Digital Security

We can't deny it: the arrival of the internet in our lives has brought so many changes! On the one hand, various facilities for everyday tasks and, on the other, some new challenges, amongst them our online security.

Today, with only a mobile phone, we can solve much of our daily needs such as: communications, diaries, payments, banking activities, purchases, sales, and we have fun, we inform ourselves, we study, we meet people...

Every day we learn to do something new.

But of course, even though everyone does almost all these things, each one of us has a different way of approaching with the internet and our digital devices.

turn the page and follow this idea!

It's important to remember that the internet is much more than the well-known social networks and sites, the internet is a gigantic network of computers and people connected all over the world! It is precisely because this place is so wide and open, where various people pass through, with the most varied information and intentions, that we need to be attentive to the use we make of this space. What happens on the internet is a reflection of the world outside it. Just as we care about our security in our physical lives, we need to take care of our online safety. We also need to protect ourselves against online crime and violence on the internet, that is, violence that happens on the internet or through the tools and platforms that connects us to the digital environment.

Some basic safety cautions are valid for both places. Remember the advice we were told as children?

So, perhaps our mothers and grandmothers didn't even get a chance to know about the internet, but they were so wise that their advice is valid to this day and very valuable for our lives on the Internet!

We can adapt their council for the internet, and they look something like this:

The truth is that there are no magical solutions that will, overnight, leave you totally safe on the internet, **it depends on a sum between daily care and attention + learning and adopting good practices of internet use.** And you can be doing this little by little, being mindful with your time and learning.

We must also talk about all the issues faced by women in online environments. Machismo, misogyny, racism, the various forms of prejudice and violence that we fight against every day, also need our attention when using the internet and we always need to talk about it!

On the following pages you will learn some of these best practices and tips for setting up your applications and turn them more secure. We also invite you to reflect on your uses of digital tools that are also valid for all internet use and how we deal with our information. As you read you can test some changes on your phone if you want. Or you can make the changes as needs arise, being respectful to your time and wishes.

The important thing to remember is that you can return to these pages whenever you have any questions and, the provocations are here to help you increase the care and attention you have in the daily use of networks and the internet. You will realize that with a few attitudes it is already possible to greatly improve your online security, so that you can also be more confident, independent, and present in the virtual world.

Before we talk about the internet and apps, we want to invite you to think a little about your relationship with your digital devices, especially your mobile phone. We've been creating a very close relation with our phones, solving almost everything through it, and take with us everywhere. If we stop to think, how much personal and intimate information does it gather?

