HOW TO STAY SAFE ONLINE: EVERYTHING YOU NEED TO KNOW

We Think Digital

FACEBOOK

Table of contents

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.

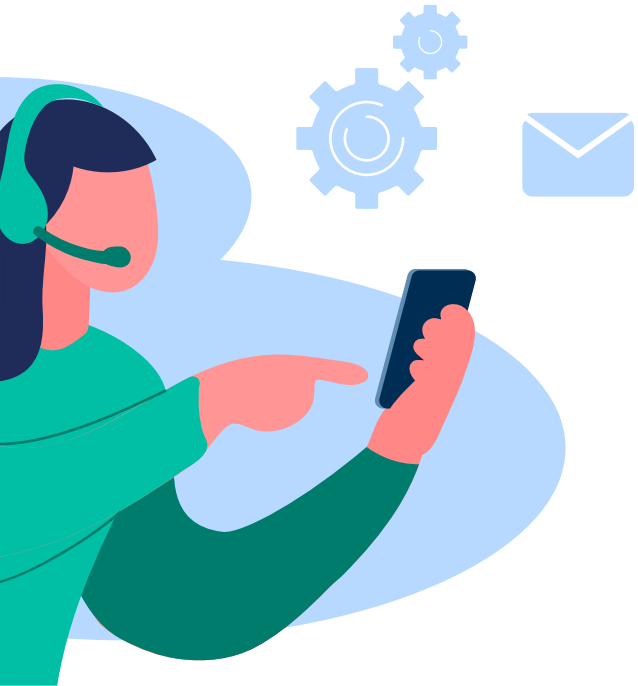
However, it's not just the good guys that are online. So it's more important than ever that we all take steps to stay safe on the internet.

We have all heard stories of online accounts being hacked and used to dupe their followers.

Take a look at this example. A message is sent from Michael's Messenger account or email to his friends asking to borrow money. Michael didn't send that message. But because the message comes from Michael's account, some of the victims agree to lend the money, unaware they are being scammed.

Online hacking comes in many forms. Some hackers pretend to be a representative of Facebook, Instagram, or WhatsApp and send a link. Others pretend to be an old friend and send a link to click. The moment we click the link, our account will be hacked.

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



YOU WANT TO TAKE CONTROL OF YOUR SAFETY AND SECURITY ON SOCIAL MEDIA BUT NOT SURE HOW? FOLLOW THESE SIMPLE STEPS!

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 multiple platforms. Keeping your login information private helps prevent you from being targeted by hackers.

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 account, and never share it with anyone.

Two-Factor Authentication (AKA 2FAC)

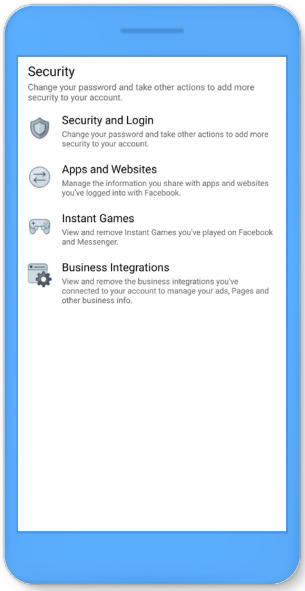
Two-Factor Authentication is an extra layer of security on your account which makes it harder for hackers to gain access.

To log into your account you will need to have access to something you know (your password) and something you have (the one time passcode we will send to your phone or app). This doubles the safety, similar to having a gate and a lock on your house.

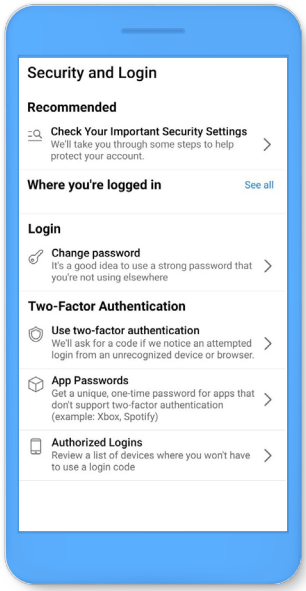
Activating this feature is a simple step you can take right now to keep your account safe.

So how do you activate 2FAC?

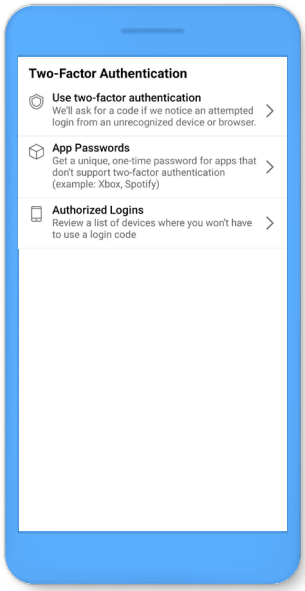
FACEBOOK



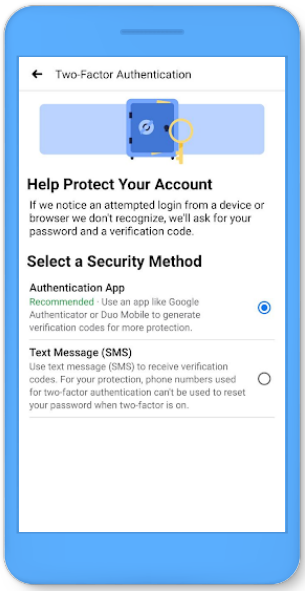
Go to your Security and Login Settings.



