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

Author Leonie G. Smith

Contact Details

Leonie Smith

Website www.thecybersafetylady.com.au

First Edition May 2011

Latest Revision Feb 2020.

Note: If you see one of these QR codes (image right) through this manual, you can use a QR scanning app on your mobile device to go directly to the link. Some devices have a scanner built into the camera. Focus the camera on the Code, and click the popup to go to the linked website. The PDF eBook version of this manual has some hyper-links included, clicking the linked text, will take you directly to the website on your PC or mobile device.

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.

Leonie Smith has been endorsed by the eSafety Commissioner as a Trusted eSafety Provider www.esafety.gov.au

Leonie focuses on practical and technical solutions to help every day users of the internet use it 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.

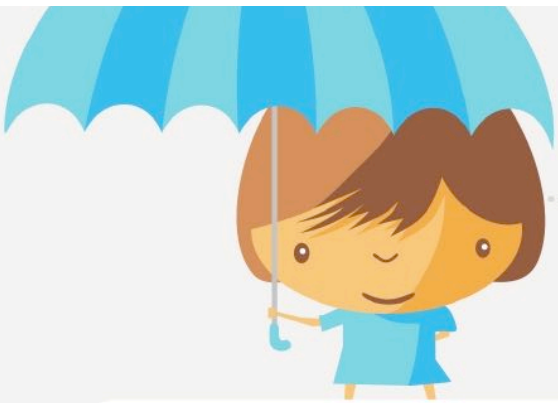
Leonie was a cyber safety ambassador for the 2013 Australian Government's "Stay Smart Online Campaign". She was a founding member and moderator for "Aussie Deaf Kids" an online support group and website for parents of hard of hearing children in 2000.

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.

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 small 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 your sensitive media.
- Upload or share pictures/videos of others online without permission.
- Take or share nude images or video. Sharing without consent is illegal.

Do:

- Be careful what you say and put on the internet. Would mum & dad approve? Can't be undone. Can be copied passed around 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 up-stander 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 docs 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, Epic.
- 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.
- Set different passwords for each account. Don't share, except with a trusted adult.

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 store 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 top right dropdown arrow/Settings & Privacy/Settings/Security&Login/Two Factor

  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

- Us an Authentication app for "Two Factor" instead of your phone number, it is more Secure. Google Authenticator, Sophos Authenticator, Microsoft Authenticator, LastPass Authenticator
- 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 scams, identity theft, hacking to www.cyber.gov.au scamwatch.gov.au. Cyber Bullying, stalking & Image based abuse eSafety.gov.au and your local police.

Phone Privacy & Safety

Do:

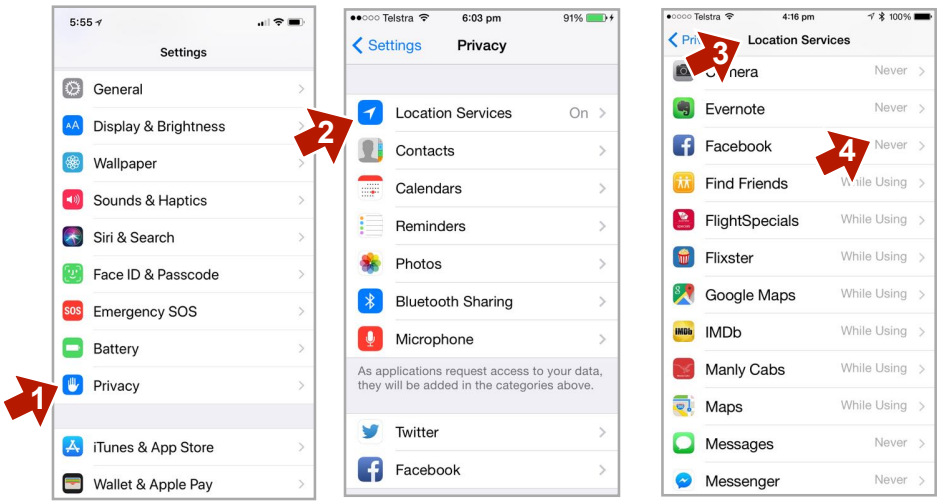
- Set screen passcode, fingerprint or face I.D to prevent unauthorised use.
- Set up “Find My Phone” on iPhone settings. Android also now has Find My Phone, there are several “Find My Phone” apps on Google Play, or use Android Device Manager App.
- For Android security settings navigate to “Settings” - “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: Sharing nude photos of people without consent is illegal.

To Disable Location Services On Apple Mobile

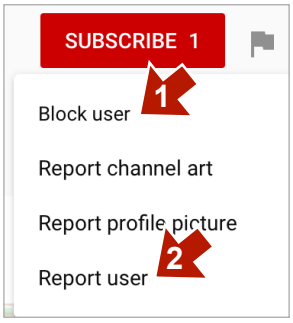


On **Android** devices, tap the “Location” option from the “Settings” menu.

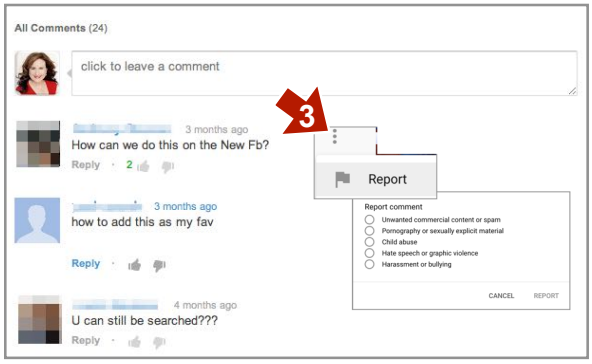
How To Block Another YouTube User

Browser Version

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 (dots) far right of the comment select “Report “and select reason from the menu.