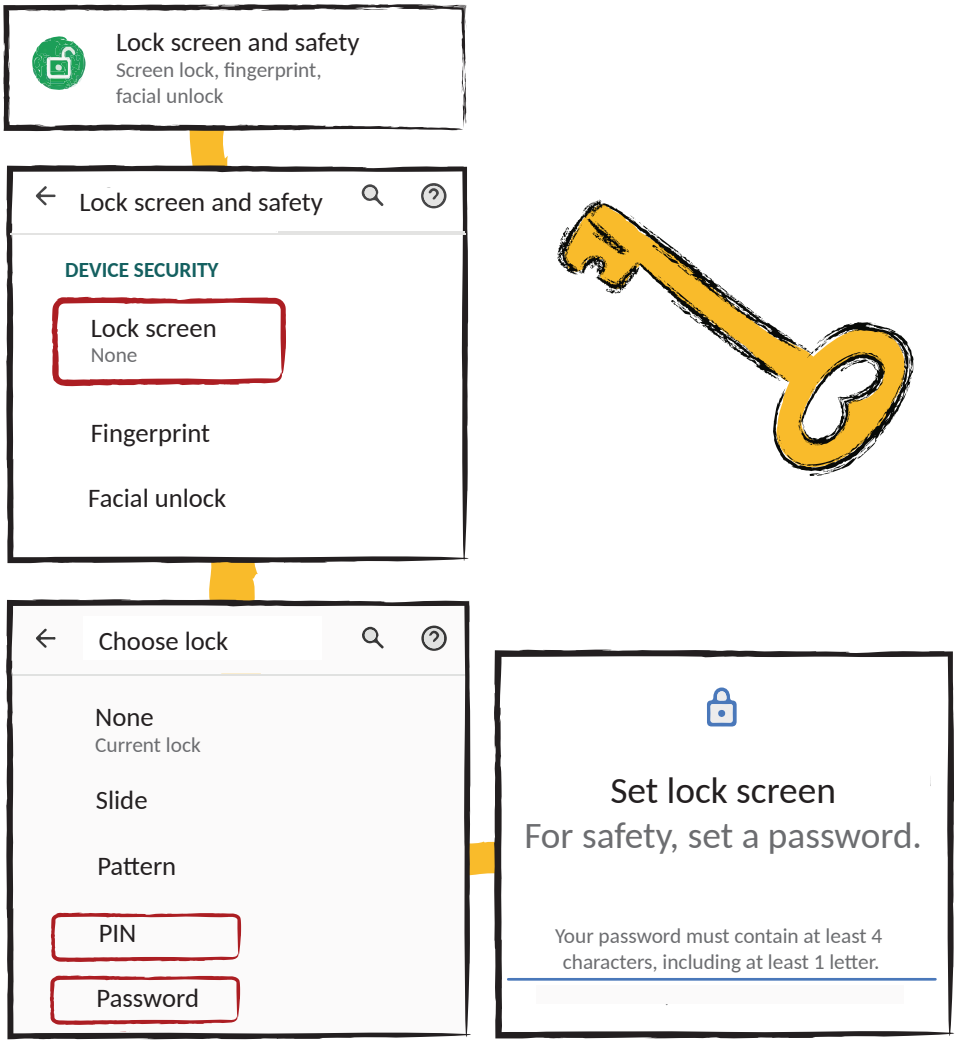
Use a password to lock your phone

When we put a password on our mobile phone, it prevents others from accessing information without our permission. Many situations of gender-based violence happens, unfortunately, between people with whom we are closely relate to and trust at some point. Therefore, it is important not to share your mobile password (or social networks) with anyone, a boyfriend, husband, or any friend. A password is personal information and a layer of security for you.

Settings

To enable a password to your phone.:

Settings > Lock screen and security > choose the options PIN or Password > register the sequence of numbers and do not forget them, you will need it whenever you are unlocking the phone. We do not recommend using "fingerprint" or "standard drawing" password or enabling the "Smart Lock" option.



We also need to talk about online violence!

It's important that you know that digital crimes aren't just crimes involving financial scams. Gender and race violence are also a crime! On the internet this has a name: Online Gender Violence. There are many ways to engage in digital violence: threats, persecution, extortion, exposure, hate speech.

Just as physical violence leaves marks of sadness and traumas on our bodies, online violence can also cause damage to our lives that affects us deeply, so it is important to take care of our digital lives in the same way we take care of our lives and bodies off the internet.

But these situations should not leave us cornered or kept away from online environments, in fact we must occupy these spaces more and more, it is our right! To do this, we must strengthen ourselves and learn safer ways to use digital networks and remain safe.

If you go through anything like this, REPORT IT! It can be at the Women's center or the nearest police station, look for the support from your closest network, talk to friends and family who can welcome and help you, you do not need to go through anything alone. And be open to supporting other women who may be living something like this and need support, it may not always be easy to face this kind of situation.

There are organizations in Brazil that already offer free support services and guidance to victims of online crime, learn more at:

https://new.safernet.org.br/helpline#

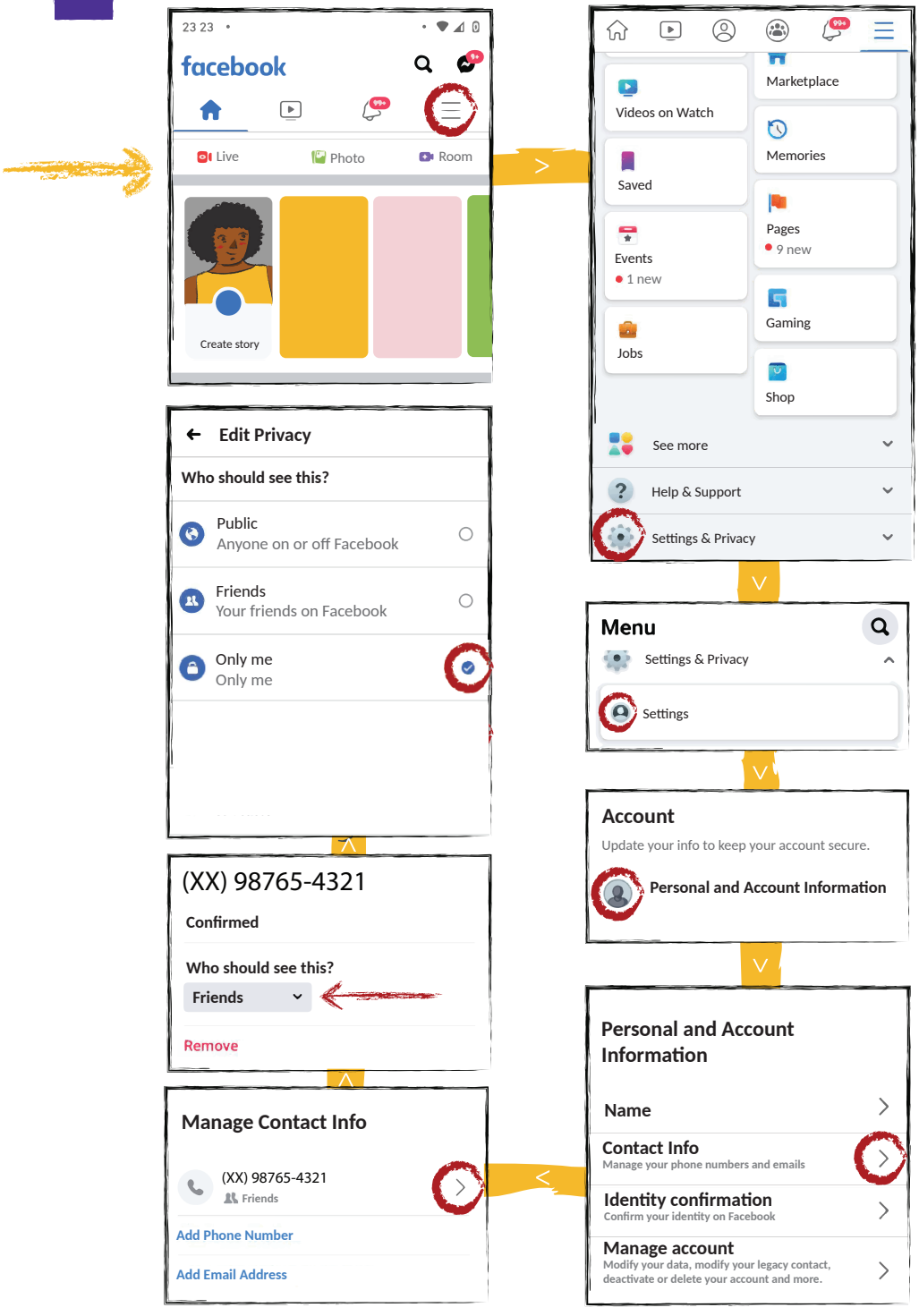
For reflection:

How about creating a network of women in your community or neighborhood who might be ready to support women who experience being exposed on the internet? This can make it easier for victims to know where to seek help and guidance to overcome what has happened.

Much of our online communication takes place today through social networks such as Facebook, Instagram, Tik Tok, Twitter and especially Whatsapp. We participate in dozens of groups and pages, sometimes we even manage some of them, that is, we cross paths with many, many people and we don't always know who they all are and if we can trust them.

