scanning app to use this link system. The PDF version of this manual has some links included, clicking the urls, will take you directly to the link address on your PC or tablet.

Advertisement



LEONIE SMITH IS
The Cyber Safety Lady

Leonie Smith is one of Australia's leading Cyber Safety educators based in Sydney's Northern Beaches in Australia.

She has presented on cyber safety to thousands nation wide. To parents, students, teachers, seniors, corporate groups and industry conferences.

Leonie is the Author of "Keeping Kids Safe Online" an essential cyber safety manual for parents and educators.

She is certified as a qualified online safety educator by the Australian Government Office of the eSafety Commissioner www.esafety.gov.au

Leonie focuses on practical and technical solutions to help every day users of the internet use the internet and social media safely and in a positive way.

As well as her extensive experience in cyber safety, Leonie was an early adopter of the internet, social media and digital technology.

She has over 20 years experience with internet marketing, online multimedia, managing online communities, and with keeping her own children safe online.

Leonie was a cyber safety ambassador for the 2013 Australian Government's "Stay Smart Online Campaign". She was a founding member and moderator for "Aussie Deaf Kids" an online support group and website for parents of hard of hearing children, started in 2000.

Leonie's message is overall a positive one about the online world. Her passion is to help all users to enjoy the digital world in a balanced and safe manner.

Leonie Smith is a sought-after media commentator on cyber safety. She has been featured on "60 Minutes", "The Project", "Studio 10", "The Morning Show" and in many other broadcasts and print media.

Leonie Smith is a Family Zone Cyber Safety Partner. www.familyzone.com

This manual is a practical step by step guide for online safety for parents and carers concerned about their children's safety and privacy online. Although re-prints are done every few months, there may be some changes to settings not yet updated.

Contents

Top Tips For students

Online Reputation

Don't:

- Don't trust others with private video or photos of yourself. Protect sensitive media.
- Upload or share pictures/videos of others online without permission.
- Take or share nude images or video. It is illegal under age 18, you could be charged.

Do:

- Be careful what you say and put on the internet. Would mum & dad approve? Can't be undone. Can be passed around, copied and downloaded.
- Respect your friend's and your family's privacy, as well as your own.
- Always ask permission before taking pictures/video, or using webcam of other people.

Privacy

Don't:

- Give out your real name or other private details on games and apps. Use a made up name.
- Post home address, phone numbers, school name, passwords, bank details, drivers licence, identity cards, real friends or families names.
- Expose another person's real identity or personal details online.
- Overshare - your privacy is important. Delete or archive old posts.

Do:

- Use a "handle" or pseudonym (made up name) for games and apps.
- Set good, secure, passwords & privacy settings on every app/platform/account.
- Log out of accounts and computer when leaving your device or computer.

Behaviour

Don't:

- Participate in "online drama" or bad behaviour. Mute or block.
- "Flag" or report a user to an online moderator out of spite. Get help if frustrated.
- Be a "Troll" (to type something annoying just to get a reaction).
- Be a "Spammer" (send constant messages over and over).
- Be a hacker or an extortionist. Hacking & blackmail is against the law.

Bullying

Don't:

- BE a bully, you may be reported and lose your account. You can be arrested and charged with harassment or cyber bullying if you join in or abuse others on the internet.
- Stand by if you see or hear bullying. Report to a responsible adult. You can help.
- Respond to bullies or "Trolls" by arguing or defending. Block, Report, Support.
- "Re-friend" a bully unless you are sure you are safe. Ask parent if not sure.

Do:

- Support the victim and tell a responsible adult.
- Save copies - Screenshot. Mac-Cmd/Shift/4, Win-Print Screen or snipping tool.
- Block the bully & tell your parents or a responsible adult straight away. Do the same if you feel uncomfortable about a message.
- Be a good friend online. You can make a big difference by being an upstander to bullying.

Safety

Don't:

- "Friend/follow" random strangers. They might be an adult NOT a child. Not all children are safe to "friend" either. This includes online games like Minecraft, Roblox, Fortnite.
- Agree to meet an "online friend" in real life, unless accompanied by a trusted adult.

Do:

- Alert parents or teacher if an adult stranger starts chatting to you online. Block the stranger.
- Tell your parents if you are sent something upsetting or rude online. They need to know.
- Do play safe, age appropriate games, and use age appropriate apps. Check age ratings.

Viruses And Malware

Don't:

- Click pop-ups on browsers, it might be spam or a virus. Click X or escape.
- Open attachments or click links in emails if you are not expecting them.
- Click links on social media if you don't know where they are going.
- Download things from the internet without checking with a parent. Beware of fake apps and "Find More Friends" style apps. Be careful of game mods and weird program updates.
- Leave your privacy settings set to public. Do protect your privacy.
- Download stolen games or films. It's a crime. You may be caught. Some contain viruses.
- Answer phone calls or messages from people you don't know. Block them. Don't call back.

Do:

- Only download apps/games from reputable stores like iTunes, Steam or Google Play.
- Tell parents if you see an alert about a virus. Be careful though, it might also be a scam.
- Set strong passwords, 8 characters, upper & lower case letters, include numerals.

Online Security

- Set different passwords for every account. Use eight digits or more, mix upper and lower case, numerals and symbols. For example - Fine*9SillyPaper - Don’t use any related words.
- Set a screen/login password on all computer/mobile devices to prevent unauthorised use.
- Password manager software is a good option for users with a lot of passwords.
- Make sure all antivirus software is up to date and still valid. Set to update automatically.
- Software updates often help to block new viruses and malware, update regularly.
- Check firewalls are switched to “On” on routers and computers through security settings.
- Set unique passwords on all internet connected devices, including baby monitors and internet connected speaker assistants like Apple Pod, Amazon Alexa & Google Home.
- Some free public Wi Fi access is insecure. Use only reputable Wi Fi sources.
- Use Paypal, pre-paid credit cards or software gift cards (available from gaming/electronic stores and supermarkets) rather than credit cards when paying online.
- Set up two-factor verification apps & secret pins or passwords on your accounts to prevent your accounts being hacked. When logging in from a different browser or devices you will then receive an SMS or app notification on your mobile device to verify your account.

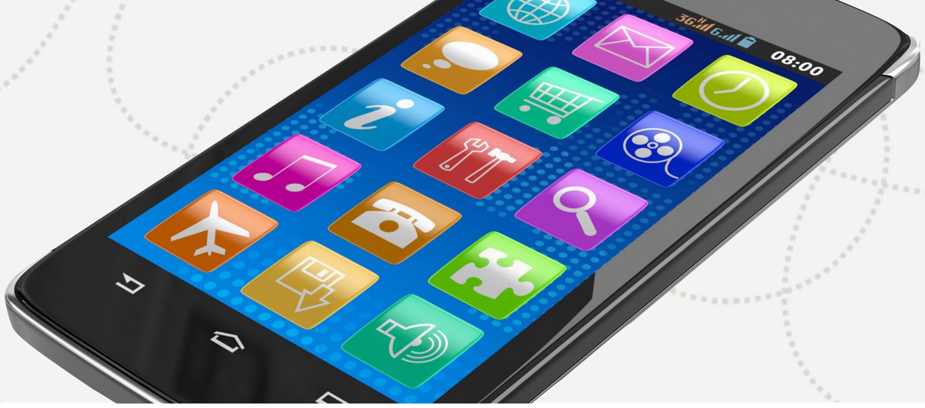
  Facebook - Go to - Account - Settings - Security & Login - 2 Factor Authentication

  Apple - https://appleid.apple.com - Manage ID

  Google - www.google.com.au/landing/2step

  Twitter - https://twitter.com/settings/security security and privacy

  Microsoft/Skype - https://account.live.com/proofs/Manage
- Set security and privacy for Google accounts here: https://myaccount.google.com
- Don’t open email attachments or click links in emails unless expecting them. Don’t click links in emails where you are asked to “Update your account details” Always go to your account via the official website address, or ring your provider using usual phone number .
- Watch out for Fake emails, and SMS & phone calls from claiming to come from reputable institutions. Go to the website via search or the web address rather than click a link from an email, SMS or Message to update account details. Don’t ring number back on messages.
- Report Cybercrime ie scams, identity theft, hacking to acorn.gov.au & scamwatch.gov.au. Cyber Bullying, stalking & Image based abuse eSafety.gov.au and your local police.



Phone Privacy & Safety

Do:

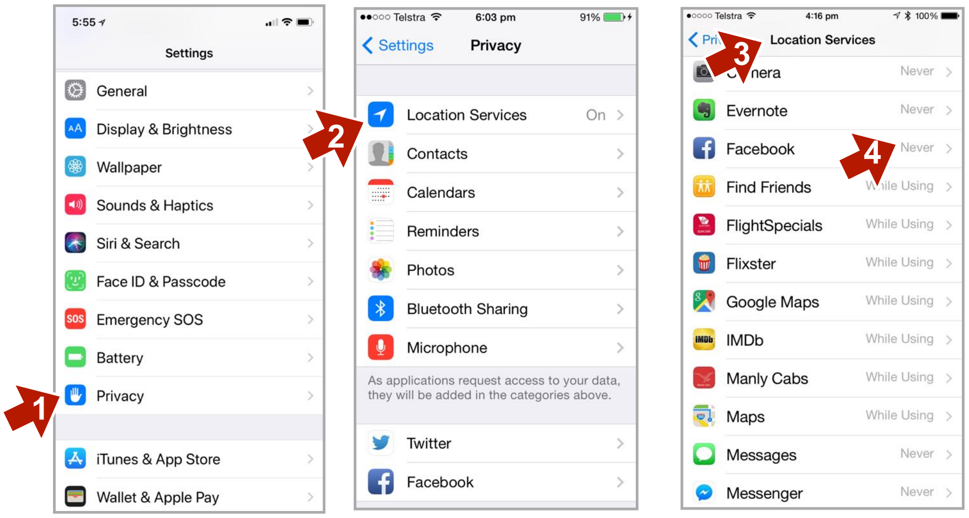
- Set screen passcode, fingerprint or face I.D to prevent unauthorised use.
- Set up “Find My Phone” on iPhone settings. Android also now has Find My Phone & there are several “Find My Phone” apps on Google Play, or use Android Device Manager App.
- For Android security settings navigate to “Settings” - “More” - “Security” and enable “Verify Apps” Un-tick “Unknown sources” Or “Settings” “Personal” “Security” “Device Admin” Tap “Unknown Sources”
- Use message/call blocking for scams or bullies. (Instructions in this manual)
- Share your mobile number only with close friends or family. Avoid putting online.
- Protect your location. Turn off location services on apps that don’t require it (see below).
- Report anything upsetting you are sent on your phone. Students should tell a trusted adult.

Don’t:

- Give your phone to another person to use, unless very trustworthy.
- Download dodgy apps from obscure app stores or websites. Check ratings first.
- Use your phone for spammy texting or bullying.
- Take photos/video/recordings without permission, or of embarrassing or bad behaviour.
- Share photos/videos without permission of all the people in the photo/video.
- Take a nude selfie or you might regret being posted around. Phones can get hacked.

Note: Taking or sharing nude photos of people under 18 years of age is illegal.

To Disable Location Services On Apple Mobile



Location Services On
Contacts

As applications request access to your data, they will be added in the categories above.

Location Services

nera	Never
Evernote	Never
Facebook	Never
Find Friends	While Using
FlightSpecials	While Using
Flixster	While Using
Google Maps	While Using
IMDb	While Using
Manly Cabs	While Using
Maps	While Using
Messages	Never
Messenger	Never

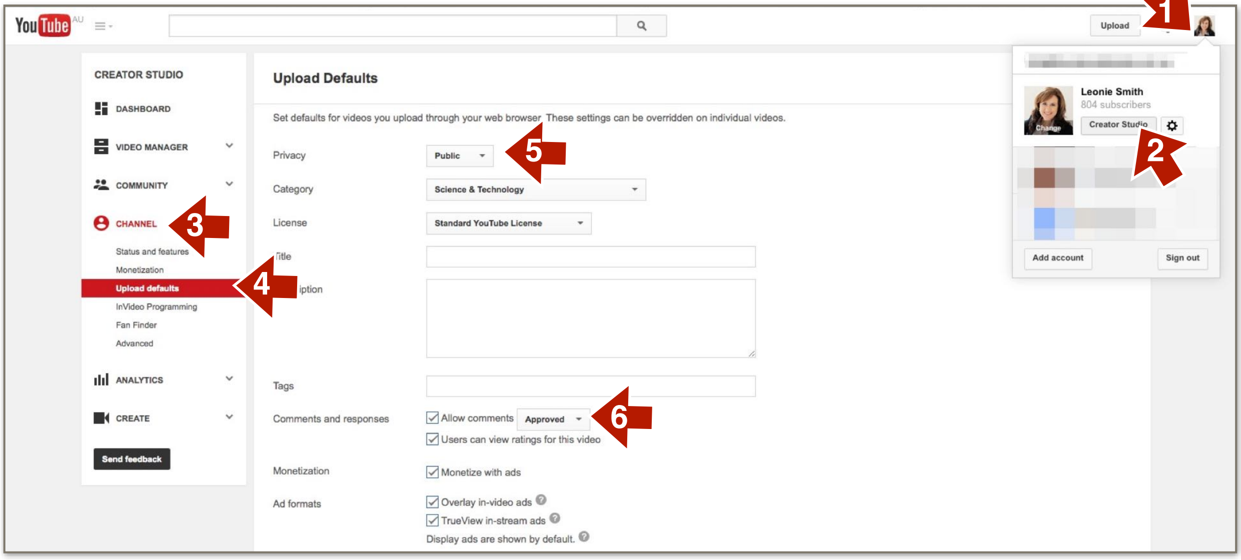
On **Android** devices, tap the “Location” option from the “Settings” menu.

YouTube Channel Privacy Settings - PC - Laptop

Creator Classic view - switch between YouTube Studio Beta in settings

Private Channel. Log into the channel you wish to make private.

1.Go to channel profile. 2.“Creator Studio”. 3.“Channel”. 4.“Upload defaults”. - 5.Change “Public” to “Private”. Un-tick “Allow Comments” if you want to block all comments. 6.Or change “All” to “Approved”, to approve comments before publishing.



Upload Defaults

Set defaults for videos you upload through your web browser. These settings can be overridden on individual videos.

Privacy: Public

Category: Science & Technology

License: Standard YouTube License

Title

Description

Tags

Comments and responses: ☑ Allow comments Approved; ☑ Users can view ratings for this video

Monetization: ☑ Monetize with ads

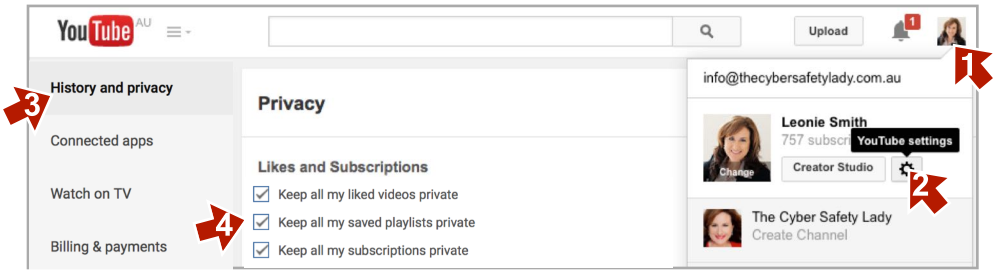
Ad formats: ☑ Overlay in-video ads; ☑ TrueView in-stream ads; Display ads are shown by default.

Hide Your Likes And Subscriptions

Log into the channel you wish to apply these settings to.

1.Click Channel “Profile pic”. 2.Click “Settings wheel” (YouTube Settings).