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

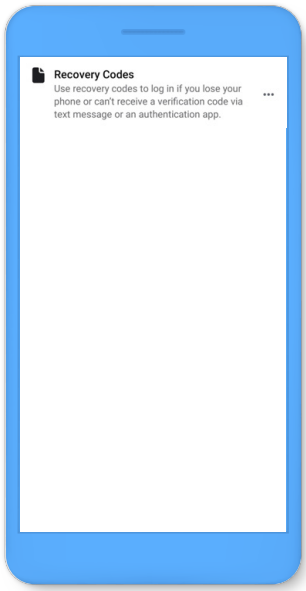


Choose the security method you want and follow the on-screen instructions.



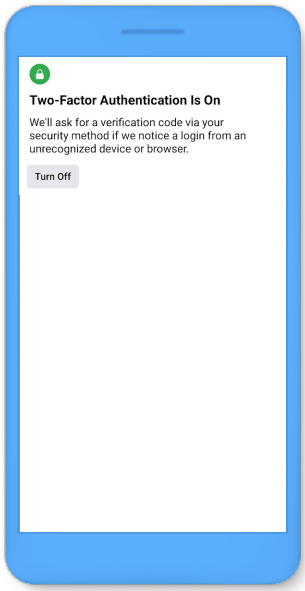
Select a security method:

- Authentication App.
- Text Message (SMS).



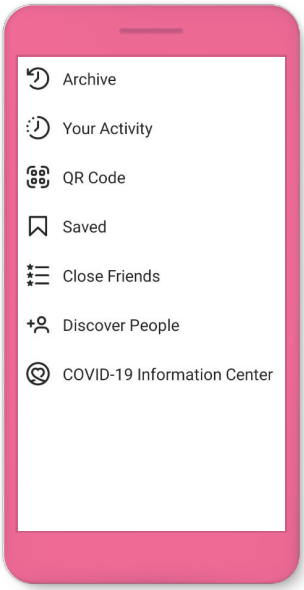
You can also use the following:

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

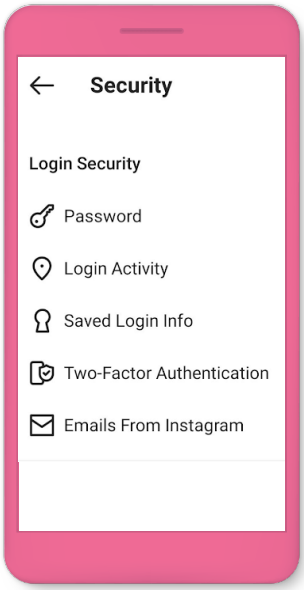


Once the two-factor authentication is activated, we have to input the code sent by Facebook to login from a different gadget.

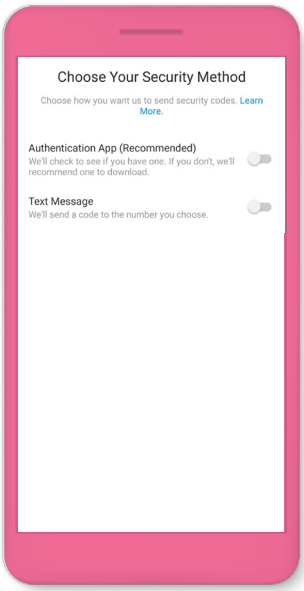
INSTAGRAM



Go to Profile and click Settings.

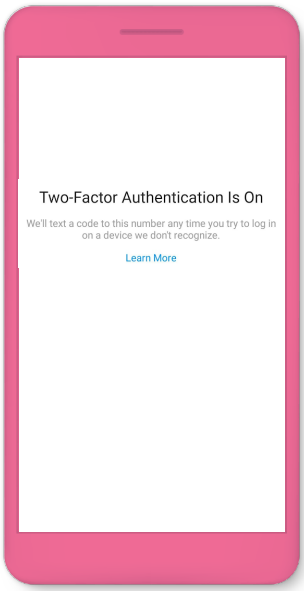


Click Security and go to Two-Factor Authentication.



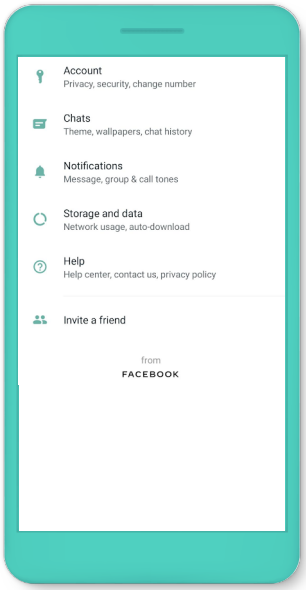
Choose from these 2 security methods:

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

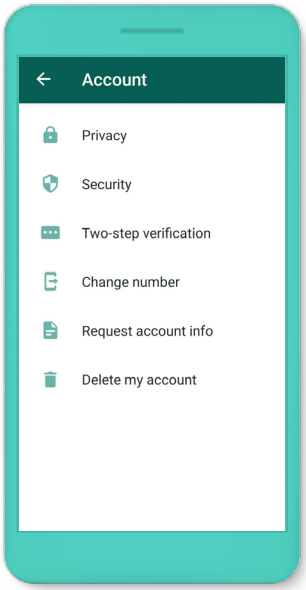


Once the two-factor authentication is activated, we have to input the code sent by Instagram to login from a different gadget.