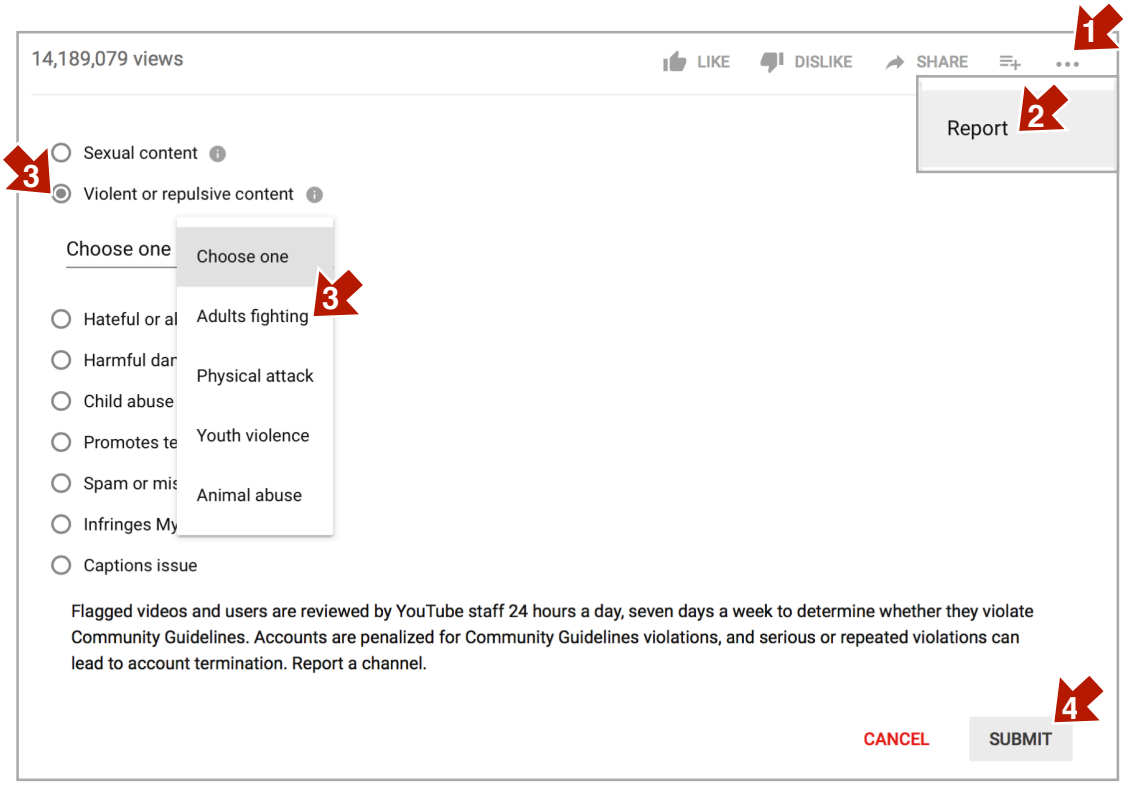


Mobile YouTube: Log in to your account. Go to their profile - click the 3 vertical dots icon, top right next to search icon to select “Block User”. Or click the 3 vertical dots next to their comment and select “Report” select the reason for the report.

Report/Flag A Video

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

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



For mobile Y.T app, click 3 vertical dots top right of video, click “Report” and select the reason

TikTok Privacy Settings

TikTok is rated 13+yrs due to adult content and public social media aspect. TikTok has important privacy settings to prevent you posting your video to the public where there are risks of bullying, adult followers and misappropriation of your content. Report any inappropriate videos or nasty comments using the report features. Only allow real friends to follow you for the safest setting. Parents: can now use "Family Pairing" (Scan QR code) to set time, content, direct message limits.

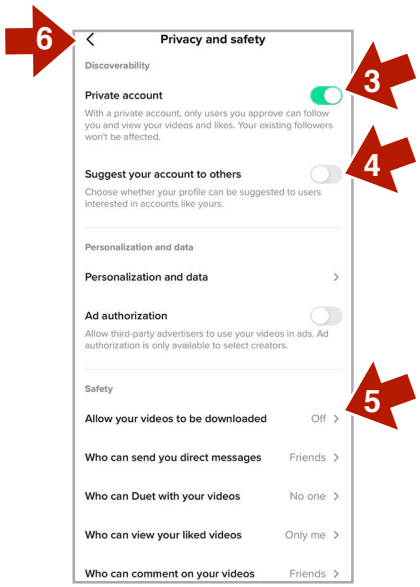
To set privacy settings:

Go to your profile icon lower right of home screen.

1. Click the settings … menu
2. Select "Privacy"
3. Enable "Private Account"
4. Disable "Suggest your account to others"
5. Downloads to off, duet, liked videos and messages to Friends.
6. Arrow back - scroll down to "Digital Wellbeing" for time limits, & to filter *some* adult content **Note:** Restricted mode doesn't block all adult content, swearing, drug/alcohol use.

Hide your location through your devices privacy settings. Settings/Privacy/Location Services/TikTok/ Never

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



Instagram Privacy Settings

Privacy Settings:

More on Instagram Safety Here: (or QR code)

1.Click lower right profile pic

2.Click on the menu bar ☰

3.Settings/Privacy/Account Privacy

4.Toggle to enable "Private Account".

5.Set "Interactions" to the safest settings. .

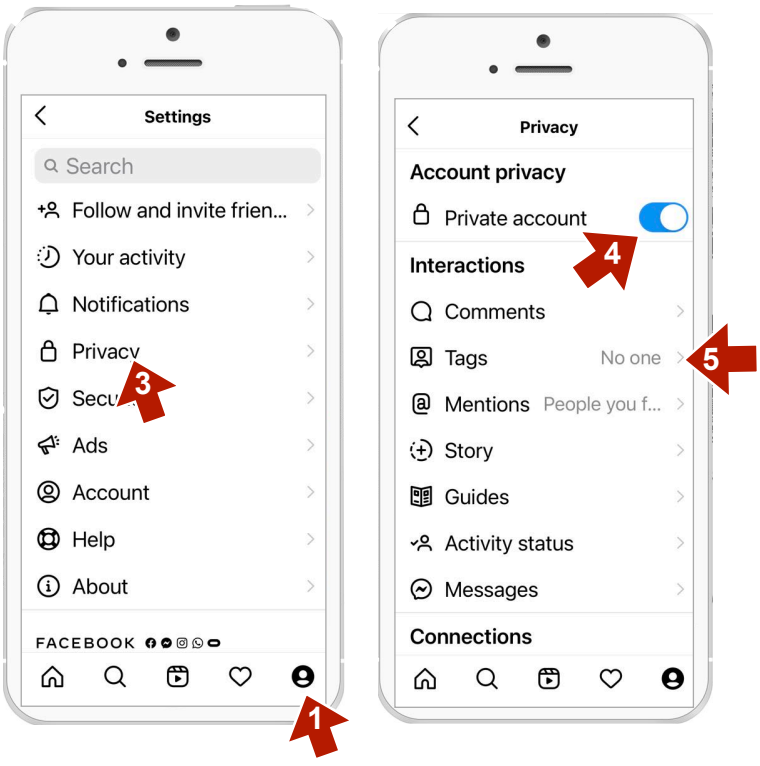
Comment Controls: Enable filters

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

Tags: Enable "Manually approve"

Click back twice to "Security" Set Two-factor Authentication to prevent hacking. Use an Authentication app like Google or Lastpass Authenticator, not a phone number.