Tips for Facebook

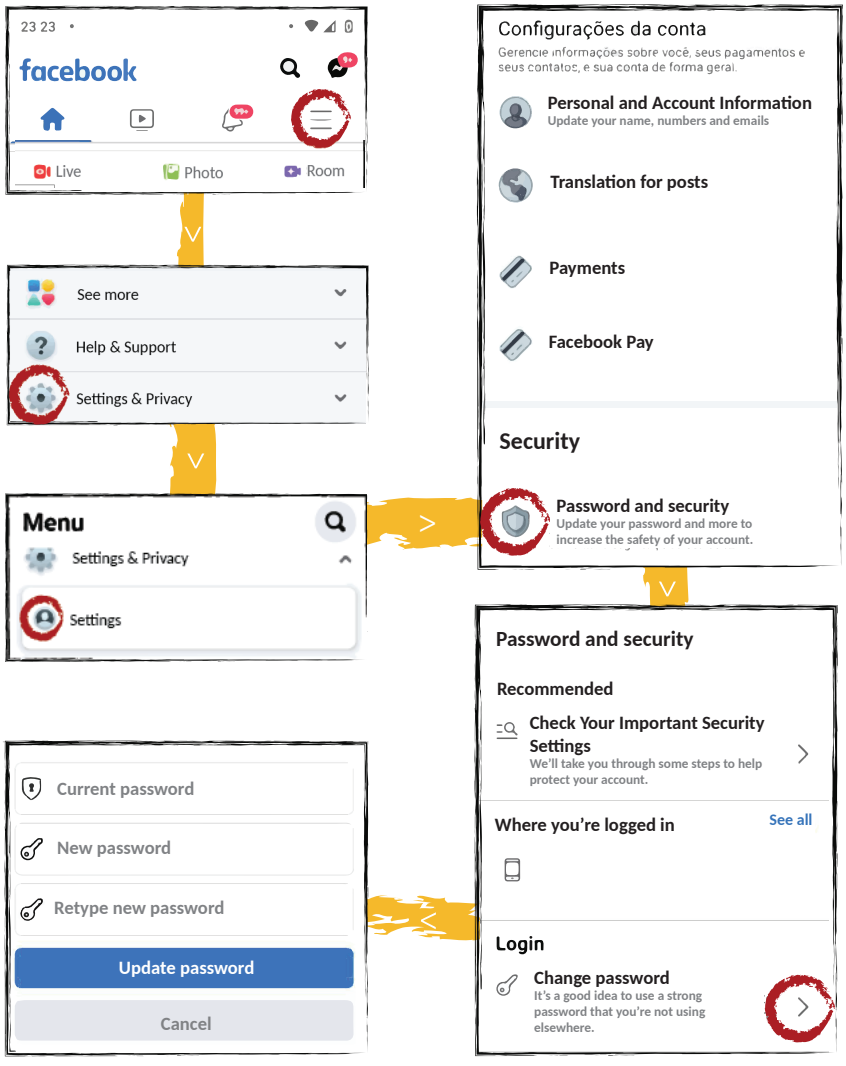
Certain information when gathered can reveal a lot about our lives and habits and can be used in crimes and threats. Avoid posting or at least restricting who can view location data (check-ins and name of the city in which you live), your full name, making your phone number, email available, family members, events attended or will attend, tagging in photos. Use the privacy settings to choose who can view all of this.


23 23
facebook
Live
Photo
Room
Create story
Videos on Watch
Saved
Events
1 new
Jobs
Marketplace
Memories
Pages
9 new
Gaming
Shop
See more
Help & Support
Settings & Privacy
Edit Privacy
Who should see this?
Public
Anyone on or off Facebook
Friends
Your friends on Facebook
Only me
Only me
Menu
Settings & Privacy
Settings
Account
Update your info to keep your account secure.
Personal and Account Information
(XX) 98765-4321
Confirmed
Who should see this?
Friends
Remove
Personal and Account Information
Name
Contact Info
Manage your phone numbers and emails
Identity confirmation
Confirm your identity on Facebook
Manage account
Modify your data, modify your legacy contact, deactivate or delete your account and more.
Manage Contact Info
(XX) 98765-4321
Friends
Add Phone Number
Add Email Address

Securing your account

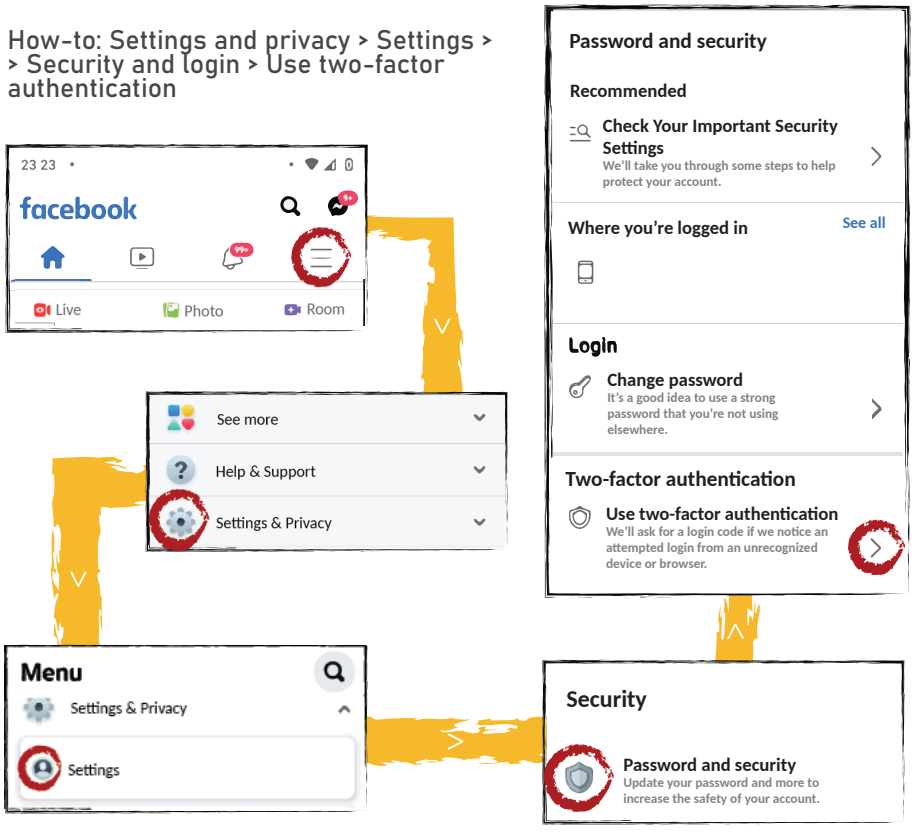
Use strong passwords and remember to change them frequently.