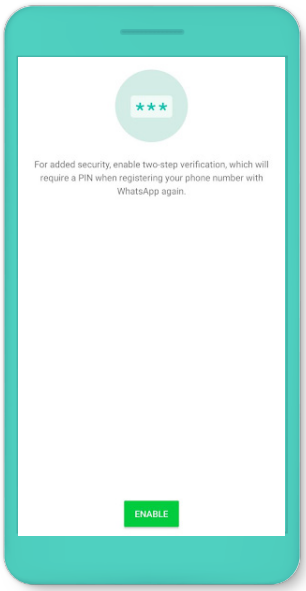
WHATSAPP



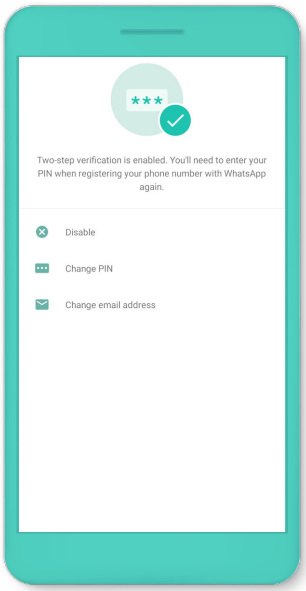
Go to Profile and click Settings.



Click Account and select Two-step verification.



Enable Two-step verification using a PIN.



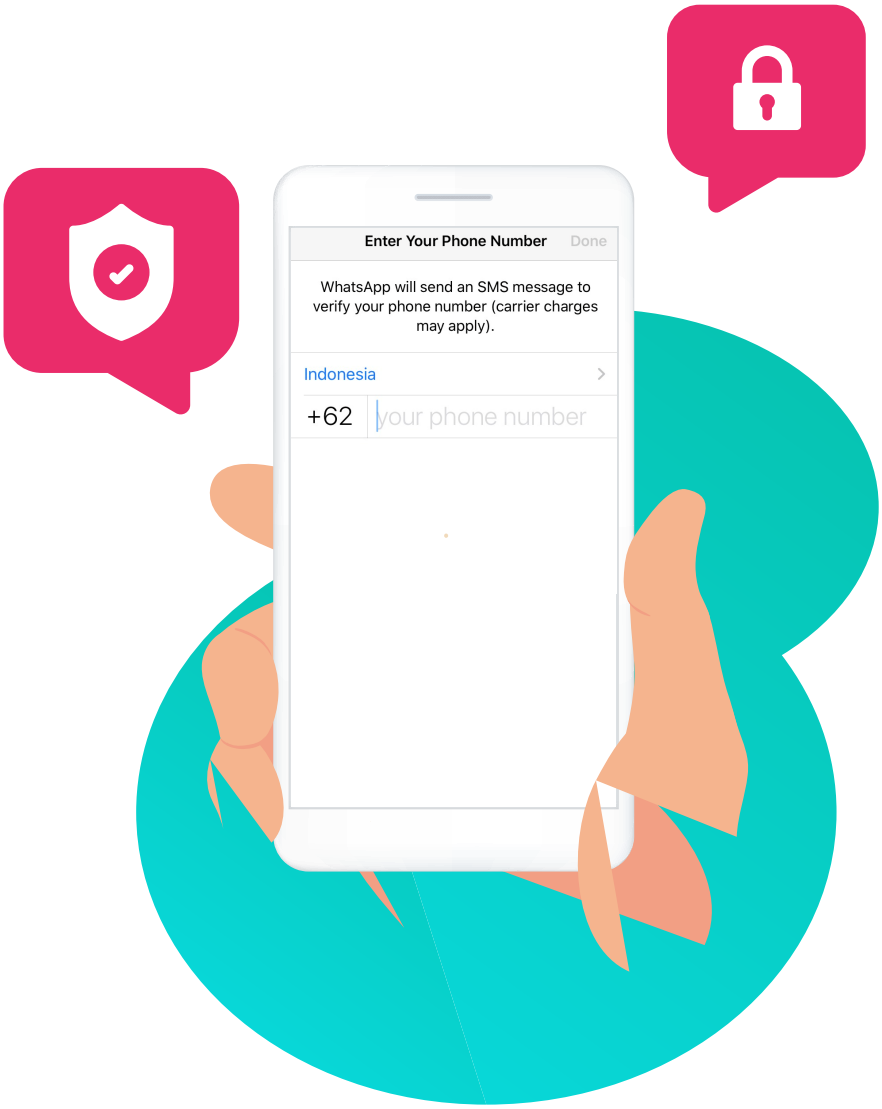
Once the two-step verification is enabled, we have to input the PIN to log in from a different gadget.

Verify Your Phone Number on WhatsApp

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

Remember these important points:

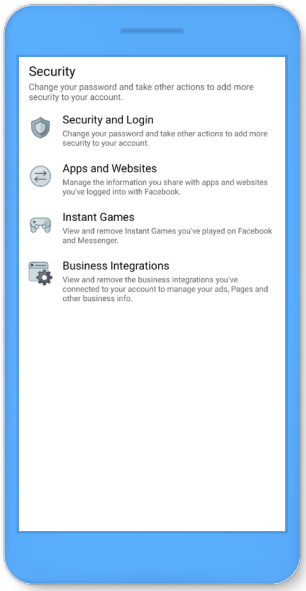
- You can only verify your own phone number
- Make sure you can receive a call and text message on the number you use for WhatsApp
- Turn off any setting or app that blocks phone calls
- Make sure you have internet access for verification



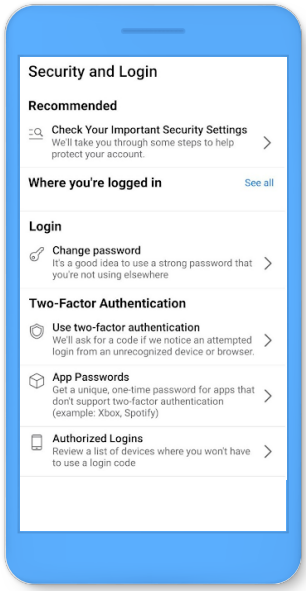
Facebook security check-up

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 our passwords and password security.

