A guide to Staying Safe on Meta

IN COLLABORATION WITH META

WESNET
The Women's Services Network

Meta

META'S SAFETY COMMITMENT

Around 3 billion people use Facebook and Instagram every day to share their life experiences, connect with loved ones, make new friends and build communities.

Meta recognises how important it is for Facebook and Instagram to be places where people feel safe and empowered to communicate. They take their role seriously in keeping abuse off Meta's services, so they have developed community standards for what is acceptable on Facebook and Instagram.

These community standards are based on feedback from people and expert advice from those in the technology, public safety and human rights arenas. To ensure that everyone feels heard and valued, Meta takes great care to create community standards that include different views and beliefs, especially from people and communities that might otherwise be overlooked or marginalised.

ACKNOWLEDGEMENT

We acknowledge Australian Aboriginal and Torres Strait Islander peoples as the traditional custodians of the lands where we live, learn and work.

We pay our respects to elders past and present.

WESNET'S WORK TO END TECHNOLOGY ABUSE AND GENDER-BASED VIOLENCE

Established in 1992, Wesnet is the national peak body for specialist women's domestic and family violence services across Australia and a leading NGO expert on the intersection of technology and violence against women. They also play an important role in bringing the voice of survivors and grass-roots services to national policy and legislative reform.

Wesnet represents around 350 specialist women's services across Australia that provide direct relief to women and children affected by domestic and family violence (DFV) and other forms of gender-based violence. Wesnet upskills members through advanced training and education on issues such as technology-facilitated abuse (TFA), providing frontline practitioners with specialist training and resources to assist them in providing the best care and support for the thousands of women experiencing DFV and other forms of gender-based violence.

Learn more about Wesnet and its programs at wesnet.org.au.

Meta has partnered with Wesnet to bring you this updated Guide to Staying Safe on Meta. It is designed specifically for those who are experiencing technology abuse and other forms of gender-based violence.

Facebook and Instagram users are invited to use this guide to make the most of their Meta experience by using safety and reporting features built into Facebook and Instagram. Learn how to maximise your privacy and security settings and set them up for your own needs. This guide will also help you know what to do if you are experiencing abuse from others.

Gender-based violence and technology

Gender-based violence is any form of violence or abuse against a person or group of people because of biassed or harmful beliefs about gender.

Although women and girls in all their diversity can experience gender-based violence, groups that experience other forms of inequality and discrimination are at greater risk of experiencing multiple forms of abuse online.

Domestic and family violence is one of the most common forms of abuse experienced by women in Australia. In today's digital world, abusers often choose to misuse technology in a variety of ways to harass, harm, stalk or otherwise control victims. When abusers weaponise technology such as social media platforms, women are often forced to stop using apps like Facebook and Instagram. These platforms are vital networks for staying connected to friends, family and communities.

How to use this guide

Social media is creating a more open and connected world, enabling people to share their most memorable and meaningful experiences with their communities. Everyone should feel empowered to connect with others and freely share their experiences online without fearing for their safety.

Unfortunately, some people use technology as a tool for abuse and may use Facebook or Instagram as their chosen instrument. Violence against women and other gender-based violence has become more prevalent in online spaces, and Meta is taking these challenges very seriously by implementing and improving features that aim to bolster the safety and privacy of the users of their platforms while holding abusers accountable for their actions.

This guide aims to advise survivors of gender-based violence on how to use Facebook and Instagram to strengthen connections with family and friends and empower them to express their authentic self online while maintaining a strong sense of safety and privacy. In response to the ever-changing nature of technology, this guide will provide direction on where to access step-by-step instructions and resources to improve your online interactions.

Remember! Technology isn't the problem; the abuse is! We shouldn't expect survivors to 'get off Facebook' or 'delete Instagram', as that does not hold the perpetrator accountable and further isolates the survivor. This guide helps those experiencing abuse turn the tables on those who misuse Meta platforms by outlining available tools, skills, and reporting mechanisms.