Use several characters such as uppercase and lowercase, numbers, and symbols (example: #SCISSORloveSKY!).
do not use personal information such as names, birthdays, name of the child, mother, dog etc., especially information which is public on social networks.



Enable two-factor authentication. This way you will decrease the possibility of having your profile stolen or accessed by people without authorization.

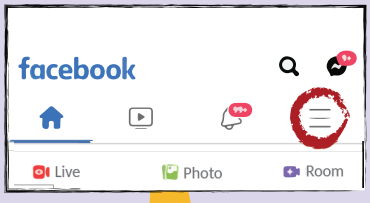
How-to: Settings and privacy > Settings > > Security and login > Use two-factor authentication

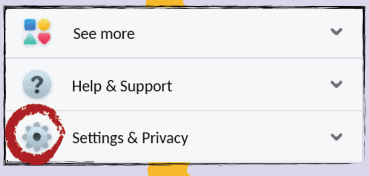


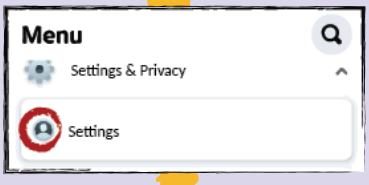
Please note: If a person is in possession of your mobile phone, choosing the option of "Text message" will not solve the problem, because when sending a text message, that message will go straight to the registered number.

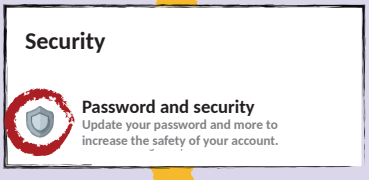
Another tips for more protection

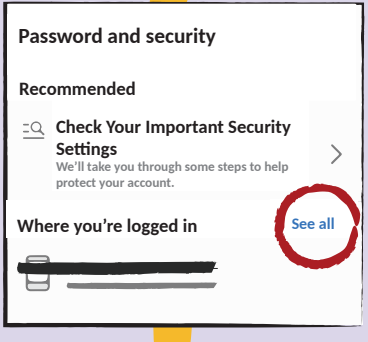
If you suspect that someone other than you is accessing your account, check the history of IPs and devices connected to it, return to the walkthrough of how to change your password, then come back to this point and end all sessions that you do not recognize.







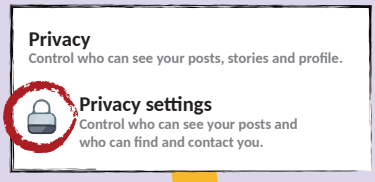


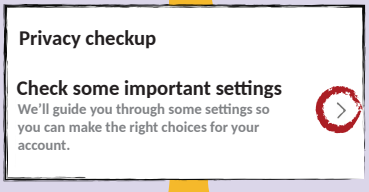


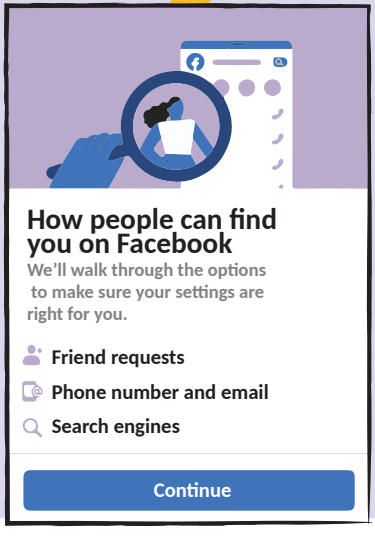
LOG OUT OF ALL SESSIONS

How to: Settings and Privacy >
> Settings > Security and login >
Where you're logged in > see all >
> Log out of all sessions

You're the one who controls your timeline! Closing post permissions and interactions on your timeline prevents others from expressing or attacking you. To do this, enable the review tags of posts where you have been tagged, so you can decide what appears or not on your timeline.

