

How to stay safe online: everything you need to know



Introduction

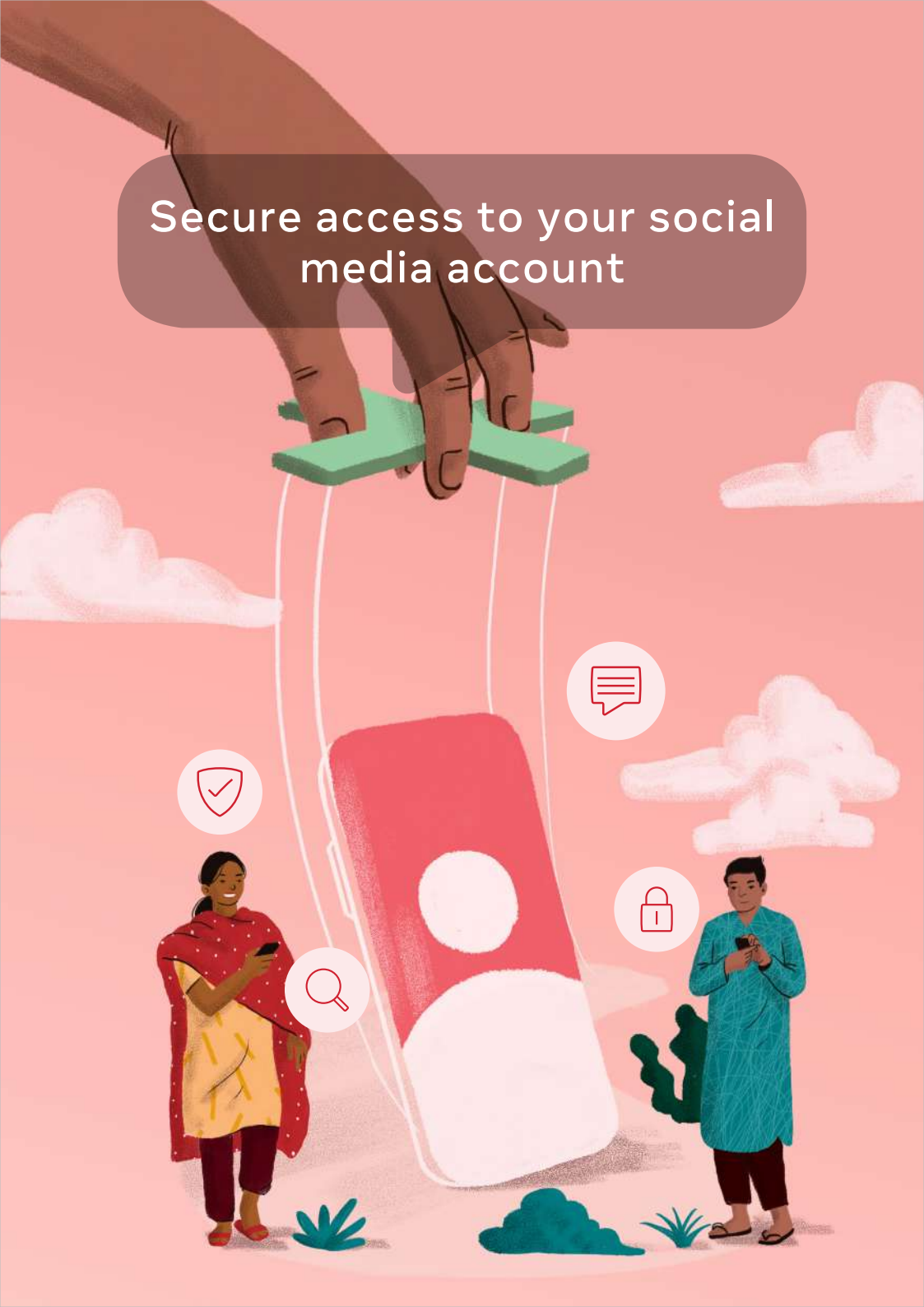
More people than ever before are now online. In an increasingly globalised world, social media helps everyone stay in touch with friends and families in different cities or countries around the world.

However, it's not just the good people that are online. So it's more important than ever that we all take steps to stay safe on the internet.

So how can we keep our online and social media accounts safe?

Keep reading.

Secure access to your social media account



This one is really important. You are the only person who should be able to access and control your social media account. Never share your login details with anyone else and never use the same passwords for different websites or social media accounts. Keeping your login information private helps prevent other people from being able to access your account.

These are several things to note to keep your social media accounts safe and secured.

Password

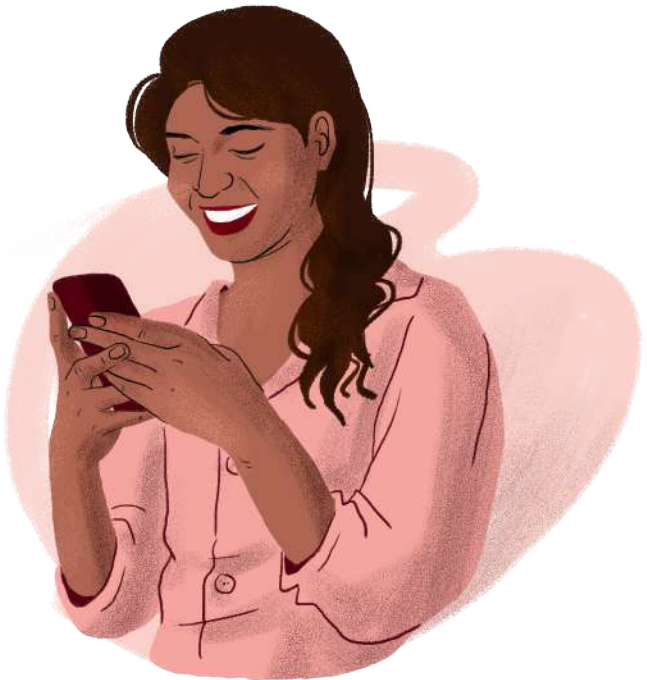
Use a password that is hard to guess and unique. The more complicated, the better. Simple, generic passwords are easy to hack. Make sure to use a different one for every website and social media account, and never share your passwords with anyone.

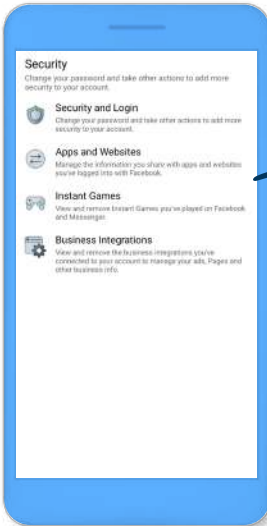
Two-Factor Authentication (AKA 2FAC)

Two-Factor Authentication is an extra layer of security on your account which makes it harder for hackers to gain access.

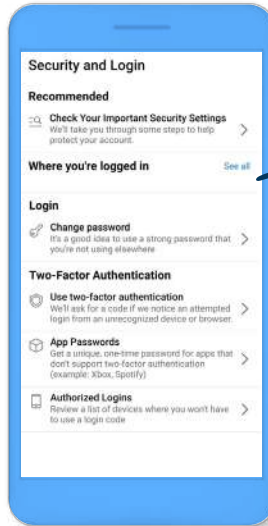
To log into your account you will need your password, along with a one-time passcode we will send to your phone or via a special app. This doubles the safety, similar to having both a gate and a lock on your house. Activating this feature is a simple step you can take right now to keep your account secure.