If you need more help, please check out the resources page at the end of this booklet.

How to find the Help Centres

Meta's Help Centres are designed as **virtual help desks** where users can **ask questions, troubleshoot issues, and access support**. There are help centres for Meta, Facebook, and Instagram.

On a web browser, you can access each Help Centre by searching:
'**Meta Help Centre**'
'**Facebook Help Centre**'
'**Instagram Help Centre**'

You can also access Facebook and Instagram's Help Centre through the application.

INSTAGRAM

Go to your account > select the hamburger icon in top right corner > help > select **Help Centre**

FACEBOOK

Go to your account > select the menu icon > help and support > select **Help Centre**

Table of contents

Meta Community Standards and Guidelines

Meta is committed to protecting your voice and fostering a safe and supportive environment to help you connect and share safely.

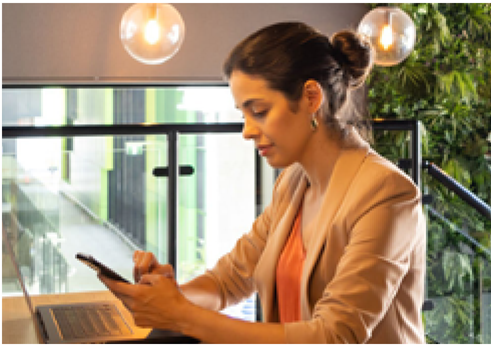
Meta works tirelessly to ensure Facebook and Instagram continue to be safe spaces for inspiration and expression.

META STRENGTHENS THIS COMMUNITY BY:

- Investing in safety. Like this guide!
- Identifying and responding to inappropriate content
- Blocking fake accounts and filtering spam
- Empowering the user to take control of their online experience
- Providing resources, tools and advice to prevent bullying and offensive behaviour
- Removing hate speech, harassment, threats of violence and other content that has the potential to silence others or cause harm.

To help foster this community, it is paramount that everyone follows and respects Meta's Community Standards and Guidelines. As a user of Instagram and Facebook, you are responsible for upholding community guidelines to contribute to a safe and open environment for everyone!

It's important to understand the community standards so you aren't tempted to breach them yourself and equip you with the skills to recognise when someone else's behaviour is not ok.



INSTAGRAM COMMUNITY GUIDELINES

- Share only photos that you have taken or have the right to share. Don't share photos, videos or digitally created content that shows sexual intercourse, genitals and close-up or fully nude buttocks.
- Don't share images or videos of nude or partially nude children. Instagram has zero tolerance when it comes to sharing sexual content involving minors or threatening to post intimate images of others.
- Don't impersonate others or create accounts to violate the guidelines or mislead others. Respect other members of the Instagram community.
- Follow the Law: Serious threats of harm to public and personal safety aren't allowed.
- Maintain our supportive environment by not glorifying self-injury.

MORE INFO

Go to help.instagram.com

FACEBOOK COMMUNITY STANDARDS

- Violence and criminal behaviour - like coordinating harm or fraud and deception is never permitted.
- Harmful actions, like child and adult sexual exploitation, bullying and harassment and privacy violations are against community standards and never allowed.
- Hate speech, fake accounts, inauthentic behaviour, misinformation and spam are largely not allowed.

MORE INFO

Go to: transparency.Meta.com/en-gb/policies/community-standards

Customising your settings /profile/experience

Unfortunately social media and messaging apps can be misused by abusers to perpetrate family violence in Australia.

Meta has a number of safety features that can help you control your online experience.

It's important to choose the right tool for your situation. Some users may want to permanently remove or block a profile, while others may need a more temporary solution. This guide can help you decide which tool is best for your situation.

Collectively, these tools help in creating a safer online environment, giving you the power to manage your social media platforms effectively.