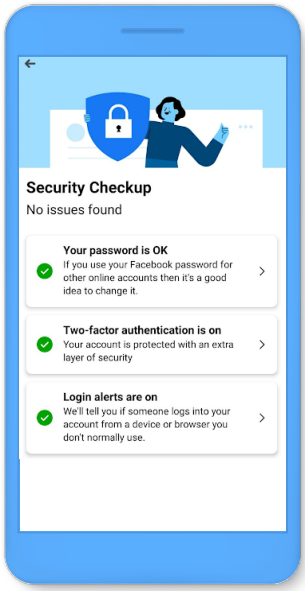
Here's how it works:



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.

Phishing and scams

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 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 emails 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, but good news, the sender 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 if 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. 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 or any attachments. 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.

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.

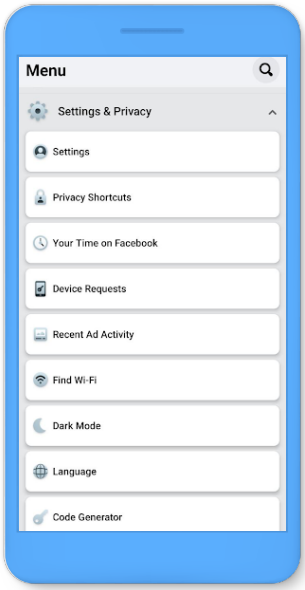
Call the police, and your bank.
If you feel you were the victim of a crime, please contact your local police department. And if you have mistakenly given your credit card details, immediately inform your bank or credit card company and also make sure you report the person or account to Facebook, Instagram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

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

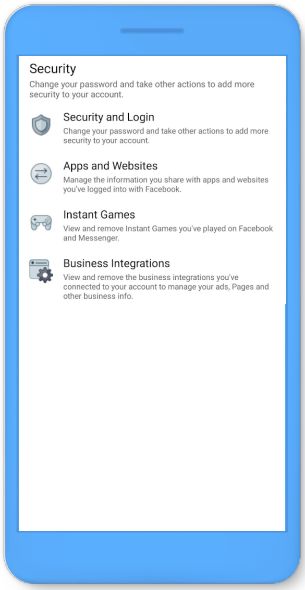
Well, this is another common tactic used by online criminals, often pretending to be from an online platform.

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.

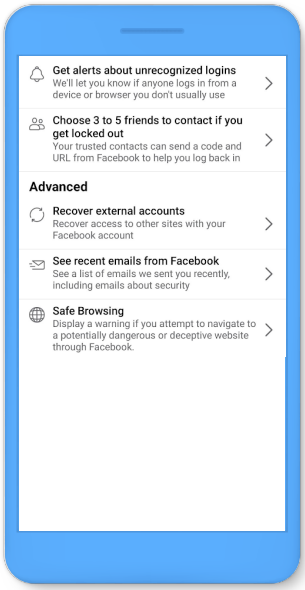
Here's how:



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

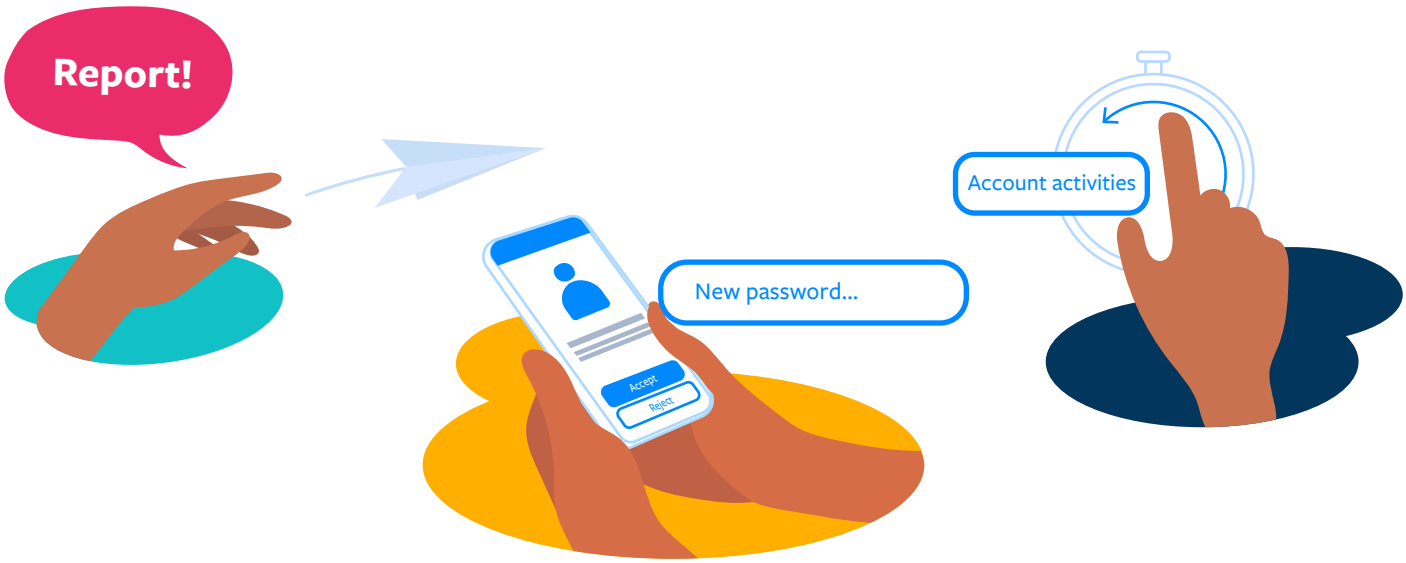


Click Settings & Privacy, then click Security and Login.