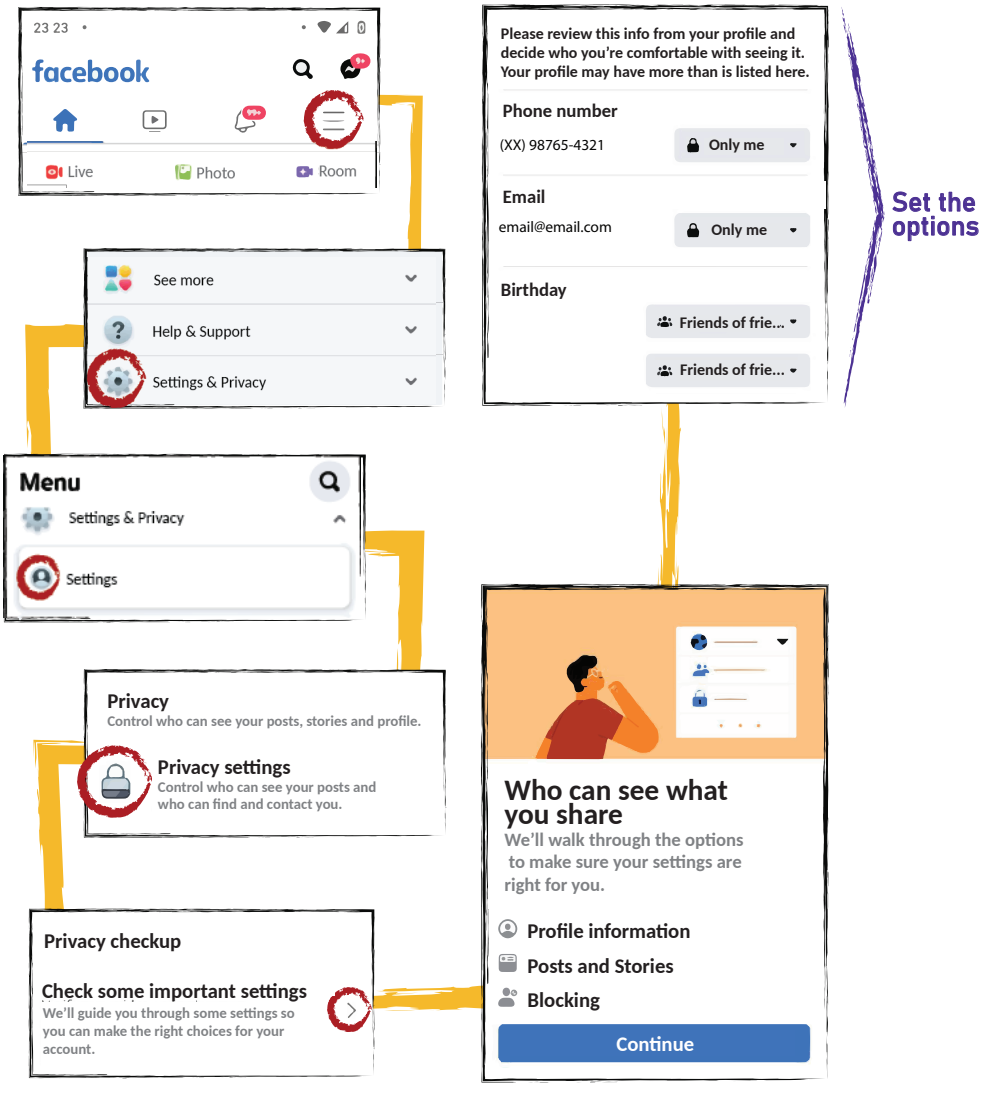






Securing your data

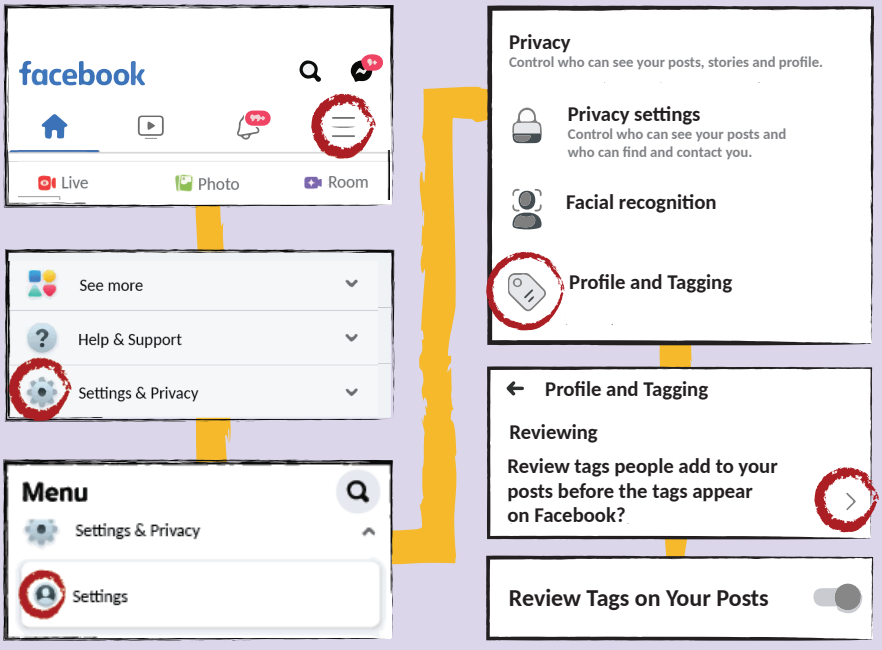
Sometimes we want a post to reach further but when these are posts with more sensitive or intimate content, it may be worth allowing only trusted people to see and interact with it.
To set up who sees your posts:



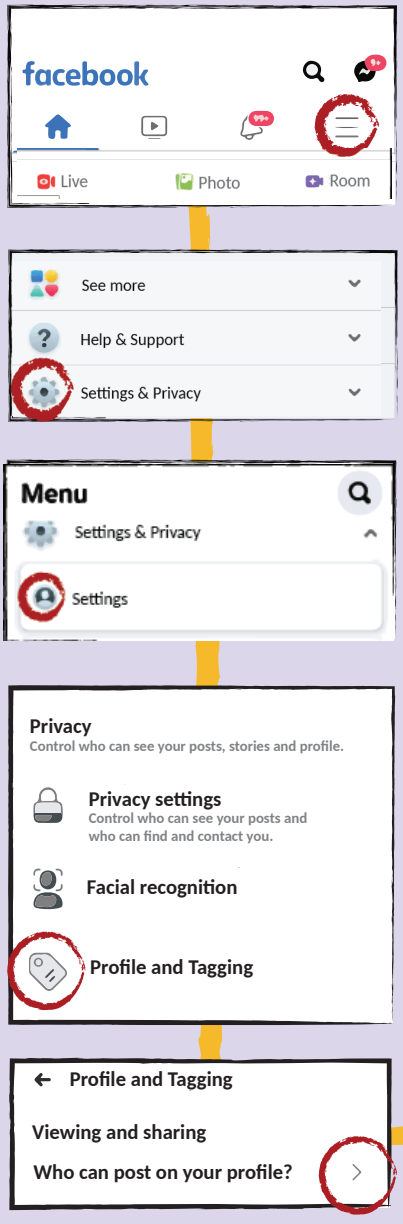
Settings & Privacy > Settings > Privacy settings > Your activity > Who can see your stories > Who can find your profile in searches?

Other tips to protect yourself more

Decrease the chances of exposure even more. Enable the analysis of posts where you have been tagged, so you can decide what appears and what does not appear on your timeline.