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

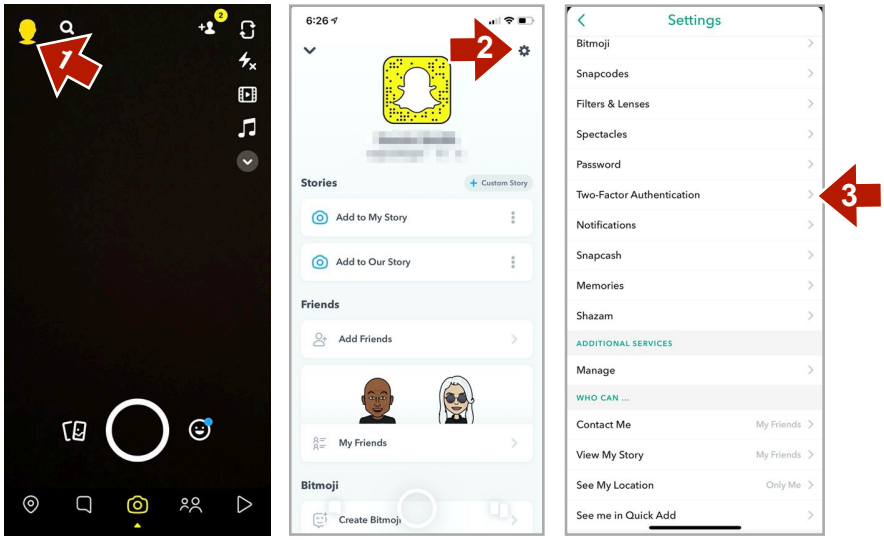


Snapchat Privacy Settings

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

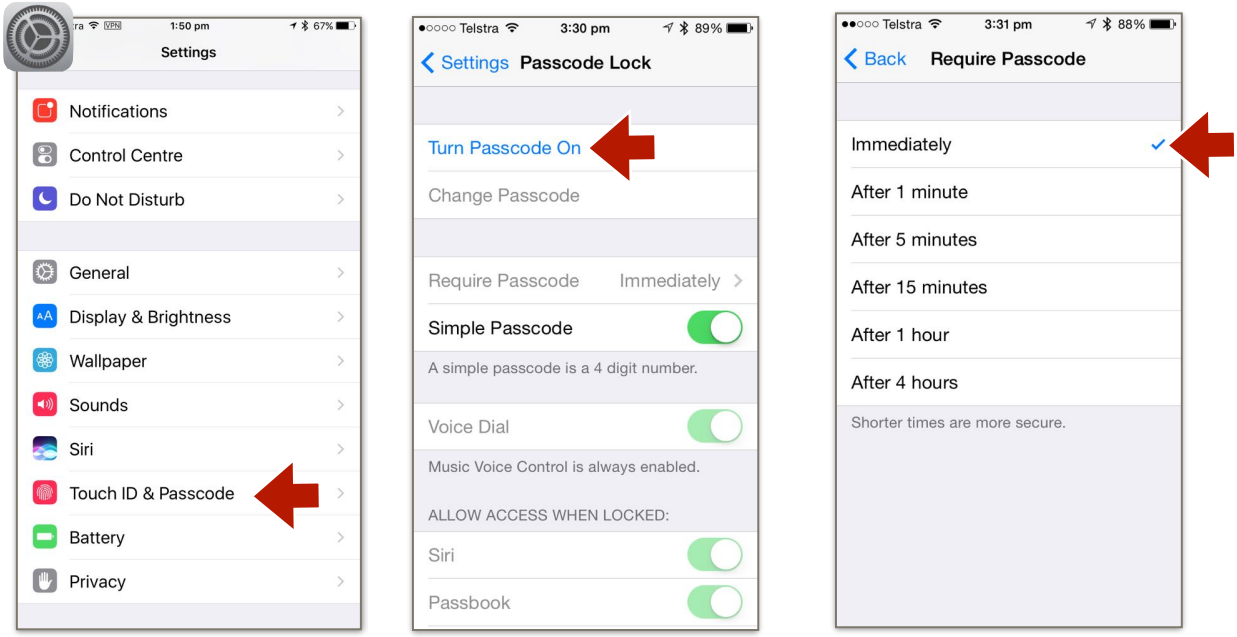
Follow settings below. More settings advice Here: or Scan QR code

1. Profile 2.Settings - Set all to “friends” or “Only Me”
3. Set up TwoFactor Authentication, to secure your account from hackers via phone number or an Authentication app like Google Authenticator.



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 and newer iPhones have Face ID & Passcode settings.



Facebook Privacy Settings

To Find Out What You Are Sharing Publicly (PC Browser settings)

1.Go to your profile (click profile pic) via www.facebook.com

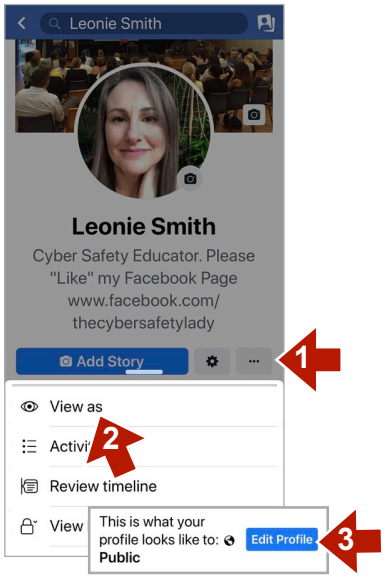
2.Click “View As” button to view your profile as a stranger would see it.

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 choose your photos with an eye to privacy.

3. 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.



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

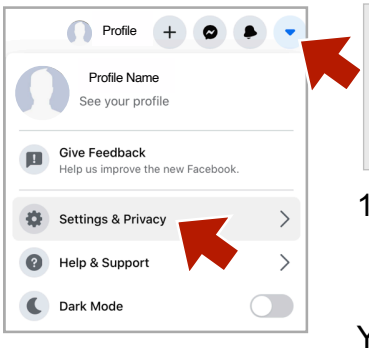
Click your profile pic to go to your profile page.

1.Click the 3 dots …
2.Click “View as” from next settings page

Scroll down to see what is being seen about you publicly.

3.Click the blue “Edit Profile” button to adjust your privacy settings to the most secure settings.