So how do you activate 2FAC?

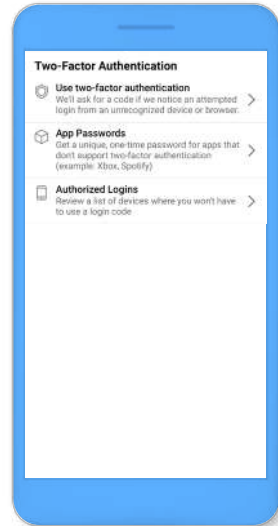




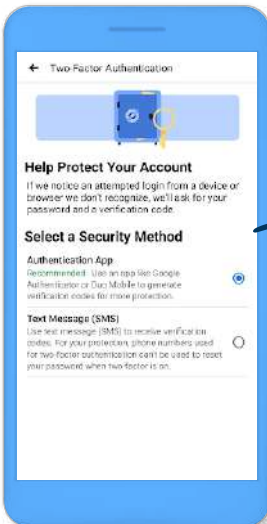
Go to your Security and Login Settings.



Scroll down to Use two-factor authentication and click Edit.

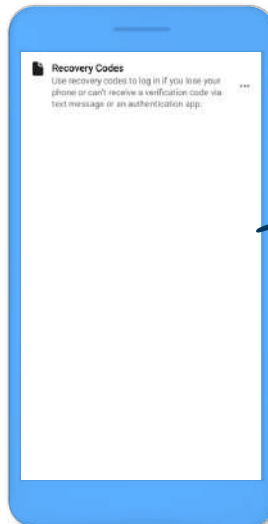


Choose the security method you want and follow the on-screen instructions.



Select a security method:

- Authentication App.
- Text Message (SMS).



You can also use the following:

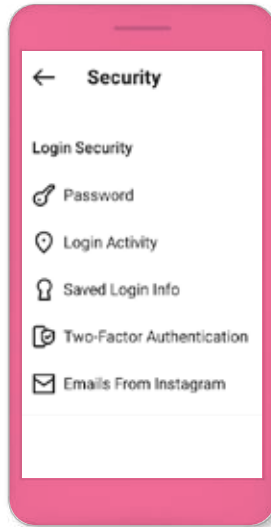
- Approve login from a device recognized by Facebook.
- Use one of the recovery codes we select.
- Tap the security lock on the recognized gadget.



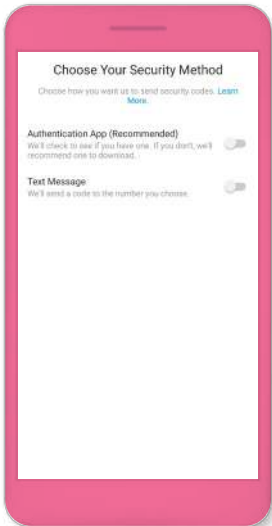
Once the two-factor authentication is activated, we have to input the code sent by Facebook to login from a different gadget.



Go to Profile and click Settings.



Click Security and go to Two-Factor Authentication.

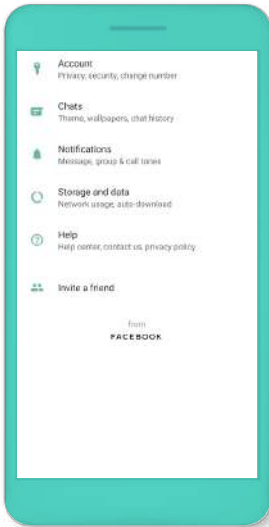


Choose from these 2 security methods:

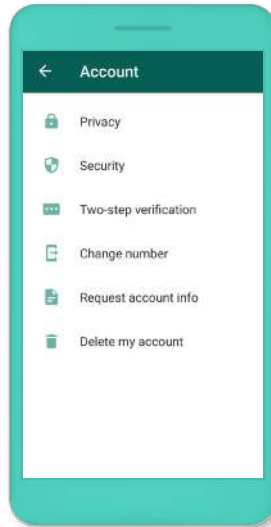
- Text Message.
- Authentication App (such as Duo Mobile or Google Authenticator).



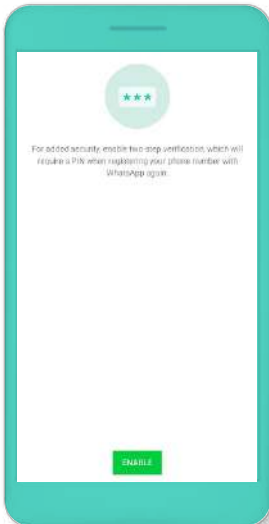
Once the two-factor authentication is activated, we have to input the code sent by Instagram to login from a different gadget.



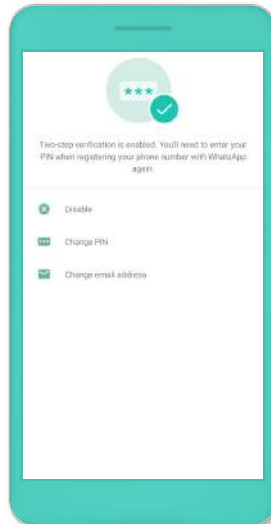
Go to Profile and click Settings.



Click Account and select Two-step verification.



Enable Two-step verification using a PIN.



Once the two-step verification is enabled, we have to input the PIN to log in from a different gadget.

Verify your phone number on WhatsApp

Before activating WhatsApp, don't forget to do this for your safety.

Remember these important points:

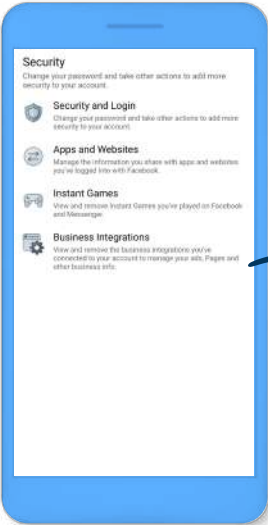
- You can only verify your own phone number
- Make sure you can receive a call and text message on the number you use for WhatsApp
- Turn off any setting or app that blocks phone calls
- Make sure you have internet access for verification



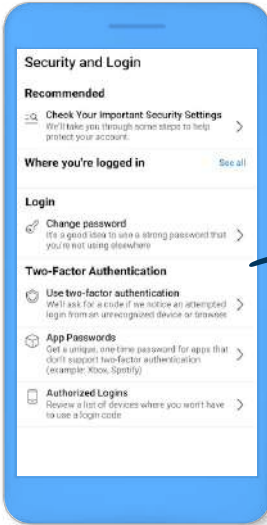
Facebook security check-up

This tool makes taking control easy! With this, you can review and update your account security settings to ensure you're aware of who's accessing your accounts and what apps you're given permission to use your information. This tool also provides detail on how you can improve your passwords and password security.

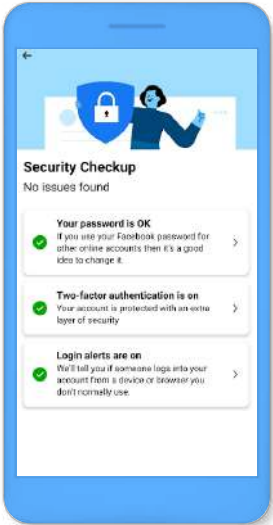
Here's how it works:



Go to your Security and Login Settings.