3.“History and Privacy”. 4.Tick the privacy options you require. Click Save



Privacy

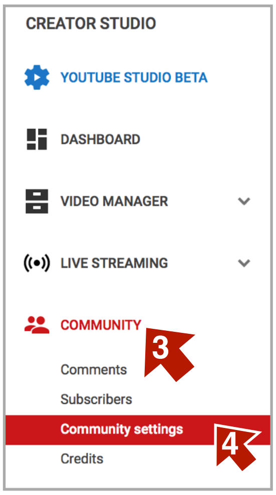
Likes and Subscriptions

☑ Keep all my liked videos private

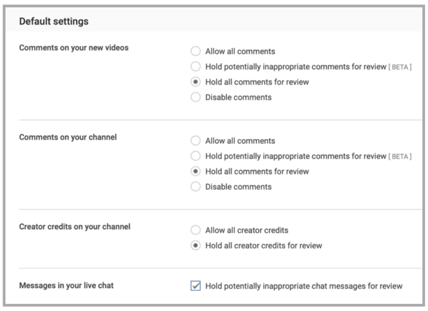
☑ Keep all my saved playlists private

☑ Keep all my subscriptions private

Control Comments And Blocked Users



Click on 1.”Profile pic”. 2.”Creator Studio”. 3.Scroll across to the left column to “Community”. 4.Scroll down to “Community Settings”. Scroll down to “Default settings” and set comment preferences as needed. You can blacklist swear words here also for extra filters.



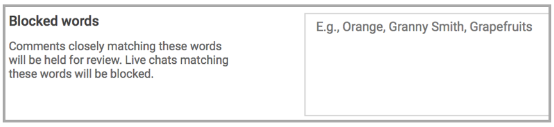
Default settings

Comments on your new videos
○ Allow all comments
○ Hold potentially inappropriate comments for review [BETA]
● Hold all comments for review
○ Disable comments

Comments on your channel
○ Allow all comments
○ Hold potentially inappropriate comments for review [BETA]
● Hold all comments for review
○ Disable comments

Creator credits on your channel
○ Allow all creator credits
● Hold all creator credits for review

Messages in your live chat
☑ Hold potentially inappropriate chat messages for review



Blocked words

Comments closely matching these words will be held for review. Live chats matching these words will be blocked.

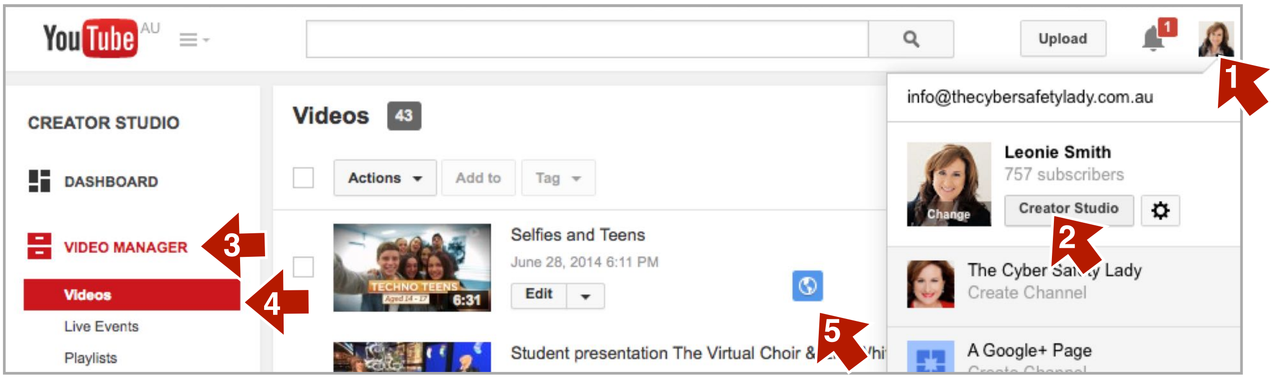
E.g., Orange, Granny Smith, Grapefruits

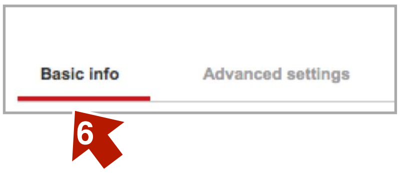
Add or remove hidden YouTube users also on this page. To hide users, use the flag menu on the Comments page.

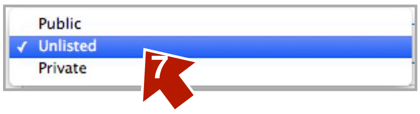
To Set A Video As Private

Log into the channel you wish to apply these settings to.

1. Click Profile pic. 2.“Creator Studio”. 3.“Video Manager”. 4.“Videos”. 5.Click the blue globe icon to the right of the video. 6 to to basic info. 7. Select “private” or “unlisted” from next window, (located lower right in “Basic Info” settings) Click “Save Changes”. **Note:** You can set the privacy options whilst uploading your video, when filling in your video’s title and other information.



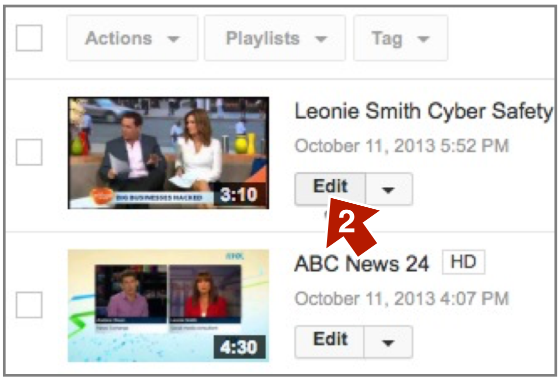


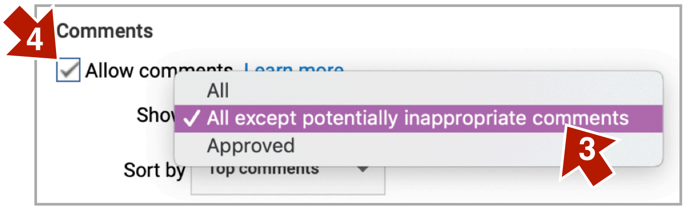


Disable Commenting On Your Video

Commenting on YouTube can be used for bullying.

1. Go to “Video Manager/Videos” as above instructions.
2. Select “Edit” on the video.
3. Under your video go to”Advanced Settings”.
4. Un-tick “Allow Comments” or set to “Approved” or “except inappropriate”.

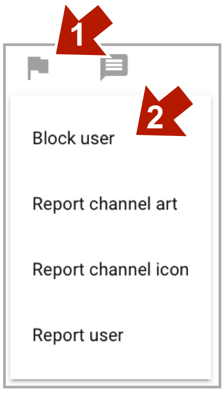




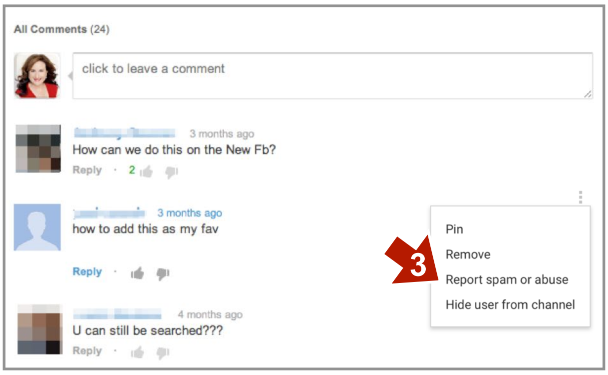
4
Comments
☑ Allow comments Learn more
Show
All
✓ All except potentially inappropriate comments
Approved
Sort by Top comments
3

How To Block Another YouTube User

Block by going to the users profile then
1. Then click the flag icon. Click "About"
To find flag if not showing.
2. Select "Block User" or "Report User"



3. Or block/report them via their comment under your video. Find drop down menu (three vertical dots) far right of the comment select "Hide User" or "Report…"


All Comments (24)

click to leave a comment

3 months ago
How can we do this on the New Fb?
Reply · 2

3 months ago
how to add this as my fav
Reply ·

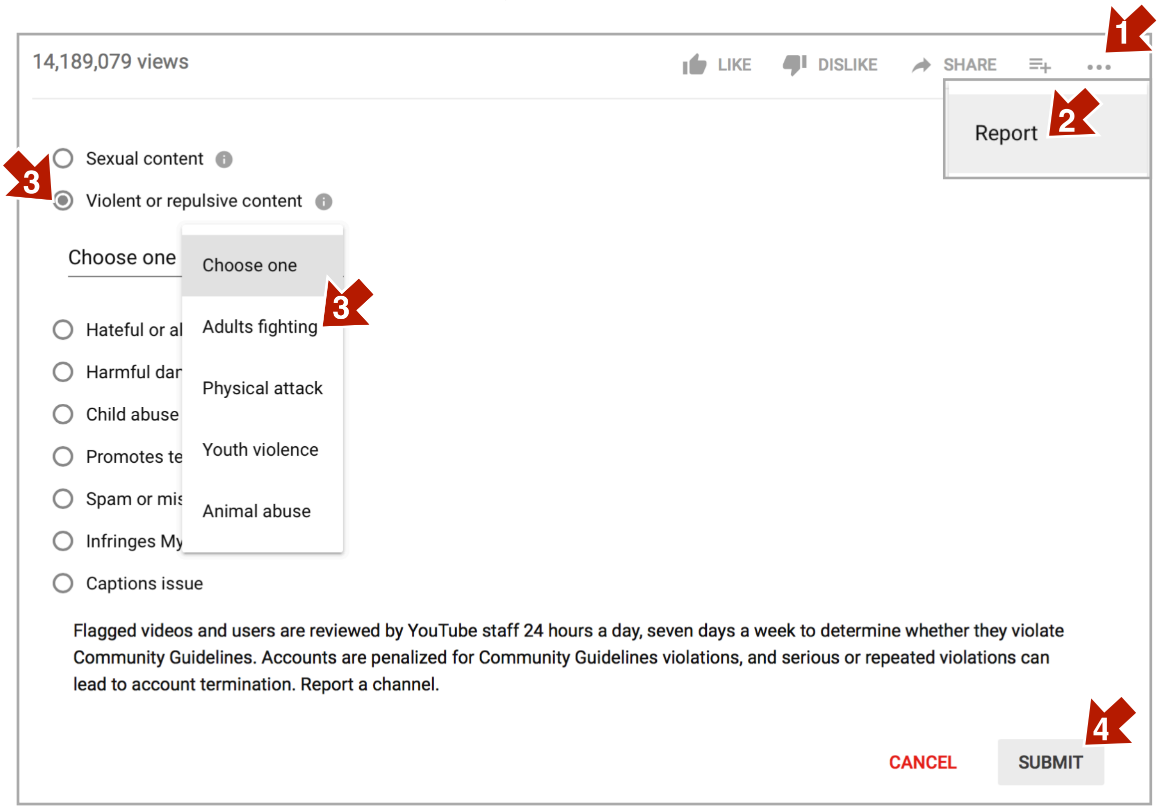
4 months ago
U can still be searched???
Reply ·

Mobile YouTube: Go to their profile - click the 3 vertical dots icon, top right next to search icon to select "Block User". Or click the 3 vertical dots next to their comment and select "Report"

Report/Flag A Video

To report a video as offensive or to have it removed, navigate to beneath the video.

1. Click "… More" 2. "Report" 3. Select the reason. 4. Click "Submit". YouTube will remove the video if it violates their community guidelines.



Flagged videos and users are reviewed by YouTube staff 24 hours a day, seven days a week to determine whether they violate Community Guidelines. Accounts are penalized for Community Guidelines violations, and serious or repeated violations can lead to account termination. Report a channel.

For mobile Y.T app, click 3 vertical dots top right of video, click "Report"

musical.ly TikTok Privacy Settings

musical.ly (now known at Tik Tok) is a video sharing app. Rated13+yrs due to adult content and public social media aspect. Tik Tok has important privacy settings to prevent you posting your video to the public, there are risks of bullying, adult followers and misappropriation of your content. It has "In App Purchases or "Coins" Some young users have spent thousands of dollars on coins. Report any inappropriate videos or nasty comments using the report features.

To set privacy settings:

Go to your profile icon lower right of home screen.

1. Click the settings … menu

2. Select "Privacy and Safety"

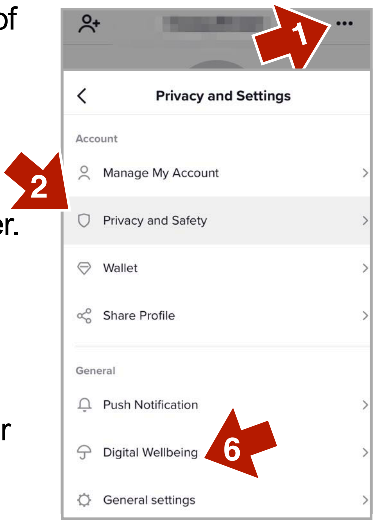
3. Set "Allow Others to Find Me", according to preference, off is safer.

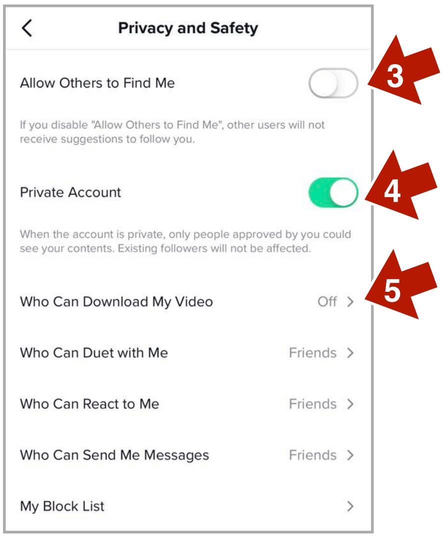
4. Enable "Private Account" set to on.

5. Set download to off, duet, react, and messages to Friends.

6. Set a time limit on your use, filter adult content.

Hide your location through your phones privacy settings. Settings/ Privacy Location Services/musical.ly





Privacy and Safety

Allow Others to Find Me: Off

If you disable "Allow Others to Find Me", other users will not receive suggestions to follow you.

Private Account: On

When the account is private, only people approved by you could see your contents. Existing followers will not be affected.

Who Can Download My Video: Off

Who Can Duet with Me: Friends

Who Can React to Me: Friends

Who Can Send Me Messages: Friends

My Block List

Beware: Allows live video streaming to a live public audience. Public live video can attract bullies and creepy people.

Instagram Privacy Settings

Privacy Settings:

1.Go to your profile page.

2.Click on the menu

3. Scroll down to "Settings" menu then scroll down to "Account Privacy"

4.Enable "Private Account".

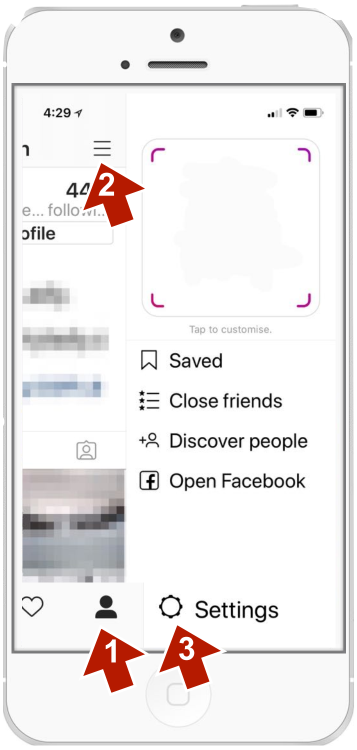
5.Go back & set all options to safest settings.

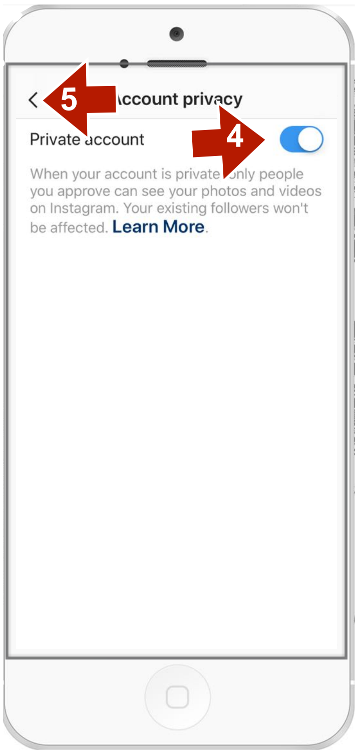
Filter inappropriate comments or keywords in "Comment Controls"

Two-factor Authentication prevents hacking. Use an Authentication app like Google Authenticator, not phone number. Keep ph numbers offline.