TOOLS INCLUDE:

- Muting (Instagram) and Snoozing (Facebook)
- Blocking and unfollowing /unfriending
- Taking a break from profiles
- Setting healthy limitations

MORE INFO

If you require step-by-step instructions or require further information, please go to the corresponding help centre, and type the desired tool name in the search bar.

Search...

Control what you see

These tools are designed to create a safe space by providing more control over what you see.

MUTING & SNOOZING

INSTAGRAM

You can mute someone's profile to stop seeing their posts, stories, or messages without unfollowing them. The user won't know you've muted them, and you can easily unmute them later.

FACEBOOK

The snooze feature allows you to temporarily stop seeing posts from specific people, pages, or groups for 30 days. This is useful for taking a break from certain content without permanently altering your feed. You can undo the snooze at any time.

CONTENT MODERATION & FILTERING

INSTAGRAM

Tools are available to filter out offensive comments automatically or based on specific keywords. The 'Hide Offensive Comments' feature uses AI to detect and hide comments that may be considered offensive or inappropriate. You can also use the 'Hidden Words' feature to create a list of words, phrases, or emojis you want to hide in your comments by adding or removing items from the list.

FACEBOOK

The 'Keyword Snooze' feature allows you to temporarily hide posts containing specific words or phrases, helping to customise your feed and reduce exposure to unwanted, offensive or inappropriate content.

Control who contacts you

These tools are designed to help you control who contacts you and manage unwanted interactions.

BLOCKING & UNFRIENDING/ UNFOLLOWING

INSTAGRAM

If someone shares content that doesn't sit right with you on Instagram, you can unfollow, block or remove them. To unfollow someone, simply go to the profile of the person you'd like to unfollow and tap 'Unfollow.' You can also opt to 'Remove' a follower and prevent them from being able to interact with your profile. You can block someone multiple ways without notifying them, preventing them from contacting you or searching for your profile. This blocks their entire account including any existing or new accounts. If they have multiple accounts, you need to block each one individually.

FACEBOOK

You can block other accounts to prevent them from viewing your profile, contacting you or tagging you. You can also reduce unwanted interactions without notifying the other person by unfriending or unfollowing. Remember that they may still be able to see any activity you post publicly.

TIP:

Although people you unfollow, unfriend or remove won't be notified, they may be able to work it out when they can no longer see what you're up to.

RESTRICT & LIMITS

INSTAGRAM

The 'Restrict' tool helps you to manage interactions with others without blocking them completely. When you 'Restrict' someone, the comments and messages they share are only visible to themselves and they will not be able to see when you are online or if you've read their messages. The 'Limits' tool on Instagram allows you to temporarily limit interaction from certain accounts, including new followers or recent followers, for a set period of time, helping to reduce unwanted interactions.

TIP:

When deciding what tool is right for you, it is important to consider abusive people may persistently try to gather information about a survivor. If unfollowed or unfriended, they could try to reconnect or create fake accounts to sneak back into a connection.

Survivors should be careful when timing their actions. Immediate action might work for some but could put others at risk. Abusers use monitoring to maintain power and control, so limiting access may result in them using other methods of control or an increase in their abusive behaviour.

Control what you experience

These tools are designed to help you control your social media experience, promoting healthier interactions with the platforms. By establishing healthy boundaries, survivors have the opportunity to strengthen existing connections within their support network to prioritise their well-being.

TAKE A BREAK

FACEBOOK

You can always take a break from seeing posts from specific profiles. When you take a break, their posts, and any posts they are tagged in, won't appear in your feed. The selected account will be added to your restricted list and will only see posts you tag them in or share publicly (outside your friends).

TIP:

Monitoring time spent on social media and setting daily time limits can also help survivors detect if an abuser is accessing their accounts through their devices.

TIME LIMITS

INSTAGRAM

Instagram makes it easy to see how much time you spend on Instagram or turn on reminders to take breaks while on a scroll roll.

FACEBOOK

Facebook provides estimates of the average time per day, time over the past seven days, and total time spent on the app on a specific device. But it's important to remember that these durations are only estimates.