Click Check Your Important Security Settings.



Choose the option you want to explore, from changing your password to controlling alerts.

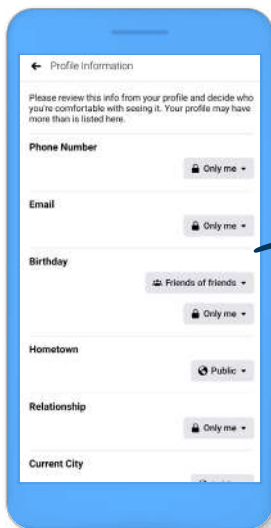
Who can see
what I share online?



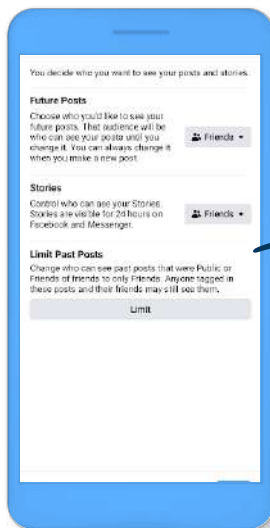
Do you know that you're in charge of how and what information you share online? Take control of how much information you share online with a few easy steps:

Facebook Privacy Checkup

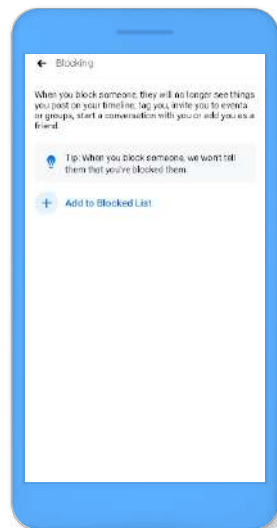
You want to review your choices to help make sure that you're sharing with who you want to share with? Easy, go to the Facebook Privacy Checkup:



See who can see your phone number, email, birthday, and relationship status.

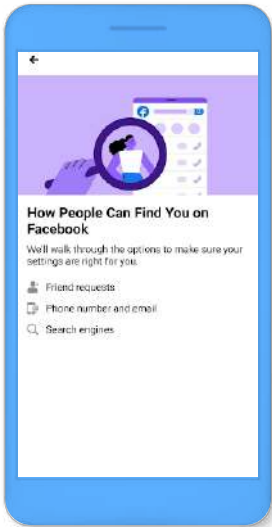


Set who can see your old and future posts.

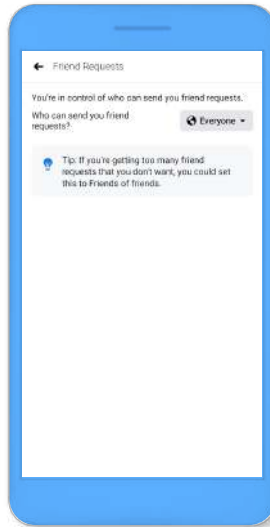


Review accounts that you've blocked on Facebook.

Who Can See What I Share Online?



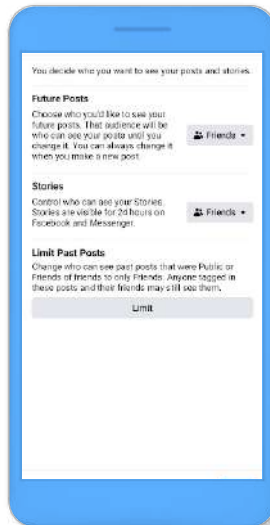
See who can find you on Facebook.



See who can send a friend request on Facebook.



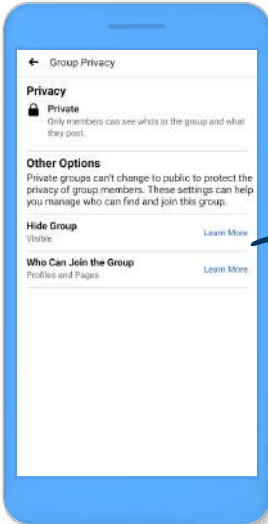
Restrict who can search for your account on Facebook through phone number and email address.



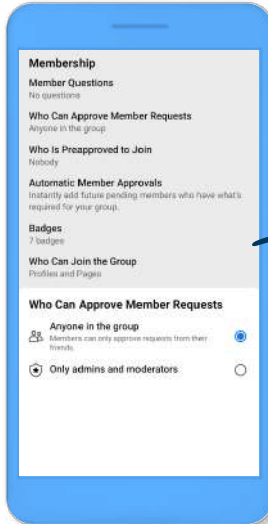
Control who can see your Facebook posts.

Facebook group

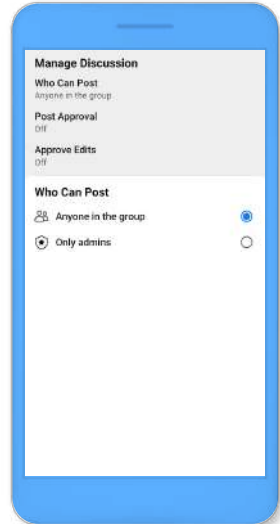
If you run a Facebook Group, this is how you maintain your Group's privacy:



Control who can see your phone number, email, birthday, and relationship status.



Control who can see your old and future posts.

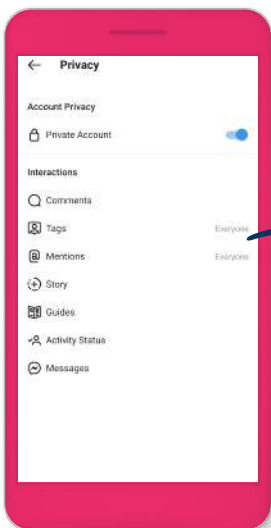


Review who you can block on Facebook.

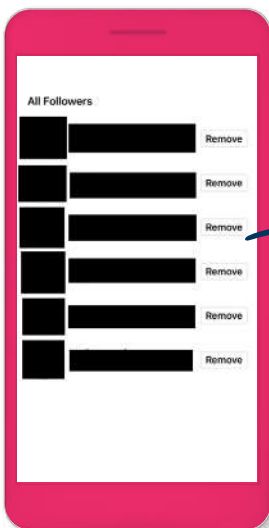


Instagram

Like Facebook, Instagram also features Privacy settings that enable you to manage who can see what you share. There are a few things you can do:



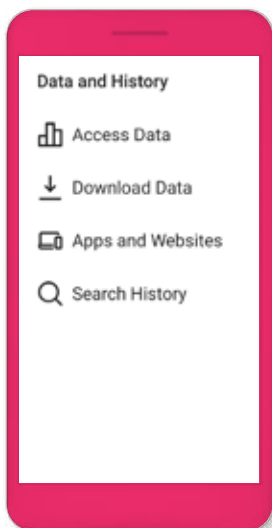
Choose a private account. So only your followers can see your posts and Stories.



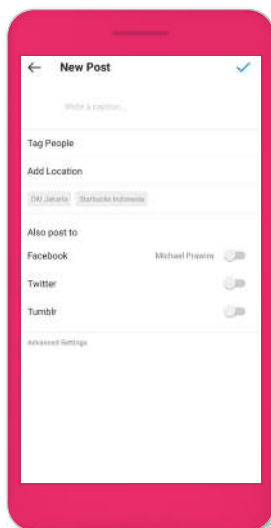
Delete followers on Instagram. You can choose who follows you and keeps up with what you share.