Story Controls: Select audience for stories and message settings. Turn off sharing.

Location Services: Disable through phone settings - Privacy - Location Services - Instagram - set to "Never".





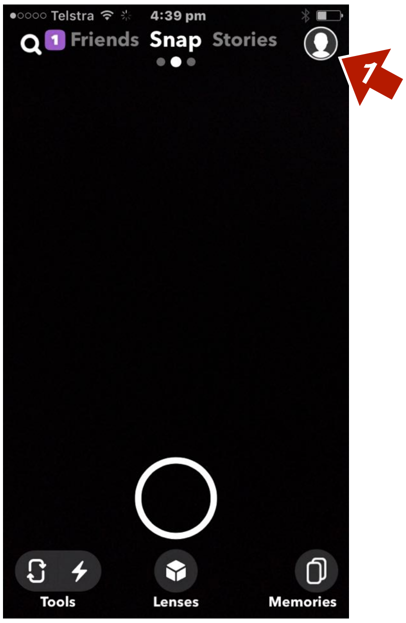
Private account: On

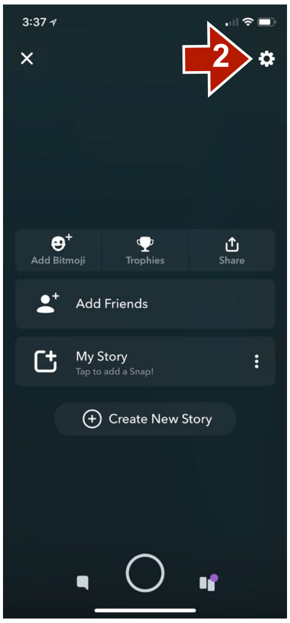
When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected. Learn More.

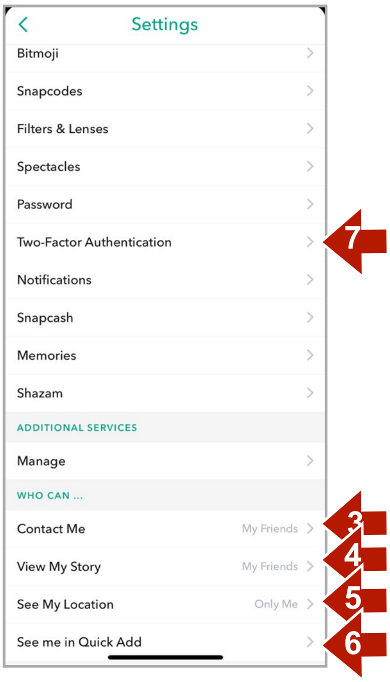
Snapchat Privacy Settings

Snapchat is advertised as a messaging app where messages “disappear”. However Snapchat photos CAN be screen-shot, saved & shared. Using the new feature “SnapMap” can be risky for your privacy & safety. Enable Ghost Mode via settings & “See My Location” Set to “Only Me”

Settings: Open app - 1.Click profile icon - 2.“Settings” - Scroll to down to “Who Can…” Set 3&4 to “My Friends” Set 5. to “Only Me” or Ghost Mode. 6.Turn off “Quick Add”. 7. Set up TwoFactor Verification, to secure your account from hackers via phone number or an Authentication app like Google Authentication or Sophos Authentication.






Settings

- Bitmoji
- Snapcodes
- Filters & Lenses
- Spectacles
- Password
- Two-Factor Authentication 7
- Notifications
- Snapcash
- Memories
- Shazam

ADDITIONAL SERVICES

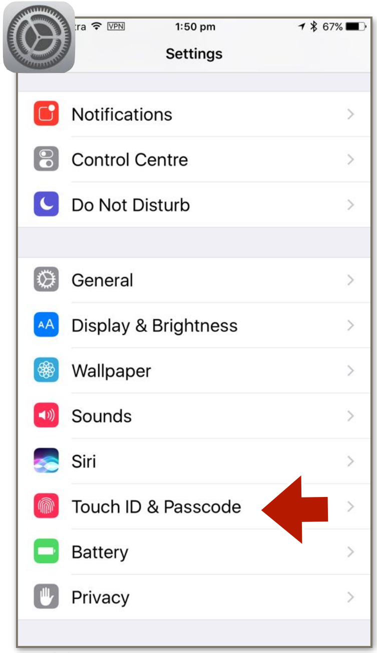
- Manage

WHO CAN ...

- Contact Me: My Friends 3
- View My Story: My Friends 4
- See My Location: Only Me 5
- See me in Quick Add 6

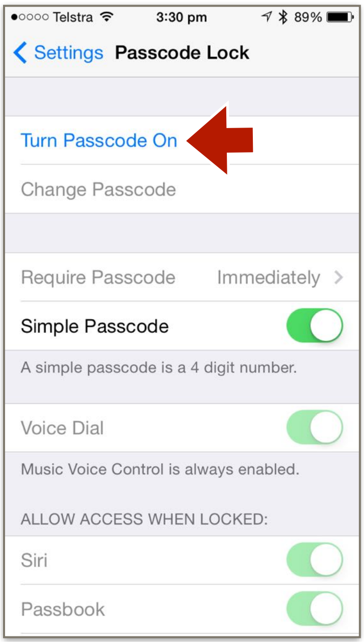
Setup Screen Lock On Apple Mobile

Set up a secret screen lock passcode, Touch I.D Or Facial recognition. You can set it so that it locks immediately or after a few minutes of inactivity. Go to your device “Settings” - “Passcode” - “Turn Passcode On” - “Set up a pass code” - set the time delay - then exit out to save. Set Touch ID to most secure settings. Select what you have access to when the phone is locked. iPhone X has Face ID & Passcode settings.



Settings

- Notifications
- Control Centre
- Do Not Disturb
- General
- Display & Brightness
- Wallpaper
- Sounds
- Siri
- Touch ID & Passcode
- Battery
- Privacy



Settings Passcode Lock

- Turn Passcode On
- Change Passcode
- Require Passcode: Immediately
- Simple Passcode: On

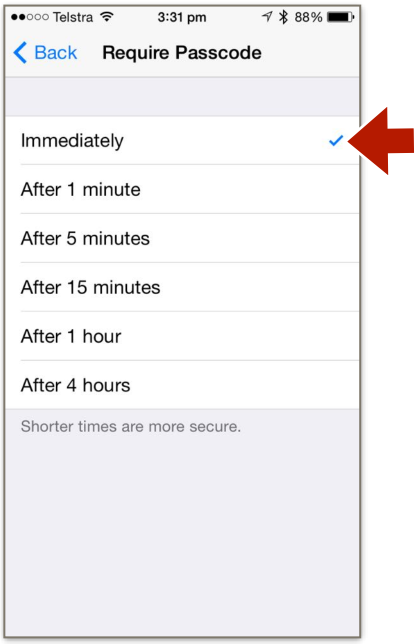
A simple passcode is a 4 digit number.

- Voice Dial: On

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

- Siri: On
- Passbook: On



Back Require Passcode

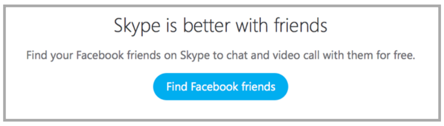
- Immediately ✓
- After 1 minute
- After 5 minutes
- After 15 minutes
- After 1 hour
- After 4 hours

Shorter times are more secure.

Skype Privacy Settings Mac P.C or Laptop

Skype has a proven history of safety if setup with privacy settings and your user name is kept private, only give it out to trusted contacts. For children and teens it is best to create a “made up” user name for extra privacy. Be careful using a webcam, it may give away private information about you. Students and children should report any messages or friend requests from strangers to adults and block. Sharing an account with younger children can help parents to supervise use. Parents and child can be logged in at the same time. These privacy settings are account “Cloud based” (no need to set on every device).

Note: Make sure you do not connect Skype with Facebook contacts, as per the prompt. See pic ⇨



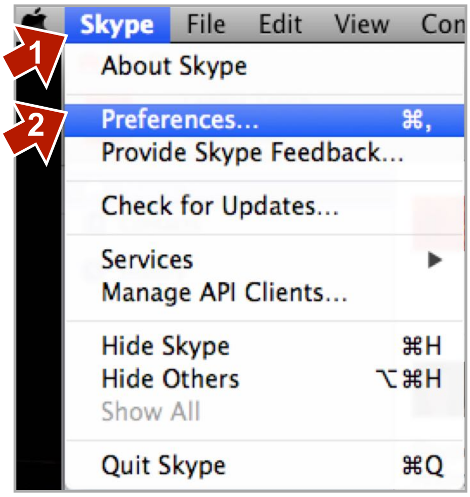
Skype is better with friends

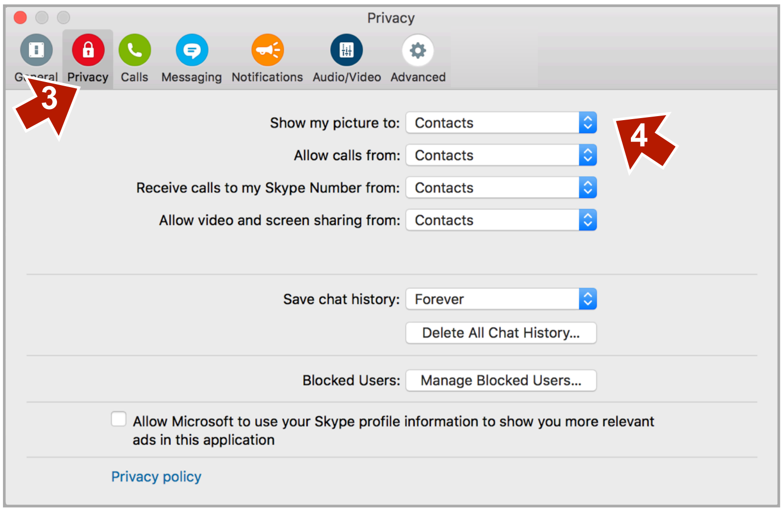
Find your Facebook friends on Skype to chat and video call with them for free.

Find Facebook friends

1. Open Skype App and click “Skype” Menu
2. Click ”Preferences"

3. Click on "Privacy"
4. Change all to "Contacts" as below





Show my picture to: Contacts

Allow calls from: Contacts

Receive calls to my Skype Number from: Contacts

Allow video and screen sharing from: Contacts

Save chat history: Forever

Delete All Chat History...

Blocked Users: Manage Blocked Users...

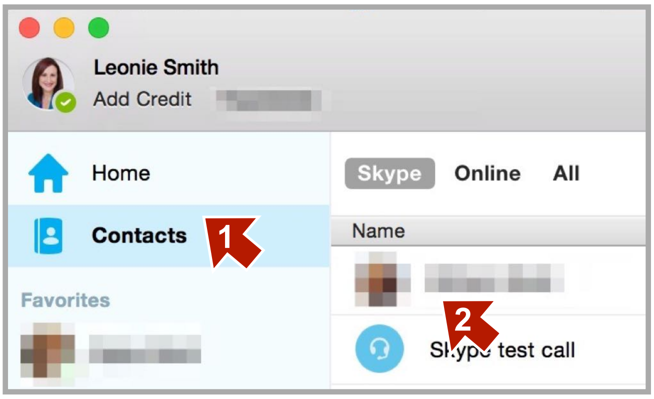
☐ Allow Microsoft to use your Skype profile information to show you more relevant ads in this application

Privacy policy

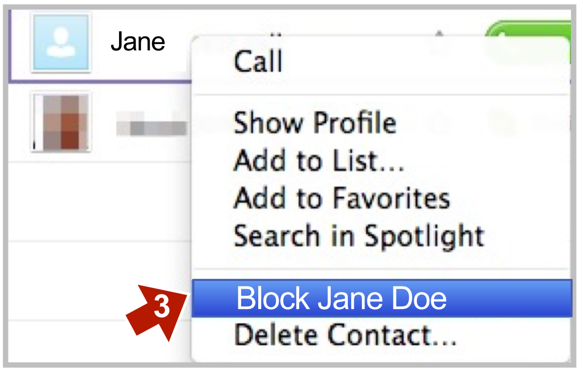
Note: Do NOT accept friend requests from people you don’t know. Click decline and block if necessary. Don’t sync your address book with Skype. Add your friends one by one.

How to Block A Contact

Go to 1. “Contacts” menu in left column.
2. Scroll to locate the contact you wish to block.



3. Right click on contact name and select the “Block” option from drop down list. Or on Mobile go to profile (hold finger on name) and scroll down to “Block contact”



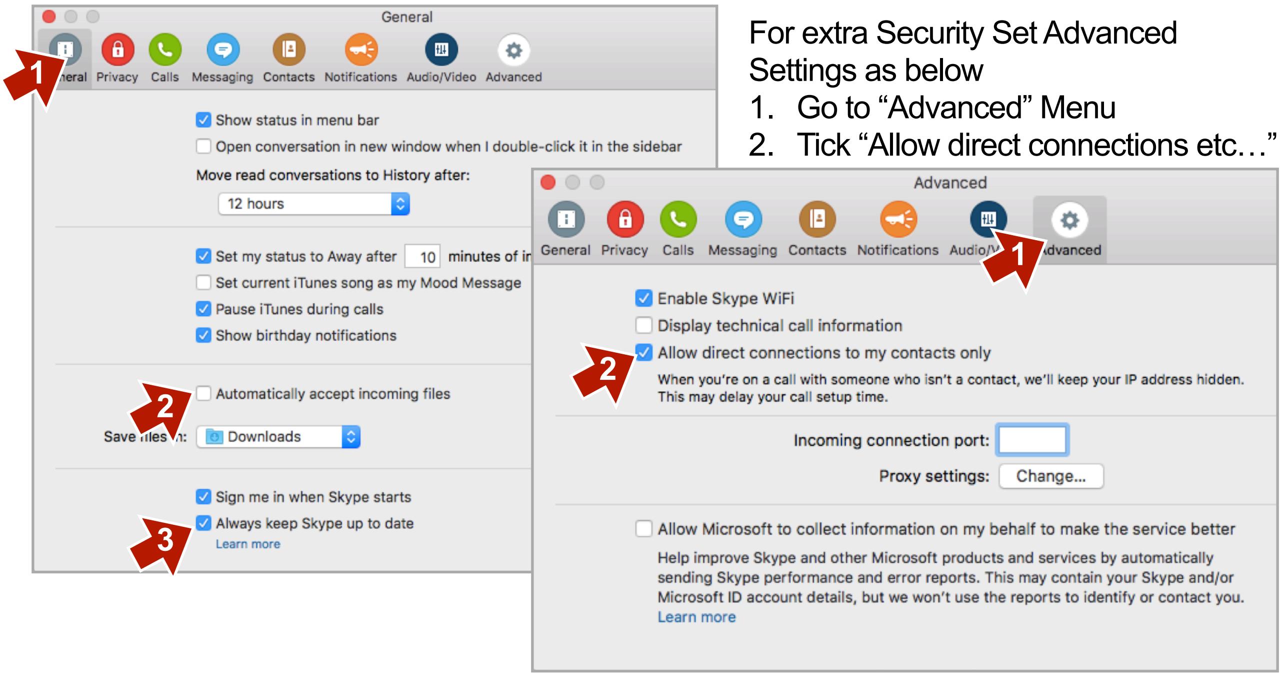
Skype Security Settings Mac PC or Laptop

To help protect against receiving a virus or unwanted content via a Skype message, you should set Skype so that it doesn't automatically download files to your computer.
Go to your Skype preferences as per previous instructions.