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, my account is 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.

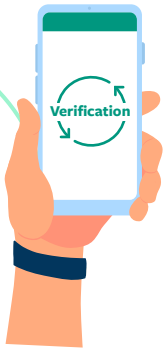
Sometimes, hackers can try to lock users out of their own account by changing passwords and contact information, or setting up the 2FAC.

If you think 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?

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/verifiying-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.

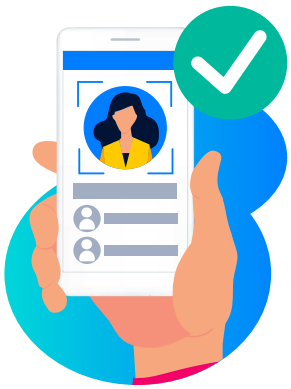
Change your security access.

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.

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.

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.

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 logs in to your account from a different device. Facebook will also tell you how to secure your account.



When someone is trying to log in from a different IP address the right name and password, Facebook can activate the Social Verification function. It will show photos of your close friends and the person logging in has to name those faces.

PRIVACY ISN'T SOMETHING TO MESS AROUND WITH. TAKE CONTROL OF HOW MUCH INFORMATION YOU SHARE ONLINE WITH A FEW EASY STEPS.

Who can see our profile and posts?

You ever got an annoying comment on your Facebook status from a stranger? Or maybe someone shares your photos after you post them on social media?

That sucks. It's annoying. Especially because you know that your profile, photos, and social media status are the perfect tools for gossip.

Well, that's the price to pay to be a celebrity. Oh, wait. Nope. We're not a celebrity. So why? Why would they do this to me?

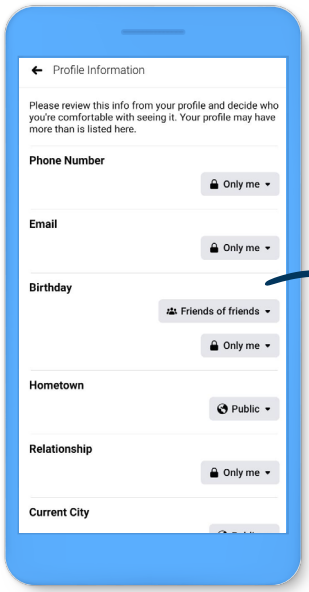
You can control who can see your profile and posts on social media. So you can post photos and update your status without the whole world knowing.

Check out the next page to find out how!

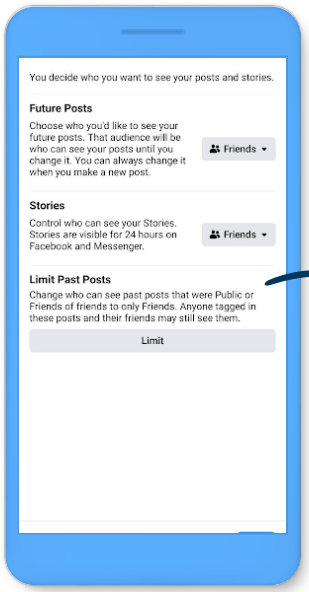
FACEBOOK

First, click **Facebook Privacy Checkup**. Through this feature, you can easily check who can see your posts on Facebook.

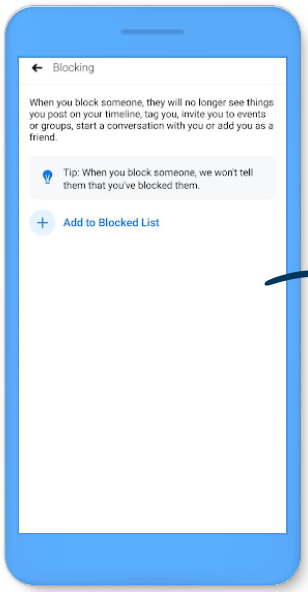
This feature can also help you to:



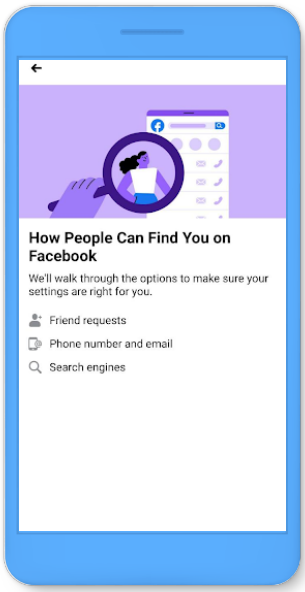
See who can see your phone number, email, birthday, and relationship status.



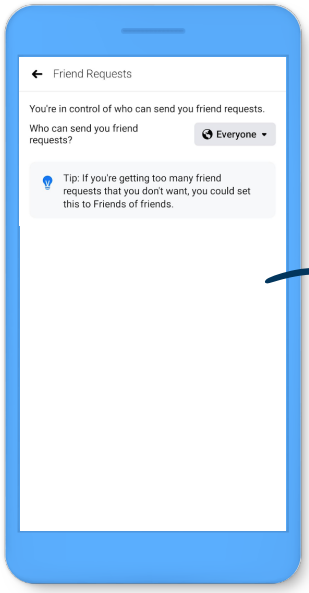
Set who can see your old and future posts.