Mute, restrict or block, depending on how much or how little you want to interact with someone: you can take a break, or keep them from interacting with you altogether.



Access and review your data on Instagram.



Turn off location on any photo or video you want to post.

Whatsapp

- **View once**
Send photos and videos that disappear after a single view.
- **Two-step verification**
Add extra security when you sign in to your account.
- **Lock your WhatsApp**
Enable Touch ID, Face ID, or Android fingerprint lock to secure your WhatsApp.
- **Read receipts**
Choose whether contacts can see if you've read their messages.
- **Last seen**
Choose if only your contacts, everyone, or nobody can see when you last opened WhatsApp.
- **Profile photo privacy**
Decide if only contacts, everyone, or nobody can see your profile photo.
- **Status privacy**
Choose who can see your status updates.
- **Group privacy settings**
Choose whether everyone, all your contacts, or only some contacts can add you to a group chat.

Girl power: taking charge of
her safety and wellbeing
online

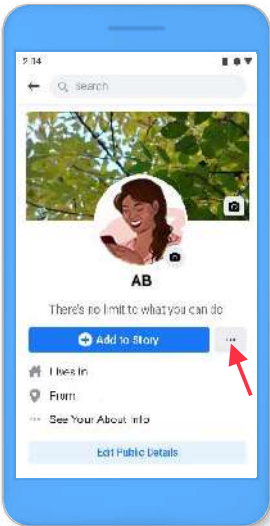


Useful Tools

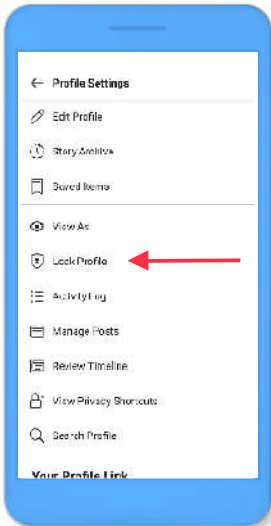
The internet has given women many opportunities and benefits, however it can also be a space where many feel unsafe - from strangers sending private messages, to unwanted comments on posts or photos. Here's some useful tools to help you control your experience on Facebook:

Locked Profile: When your profile is locked, people who aren't your friends can't download, enlarge or share your profile photo. They also can't see any posts or other photos on your timeline, regardless of when you may have posted it.

Here's how:

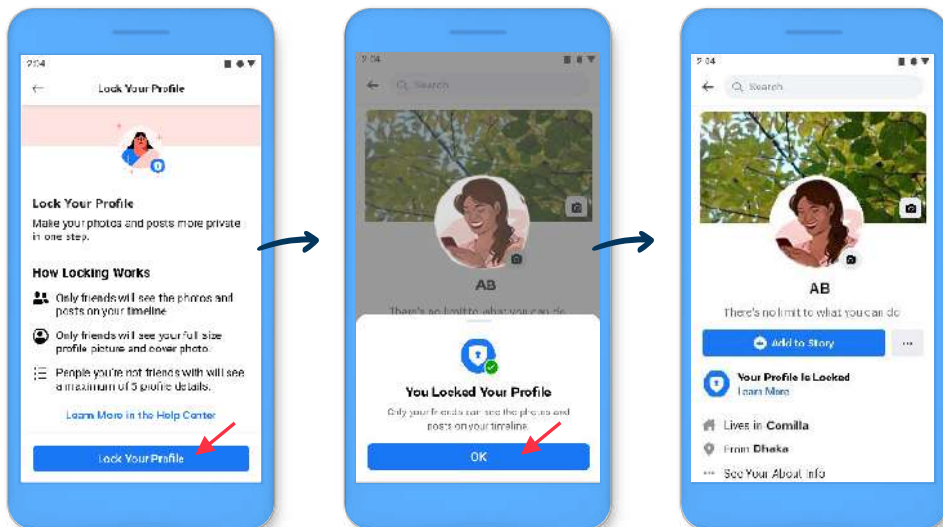


On app homepage, tap your Profile picture.



On the profile page, tap Menu (three dots) and enter Profile Settings.

Girl Power: Taking Charge of Her Safety And Wellbeing Online



From the given options, tap the Lock Profile option.

A pop message will appear on the screen saying "You locked your profile. Only your friends can see the photos and posts on your timeline". Tap Ok.


Your Profile is now locked.

Once the lock feature is enabled, you can see an indicator is added to your profile which signifies that the profile is locked.

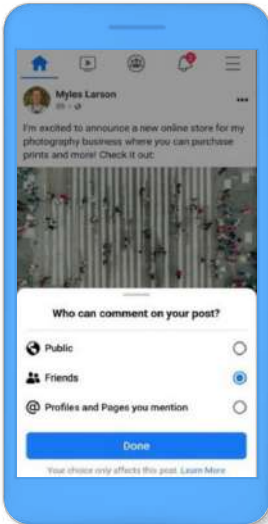
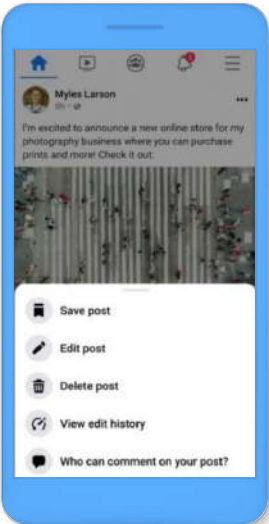
Comment controls:

You can control who can comment on your public posts by choosing from a menu of options ranging from anyone who can see the post to only the people and Pages you tag.

To change who can comment on your public posts:

1. Click  in the top right of Facebook.
2. Select Settings & privacy, then click Settings.
3. Click Public posts on the left-hand side.
4. Go to Who Can Follow Me and make sure that Public is selected.
5. Click Edit next to Public post comments.
6. Select who is allowed to comment on your public posts:
 - Public: Includes everyone, even people who are not following you.
 - Friends: Includes your friends on Facebook. If anyone else is tagged in a post, then the audience expands to also include the tagged person and their friends.
 - Friends of friends: Includes all your friends and any friends they have.

Bear in mind that you can also choose who can comment on individual public posts on your profile. Choosing who can comment on an individual public post applies to that post only. It does not change your settings for who can comment on your other public posts or your public profile information.



Profanity and keyword filters on Facebook: You can choose to hide comments with profanity from your Page. We determine what to hide by using the most commonly reported words and phrases marked offensive by the community. You can choose up to 1,000 keywords in any language (example: words, phrases or emojis) to block from your Page. When people include a keyword you've blocked in a comment, we'll hide the comment so that it doesn't appear on your Page.

To block keywords from your Page:

1. From your News Feed, click Pages in the left menu.
2. Go to your Page, then click Settings in the left menu.
3. From General, click Page moderation.
4. Add keywords that you want to block:
 - To add words or phrases: Type the words or phrases separated by commas, then click Add.
 - To add an emoji: Click , select the emoji that you want to block, then click Add.
 - To add a list of keywords: Click Upload from .CSV, then follow the instructions to upload your file.
5. Click Save.



Not without my consent!

When someone shares or threatens to share your private and intimate images without your consent, it can be upsetting and hard to know what to do next.

Facebook policies prohibit people from sharing non-consensual intimate images (sometimes referred to as ‘revenge porn’) — and in recent years Facebook has used technology to stop people from being able to re-share these images.