1. Click on "General" Menu
2-3. Scroll down and un-tick both settings as per below picture.

For extra Security Set Advanced Settings as below

1. Go to "Advanced" Menu
2. Tick "Allow direct connections etc…"



☑ Show status in menu bar
☐ Open conversation in new window when I double-click it in the sidebar
Move read conversations to History after: 12 hours

☑ Set my status to Away after 10 minutes of i
☐ Set current iTunes song as my Mood Message
☑ Pause iTunes during calls
☑ Show birthday notifications

☐ Automatically accept incoming files
Save files in: Downloads

☑ Sign me in when Skype starts
☑ Always keep Skype up to date
Learn more

☑ Enable Skype WiFi
☐ Display technical call information
☑ Allow direct connections to my contacts only
When you're on a call with someone who isn't a contact, we'll keep your IP address hidden. This may delay your call setup time.

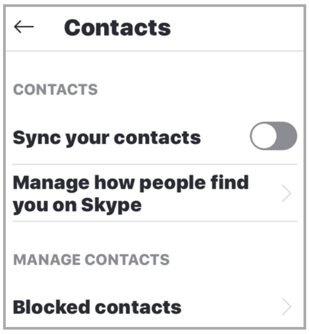
Incoming connection port:
Proxy settings: Change...

☐ Allow Microsoft to collect information on my behalf to make the service better
Help improve Skype and other Microsoft products and services by automatically sending Skype performance and error reports. This may contain your Skype and/or Microsoft ID account details, but we won't use the reports to identify or contact you.
Learn more

Mobile Skype

Privacy Security Settings:

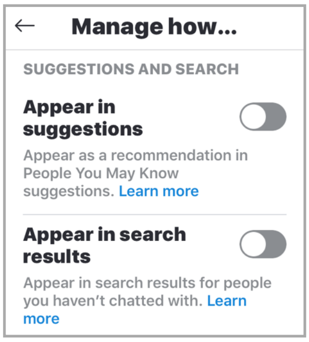
Apple Mobile Skype: First open Skype
1.Click your profile picture - top/centre
2.Click settings icon far top right.
3. Scroll down to Contacts and Manage how people find you.
Don't sync contact, but add contacts manually and carefully.



← Contacts

CONTACTS
Sync your contacts ○
Manage how people find you on Skype ›

MANAGE CONTACTS
Blocked contacts ›



← Manage how...

SUGGESTIONS AND SEARCH
Appear in suggestions ○
Appear as a recommendation in People You May Know suggestions. Learn more

Appear in search results ○
Appear in search results for people you haven't chatted with. Learn more

To Block:
1. Go to the name of the profile you wish to block.
2. Click their name top left to open full profile
3. Scroll down and click "Block Contact" Report Abuse if necessary.

Android Mobile Skype: First open Skype
1. Go to "Settings"
2. Under "Contacts" Set "Don't Copy Contacts".
3. Under "Privacy" - Set "Allow IMs From" and "Receive Calls From" to "Contacts Only."

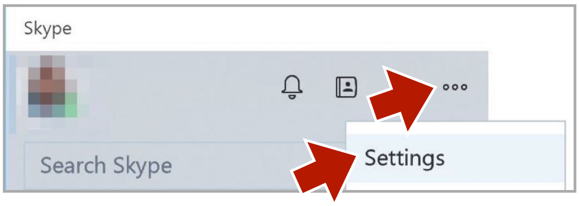
To Block:
1. Go to the profile of the person you wish to block. 2. Click "Settings" via 3 dots top right 3. Select "Block Contact" from menu

Skype Privacy Settings Windows 10

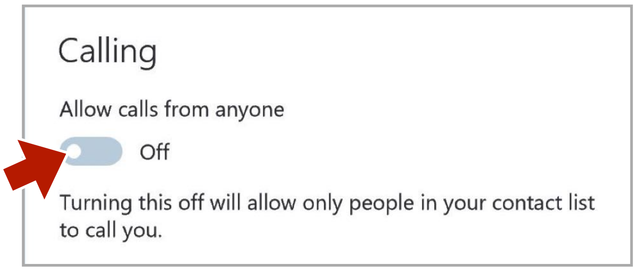
Prevent random strangers from sending you a direct message.

Use a made up name for extra privacy. Set the privacy so that only approved contacts can message you. Decline friend requests from people you don’t know. Block if necessary.

1. Go to … more menu top Right - click “Settings" from drop down menu.



2. Set all contact/calling and notification settings to Contacts only.

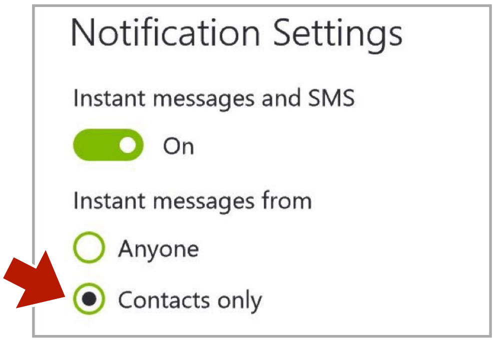


Calling

Allow calls from anyone

Off

Turning this off will allow only people in your contact list to call you.



Notification Settings

Instant messages and SMS

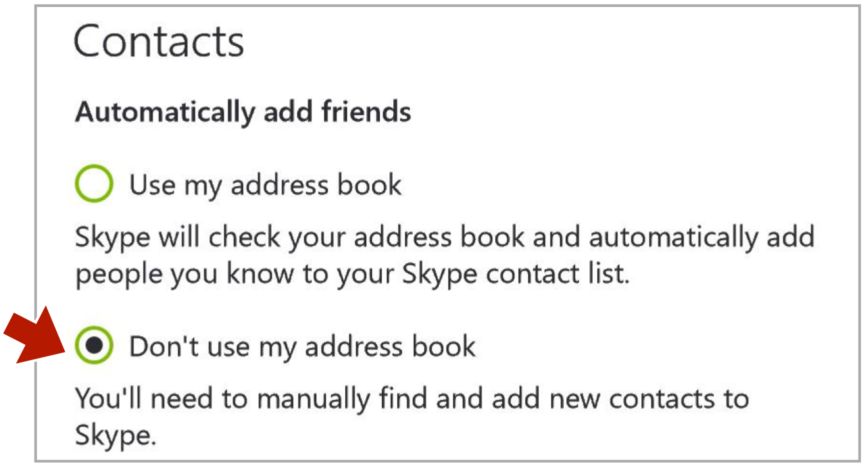
On

Instant messages from

○ Anyone

● Contacts only

3. Avoid Syncing your address book with Skype. Add contacts manually as you need them.



Contacts

Automatically add friends

○ Use my address book

Skype will check your address book and automatically add people you know to your Skype contact list.

● Don't use my address book

You'll need to manually find and add new contacts to Skype.

Blocking:
Right click on the profile name of the person you wish to block and click “Block This Person”.

Children & Teens should tell an adult they trust if they have been sent messages on Skype from someone they don’t know.

Note: Some people have been using “Voice Changers” over Skype and other voice apps to pretend to be someone they are not. Don’t trust a voice to determine if your Skype “Friend” is who they say they are. Adults can pretend to be younger, men can pretend to be women

Facebook Privacy Settings

To Find Out What You Are Sharing Publicly For Facebook on computers

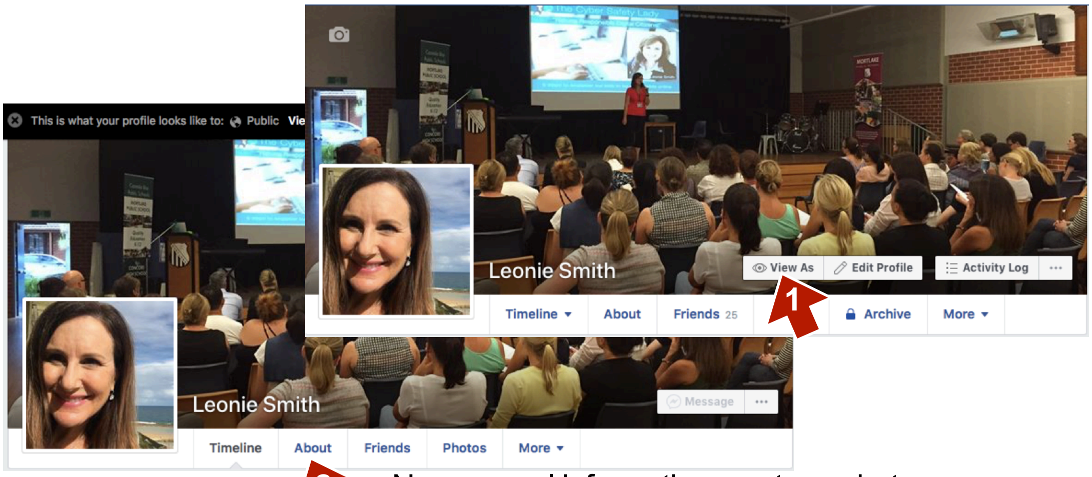
Go to your profile 1. Click “View As” on cover picture. **(Oct 2018: this option may be missing, Facebook disabled it after a recent hacking event - hopefully it will be restored)**

A truly private profile should only show your name, cover and profile picture, no posts or groups or other personal info or “likes”. You can’t hide your profile pic or cover pic, but set them carefully with an eye to privacy. Go through all the tabs to check what is showing, then exit out of “View As” and change and delete anything you don’t want public. Check back to “view as” to see if you have deleted/changed enough.

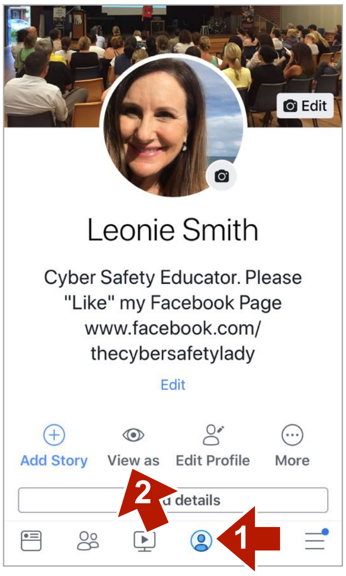
2. Hide all your personal information posts and photos through the “About” or “Edit Profile” menu and set all your personal information, including your relationship status, your likes, your location and employment to “Only Me” or “Friends Only”. Delete any information or posts you don’t need to share.

Don’t Leave It All Up There. Hacking happens. Delete your old posts occasionally for better privacy. Delete/hide old profile and cover pics from your photo albums. Go to “View Activity Log” and delete your old posts one by one. Unfortunately there is no “Delete All” button.

Note: Facebook settings are cloud based, setting them on your computer or mobile device will set them across all your devices.



No personal information, posts or photos.



Cyber Safety Educator. Please "Like" my Facebook Page www.facebook.com/thecybersafetylady

The Mobile version of Facebook (see left pic) now has the “View as” setting available from your profile page.

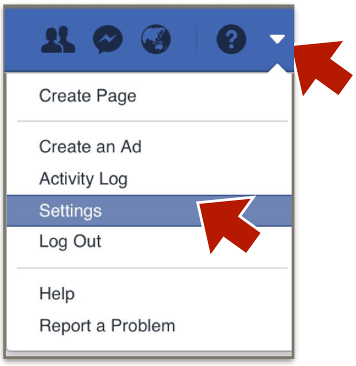
1.Click the profile icon - bottom menu - to go to your profile page.

2.Click the “View as” link.

Go through each tab - About - Photos - Friends, to see what is showing.

To edit your content exit out of “View as” click back arrow, and delete and hide your data as needed.

Facebook Privacy Settings P.C or Laptop

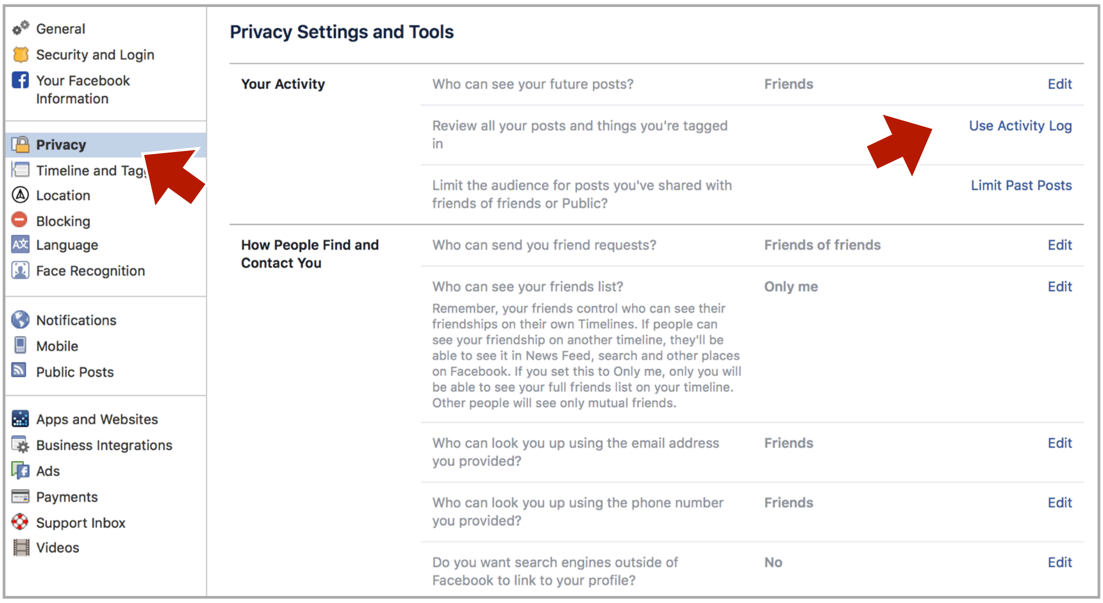


Apple Mobile F.B - click ≡ symbol lower right menu, scroll down to “Settings & Privacy” - “Settings” - “Privacy”. **Android Mobile F.B** - Click “More” Symbol - Scroll to “Privacy” set all as below.

1. Go to downward arrow top right, scroll down to “Settings” on drop down menu. In next window click “Privacy” in left side menu. Set all to the most private options, as below.

Note: “Use Activity Log” is where all your posts, comments and likes are listed. You can delete your past posts one by one from there if needed. Or set all past posts back to “Friends Only”

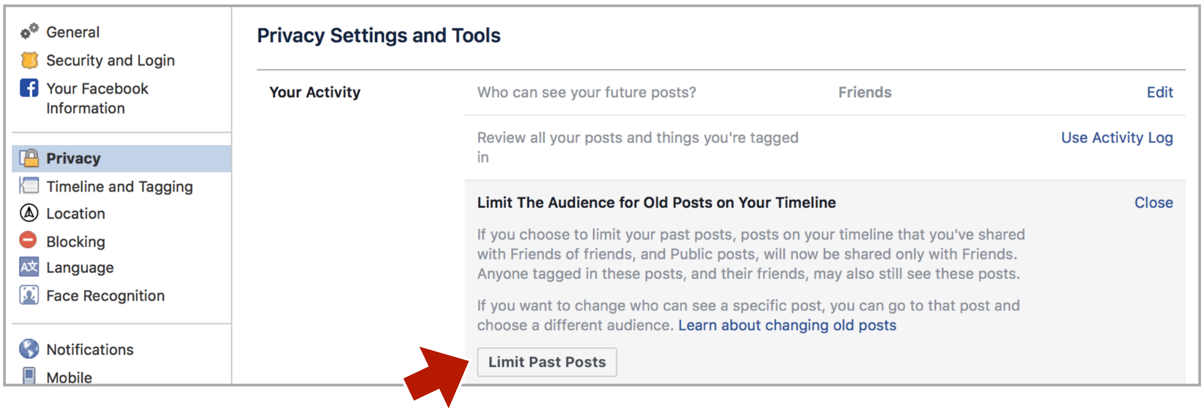
2. Set all settings as per below picture.