Control what you share

These tools and privacy settings help you to manage what you share, allowing you to control who can see your content and personal information.

PUBLIC & PRIVATE ACCOUNTS

Strengthen your account security by considering whether you want a public or private account.

The process of setting up an account is different across Instagram and Facebook. Instagram allows any name and multiple accounts, while Facebook requires a recognised name to prevent impersonation or scams. Meta has made it easier for users to add more information to their name choice, acknowledging that using an authentic name may be a challenge for some.

TIP:

Online privacy is not just a preference, it may become a necessity for physical and emotional well-being. Meta understands this and provides robust privacy options on Facebook and Instagram.

TIP:

Survivors can hide their activities and connections from their abuser on social media by being strategic about what they share. They can avoid engaging with individuals or groups on the platform and use a generic profile picture or no profile photo. It's harder for an abusive person to contact a survivor through social media if they can't find the survivor's profile.

INSTAGRAM

If you leave your Instagram account on default settings, it will be visible to everyone as a public account. If you need to limit who can see your account you can set your Instagram account to private, then only your approved followers can see your posts. However, your profile details, such as profile picture, account name and bio are viewable by anyone.

FACEBOOK

Your public Facebook profile includes your name, profile photo, cover photo, friend networks, gender, username, and user ID. However, in the account settings, you can control who can search and send friend requests to your profile. You can also manage who can see your friends lists with different preferences, such as public or private. You also have control over if you want search engines to link your profile to their results.

MORE INFO

Search facebook.com/help

🔍 Friending

LOCK YOUR PROFILE

In Australia, there is also a feature available to Lock your profile. When this is turned on then only friends can see the photos, posts and stories on your profile. Only friends can see the full resolution profile picture and cover photo. People can still search for you and send you friend requests.

TIP:
Locking your profile can be useful if you have blocked or unfriended an abuser and you don't want them to be able to see your photos or copy them.

TIP:
Sometimes abusers will target friends and family of survivors to try and humiliate, shame or isolate the victim-survivor. Hiding your friend's list can help prevent the abuser from contacting your friends and family. This is particularly important if you are worried about being impersonated by the abuser.

TAGGING & VISIBILITY

Tagging on social media is a way for people to link other people's account to their own posts and activities. Being tagged by someone can also reveal that person's activities, location, and friendships. It could potentially provide the current location status of the survivor who might need to be staying hidden for safety reasons. See the advice below about how to control who tags you.

TIP:
Survivors' privacy can be at risk due to online tagging and posting of content, even if they manage their accounts. Friends of survivors may also have public accounts or be connected to the abuser on social media platforms.

INSTAGRAM

Tagged photos and videos may appear on your profile, but who can see them depends on your visibility settings. Public posts allow anyone to view them, while private posts limit the viewership to your followers only.

Control your tagging settings through account activity and settings on your profile. Click Tags and mentions to manage your preferences.

FACEBOOK

Manage your Facebook Timeline by adjusting your privacy settings to control who can tag your profile. Use timeline review to decide who can view and post on your Timeline. You can control your Facebook Timeline by approving tags, limiting your audience, and disabling tag suggestions. Removing tags won't delete the post or photo.

INTERACTIONS ONLINE

Interactions online not only include what you post, but who you connect with, when you like or comment on a post or in a group, and when you share or repost anything on your feed or timeline.

When you are responding, replying or commenting on someone else's post, story, reel, then the audience settings are determined by the original poster. For example, if you reply to a post that has an audience set to public, then your comment will also be public.

TIP:

Everyone, including survivors, need to be careful when sharing personal information with strangers or unfamiliar profiles. Personal identifying information includes details such as home address, age, connections with friends and family, preferred cafes, or activities and events. Always consider who may see what you are interacting with.

INSTAGRAM

Determining who can see your interactions will depend on whether your account is public or private.