If you're under 18, we recommend also talking with a parent or other adult you trust to help you think through what to do.

You can also talk to a teacher or local administrator who you feel comfortable with.

Check out these steps that you can take to remove the images from Facebook and Instagram, and prevent them from being shared or re-shared.

Report it!: On Facebook, Instagram or Messenger, you can report when someone shares your intimate images without your consent or is threatening to do so by reporting them.

Here's how you do it:

1. Click on the photo or video to expand it. If the profile is locked and you can't view the full-sized photo, click Find support or report photo.
2. Click to the right of the photo or video.
3. Click Find Support or Report Photo for photos or Report Video for videos.
4. Select the option that best describes the issue and follow the on-screen instructions.

If you're having trouble reporting something, please log in from a computer and use the report links.

To stop the sharing of NCII, a new website StopNCII.org has been launched, which will create a secure digital fingerprint to pro actively stop it being shared anywhere on FB or Instagram

Contact local law enforcement: if you're concerned about your physical safety or the physical safety of your loved ones.

Take screenshots and print outs pages of photos and threats before taking any steps to delete the images: It may be illegal where you live to post or threaten to post things like this, and you might need a screenshot or other record of the post to serve as evidence if you pursue legal action.

Consider seeking additional support or guidance: There are organizations that specialize in women's safety online and they can offer you confidential support. You can contact the relevant Country helpline for more additional guidance.

We need a break!

Sometimes all of us need to take a break - and that includes online. The good news is we have a range of tools to help with this.

Snooze and Unfollow: Facebook launched Snooze, which gives people the option to hide a person, Page or Group for 30 days, without having to permanently unfollow or unfriend them. You can also unfollow people so that they remain-friends but their content does not appear in your News Feed.

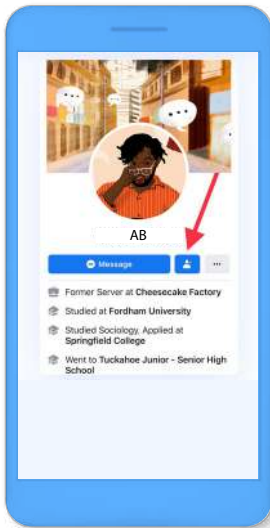
Mute: You can also mute notifications for specific contacts or groups on WhatsApp. Open WhatsApp > Settings > Notifications > In-App Notifications.

Take a Break: Millions of people break up on Facebook each week, changing their relationship status from “in a relationship” to “single.” To help make this experience easier, Facebook built a tool called Take a Break, which gives people more centralized control over when they see their ex on Facebook, what their ex can see, and who can see their past posts.

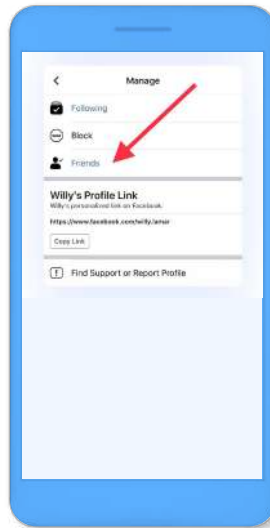
See less of someone: Limit where you see someone on Facebook. If you choose to see them less, their posts and posts they're tagged in won't appear in your News Feed and you won't be prompted to message them or tag them in photos. To see their posts again, you can follow them.


Limit someone's ability to see your posts and posts you're tagged in: Hide your posts from the person you want to take a break from. They'll be added to your Restricted list and will only see posts that you tag them in or share publicly.

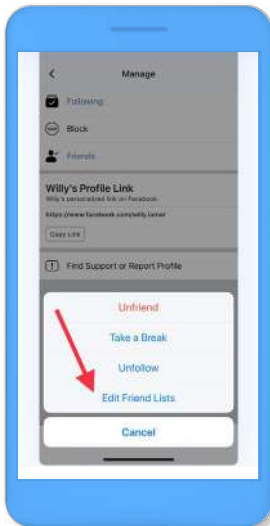
To add someone to your Restricted list on Facebook:



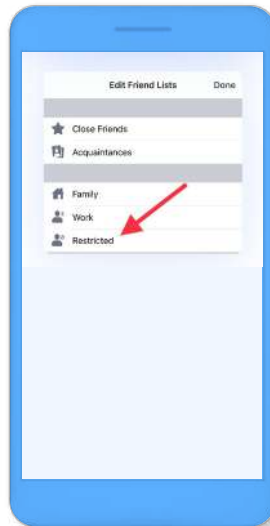
Go to their profile.



Click  at the top of their profile.

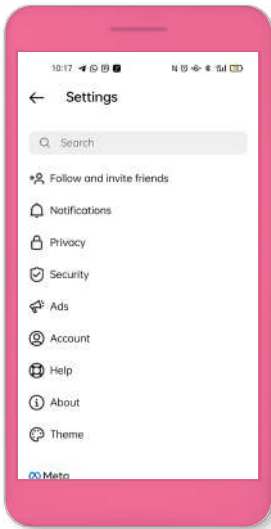


Select Edit friend list.

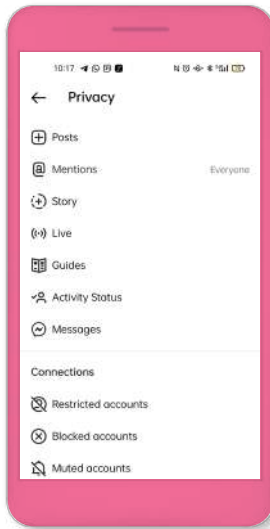


Select Restricted.

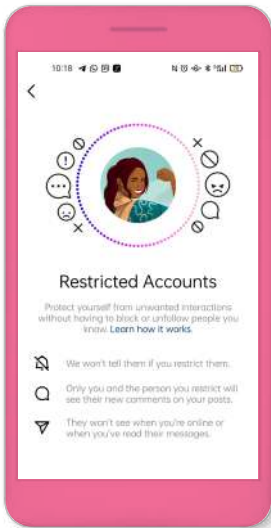
To add someone to your Restricted list on Instagram:



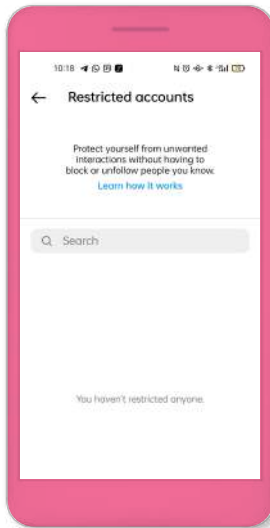
Go to your profile setting.



Click Privacy.

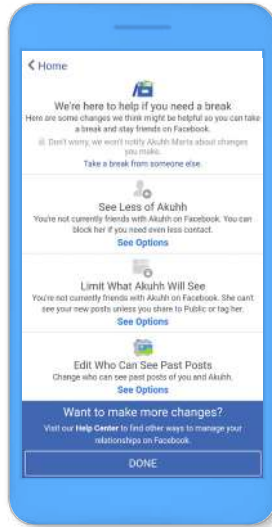


Select Restricted Accounts.