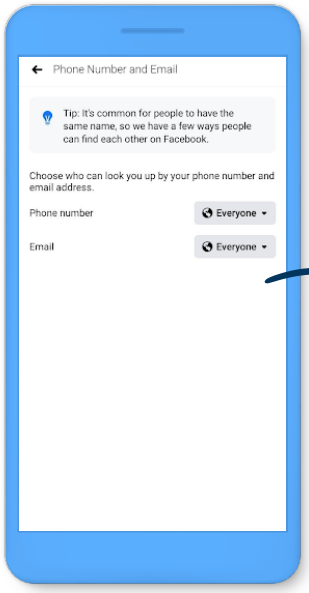
Review accounts that you've blocked on Facebook.



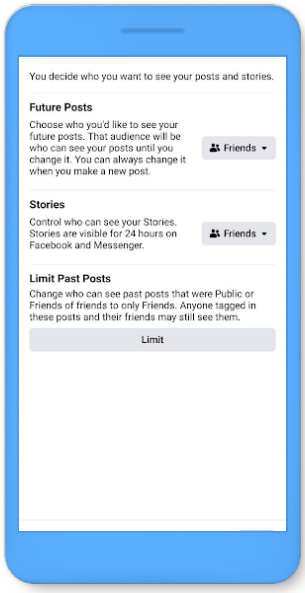
See who can find you on Facebook.



See who can send a friend request on Facebook.



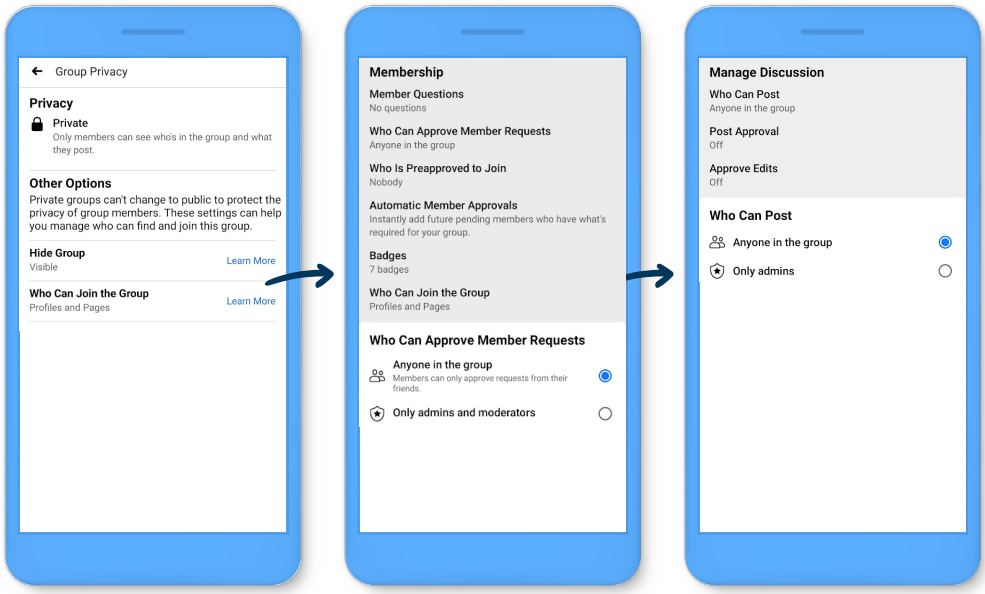
Restrict who can search for your account on Facebook through phone number and email address.



Control who can see your Facebook posts.

FACEBOOK GROUP

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



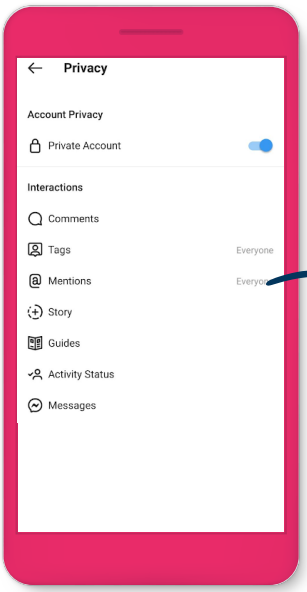
Control who can see your phone number, email, birthday, and relationship status.

Control who can see your old and future posts.

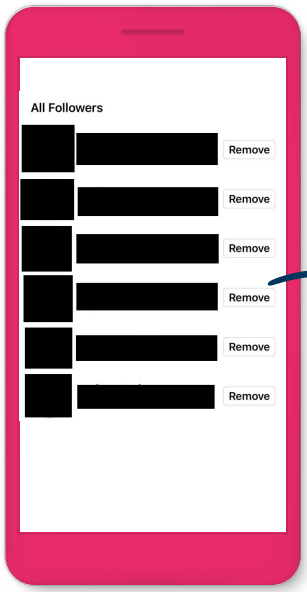
Review who you can block on Facebook.

INSTAGRAM

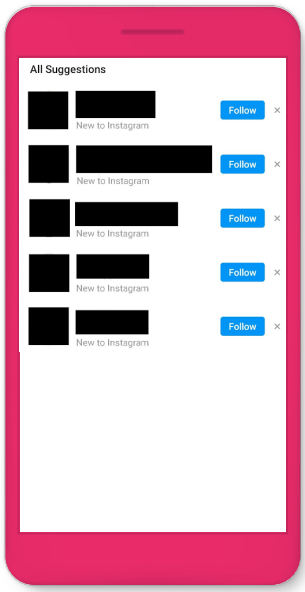
Like Facebook, Instagram features Privacy settings that enable you to manage who can see what you share. There are a few things you can do:



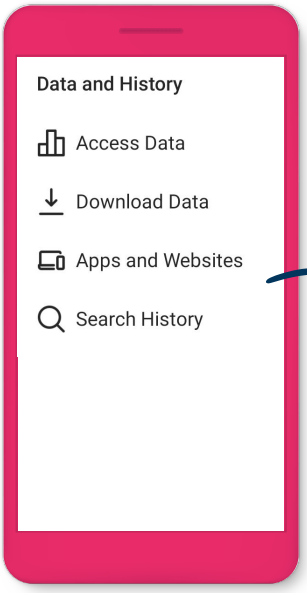
Choose a private account. So only your followers can see your posts and Stories.