Privacy Settings and Tools

Your Activity	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
How People Find and Contact You	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list? Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.	Only me	Edit
	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

3. Select “Limit Old Posts”. This sets all past posts back to “Friends” (not public).



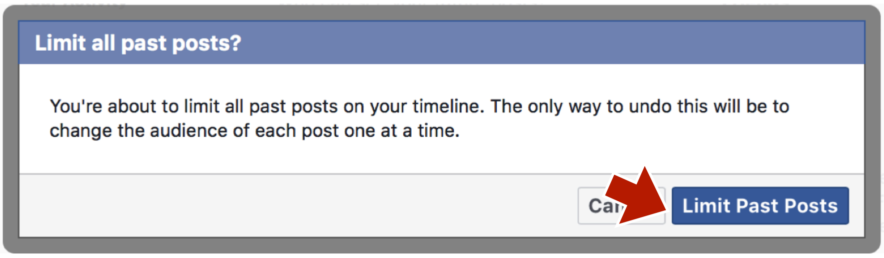
Privacy Settings and Tools

Your Activity	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 Old Posts on Your Timeline — Close

If you choose to limit your past posts, posts on your timeline that you've shared with Friends of friends, and Public posts, will now be shared only with Friends. Anyone tagged in these posts, and their friends, may also still see these posts.

If you want to change who can see a specific post, you can go to that post and choose a different audience. Learn about changing old posts



Limit all past posts?

You're about to limit all past posts on your timeline. The only way to undo this will be to change the audience of each post one at a time.

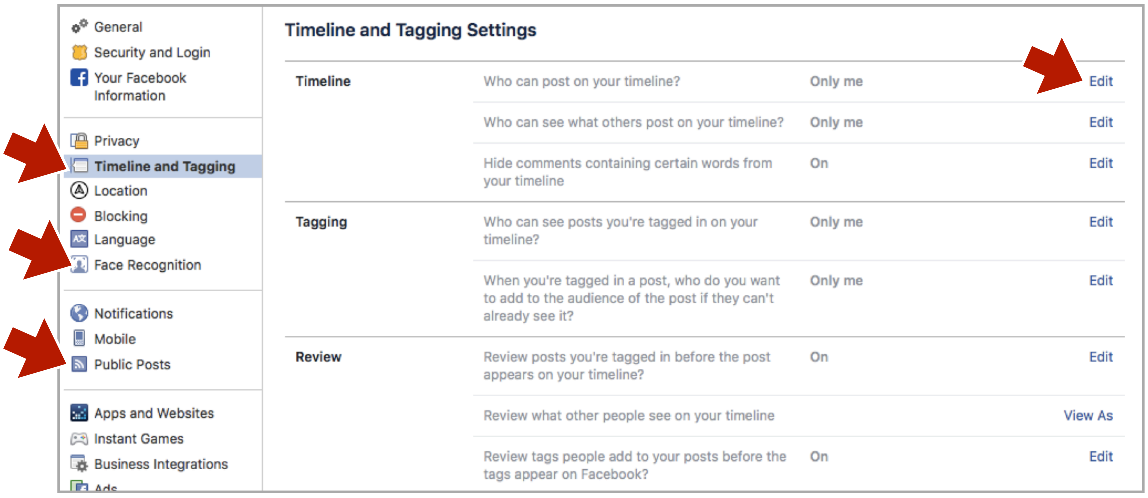
4. Select “Limit Past Posts”

Facebook Privacy Settings

Still in “Settings” go down to “Timeline and Tagging” and set all settings to “Friends” or “Only Me” etc, as below by clicking “Edit” next to each setting.

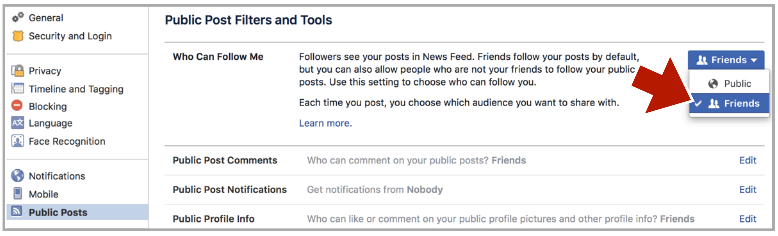
Scroll down to Face Recognition and select your preference. Do you want Facebook to scan your face in photos?

Scroll down to “Public Posts”: Set all to most private settings “Friends” not “Public”.



Timeline and Tagging Settings

Timeline	Who can post on your timeline?	Only me	Edit
	Who can see what others post on your timeline?	Only me	Edit
	Hide comments containing certain words from your timeline	On	Edit
Tagging	Who can see posts you're tagged in on your timeline?	Only me	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Only me	Edit
Review	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review what other people see on your timeline		View As
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit



Public Post Filters and Tools

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 public posts. Use this setting to choose who can follow you.

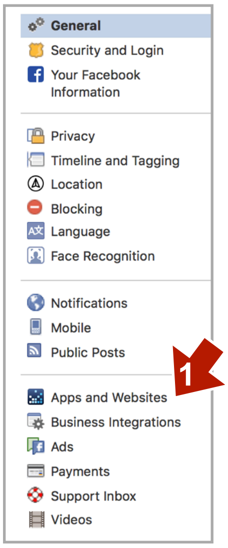
Each time you post, you choose which audience you want to share with.

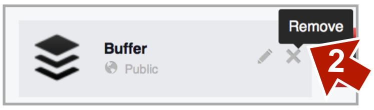
Learn more.

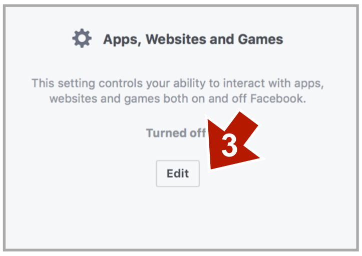
Public Post Comments	Who can comment on your public posts? Friends	Edit
Public Post Notifications	Get notifications from Nobody	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? Friends	Edit

App Settings

1. Apps can share your information and preferences. Go to “Apps and Websites: Then the “Active” Tab and delete Apps you don’t use by ticking and click “Remove”. 2. Or click “View and edit” and set privacy to “Only Me”. 3. If you have removed all apps you can turn off this facility if you don’t wish to connect apps or other websites to your account by clicking “Edit” 4. Set this box “Old versions…” to “Only Me”



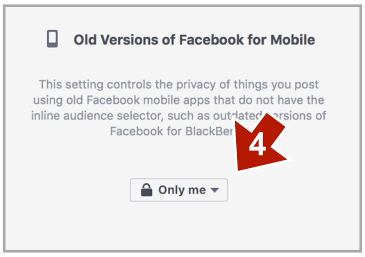




Apps, Websites and Games

This setting controls your ability to interact with apps, websites and games both on and off Facebook.

Turned off



Old Versions of Facebook for Mobile

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

Mobile FB Go to “More” ☰ 1. “Settings & Privacy” - “Settings” 2. scroll to “Apps and websites” - Preferences - “Apps,websites and games” Click “Edit” next to the app and set privacy to “Only Me” or scroll down to “Remove App” 3. Turn off “Apps, websites” facility if not needed On previous page 4. Set “Games and app notifications to “No” 5. “Old versions of Facebook” set to “Only Me” Exit back out to save settings.

Blocking Abuse On Facebook P.C or Laptop

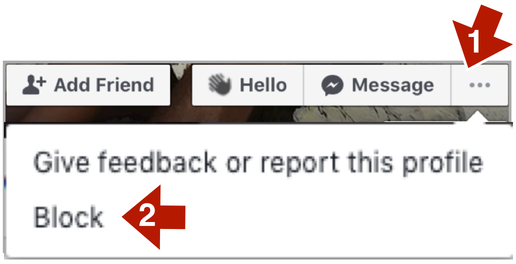
Mobile FB click “More” ☰ lower right menu - scroll right down to “Settings & Privacy” “Settings” scroll down to blocking

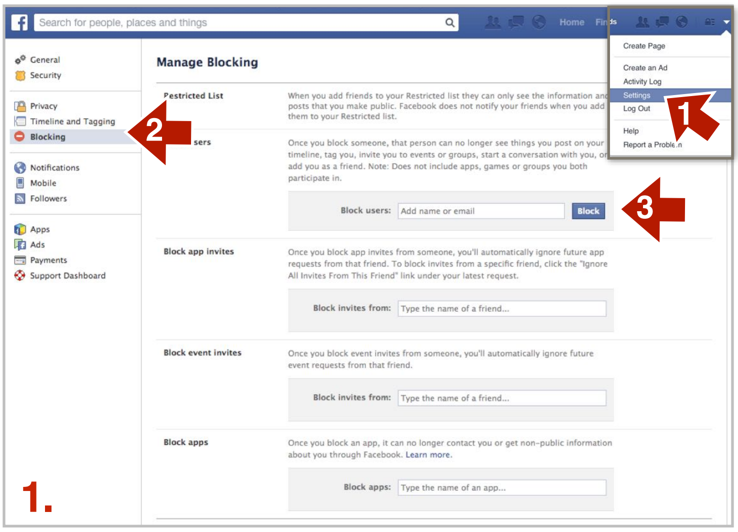
1. Blocking Apps And Users

1. Go to Facebook “Settings”
2. “Blocking”
3. “Block users” enter details.

Block messages, apps etc here.

2. You can also block users by going to their profile and blocking them from the (…) Menu. (as below).





Manage Blocking

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

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

Block users: Add name or email

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

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

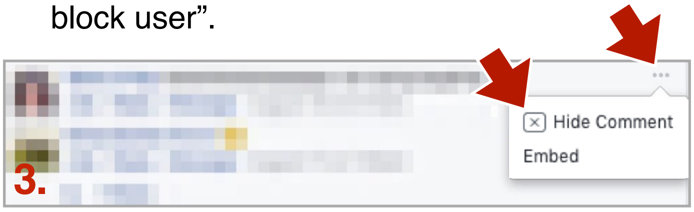
Block event invites Once you block event invites from someone, you'll automatically ignore future event requests from that friend.

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

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

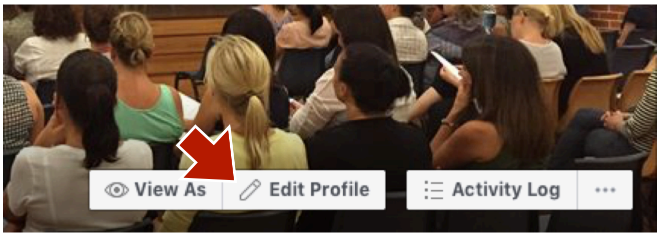
Block apps: Type the name of an app...

3. Hide and report comments by clicking the … menu top right of the comment. Then select “Hide Comment” or “Delete comment and block user”.

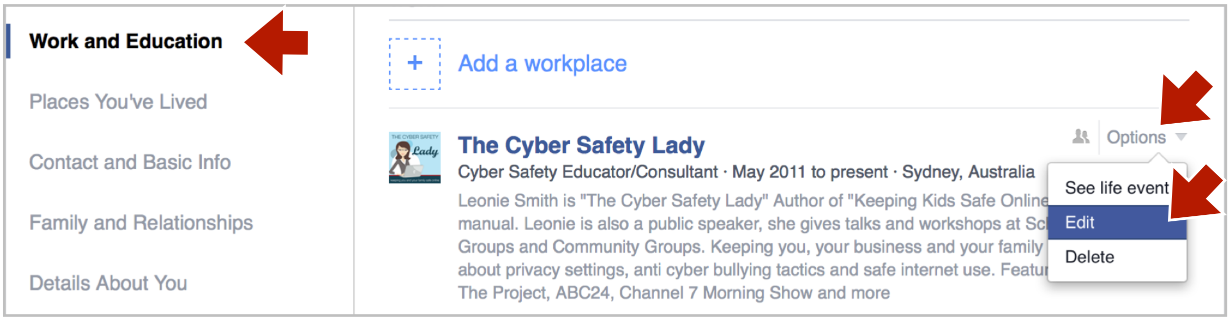


Hide Your Personal Information on Facebook

To protect all your private information from scammers and bullies select “Edit Profile” from your profile page, scroll down to “Edit Your About Info” and set all your info in every section to “Only Me” or “Friends” by clicking “Options” - “Edit” and then change the visibility. (P.C or Laptop Settings)



Mobile FB go to your profile page by clicking your profile pic. Click “Edit Profile” icon top right. Then Scroll down to “Edit your About Info” Click the edit icon for each section and one by one, set all to “Only Me” or “Friends”. Hide birthdate or change.



The Cyber Safety Lady

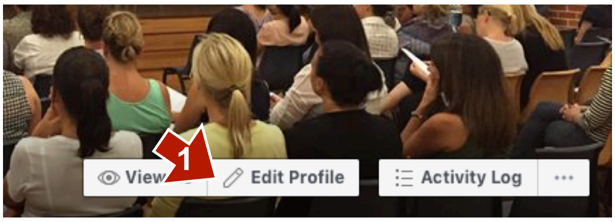
Cyber Safety Educator/Consultant · May 2011 to present · Sydney, Australia

Leonie Smith is "The Cyber Safety Lady" Author of "Keeping Kids Safe Online manual. Leonie is also a public speaker, she gives talks and workshops at Sc Groups and Community Groups. Keeping you, your business and your family about privacy settings, anti cyber bullying tactics and safe internet use. Featur The Project, ABC24, Channel 7 Morning Show and more

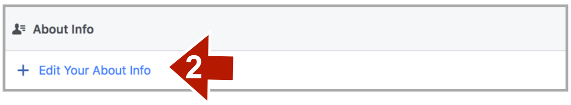
Hide Birthdate On Facebook P.C or Laptop

Hiding your birth date is important for security and to protect against identity theft. You can leave the day of your birthday visible to friends so that you get “Happy Birthday” wishes, but it is best to set the year of birth to “Only Me” for extra security.

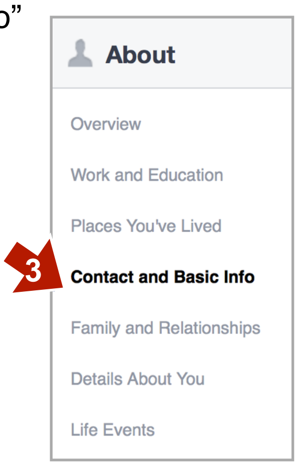
1. Go To Your Profile Page, then to "Edit Profile" bottom right of your “Cover Picture”



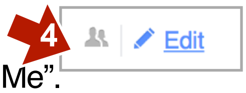
2. Scroll down the bottom of pop up menu, click “Edit Your About Info”



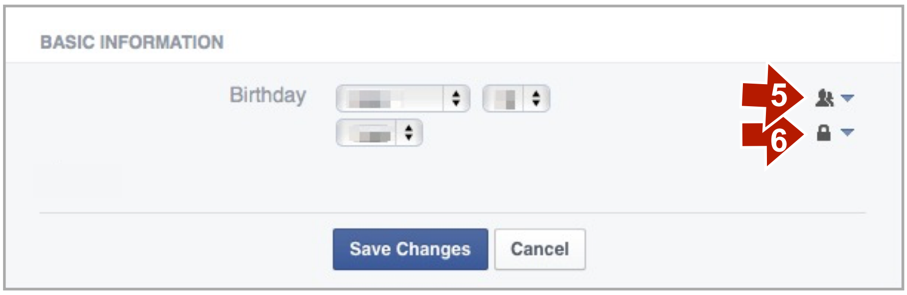
3. Scroll down to “Contact and Basic Info”



4. Hover cursor over “Edit” on the far right of “Basic Information” Birthday settings, click to edit.

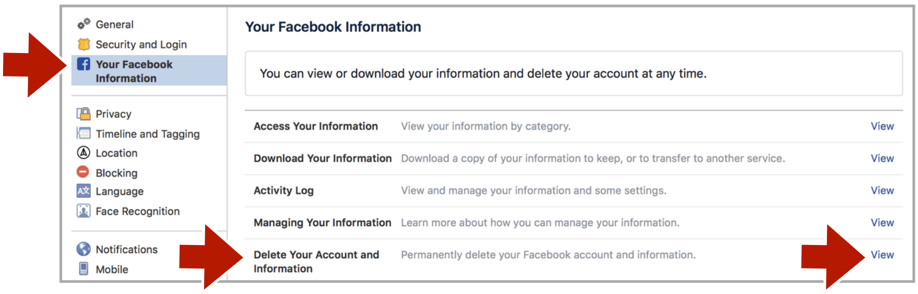


5. Set to “Friends” or “Only Me” 6. Birth year to “Only Me”.



How To Delete or Deactivate Your Facebook Account

You can either “Deactivate” your Facebook account temporarily, or you can delete your existing Facebook account permanently with all your content deleted after 30 days. To delete permanently go to your Facebook settings - “Your Facebook Information” scroll down to Delete Your Account and Information. Click “View” and follow instructions.