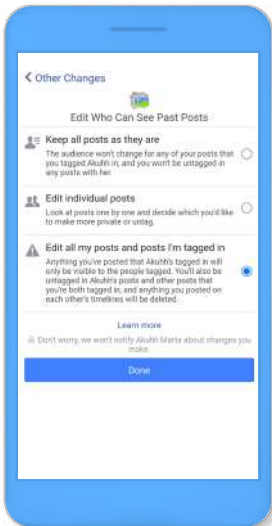
Select friend and click Restrict.

To limit which posts someone can see:



Go to facebook.com/take_a_break.

Select the person you'd like to see less of.



Below Edit who can see past posts, choose the option that best fits your preferences.

Do bear in mind that you can always do these too:

Friending/Following (Facebook and Instagram): Before accepting someone as a friend, you might want to take a look at the person's profile. Have you ever met them in person? Do you have friends in common?

Unfollowing (Facebook and Instagram): When you unfollow someone on Facebook and Instagram, you won't see their posts in your Feed, but you'll still be friends with them.

Unfriending (Facebook): If you choose to unfriend someone, Facebook won't notify the person but you'll be removed from their friends list. If you want to be friends with this person again, you'll need to send a new friend request.

Blocking (Facebook and Instagram): You can block someone to unfriend them. This will prevent them from starting conversations with you or seeing things you post on your profile. In addition, people you block can no longer tag you, invite you to events or groups, or add you as a friend. Blocking is reciprocal, so you also won't be able to see things they post or start conversations with them. When you block someone, we don't notify them.



Blocking (WhatsApp): When you block someone, your last seen, online, status updates, and any changes made to your profile photo will no longer be visible to contacts you've blocked. Messages, calls, and status updates sent by the contact won't show up on your phone and won't be delivered to you. Please note that blocking a contact won't remove them from your contacts list, nor will it remove you from the list on the contact's phone. To delete a contact, you must delete the contact from your phone's address book.

Reporting (Facebook and Instagram): Facebook includes a link on nearly every piece of content for reporting abuse, bullying, harassment and other issues. Facebook global teams work 24 hours a day, 7 days a week, to review things you report and remove anything that violates its Community Standards. To report a post, click on the top right of the post and choose the option that best describes the issue, then follow the on-screen instructions.

Reporting (WhatsApp): When you report someone: WhatsApp receives the last five messages sent to you by the reported user or group, and they won't be notified. WhatsApp also receives the reported group or user ID, information on when the message was sent, and the type of message sent (image, video, text, etc.). You can also choose to report an account by long pressing a single message.

Talking with kids about online safety



Now, you know how to keep your accounts secured and know what to do to control your experience online. But wondering what would be the best way to talk to your kids about online safety?

Here are a few tips you might find useful:



Start early: These days, children are often exposed to devices from birth - even just observing their parents, so it's never too soon to talk about online safety. Online safety conversations should become part of everyday life, just like conversations about 'stranger danger' or crossing the road, and they should start early. Talk to them about technology, before they are on social media.



Stay involved in their digital world: Spend time with your kids online. If your kids like playing video games, sit with them while they're doing this. If your teen is on Facebook or Instagram, have a discussion about friending or following them. Talk to them frequently about who they are connecting with and what they are sharing. Let them know they can come to you if they see or experience something online that makes them feel uncomfortable.



Use privacy and security settings:

Facebook, Instagram, WhatsApp and Messenger have settings to give people control over what they share, who they share it with, what they see, and who can contact them. Many of these are turned on by default for minors, but you should run through the privacy and security settings regularly.



Set family rules:

Agree as a family on the rules for using devices, accessing the internet and social media and be clear on the consequences for violating these rules. Depending on the age of your kids, you may talk about more serious consequences (such as legal consequences) of sharing certain types of content such as non-consensual intimate imagery.



Identify and seize key moments: For example, your child getting their first mobile phone is a good time to set ground rules. When your child is old enough to join Facebook and other social media, it's a good time to talk about safe sharing. Your child getting their driving licence is a good time to discuss the importance of not texting and driving.



Lead by example: If you set a rule like ‘no screen time after 8pm’ or ‘no devices in the bedroom’ - you should try to follow this too!

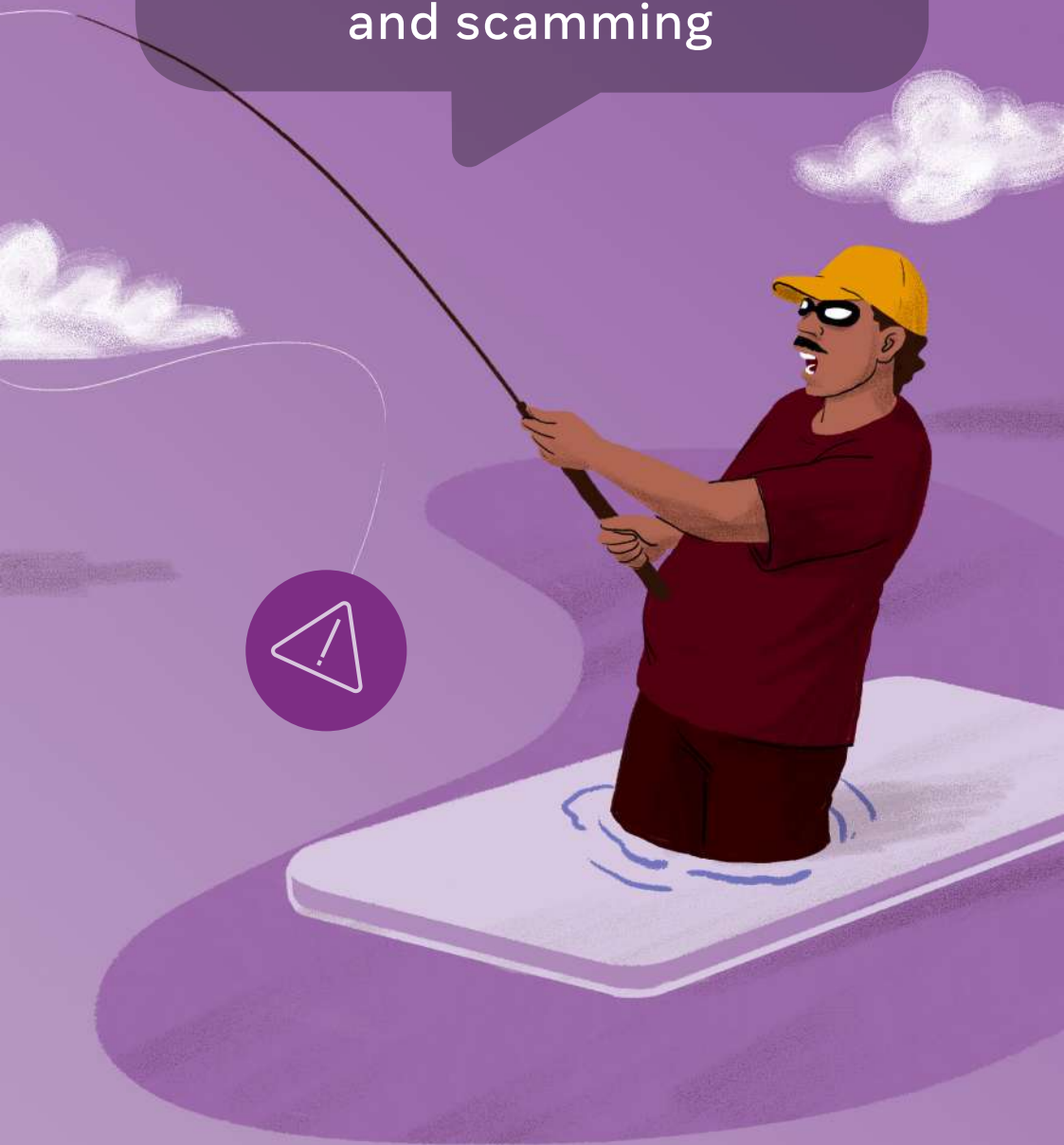


Learn from your kids: Technology evolves constantly and young people are fast adopters. If your kids start using a new app, ask them to show you how it works. It’s an opportunity to connect with your child, see what they are doing online and have a conversation about online safety. You should also do your own research on the app’s privacy, safety and security features.