Facebook Privacy Settings P.C or Laptop

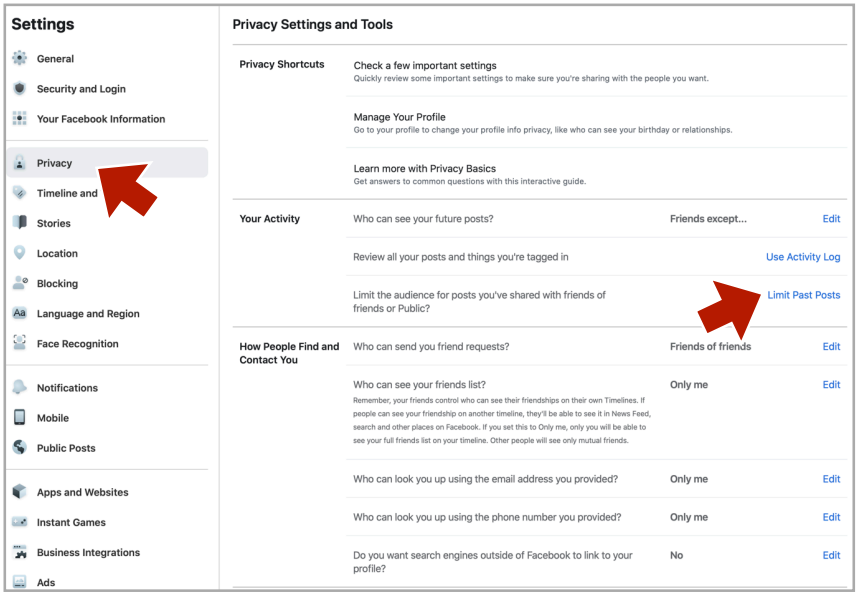


Apple Mobile F.B - click ☰ symbol lower right menu, scroll down to "Settings & Privacy" - "Settings" - "Privacy".
Android Mobile F.B - Click "More" Symbol - Scroll to "Privacy" set all as below.

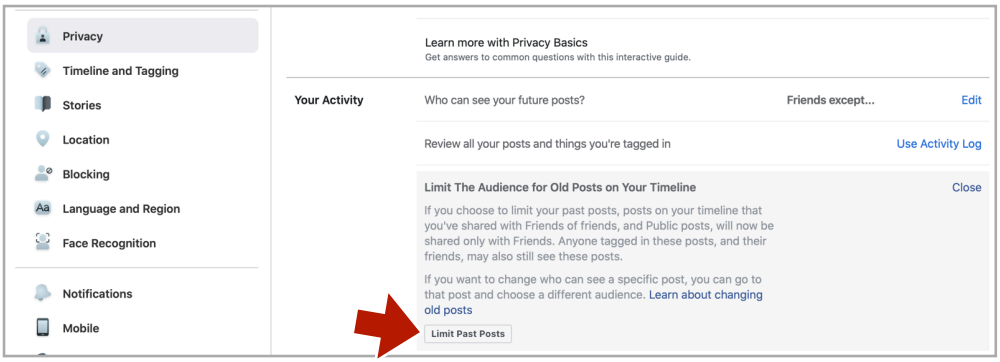
1. Go to downward arrow top right, scroll down to "Settings & Privacy" on drop down menu. In next dropdown window click "Settings". Set all to the most private options, as below.

You can use "Privacy Shortcuts" if you want a quick fix.

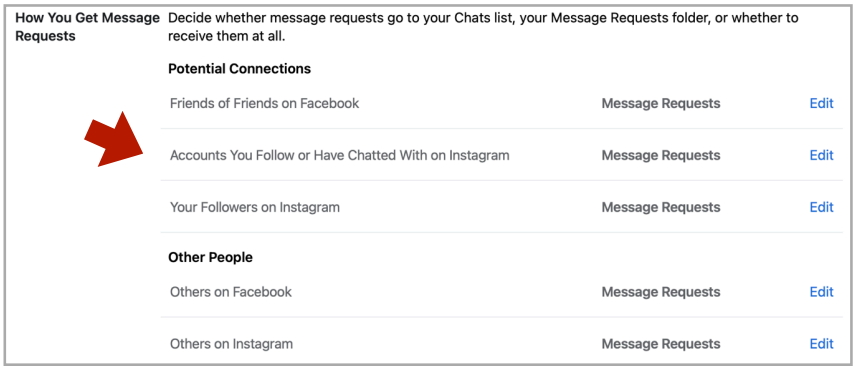
2. Set all settings as per below picture. For extra security set most to "Only Me"