If your account is public, anyone can like or comment on your photos or videos and see what photos you have liked or commented on and stories you have shared. If your account is private, only approved followers can see this content.

FACEBOOK

To check what others can see on your Facebook profile, use the "View As" feature. Click on your profile picture, then select "View As" below your name.

TIP:

Survivors can limit an abusive person's access by hiding posts or placing them on a Restricted List.

CHOOSE YOUR AUDIENCE

Both Facebook and Instagram enable you to set who sees what you share on your own account. You can share it to everyone on the platform, or you can share it to just one or a few people.

☆ **TIP:**

When you interact with public media, such as public posts, it may reach a wider audience, including parents, teachers, colleagues, and employers.

INSTAGRAM

Instagram offers useful features that allow you to publish and share with specific audiences. To share an Instagram post with specific people on Instagram, click the direct icon (looks like an arrow). You can choose up to 15 people to share with

Another good option is to create your list of Close Friends so that you can share to a specific group of trusted followers or friends when you post or share.

INSTRUCTIONS

Search help.instagram.com

🔍 Close friends

FACEBOOK

To control who sees your social media posts, adjust your privacy settings to select a specific audience. Choose from either, public, friends, friends except (select accounts you wish to exclude), specific friends and only me (self-explanatory!).

You can use lists to limit who can see a post or restrict its visibility to a select group of friends, for example; close friends, acquaintances or restricted. You can create custom lists, such as family members or co-workers.

You can also adjust your audience on posts you have already made.

MORE INFO

Search facebook.com/help

🔍 Audience and list

Location Sharing and Location Tagging

IF YOU NEED TO KEEP YOUR LOCATION PRIVATE

Sometimes, location privacy is critical to a survivor's safety. Phones and apps can share locations with other people, sometimes without our knowledge. You can also completely turn off location through your phone settings.

For iPhones, go into your phone settings, tap Privacy & Security, then tap Location Services, scroll to Facebook/Instagram and select either 'never' or 'while using the app'.

For Androids, go to your phone settings, tap Location, then select either Instagram/Facebook and determine if you want your location on or off.

For more information on location sharing and location tagging, please review the resources page at the end of this guide.

TIP:

With today's technology, there are now other ways that your location might be given away. For example, a reverse image search on a picture you post in a new location might be able to connect it to a particular landmark or building e.g. a picture of the Harbour Bridge.

So be selective about the photos you post online if you are trying to keep your current location secret.

Securing your account

Meta offers many tools and services to ensure your account is secure and that you are the only person able to access and manage it. By using the built-in features, you'll have more control over your social media experience, strengthening both security and privacy.

TOP THREE TIPS FOR SECURING YOUR ACCOUNTS

1. STRONG PASSWORDS

For both Instagram and Facebook, ensure you have a strong password that is different to your other accounts and known only to you. Change your password regularly and immediately if you receive a prompt. Do not store your password in public spaces or share it with anyone.

For more information, please access Wesnet's Password Safety Handout at techsafety.org.au/passwords.

2. TWO-FACTOR AUTHENTICATION

Turn on two-factor authentication to create an extra layer of protection when accessing your account from a new computer, phone or tablet.

INSTRUCTIONS

Search about.Meta.com/actions/safety

Two-factor authentication

3. RECOVERY CODES

Recovery codes are a one-time use code that provides access to your account in case you have lost access to the device or email address through which you normally receive 2FA codes. These codes can be used instead of your authenticator code when logging in. You can print or write down these codes and store them in a secure location. You will only be able to use each code once, if you have used all the codes, request new ones.

You can find these codes under the Two-Factor authentication section in your Facebook and Instagram settings.

INSTRUCTIONS

Search facebook.com/help

Recovery codes

THREE MORE TIPS TO GO THE EXTRA MILE

4. LOG IN ALERTS

You can set up an alert to notify you each time someone tries logging in to your account from an unrecognisable device. These alerts tell you which device tried logging in and where it was located.