Trust yourself: Typically, you can adopt the same parenting style for your child's online activities as you use for their offline activities. If you find that your child responds best to a negotiated agreement, create a contract that you can both sign. Or maybe your child just needs to know the basic rules

Staying away from phishing
and scamming



Phishing is one of the oldest types of cyber-attacks, where someone pretends to be someone they are not in an attempt to fool you into handing over personal information. The techniques scammers use have become increasingly sophisticated and it can sometimes be hard to tell if a message is legitimate or not.

Phishing takes many forms including text messages, emails, social media profiles, posts and messages, or fake websites. Typically, a scammer will send a message claiming to be from a reputable company or pretending to be someone you know in an effort to get you to give up money, or important personal information such as passwords or financial details. Once they have this information, they will attempt to profit from it.

Most of the common phishing and scamming tactics prey on human emotions in an attempt to mislead!



Example 1:

"I really, really need your help, please!" Someone claiming to be your relative or friend sends you a message saying they are in trouble and need funds. Once you reply, the scammers then work to take advantage of your good nature and lure you into transferring money or giving our personal details that they can use. Look out for generic greetings and suspiciously long or complex websites or email addresses. If you're not sure, call your friend to check if they sent the message.

Example 2:

"Congratulations, you're a winner!" These messages will claim that you have struck the lottery and won big, but there's always a catch. To claim your 'prize' you'll need to pay a membership or joining fee or share your personal details. Like many phishing messages, these often come with misspellings and poor grammar. If you look carefully, they often have forged links - that is, web links containing an official company name or brand, but with misspellings (e.g. www.1ottery.com instead of www.lottery.com).

Example 3:

"You've been hacked, but it's ok I can help you!" This works by falsely claiming that one of your online accounts has been compromised or deleted, and they can help you recover the situation - so long as you provide your personal information.

Now, here's a simple guide to staying phishing and scamming-free.

Don't click links sent to you in messages.

If someone sends you a link, before clicking it, do a quick Google search to check if the information is legitimate - or call your friend and check they sent you the message.

Keep it to yourself.

Never reveal your log-in details: Facebook, Instagram and WhatsApp will never ask you for your password in an email or send you a password as an attachment. Never reveal your login information to anyone, even friends or family.

Just like real-life, don't automatically accept friend requests from strangers.

Scammers may create fake accounts to attempt to be your friend. This will allow them to spam your feed or inbox.

Secure your account like you would any other valuables.

Change your password regularly and use complex, hard to guess passwords. This can prevent your account from being compromised by scammers who would use your account to contact your friends and family.

Review your account activity and remove spam.

You can check your login history for suspicious logins, and also check your installed apps and games that have access to your data. Remove those that you do not use.

Check out Facebook, Instagram and WhatsApp's extra security tools features.

It always pays to take advantage of the latest security tools and features.

Take action and report it!

If an email or Facebook message looks strange, don't open it, don't open any attachments and don't click on any links. Instead, report it to phish@fb.com. If you want to report the conversation, remember to take a screenshot before you delete it. Keep in mind that this won't delete the message from the other party's inbox.

On WhatsApp, you can open the chat with the user you wish to report. Tap More options > More > Report. Then check the box if you would like to also block the user and delete messages in the chat. And tap REPORT.

If you think your friend is the victim of a hack, let them know.

Visit the Help Center on Facebook, Instagram and WhatsApp to take back control of your accounts.

Call the police, and your bank.

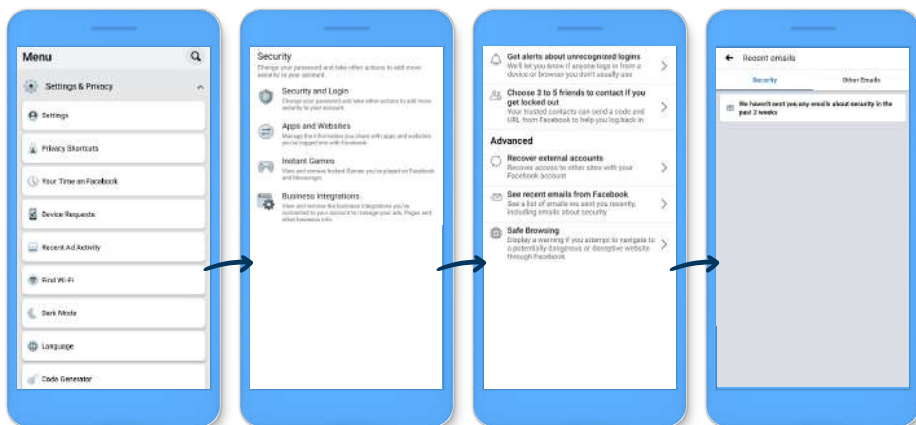
If you feel you were the victim of a crime, please contact your local police department. And if you have mistakenly given your credit card details, immediately inform your bank or credit card company, and also make sure you report the person or account to Facebook, Instagram and WhatsApp.

Oh no, my account will be suspended in 24 hours!

Well, this is another common tactic used by online criminals, often pretending to be from an online platform.

If you get notifications like this, don't click the link. Instead, check if it's legitimate with Emails from Facebook and Emails from Instagram feature on your app.

Here's how:



Go to Settings by clicking on the top right corner on Facebook

Click Settings & Privacy, then click Security and Login.

Scroll down and tap See recent emails from Facebook.

You'll see emails sent by Facebook. If the email you get is not on that list, ignore it.