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



4. Scroll down to "How You Get Message Requests" Set as secure as needed

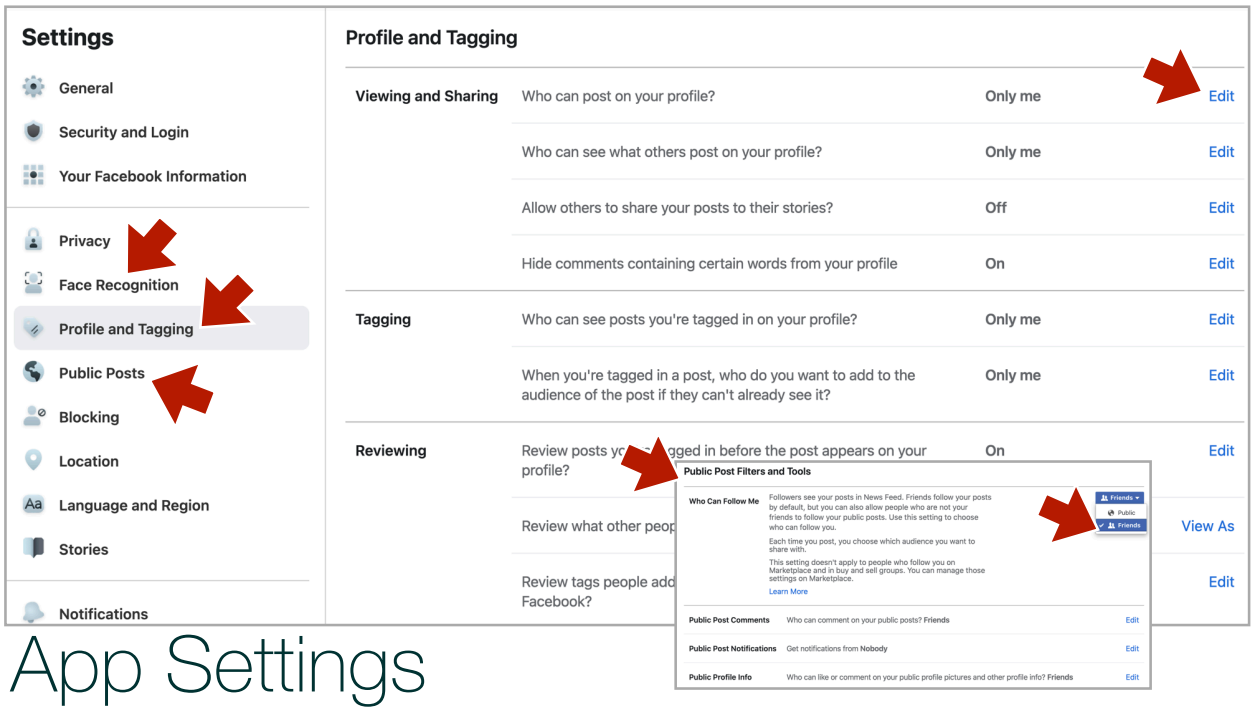


Facebook Privacy Settings

Still in “Settings” go down to “Profile and Tagging” set to “Friends” or “Only Me”.

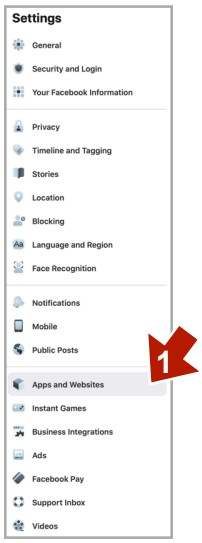
Go to Face Recognition select your preference. Do you want Facebook to scan your face in photos?

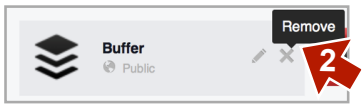
Scroll down to “Public Posts”: Set all to most private settings “Friends” not “Public”.

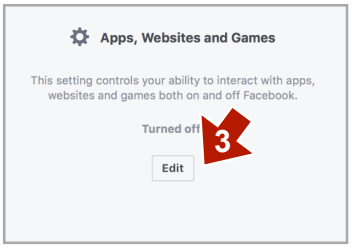


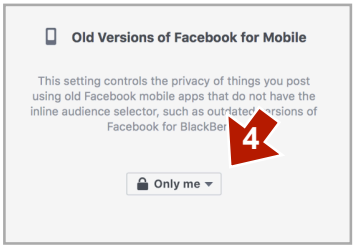
App Settings

1. Apps can share your information and preferences. Go to Settings then “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”







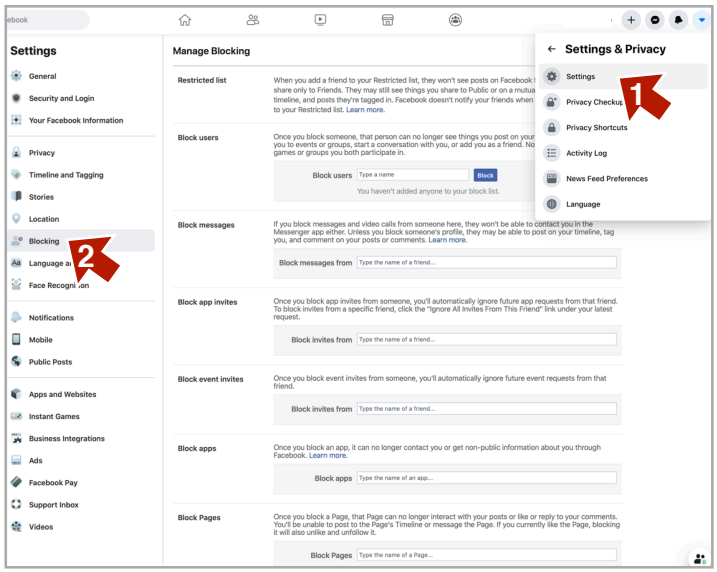


Mobile FB Go to ☰ “Menu” 1. “Settings & Privacy” - “Settings” 2. scroll to “Apps and websites” - Preferences - “Apps, websites and games” Click “Edit” next to the app and set privacy to “Only Me” or scroll down to “Remove App” 3. Turn off “Apps, websites” facility if not needed On previous page 4. Set “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 ☰ "Menu" lower right menu - scroll right down to "Settings & Privacy" "Settings" scroll down to blocking

1.



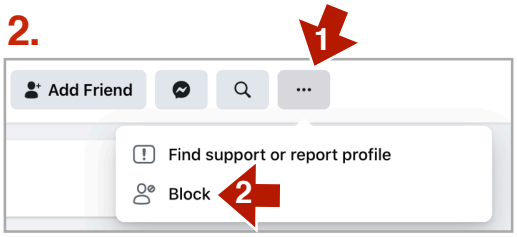
1. Blocking Apps And Users

1. Go "Privacy/Settings then "Settings"
2. Scroll to "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).

2.



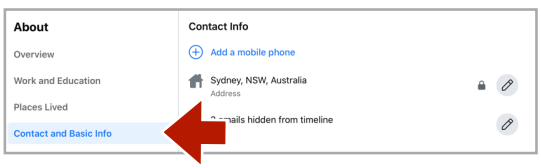
3. Hide and report comments by clicking the … menu top right of the comment. Then select "Hide Comment" or "Find Support…."

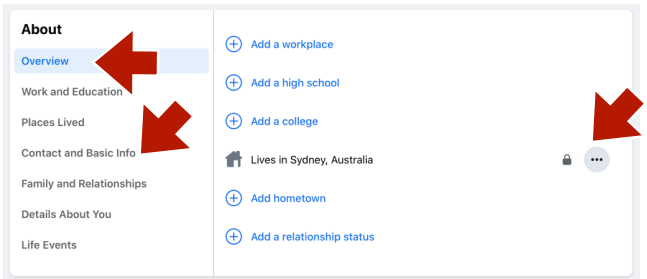
Hide Your Personal Information on Facebook

To protect all your private information from scammers and bullies select "Edit Profile" from your profile page, scroll down to edit each panel as you wish. Scroll down to "Edit your about info" to hide personal details. Set all your info in every section to "Only Me" or "Friends" by clicking each item - "Edit" and then change the visibility. (P.C or Laptop)

Mobile FB go to your profile page by clicking your profile pic. - Click the "Edit Profile" icon top right. Then Scroll down. Click the "Edit" for each section. Also "Edit Your About Info" Note: Hide your full birthdate set only the day not the year to friends or "Only Me".

Go to "Contact and Basic Info"
To hide your email address and Phone Number. It is safer to keep both to "Only Me" Safer still to delete your phone number





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.