INSTRUCTIONS

Search about.Meta.com/actions/safety

Login alerts

TIP:

Log In Alerts are crucial for survivors as abusers often attempt to access accounts by guessing or already knowing the password.

5. LOGGING OUT

The "Where You're Logged In" section of your "Security and Login" settings shows you a list of devices that have been recently used to log in to your account.

INSTRUCTIONS

Search about.Meta.com/actions/safety

Logging out

TIP:

Remember to be cautious of when and where you log into your account. It's essential for everyone, but survivors should be extra cautious when logging in from shared computers or devices the abuser has access to.

6. PERMISSION STATUS

You can review and update your account security settings to ensure you're aware of who's accessing your accounts and which apps you've given permission to use your account.

INSTRUCTIONS

Search about.Meta.com/actions/safety

Permission status

Account takeover

PERSONAL ACCOUNTS

You may notice your account has been taken over if the email and password have been changed, friend or follow requests have been sent to people you do not know, messages have been sent that you did not write or posts have been made that you didn't create. Trusted friends and family may inform you of these changes, it is important to review the account settings and controls immediately.

FACEBOOK

For Facebook accounts, when an email is changed, Facebook will send a message to the previous email with a special recovery link. By clicking this link, you will reverse the email change and have the opportunity to secure your account. If you do not have access to your account, you can report a compromised account to Facebook. This process will alert Facebook that your account has been compromised and they will help you log back into your account so that you can regain control.

To report a compromised account, go to: facebook.com/hacked

INSTAGRAM

For Instagram, if the email address has been changed, Instagram will send two emails asking you to reverse or accept the request. If you do not have access to your Instagram account and email address, you can request support from Instagram to gain control of your account.

To report a compromised account, go to: instagram.com/hacked

BUSINESS ACCOUNTS

Meta provides great platforms and support for businesses that use Facebook and Instagram to promote and manage their businesses and organisations. If you manage a business on Facebook and Instagram, it is important to implement a strong account recovery process that incorporates TFA, recovery codes, log-in alerts, and ensuring you have two admin recovery accounts linked.

If you do not have access to your account, follow the links mentioned to request support from Facebook or Instagram.

Fake or imposter accounts

If you believe someone has created an account pretending to be you, or someone you know, file a report. Further information about filing a report is on pages 23 and 25 of this guide. If your account has been hacked or compromised, secure it immediately.

INSTRUCTIONS

Search about.Meta.com/actions/safety

fake, imposter, hacked accounts

TIP:

Be aware of suspicious accounts that may try to connect with your profile, if you do not know the account holder or recognise the account name, it is best to decline the follow or friend request.

Image-based Abuse

WHAT IS IMAGE-BASED ABUSE?

Image-based abuse is when someone shares or threatens to share an intimate image of another person without their consent. This includes AI-generated intimate images ('deepfakes') featuring someone who has not given their consent.

In the context of domestic violence, abusers will often share or threaten to share intimate photos or videos of survivors in order to manipulate, punish, or control the survivor. Many of these videos or photos are posted and shared online to popular social media or pornography sites or "revenge porn" websites.

When posted online, some intimate images include identifying information of the individual, such as their full name, address, phone number, and place of employment or school, which can pose further risk of abuse, stalking, and harassment by other perpetrators.

Abusers may also send or threaten to send images directly to friends, family, and others in the community who know the survivor via email or text.

LEGAL CONSIDERATIONS:

In Australia, it is illegal in most States and Territories to share an intimate image of someone who is under the age of 18, but also to threaten to share someone's intimate image without their consent, regardless of their age. An intimate image could show or appear to show a nude or partially nude individual, genitals, bottoms or breasts, private activity such as undressing or an individual without clothing of religious or cultural significance, such as a hijab or turban. The image or video can be real, altered or faked to look like a specific individual or shared in a way to target an individual, such as a nude image of someone else tagged with a survivor's name or account.