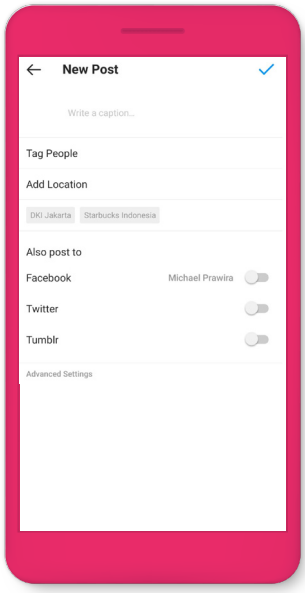
Delete followers on Instagram. You can choose who follows you and keeps up with what you share.



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

Your WhatsApp status tells your friends what you're up to - and we all have friends who change their status very often!

But did you also know that you can change your WhatsApp status privacy setting? So if you don't want everyone you know to see your status, just change your setting.

Here's how you do it:
Go to your status, click on the three dots on top right corner and click Status Privacy. Set who can see your WhatsApp status. Easy peasy.

Facebook Mythbusters

All the questions you want answered.

Does Facebook Listen to My Conversations?

Absolutely not. Facebook does not use your phone's microphone to inform ads or to change what you see in News Feed. We show ads based on people's interests and other profile information – not what you're talking out loud about.

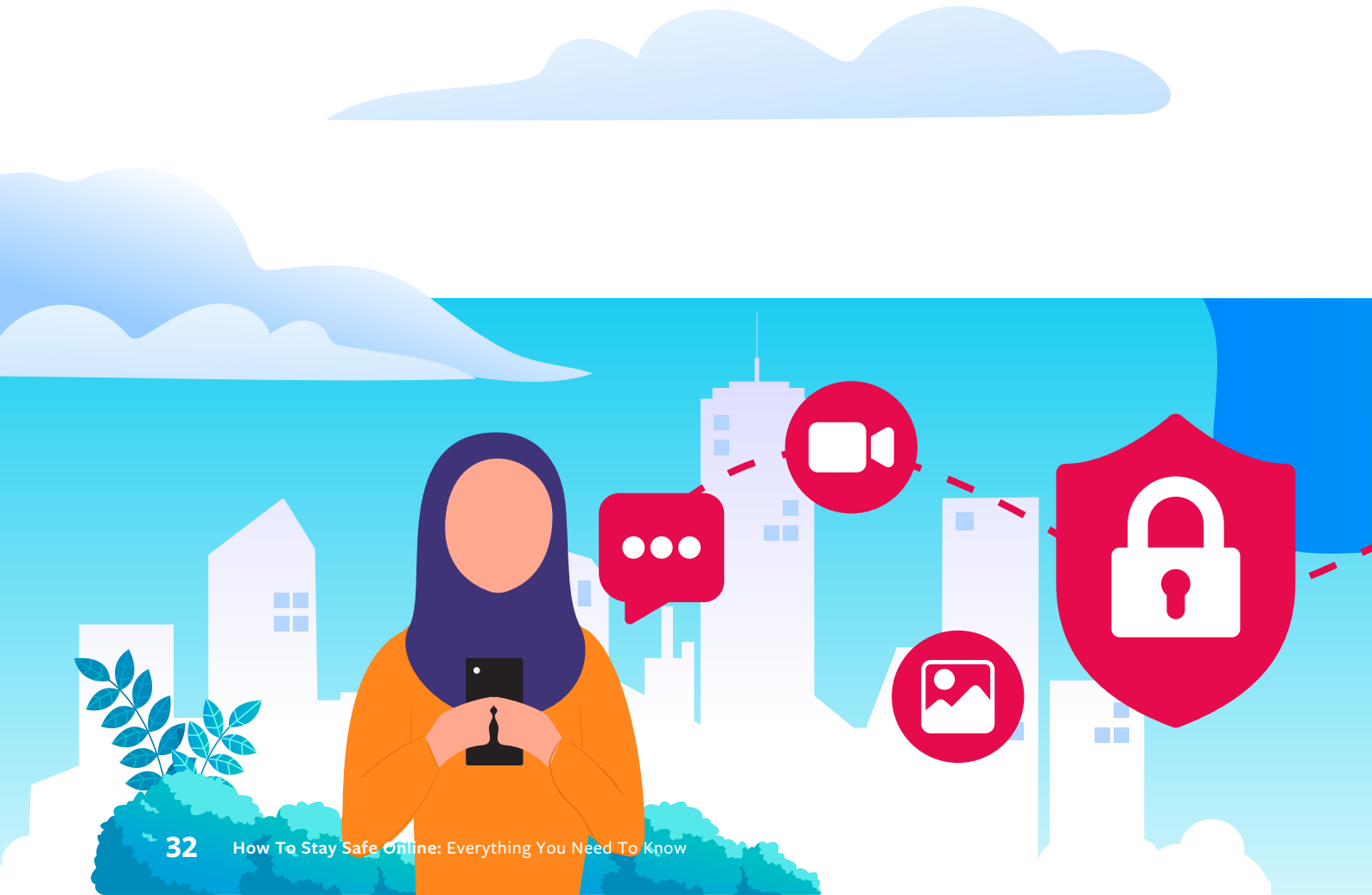
Facebook only accesses your microphone with your permission when you use a feature that requires audio. For example, you want to record a video. You need your microphone, right?