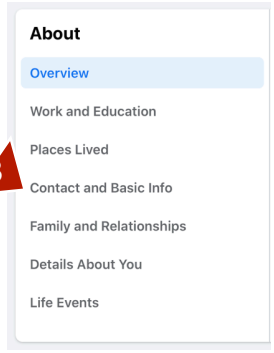
1. Go To Your Profile Page by clicking your profile pic, then to "Edit Profile" bottom right of your “Cover Picture”

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

3. Scroll down to “Contact and Basic Info” in left column

4. Scroll down to Gender and Birthdate details and edit

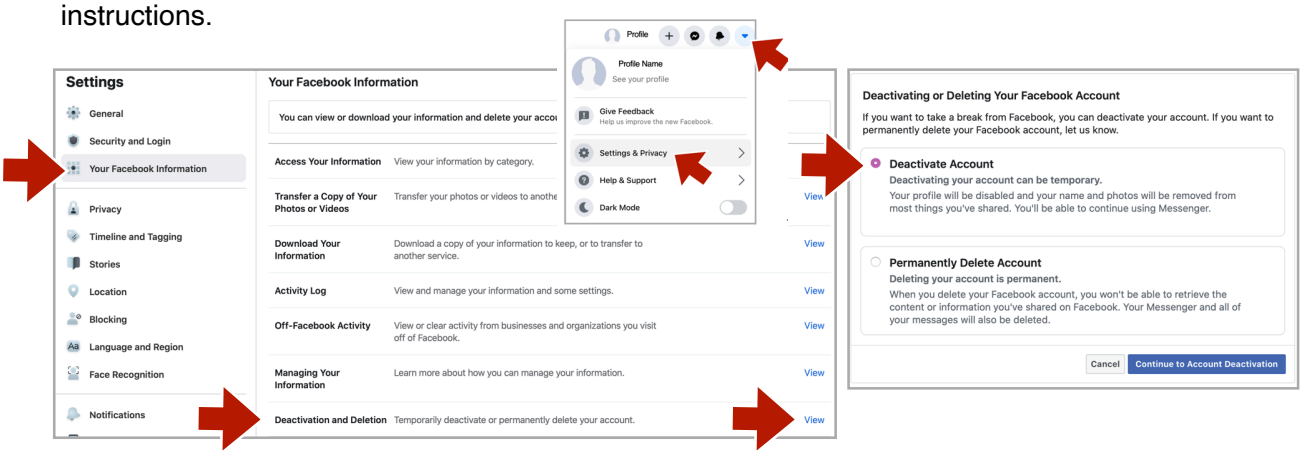
5. Set to “Friends” or “Only Me” 6. Birth year to “Only Me”.



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 or deactivate go to “Settings&Privacy” from top left dropdown arrow then “Settings” - “Your Facebook Information” scroll down to Deactivation and Deletion. Click “View” and follow instructions.

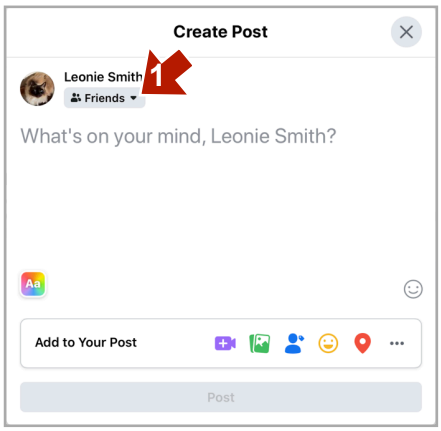


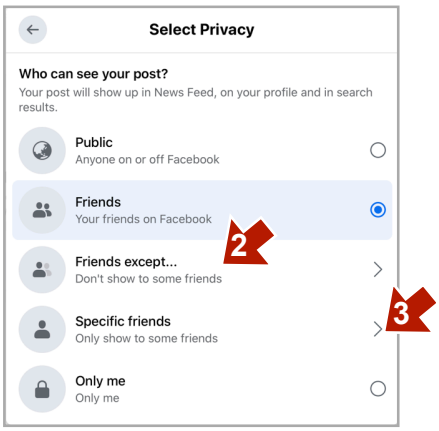
Facebook Mobile - click ☰ - Scroll down to “Settings & Privacy” then “Settings” then “Account ownership & control” then “Deactivation & Deletion” select your option and continue”

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. Specific friends.

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

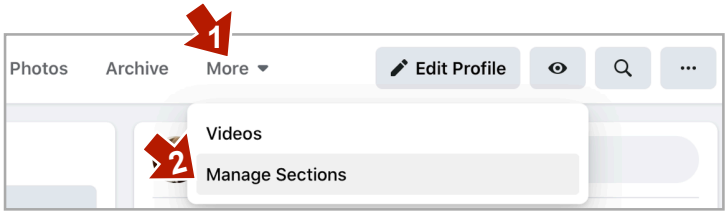
Keeping your friends list private on Facebook is more secure than leaving it public. Scammers, blackmailers or cyber bullies can use your friends list to spread scams or cyber bullying messages about you. Scammers can impersonate you and “re-friend” your real friends and send them misinformation or even blackmail you via your own friends.

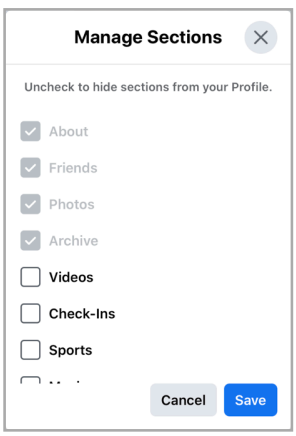
On a PC browser hide your friends list through Settings & Privacy “Settings” “Privacy” “How people find and contact you” - “Who can see your friends list?” Set to “Only Me”

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”

Hide Your Groups And Personal Preferences: Scammers and stalkers can use your private information, likes, and preferences to steal your identity or send scams to you. Hide all.