Making such a threat can lead to charges, even if you don't have the actual image or the image doesn't exist.

If you want to take legal action, you may need evidence, such as a screenshot. Meta promptly removes reported content that violates their policies.

WHAT SHOULD I DO?

Reach out! It can be highly distressing to discover that your intimate images are being shared online without your consent. If you are in a difficult situation, seek support from trusted friends, family, or professionals like a therapist, counsellor, domestic violence support centre, or social worker.

If you've experienced abuse, it's important to document it, noting how it made you feel and its impact. Save screenshots to a secure location and consider printing them as well. Having someone from your support network with you during the process is advisable.

Directions on creating screenshots can be found in the Facebook Help Center and the Instagram Help Centre.

SERVICES ARE HERE TO HELP!

Various teams at Meta work 24/7 in multiple languages and time zones to ensure policy enforcement. You can report nude or sexual photos or videos of yourself or threats to share these images or videos to Meta to prevent them from being reshared. Meta teams review reports 24/7 in more than 70 languages and will take action on violating content and behavior. For more information, access Meta's Safety Centre.

If you have the images, you can create a case at StopNCII.org to enable participating companies to remove intimate images of you if they have been posted on their platforms.

Additionally, you can report image-based abuse to eSafety or contact **1800RESPECT** on **1800 737 732** for further support.

For further information, please see Wesnet's handout on Image-Based Abuse at techsafety.org.au/image-based-abuse.

In-app reporting, other tools and resources

REPORTING

Meta has comprehensive reporting mechanisms built into the apps so that users can report others who are violating Meta community guidelines. Prohibited content across all Meta platforms includes violence, threats, bullying, harassment, hate speech, sexual violence, exploitation, and impersonation. Reporting helps make the platform safer for everyone.

TIP:
If they feel comfortable doing so, survivors can ask the person responsible to remove or edit the post, or they can inform a trusted person about the content.

Alternatively, survivors can report harmful posts or abusive behaviour on Meta from their Timeline, DMs, News Feed, or any post they're tagged in.

If you report something on Facebook or Instagram, it will be reviewed to determine if the content is a breach of community standards. Unless the report is regarding an intellectual property infringement, the report will remain confidential and the reported account holder will not be able to see who has reported them.

INSTAGRAM

You can report anything you believe violates Meta's Community Guidelines directly from the Instagram app. You can report a post, story, message or chat, a hashtag and an account.

INSTRUCTIONS
Search help.instagram.com

How to report

FACEBOOK

You can report a profile, post, message, page, group, event, comment, advertisement or hashtags on Facebook. If you don't have an account or can't see the content that you would like to report (e.g. someone has blocked you), you can ask a friend to report the content using the Find Support or Report link near the post, photo or comment.

INSTRUCTIONS
Search facebook.com/help

Reporting abuse

DOWNLOAD YOUR INFORMATION

To access your personal account data on Meta's self-service tools, you must confirm your identity and complete a security check. The data includes login activity and messages that may have been filtered out by Meta's safety tools, which can help you save evidence of abuse and harassment.

☆

TIP:

Survivors should use a safe device to capture photos or screenshots of unwanted content. Saving important information to an external hard drive, stored in a secure location, can also help ensure abusers cannot access it.

INSTAGRAM

Use Instagram's Download Your Data tool to get a copy of everything you've shared. You can download your data in multiple formats and with customisable filters through the Accounts Centre.

INSTRUCTIONS

Search help.instagram.com

Download your information

FACEBOOK

You can use the Download Your Information tool to access your profile and activity log. To download a copy of your Facebook data, go to Accounts Centre or Settings.

INSTRUCTIONS

Search facebook.com/help

Download your information

REPORTING OUTSIDE OF INSTAGRAM AND FACEBOOK

Not all threatening or harassing comments can be removed by Meta if they do not violate their Terms of Service or Community Guidelines. However, there are other ways to report technology-facilitated abuse.