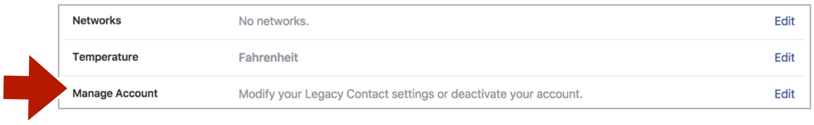


Your Facebook Information

You can view or download your information and delete your account at any time.

Access Your Information	View your information by category.	View
Download Your Information	Download a copy of your information to keep, or to transfer to another service.	View
Activity Log	View and manage your information and some settings.	View
Managing Your Information	Learn more about how you can manage your information.	View
Delete Your Account and Information	Permanently delete your Facebook account and information.	View

To “Deactivate” or suspend your account temporarily, go to your Facebook settings then to “General” and go down to “Manage Account” and scroll to “Deactivate your account” linked text.



Networks	No networks.	Edit
Temperature	Fahrenheit	Edit
Manage Account	Modify your Legacy Contact settings or deactivate your account.	Edit

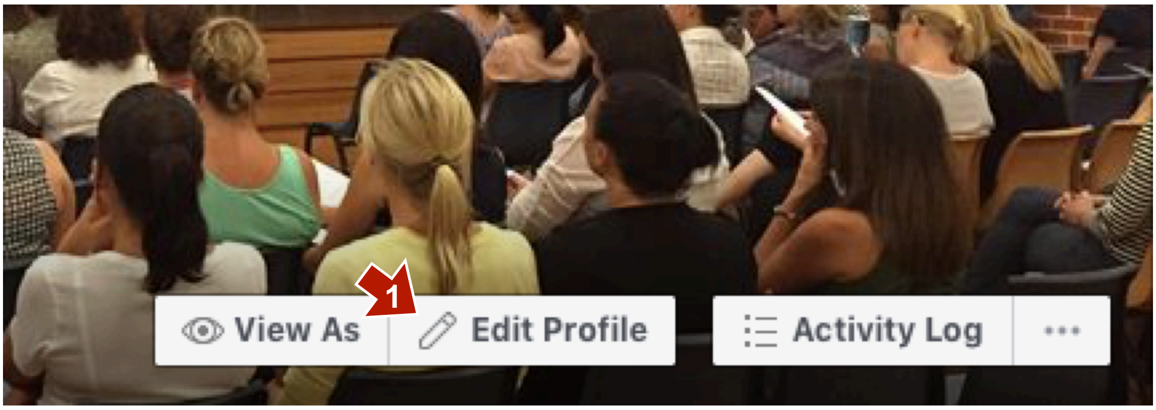
(On Mobile - click ☰ - Scroll to “Settings & Privacy/Settings/Personal Information/Manage account/Tap Deactivate, follow instructions. To delete, “Settings & Privacy/Settings”, scroll to “Your Facebook Information” then “Delete your account & information”.)

Hide Phone Number & Email On Facebook

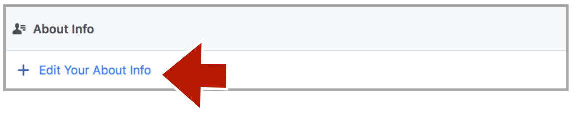
PC Laptop Browser Settings

Hiding your phone number and email on Facebook can prevent spam and scams being sent to your email, phone and Facebook Messenger. A lot of cyber crime and scams are being spread through email and phone numbers. Avoid putting either online anywhere.

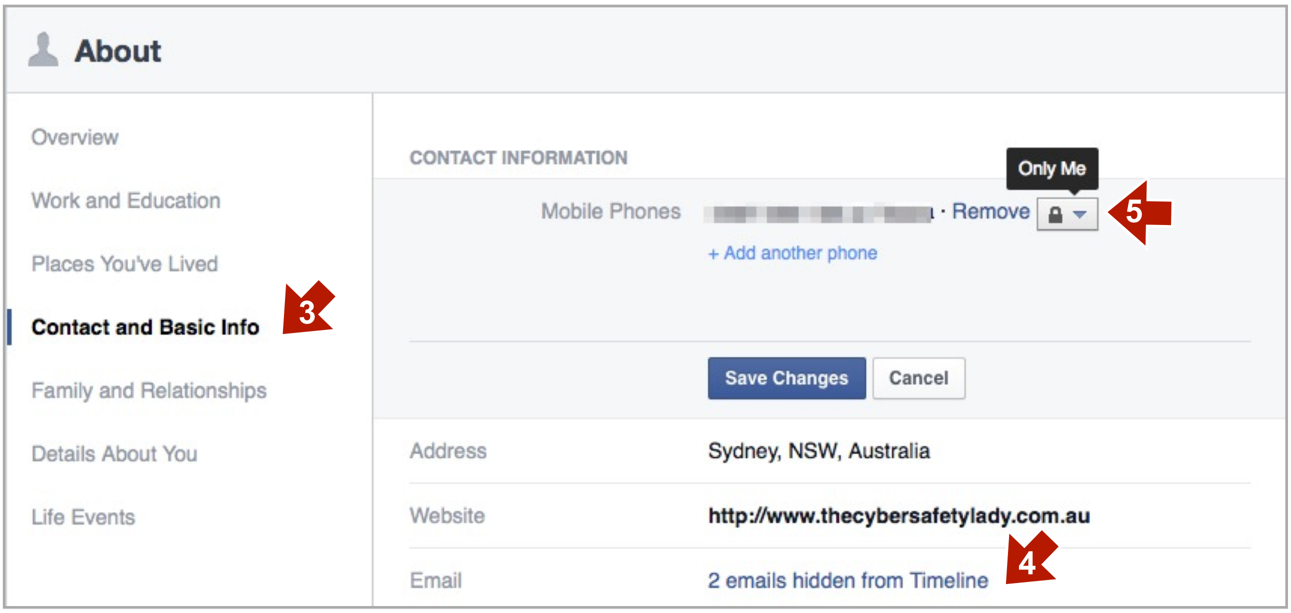
1. First go to your Facebook Profile and Click “Edit Profile” bottom of your “Cover Picture”



2. Scroll down the bottom of pop up menu, click “Edit Your About Info”



3. On next page click “Contact and Basic Info” in the left column.
4. Then scroll down to Email click “Edit” (far right of panel) set to “Only Me”.
5.Scroll to “Mobile Phones” and remove the number or set to "Only Me”.



CONTACT INFORMATION

Mobile Phones [redacted] · Remove

Address Sydney, NSW, Australia

Website http://www.thecybersafetylady.com.au

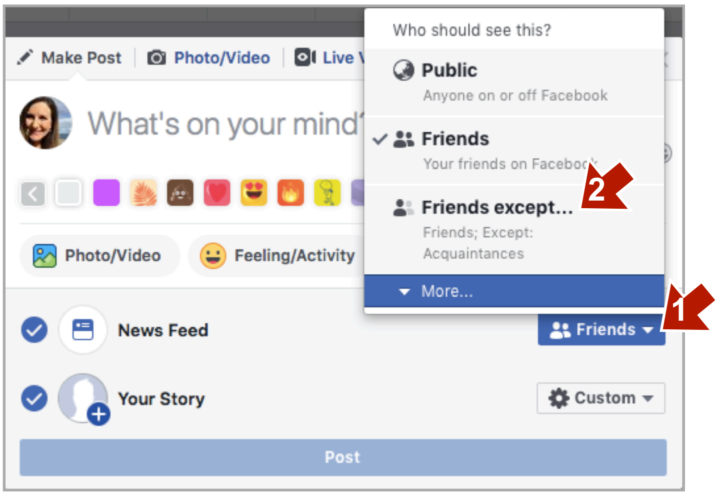
Email 2 emails hidden from Timeline

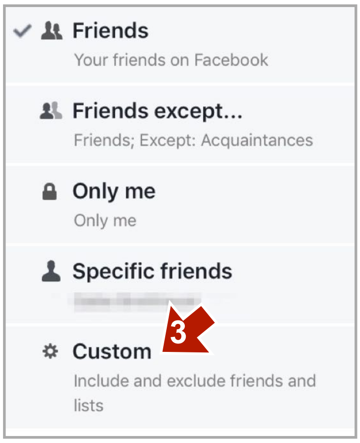
Note: It is good security to hide as much as you can in this panel.

How To Post With More Privacy On Facebook

1. Before you post an update choose who you want to post to from the drop down menu bottom right. If you choose "Public" it means the post can be seen by everyone including to people who are NOT your friends. 2. “Friends except Acquaintances” means close friends only. Go to your friends list and set your friends to either “Close Friends” or Acquaintances or leave as “friends” this helps decide what they see, and how much you see of their posts. Exclude or include friends in 3. Custom tab.

Note: If you do want to post publicly remember to change it back to “Friends” later if needed, your future posts will default to public until you do!



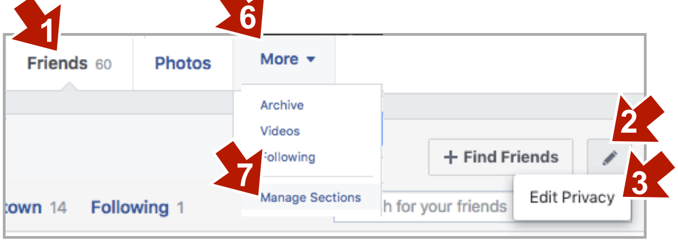


Hide Your Friends List On Facebook

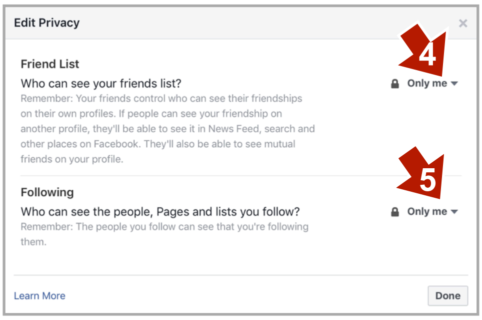
P.C - laptop only **Top Tip!** See step by step video here or scan code

Keeping your friends list private is more secure than leaving it public. Scammers, blackmailers or cyber bullies can use your friends list to spread scams or cyber bullying messages about you. Hide your friends list through Settings/Privacy “How people find and contact you” - “Who can see your friends list?” Set to “Only Me” Or as below - Note: for Mobile F.B app go to ”Settings & Privacy” “Settings” “Privacy Settings” scroll down to “Who can see your friends list” set to “Only Me”

1. Go to your profile, then to the "Friends" tab below your cover pic. 2. Click the pencil icon next to “Find Friends” & then click 3. “Edit Privacy”.



4. Then select “Only Me” or “Friends” For the “Friend List” and 5. “Only Me” for “Following” options.



Edit Privacy

Friend List

Who can see your friends list? Only me

Remember: Your friends control who can see their friendships on their own profiles. If people can see your friendship on another profile, they'll be able to see it in News Feed, search and other places on Facebook. They'll also be able to see mutual friends on your profile.

Following

Who can see the people, Pages and lists you follow? Only me

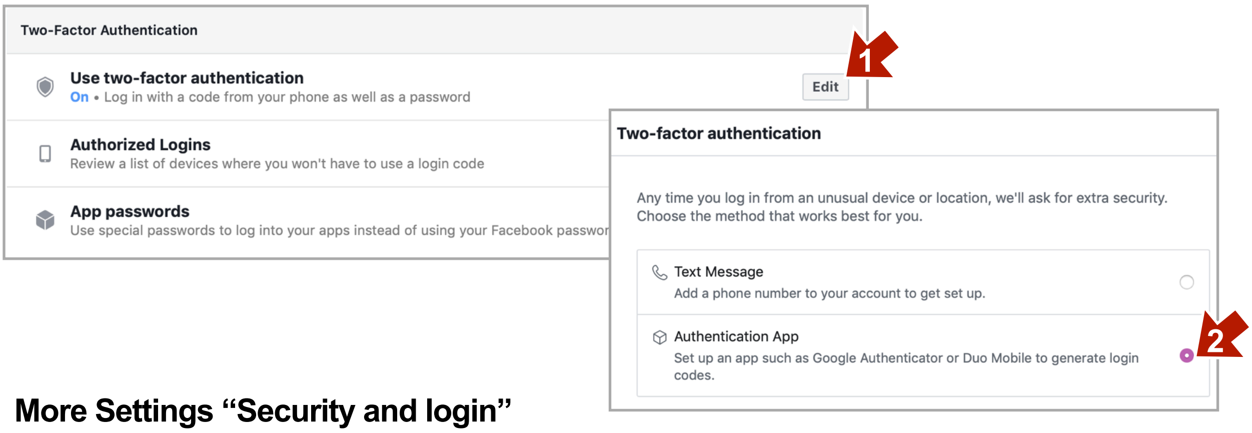
Remember: The people you follow can see that you're following them.

Hide Your Groups And Personal Preferences: Scammers and stalkers can use your private information, likes, and preferences to steal your identity or market scams to you. (See pic above left) Clicking 6. “More” & 7. “Manage Sections” displays a list of information that can be displayed publicly on your profile. Un-tick all of them to hide your groups, preferences and likes. The greyed out ticked options on the list cannot be un-ticked. Untick “questions” and it will disappear from the menu. (Can’t be set via a mobile device. Open settings on a P.C or Laptop)

Facebook Security Settings P.C or Laptop

Don't get your Facebook Profile Hacked! Set extra security by going to Facebooks Security settings and setting Two Factor Authentication so that you will be sent a notification through an Authenticator app like Google Authenticator or Sophos Authenticator, if someone is trying to hack into your account. Don't use SMS or your phone number unless you have to, keep your phone number off Facebook. Download an Authenticator app first on your mobile, then come back to set up, and follow the instructions on the screen.

Go to Settings/Security and Login - "Two Factor Authentication" click "Edit" and set up.



Two-Factor Authentication

Use two-factor authentication
On • Log in with a code from your phone as well as a password
Edit

Authorized Logins
Review a list of devices where you won't have to use a login code

App passwords
Use special passwords to log into your apps instead of using your Facebook passwor

Two-factor authentication

Any time you log in from an unusual device or location, we'll ask for extra security. Choose the method that works best for you.

Text Message
Add a phone number to your account to get set up. ○

Authentication App
Set up an app such as Google Authenticator or Duo Mobile to generate login codes. ●

More Settings "Security and login"

Be sure you have a good strong password on your Facebook account and store it safely. 9 Letters or more, random letters symbols and numbers or use unrelated words and numbers.

Choose 3 to 5 trusted friends who can help you get your account back if the hacker has changed your password and logged you out. Be sure they really are TRUSTWORTHY!

Future Proof Your Digital Footprint!

Don't leave your personal content up online.

If you are sharing personal family photos or videos on social media or a social photo hosting site, consider deleting or archiving some past personal posts after sharing them. Keeping past posts, personal videos and photos on any social media site, may not be secure. You risk public exposure if your account is ever hacked, or if your content is shared beyond your original wishes. Be sure to use good safe passwords (8 characters/ digits or more of unrelated phrase or wording) and Two Factor verification where ever possible to prevent hacking of your accounts or cloud storage.