How does Facebook decide what to show me?

- How much you interact with posts from a friend, a group, or a Page. Keep in mind that Facebook prioritizes your friends and family on your Feed
- What kind of posts you usually like and comment on. These can be photos, videos, or links
- How popular is the post from a friend, group, and Page you follow. The more likes, comments, and shares a post has, the more it will show up on your Feed
- Posting time
- Our interaction with a friend or Page. You remember that friend or sister whose posts you like and comment on all the time? Yeah, you'll keep seeing their posts on your Feed
- A mutual interest, like shared friends or groups

What personal information does WhatsApp keep?

Sometimes you may wonder if Facebook or WhatsApp can read your messages. We've heard rumours that your chats, photos and videos are stored centrally by WhatsApp, or that your information will be sold for money. But here's the thing - when you're chatting on WhatsApp, you see that note saying end-to-end encryption? It means that whatever you say can't be read by anyone else. Your convo, video, and chat can only be seen by you and whoever you're talking to.

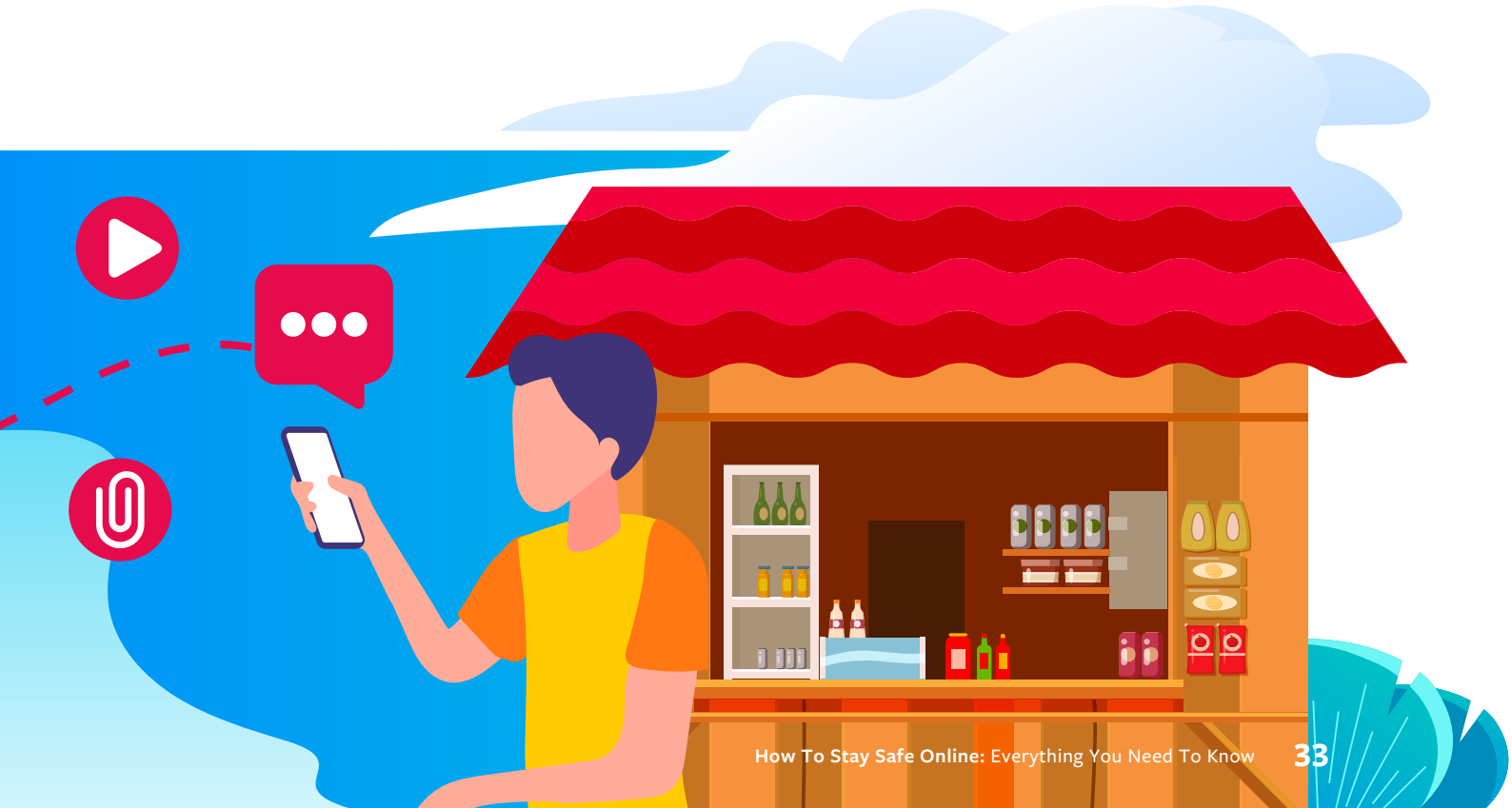


Well, someone can read it if they take a peek at your phone.

It's a bit difficult to explain what end-to-end encryption means. But rest assured. If you see that on WhatsApp, it means that your chat is protected and secure. And your messages stay between you and the person you're communicating with.

Another thing. WhatsApp now has a feature where you can download information on your account. This is all the information that WhatsApp has stored on you.

This "Request Account Info" feature can help you get information on your account, setting, and profile picture, plus the name of the groups you're in.



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, check out the following:
Facebook: facebook.com/help
Instagram: help.instagram.com
WhatsApp: faq.whatsapp.com

Bye!