Go to your profile and Click 1. “More” & 2. “Manage Sections” this displays a list of information that can be shown 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. (Can’t be set via a mobile device. Open Facebook settings on a P.C or Laptop)

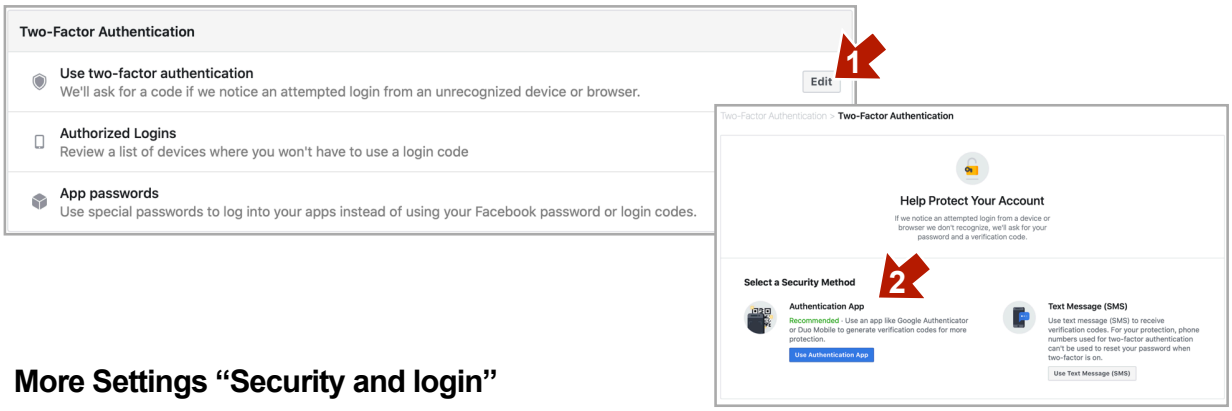




Facebook Security Settings P.C or Laptop

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 LastPass 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 & Privacy" "Settings" "Security and Login" - "Two Factor Authentication" click "Edit" and set up.



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 if you get locked out" if a hacker has changed your password and logged you out. Be sure they really are TRUSTWORTHY!

Future Proof Your Digital Footprint!

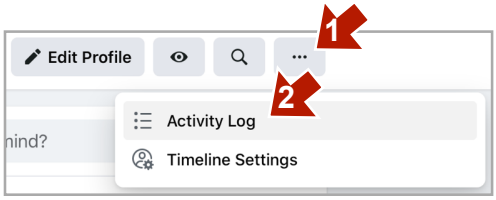
Don't leave your personal content up online.

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.

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 "Activity Log" menu located under your profile cover pic, delete your activity on F.B or set to "Only Me" On F.B mobile go to your profile click The … tab and scroll down to activity log.

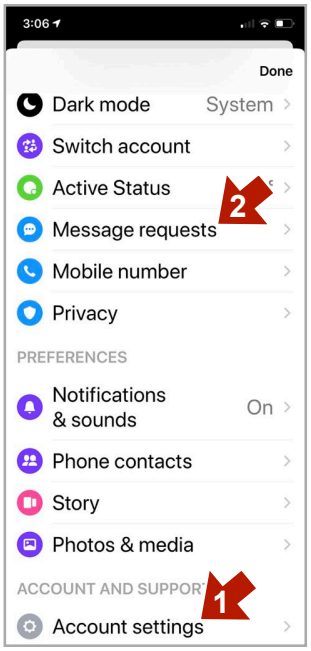


For Instagram delete posts one by one from your account. Or select photo and then click … Menu and select "Archive" or "Delete".

Facebook Messenger - Mobile

Privacy Settings

All your privacy settings for Messenger can be managed through your normal Facebook profile. See Facebook privacy settings in this manual. Go to Privacy Settings and Scroll down to “How You Get Message Requests” Set your message settings for Facebook and Instagram according to your needs.



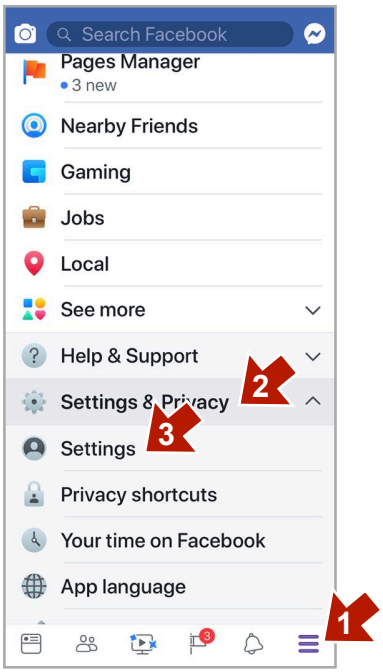
Filtering Message Contacts

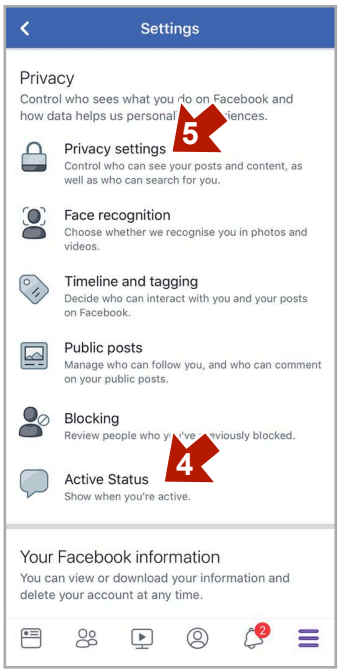
You can no longer filter who contacts you on Facebook Messenger. Anyone who has Facebook Messenger can now contact you on your Facebook Messenger app by sending a Facebook Message request. You can block them on messenger however.

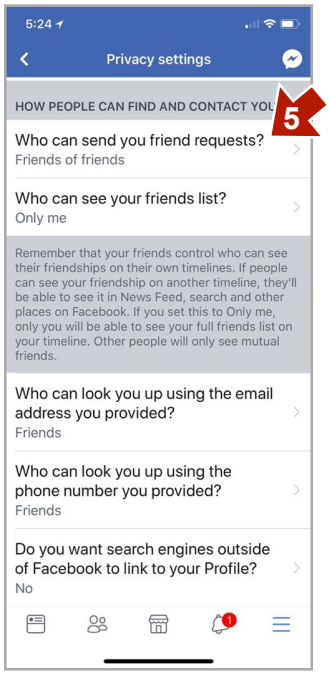
Non friends messages will show up in the “Message requests tab”. Tap on your profile pic after opening F.B Messenger, scroll down to “Message requests”
Block or accept as needed. “Account Settings” are the same as the main Facebook Settings for privacy and security”

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 through 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.