E-SAFETY COMMISSIONER

You can make a report about online harm through the e-Safety Commissioner at esafety.gov.au/report/forms. There are four different schemes you can report under: cyberbullying, cyber abuse, image-based abuse and illegal or restricted online content.

STOPNCII.ORG

You can create a case on StopNCII.org if you have been a victim of image-based abuse. StopNCII.org will work with associated companies to have the image removed.

POLICE

If you fear you are in immediate danger or require legal support, you can access your local police station to report incidents of harm or abuse, or contact a community or women's legal service.

WESNET TECHSAFETY

For support, resources and advice regarding technology-facilitated abuse. Access Wesnet's tech safety website at techsafety.org.au.

TIP:

Even if an abuser's actions on Meta's Services do not violate Meta's Terms of Service or break any laws, when grouped, such as a series of vague harassing messages, they can constitute stalking or harassment or other forms of abuse, like coercive control. If a survivor has or is seeking a domestic violence order or intervention order against an abuser, request that the order include language that restricts the person from contacting the survivor through any means. Online contact and sharing of survivor's information or photos could violate existing orders.

Abuse in intimate partner, dating and family relationships

STRENGTHENING YOUR SAFETY PLAN

If you are experiencing abuse in a dating or intimate partner relationship or in your family, it is a good idea to have a safety plan in place. Below you will find general advice to strengthen your safety plan, please contact a local support worker who can help you develop a more thorough safety plan.

Abusers, stalkers, and perpetrators can be incredibly persistent and creative in maintaining control, and technology is another tool for them to misuse.

Trust your instincts: If you suspect that the abusive person is stalking, or monitoring you using technology, it is possible that they are. Think about whether or not it is safe to suddenly remove or block their access. It may be safer to let the monitoring continue while you use separate, safer devices that the abuser does not have access to plan your next steps.

Stalking is a red flag. If someone has been stalking you for longer than two-weeks, definitely report it to the police and consider seeking support from a DV helpline or local crisis services.

The most dangerous time for women and those experiencing gender-based violence is when they have just left, are leaving, or are planning to leave abuse.

It can be complex and there are services available that can help you. There are also emergency payments and other support available for those in Australia.

Get more information: Navigating violence, abuse, and stalking is very difficult and dangerous. Work with a Domestic Violence support centre to discuss your options and to help you plan for your safety. You can call 1800-RESPECT on 1-800-737-732 or www.1800respect.org.au.

Look for patterns to identify misused technology. Carefully try to figure out how or which technology is being used to harass, stalk, or monitor you. Narrowing down the potential source of technology will help you create a more precise safety plan.

DOCUMENT YOUR EXPERIENCES

As mentioned throughout this guide, it is important that you document your experience, such as keeping a report log, taking screenshots or photos and writing down events. Remember to keep your documentation in a secure location.

REACH OUT!

If you are in danger, feel uncomfortable, confused or anxious, it is important you reach out and seek support from trusted friends, family, or professionals like a therapist, counsellor, DV specialist , or social worker. For support contacts and direction, please go to page 27 of this guide.

RESOURCES

PROVIDER	SERVICES	CONTACT
META	• Instagram and Facebook Help Centre	help.Instagram.com Facebook.com/help
	• Meta Safety Centre	about.Meta.com/actions/safety
	• Womens Safety Resources	about.Meta.com/actions/safety/audiences/women/abusevictims
WESNET	• Wesnet website	wesnet.org.au
	• SafetyNet Resources on Online Safety	techsafety.org.au/resources
1800 RESPECT	• Confidential information, counselling and support service, free, 24/7	1800respect.org.au
ESAFETY COMMISSIONER	• Australia's independent regulator for online safety	esafety.gov.au
STOP NCII	• A free tool designed to support victims of image-based abuse.	stopncii.org

For full list of resources and help across Australia, please visit wesnet.org.au/help

WESNET
The Women's Services Network

wesnet.org.au

Meta