Your Digital Footprint

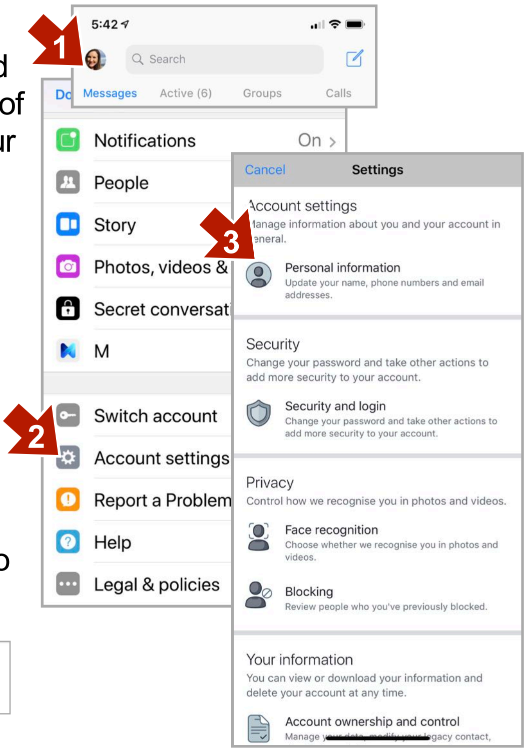
Parents: Your children may one day have a role in their community or a career that demands privacy. If you are then asked by your child to delete all the personal content that you have shared online about them, it will be more difficult to do so years down the track. Of course you cannot guarantee that copies of the posts have not already been shared. Archiving or deleting as you go certainly minimises later risk, and makes it easier to protect your child's online footprint.

To archive past Facebook posts go to the "View Activity Log" menu located under your profile cover pic and delete each post one by one. For Instagram delete posts one by one from your account. Or select photo and then click … Menu and select "Archive" or "Delete".

Facebook Messenger - Mobile

Privacy Settings

All your privacy settings for Messenger must be managed through your normal Facebook profile. To manage some of the settings on Messenger, Open Messenger 1. Click your profile Pic 2. Scroll down to "Account Settings" Click and adjust settings for your preferences.



Account settings
Manage information about you and your account in general.

Personal information
Update your name, phone numbers and email addresses.

Security
Change your password and take other actions to add more security to your account.

Security and login
Change your password and take other actions to add more security to your account.

Privacy
Control how we recognise you in photos and videos.

Face recognition
Choose whether we recognise you in photos and videos.

Blocking
Review people who you've previously blocked.

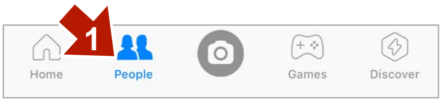
Your information
You can view or download your information and delete your account at any time.

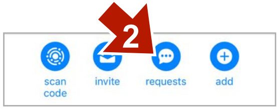
Account ownership and control
Manage your data, modify your legacy contact,

Filtering Message Contacts

You can no longer filter who contacts you on Facebook Messenger. Anyone who has Facebook Messenger can now contact you on your Facebook Messenger app by sending a Facebook Message request.

Non friends messages will show up in the "Request" tab. Open Messenger - Go to 1. "People" then 2."Requests" to review invitations. Block or accept as needed.

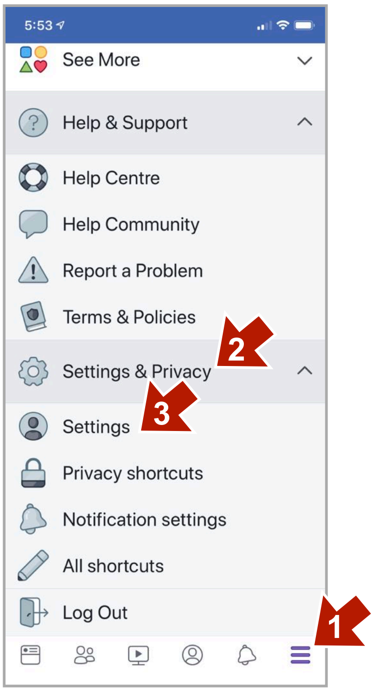


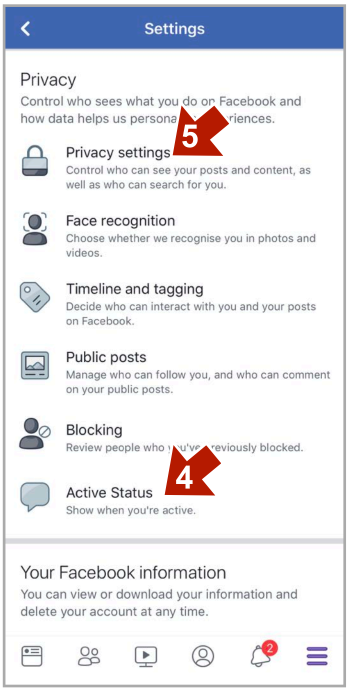


Make sure you have all your Facebook privacy settings secure by also following the "Facebook Privacy and Hiding your Private Information" instructions in this manual.

When A Stranger Calls!

Some users are reporting that they are getting random messages from strangers on Facebook Messenger. You can't set FB Messenger to only receive "Friend" messages, but you can reduce the likelihood of getting strangers messaging you by setting up strict privacy settings the Facebook mobile app via 1."Menu" 2.Scroll down to"Settings & Privacy" 3"Settings" 4.Turn off Active Status. 5."Privacy settings" Set all as below.





Privacy
Control who sees what you do on Facebook and how data helps us personalise experiences.

Privacy settings
Control who can see your posts and content, as well as who can search for you.

Face recognition
Choose whether we recognise you in photos and videos.

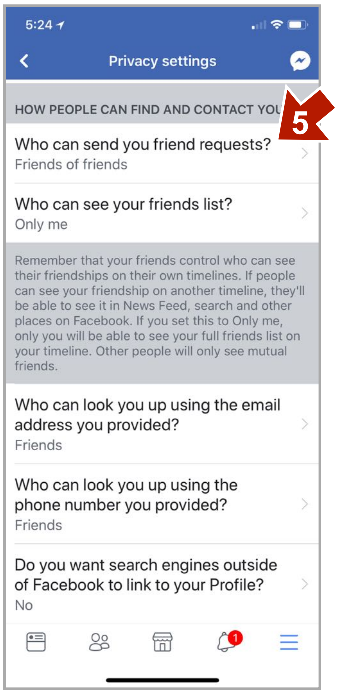
Timeline and tagging
Decide who can interact with you and your posts on Facebook.

Public posts
Manage who can follow you, and who can comment on your public posts.

Blocking
Review people who you've previously blocked.

Active Status
Show when you're active.

Your Facebook information
You can view or download your information and delete your account at any time.



HOW PEOPLE CAN FIND AND CONTACT YOU

Who can send you friend requests?
Friends of friends

Who can see your friends list?
Only me

Remember that your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will only see mutual friends.

Who can look you up using the email address you provided?
Friends

Who can look you up using the phone number you provided?
Friends

Do you want search engines outside of Facebook to link to your Profile?
No

Facebook Messenger - Blocking - Muting

You can block a contact directly through Facebook Messenger and you can “Mute” a conversation if you no longer want notifications from that chat.

To Mute

1. Go to your Messager “Home” messages list (house “Home” icon).
2. Tap and hold the message you want, select “Mute” from the pop up menu.
3. “Mute” forever or temporarily.

This will only Mute a past conversation NOT block someone from contacting you.

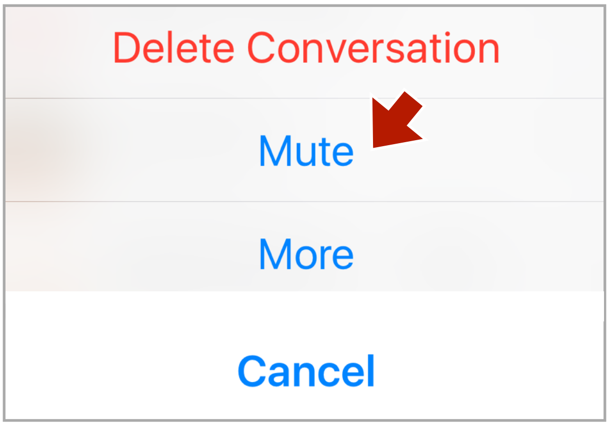
To Block A Contact

Tap and hold message from the contact you want to block in the “Home” menu - slide up. 1.Select “More” 2. Select “Block” and then slide “Block Messages” toggle to the right (Green) & click “Done” To set.

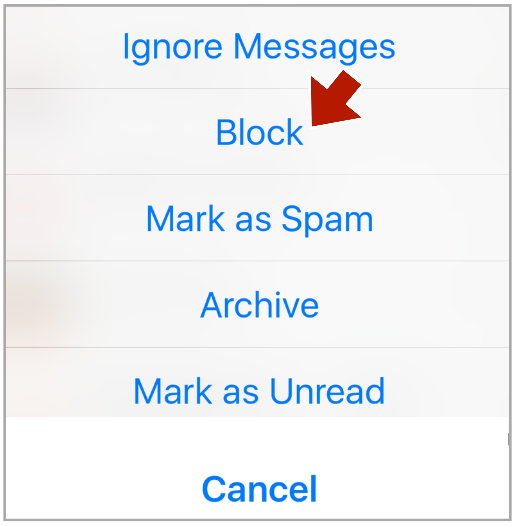
This only blocks them from messaging you. They can still be friends with you on Facebook. To block them completely also select “Block on Facebook”

You can also add them to block list in Messenger Settings. Click your profile pic to navigate to settings. Settings/People/Blocked - “Add Someone” Type in Name.

To Mute



To Block



To Delete Messages

Delete messages you don’t want, by tap and hold in “recent” “Home” view, select “Delete Conversation”.

Android Facebook Messenger Privacy: Go to “Settings” icon top right, and turn off “Synced contacts” and “location”. Scroll down to and click “Privacy” in the small print links at the bottom of settings, opens in a browser. Follow the instructions from above when in mobile Facebook privacy settings. Note: You can’t block through F.B messenger on Android use “Mark As Spam”

Note: This app is listed at 12+ on the iTunes store, but cannot be used without a Facebook Profile. So it is only available for children aged 13years and over, as per Facebook’s Terms Of Service age restrictions. Facebook Messenger Kids App had not been released for Australia as of publication. Oct 2018.

Screen Time Tips

Dealing With Distractions And Device Addiction

Moderating your own screen time is essential when you are in mid high school and beyond. Technology is integrated with every aspect of your life, but doesn't have to rule your life. Technical distractions can interfere with study, fun, sleep and relationships if you let it. Set your own timetable don't rely on your parents or carers to remind you. This will help you for life!

- Turn off unnecessary notifications on Email, Facebook, Messaging, Snapchat. Set a time to check your notifications and messaging
- Set favourites for notifications so that you only get notifications from important people, like mum or dad
- Set a schedule for online social time, including gaming and social media and messaging. Set a reminder to study, meditate, or exercise. Adjust if it doesn't work
- Reward yourself with something, for being mindful on technology, and achieving goals
- Always have a break,10 mins every hour on screens. Stretch, go for a walk, pat the dog/cat/ferret get some snacks or water. Do something other than sitting and looking closely at something
- Use an app like "Moment" or Apples New iOS12 Screentime settings to help you moderate your screen time
- Try not to multi task, focus on what you are doing or listening to, including your friends and family
- Use audio to help you relax, music or audio books or podcasts. Great for going for a walk

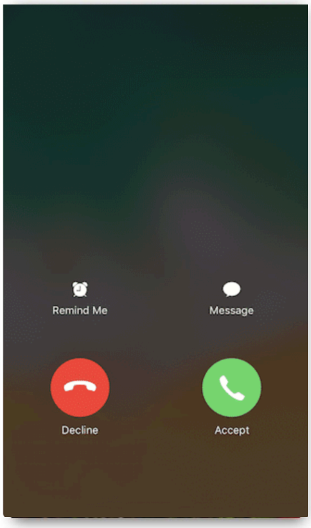
- Drastic Action! Log out of social media or delete the distracting app from your mobile

Call Message & Text Blocking On Apple Mobile

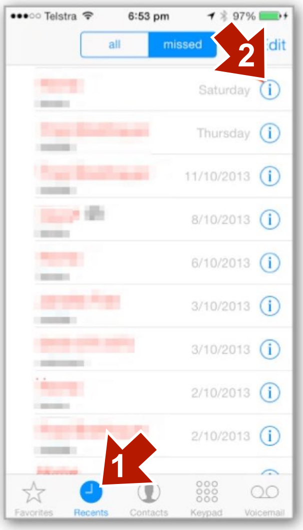
Note: You cannot block any calls from "Blocked" or "No Caller ID" calls.

How To Block:
Decline the incoming call. Then tap the "Phone" icon & your 1."Recents" calls list, select the 2. "i" for information icon, scroll down to the very bottom of the page and select 3. "Block this Caller" Then 4. "Block Contact". Do the same for messages or texts.

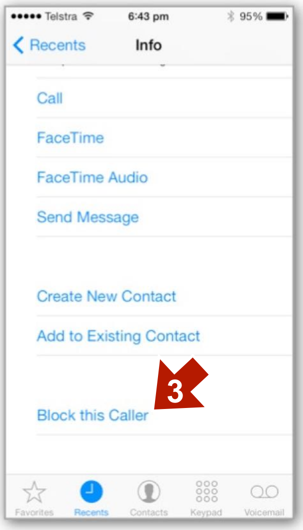
Android: Open the Phone app. Tap the 3-dot icon (top-right corner). Select "Call Settings." Select "Reject Calls." Tap the "+" button and add the numbers you want blocked.



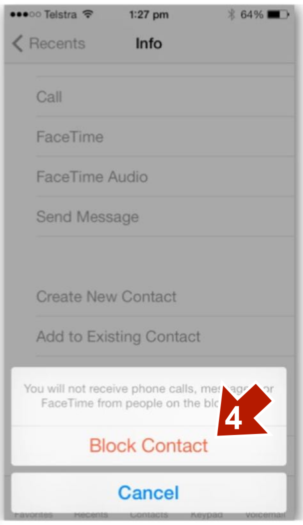
Ignore Phone Call



Click on Recents - i



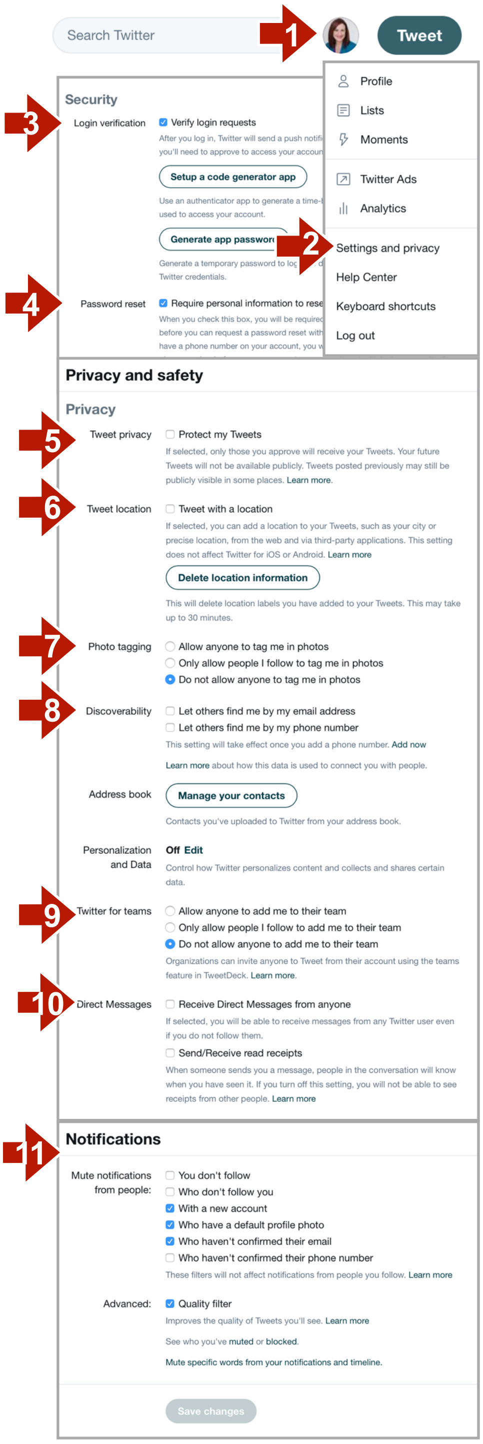
Scroll to bottom of screen



Click "Block Contact"

Security Settings For Twitter PC or Laptop Browser

1. Log into Twitter - click your profile picture to bring up settings menu.
2. Scroll down click “Settings & Privacy”.
3. Scroll down the “Account” menu and set up “Verify login requests” under “Security”. This will then send a code to your phone or Authentication app, when logging in from a new browser or device. Protects account from hackers.
4. Password Reset: Tick “Require personal information” to reset your password.
5. Go to Privacy & Safety in left column: Select “Protect My Tweets” to approve all followers, your Tweets will then be private, shown to followers only. **Note:** All tweets can be screen captured & shared.
6. Tweet Location: Un-tick “Tweet with a location” and “Delete all location information” for extra privacy.
7. Set “Photo Tagging” to “Do not allow anyone to tag me in photos”.
8. Un-tick both settings in “Discoverability” to prevent others with your email or phone number finding you on Twitter. Don’t sync address book with Twitter
9. Twitter For Teams: Disable unless you want to share a Twitter account.
10. Untick “Receive Direct Messages From Anyone”
11. Safety: “Hide sensitive Content” and “Remove blocked and muted accounts” Also click on “Notifications” side menu. Note: New unverified accounts without a profile pic can be used for spam and trolling. Set as needed and tick quality filter.