Facebook Messenger - Blocking - Muting

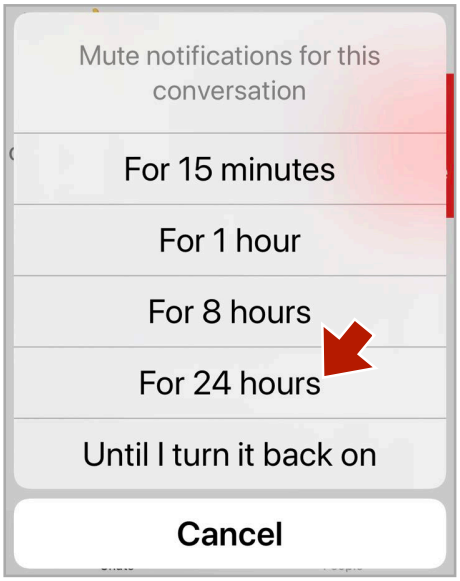
You can block a contact directly through Facebook Messenger and you can "ignore" a conversation if you no longer want notifications from that chat.

To Mute or Block

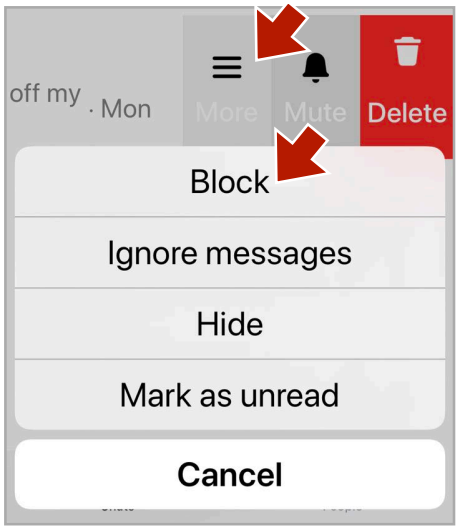
1. Go to your Messenger "Chats" messages list (Click speech bubble icon lower left).
2. Tap & slide the message to the left, select your options from the ☰ "More" menu.
3. Mute notifications temporarily by clicking the "Bell" icon from the slide menu.
4. Delete messages from the slide left menu.

Blocking a profile on messenger only blocks them from messaging you. They can still be friends with you on Facebook. To block them completely also select the "Block on Facebook" option

To Mute



To Block



Android Facebook Messenger: Tap and hold message to bring up options to archive, mark as spam, delete, or manage. **To Block:** Tap the profile pic of the person you want to block to go to their profile then click the information icon top right of their profile to scroll to the bottom to select "Block"

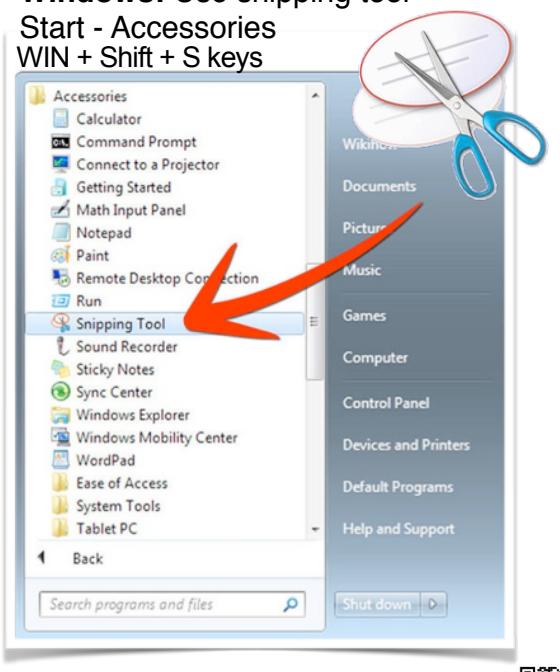
Note: This app is listed at 12+ on the iTunes store, but cannot be used without a Facebook Profile. So it is only available for children aged 13years and over, as per Facebook's Terms Of Service age restrictions. Facebook Messenger Kids App is an alternative for children aged 4 - 12yrs. It includes monitoring for parents. See the reviews for this app on the iTunes Store, or on www.commonsensemedia.org

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.

Alt-Windows Key-Print Screen

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



[See More Here About Windows Screen Capture]

Mobile Devices: Press Home and On/Off Switch at same time. iPhone X upwards 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.

[See More Here About Apple Screen Capture]

Cyber Bullying What To Do?

Cyber Bullying is repeated cruel behaviour used to intimidate, embarrass and harass over the internet. 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:

- 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.
- Block the cyber bully (find the blocking tools on each software) This cyber safety manual shows some of the blocking tools for some apps.
- If via text 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 publicly.
- If the abuse is illegal (stalking, threats of violence) report it to your local police, your internet provider. For Adult victims report serious matters to https://www.cyber.gov.au

How To Report:

If in Australia you can contact the Australian Government organisation eSafety.gov.au to report cyberbullying for under 18yrs and to get 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 from Youth Law Australia https://yla.org.au

It is important to know that each state and territory in Australia has different laws for bullying. YLA 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 24/7 phone and text 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 https://www.cyber.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.

Only 5% of teens have sent a nude or nearly nude image.
Nearly 1 in 3 aged 14-17 had some experience with sexting
52% of nudes are sent by strangers. eSafety Commissioner "YOUNG PEOPLE AND SEXTING—ATTITUDES AND BEHAVIOURS " 2017

There are different sexting laws in each country and state. In some states it is illegal for children under 18 years to take and share nudes. Check on https://yla.org.au

Many teens see sexting as flirting or as a joke, and don't understand that if reported 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. https://yla.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 and on social media 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.

What Should You Do With It?

If you see or are sent an inappropriate photo/video of a person under 18years of age, you have to 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 save it. If you view it on social media also report it to authorities.

"Image Based Abuse"
The sharing of sexual or nude images of another person without their permission was previously known as revenge porn, or more accurately, 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 (Australia)

Sexting can be a crime if it is non consenting or there is a large age gap between sharers. If you're under 18 and you've sent a nude picture of yourself, you will NOT necessarily get charged by police. In Australia in NSW and Vic there are new laws around sexting.

In some states and countries nudes can be illegal if they are:
Produced by a minor, asked for by an adult, more than 2 years in age difference or shared on without consent.

Check the law at www.yla.org.au (Australia)
Get help to remove images at www.eSafety.gov.au (Australia)
Report to local police as soon as possible.
Don't copy or screenshot or save a copy of evidence

Leonie Smith "The Cyber Safety Lady" Can Help!

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!

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.

Virtual Presentations

Leonie is now presenting her talks virtually.
See more about her presentations here: https://thecybersafetylady.com.au

Personal Consultations On Cyber Safety

Leonie also provides parents with personal consultations to help parents set up safer environments on digital tech. https://thecybersafetylady.com.au/services-4/

- Parental Controls
- Screentime timetables
- Information about gaming and apps
- Supervising children 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
"Digital Families Podcast" https://anchor.fm/leonie-smith0

“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