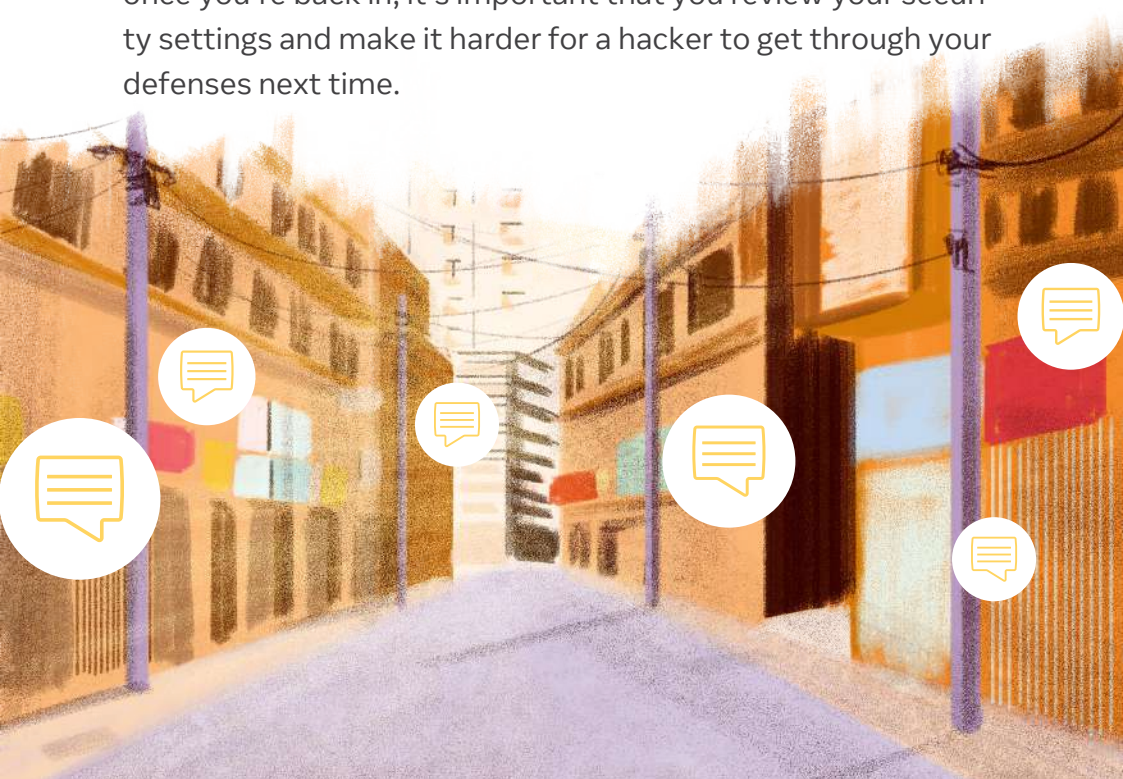
Help, someone took over
my account!



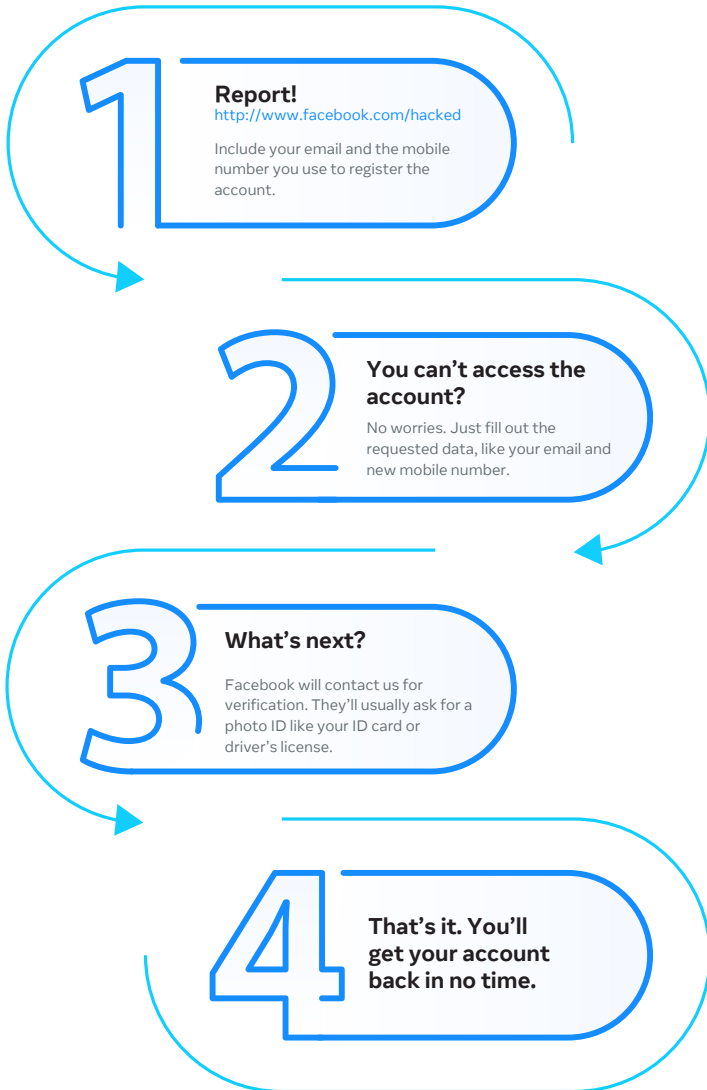
If you think your account has been taken over by someone, it means you're being hacked.

Hackers are an ever-present danger online. They can exploit security gaps, perhaps by guessing a password, or by exploiting a vulnerability in an app, website or program to gain access to your personal information. Sometimes, hackers can try to lock users out of their own account by changing passwords and contact information, or setting up the 2FAC.

If you've been hacked, there are a number of steps you can take to recover your account and get connected again. And once you're back in, it's important that you review your security settings and make it harder for a hacker to get through your defenses next time.



Your Facebook account is hacked?



Your Instagram account is hacked?

1

Report!

help.instagram.com

At the Help Centre, go to policies and reporting – report something – my account has been hacked

2

Oh no. My account is gone.

Your account is gone after you submit the report? Don't worry! That's how Instagram makes sure that your account is actually hacked.

3

Check your email from time to time!

Instagram only sends information on your account through your registered email. Sometimes, Instagram will ask you to fill out a form and send your data, like your photo and ID card.

4

Just wait!

This process usually takes 4-7 days. Just be patient and wait for an email from Instagram.

What if your Whatsapp account has been taken over?

1

Verify your number right away!

Don't panic! Try to access your WhatsApp using your number and verify right away. How do you do that? See here: <http://faq.whatsapp.com/android/verification/verifying-your-number>

2

Enter the 6-digit code sent through a text message.

After you verify your number, a 6-digit code will be sent to your phone. Just enter that code to your WhatsApp to kick the scammer out.

3

Two-step verification

Wait, there's more. After you enter the code, sometimes they'll ask you to enter a two-step verification code. If you don't have the code, it means that it's been enabled by the scammer.

4

So what now?

No worries. You just need to wait 7 days to access your WhatsApp account without the two-step verification code.

5

OK, it's day 7.

Since you've entered the verification code, you can try to access your WhatsApp account again on day 7. The scammer should be kicked out after you enter the verification code.

Making it harder for hackers to take over your account again

Notify your friends

You should let your friends know when your account has been hacked. Tell them not to access or click on any suspicious link or post from the hacked account.

Change your security access

Once you get your account back. Don't forget to secure your account by changing your password from time to time, using a password that is hard to guess, and turning on two-factor authentication.

Review the apps with access to your data

Facebook recommends regularly reviewing the apps that can access data on your Facebook account and removing access to apps you no longer use. Go to Settings > Apps and Websites to do this.

Turn on login alerts

You can get alerts about unrecognized logins from Settings > Security and Login on your Facebook account. When you turn on this feature, Facebook will let you know if someone login to your account from a different device. Facebook will also tell you how to secure your account. And never share the 6-digit registration code or verification code you received via SMS with others.

And you're done!

Now you're ready to not only keep yourself safe online, but to show your friends and family how they can stay safe too.



We hope this guidebook sets out useful tips to keep us all safe online.

Remember, if something seems too good to be true, it usually is.

And if in doubt, report it.

For more information on how to stay safe online, check out the following:

Facebook: [facebook.com/help](https://www.facebook.com/help)

Instagram: help.instagram.com

WhatsApp: faq.whatsapp.com

Instagram Parent's Guide:

<https://about.instagram.com/community/parents>

Bye!