Security

Login verification ☑ Verify login requests
After you log in, Twitter will send a push notifi
you'll need to approve to access your accoun
Setup a code generator app
Use an authenticator app to generate a time-
used to access your account.
Generate app passwor
Generate a temporary password to log
Twitter credentials.

Password reset ☑ Require personal information to rese
When you check this box, you will be require
before you can request a password reset with
have a phone number on your account, you w

Privacy and safety

Privacy

Tweet privacy □ Protect my Tweets
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location □ Tweet with a location
If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. Learn more
Delete location information
This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Photo tagging ○ Allow anyone to tag me in photos
○ Only allow people I follow to tag me in photos
● Do not allow anyone to tag me in photos

Discoverability □ Let others find me by my email address
□ Let others find me by my phone number
This setting will take effect once you add a phone number. Add now
Learn more about how this data is used to connect you with people.

Address book Manage your contacts
Contacts you've uploaded to Twitter from your address book.

Personalization and Data Off Edit
Control how Twitter personalizes content and collects and shares certain data.

Twitter for teams ○ Allow anyone to add me to their team
○ Only allow people I follow to add me to their team
● Do not allow anyone to add me to their team
Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. Learn more.

Direct Messages □ Receive Direct Messages from anyone
If selected, you will be able to receive messages from any Twitter user even if you do not follow them.
□ Send/Receive read receipts
When someone sends you a message, people in the conversation will know when you have seen it. If you turn off this setting, you will not be able to see receipts from other people. Learn more

Notifications

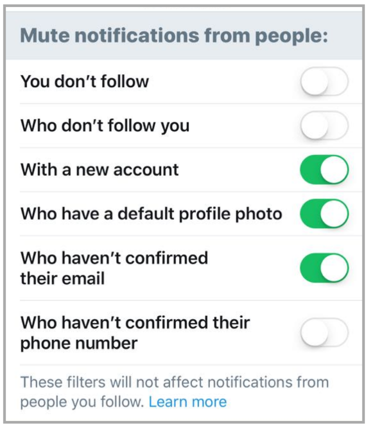
Mute notifications from people: □ You don't follow
□ Who don't follow you
☑ With a new account
☑ Who have a default profile photo
☑ Who haven't confirmed their email
□ Who haven't confirmed their phone number
These filters will not affect notifications from people you follow. Learn more

Advanced: ☑ Quality filter
Improves the quality of Tweets you'll see. Learn more
See who you've muted or blocked.
Mute specific words from your notifications and timeline.

Save changes

Twitter Mobile App

Open mobile Twitter.
1. Click on your profile pic.
2. Click “Settings and Privacy”
3. Click “Privacy and Safety” where you can protect your tweets, prevent direct messaging and through “Discoverability filter how others find you on Twitter. Don’t sync address book.
4. Scroll down and click “Notifications” Where you can set a Quality filter and also click “Advanced Filters” to Mute notifications from new or unverified accounts if you have a problem with trolls.
5. Disable precise location for safety and privacy.



Mute notifications from people:

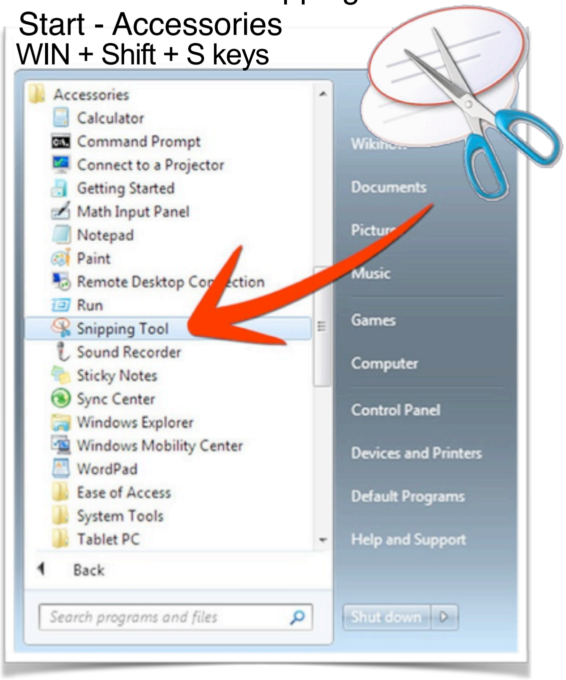
You don’t follow ○
Who don’t follow you ○
With a new account ●
Who have a default profile photo ●
Who haven’t confirmed their email ●
Who haven’t confirmed their phone number ○

These filters will not affect notifications from people you follow. Learn more

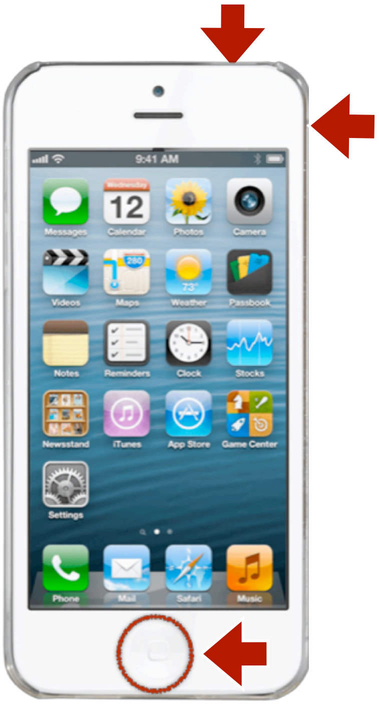
How To Screen Capture

Screen capture is a good way to keep evidence if you are abused in some way online. If someone has sent you a nasty SMS message don't delete it, save it for evidence. For comments or fake accounts (set up to bully), taking a screen capture of the incident might be the only evidence you can save to take to your school or the authorities to have some action taken, before the user that posted it deletes it.

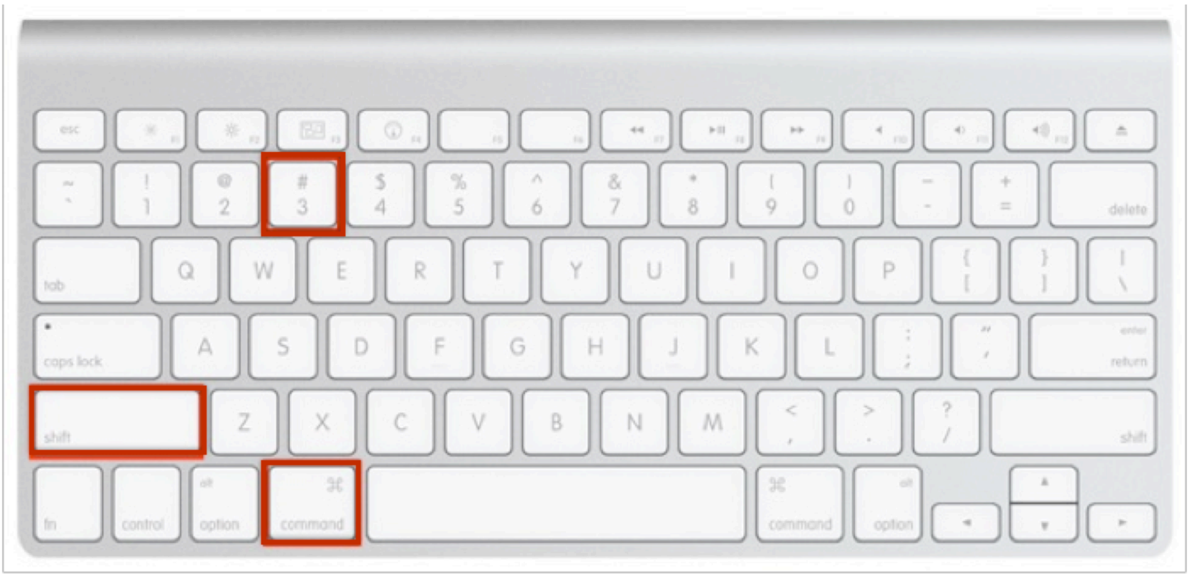
Windows: Use snipping tool
Start - Accessories
WIN + Shift + S keys



Mobile Devices: Press Home and On/Off Switch at same time. iPhone X On/Off and volume up button. Do a search online on how to screen capture, if your device is different.



Apple Macintosh: Click Command/Shift/3 (or 4 to capture partial screen.) Be sure to hold down all 3 keys one after the other.



Cyber Bullying What To Do?

Cyber Bullying is repeated cruel behaviour used to intimidate, embarrass and harass over telephone or internet connection. It can be anything from name calling to uploading embarrassing photos, impersonating accounts, posting private information or photos of you or your family online. It can also be interfering with your content in some way online without your consent and in such a way to harass.

How To Deal With Cyber Bullying:

- Block the cyber bully (find the blocking tools on each software) This cyber safety manual shows some of the blocking tools for some apps.
- Keep evidence of the bullying by copying the content and saving it before it can be deleted. If on a Windows computer take a screen shot by clicking the Prt Sc SudRq Key (usually top right 3rd key from right on any Windows Computer) or search for the “Snipping tool”. On a Mac hold down Command-Shift-4, then select an area: Take a screenshot of the abuse and save it. Use a separate camera if unable to screen shot.
- If it's by SMS don't delete the messages. You can take screen shots on most smart phones by clicking the off/ on switch and home or volume up button simultaneously for a second.
- Report the cyber bullying to the platform it has occurred on via the reporting tools and a trusted adult or person of authority.
- Do not retaliate in anyway, in person or in text. Don’t share or repost the abuse to shame the abuser.
- If the abuse is illegal (stalking, threats of violence) report it to your local police, your ISP or telephone provider. For Adult victims report serious matters to http://acorn.gov.au

How To Report:

If in Australia you can contact the Australian Government organisation eSafety.gov.au to report cyberbullying and to source further advice.

Report to school if it involves another student, or even a student from another school .

Death threats, stalking, harassment are considered illegal, and should be reported to police.

Check up on your legal rights in regard to cyber bullying from http://www.lawstuff.org.au

It is important to know that each state and territory in Australia has different laws for bullying. Lawstuff provides legal information to children and young people in Australia. Please check your State or Territory to get legal information related to Cyber bullying in your area:

Kids Helpline has 24hr phone help.
Kids Helpline - http://www.kidshelp.com.au/teens/ or phone 1800 55 1800

Bullying No Way - http://bullyingnoway.gov.au

For Cyber Crime, hacking, scams report to http://www.acorn.gov.au
To report scams go to http://www.scamwatch.gov.au sign up for their alert emails.

Sexting & Sharing Nudes - Getting Help

Sexting is sexual texting. The sending of sexual or nude pics or video via SMS or Messaging.

It is illegal to take or keep a sexually explicit or nude photo or video of a person under 18 years of age, or to share it with others, in person or via messaging.

"It's No Big Deal!"
Many teens see sexting as flirting or as a joke, and don't understand that if reported, they may be charged with possession or sharing of child abuse material. In some states a teen may end up being charged and could be listed on the sex offenders registry. Different states have different laws around under age children taking and sending nude or partially nude photos with consent. www.lawstuff.org.au has the latest laws around sexting for each state.

The other consequence of sharing or taking sexual or unclothed photos is that the photo may end up being seen by persons not originally intended. In some cases phones and online photo apps have been hacked, and images never intended to be shared, have subsequently been posted online in image forums along with names and locations of the victim. Teens who think their nude photo/video has been shared without permission should report to a trusted adult as soon as possible to stop the spread. You can also report to eSafety.gov.au to assist with removal and report to your local police. Police may not press charges against the victim for sharing a sexual image that was then shared on to others.

What Should You Do With It?

If you see or are sent an inappropriate photo/video of a person under 18years of age, you should report it, and delete it. Keeping such a photo in your possession without reporting it to the authorities may result in charges. Report it to school, if you suspect it was sent from another student. Delete it, never share it on, or screen shot it. If you view it on social media also report it to authorities.

"Revenge Porn"
The sharing of sexual or nude images of another person without their permission is known as revenge porn or image based abuse. Image based abuse is illegal and a form of harassment. Report to police or get help here https://www.esafety.gov.au/image-based-abuse

Being Asked For Nudes

If a young person under 18 years of age is asked to send a nude or sexy photo or video of themselves it is very important that the person asking for the photo is reported to a trusted adult and the police. It is important that this person is stopped and prevented from asking others for the same. Schools and the police need to be told if an underage person is being asked for rude or nude photos. It is against the law to ask for images or video of a sexual nature from a person under 18years. Be sure to block the person to prevent further contact.

How To Report:

Report to your school and the local Police. It can be up to the discretion of the police as to how the matter is handled depending on the circumstances. eSafety.gov.au can help you have pics removed if they end up on a social media platform or a website.

Each state and territory in Australia has different laws for sexting and revenge porn. Check your State or Territory to get legal information related to sexting in your area:
http://www.lawstuff.org.au

Leonie Smith "The Cyber Safety Lady" Can Help!

'Peace of mind' cyber safety solutions for students, teachers families, community groups and business.

Leonie Smith is one of Australia's leading cyber safety experts, she has helped thousands of students, parents, teachers, seniors, childcare workers business and other community organisations to learn how to navigate the internet with better safety.

Leonie is also a cyber savvy mum, she knows what it's like to be a parent with kids who are computer experts. She also knows how hard it is to be a digital parent…yes even for a cyber safety expert!

Invite "The Cyber Safety Lady" to speak at your next event!

Though based in Sydney The Cyber Safety Lady travels all over Australia. Take advantage of Leonie's expert advice and set up good habits, privacy settings and internet security now, BEFORE you or your family have a distressing experience online.

- Leonie Smith is a certified cyber safety education provider with the Australian Government Office of the eSafety Commissioner www.esafety.org.au.

From A Grateful Parent!

"Hi Leonie, without your expertise in all of this I think I would have had my 11yr old son off to the psychologist & completely stressed out myself. You have paved a safe way forward for us, & I feel a lot more in control of what my son is exposed to online" Many thanks A. Finnegan

To keep up with the latest on cyber safety and privacy you can connect with
Leonie on -

info@thecybersafetylady.com.au
www.twitter.com/LeonieGSmith
www.facebook.com/thecybersafetylady
www.thecybersafetylady.com.au
See www.youtube.com/LeonieGSmith
for some great step by step videos

“Keeping Kids Safe Online" is an up-to-date manual that gives Parents practical advice on how set up social media apps and online platforms safely

This manual is essential for all parents who want to their children to use the internet safely and with privacy.

It includes advice for cyber bullying, privacy settings for popular social media platforms, safe apps, screen time limits.

Keeping you and your family safe online.

Author Leonie Smith
www.thecybersafetylady.com.au