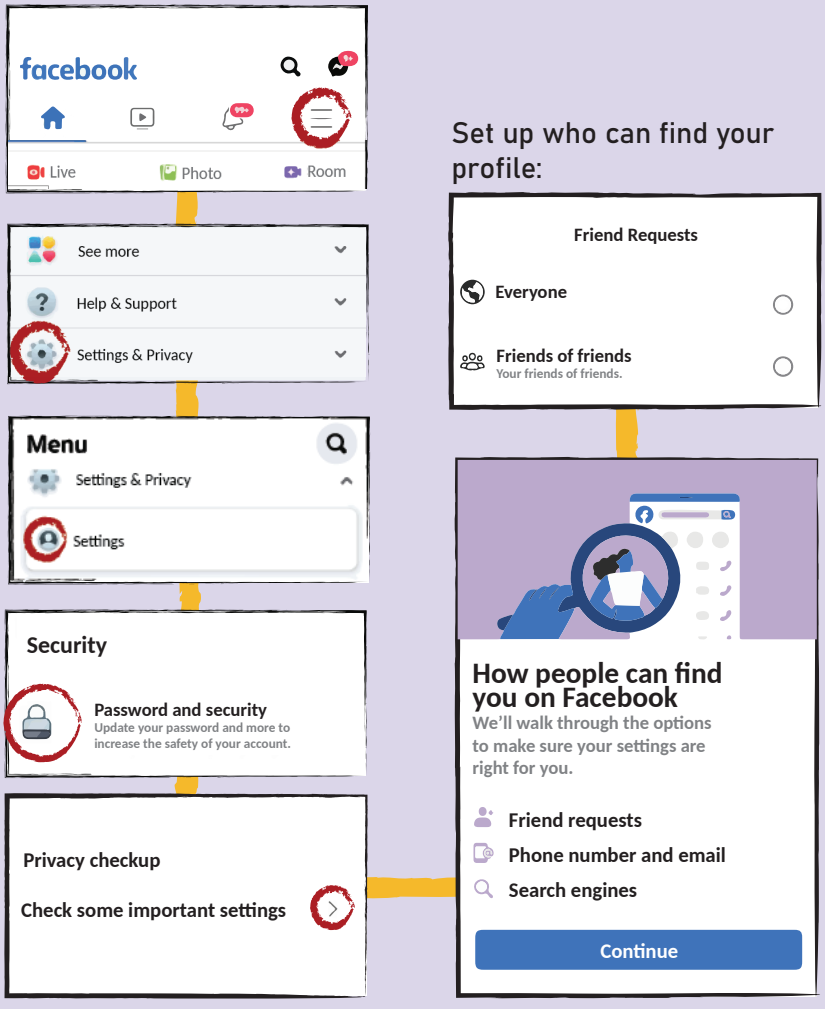


Tip: After turning on the "Review tags in your posts" option, try setting up other options available under "Profile and tagging." The settings you choose for these other options will be valid as soon as they go through your review.



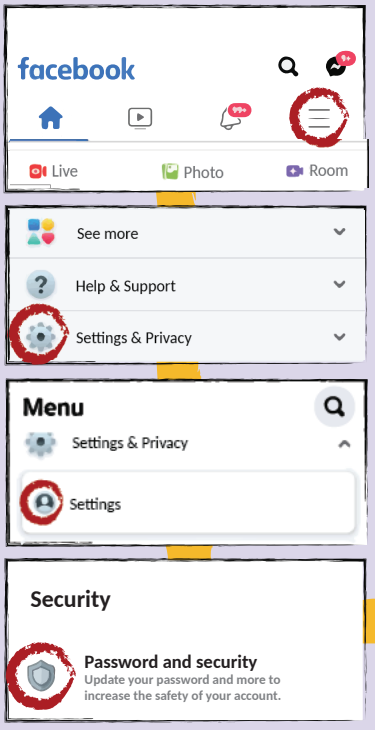
For example: In the "Who can post on your profile" option if you choose "Friends", after the time the post goes through your review, all your friends will be able to view, but if you choose "Only Me".

We invite you to spend time figuring out what other options are possible in these settings and adjust according to your needs or interests.

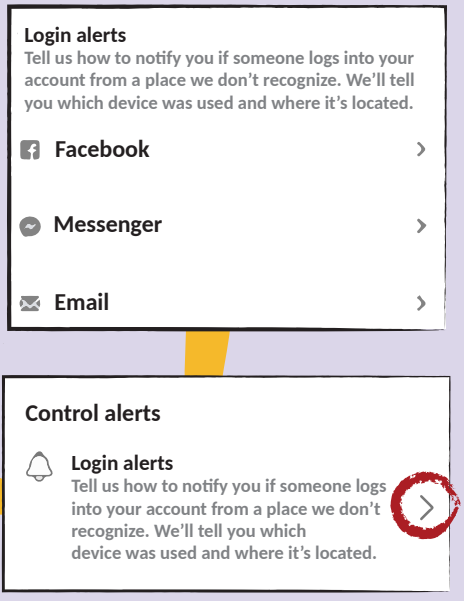


Did you know?

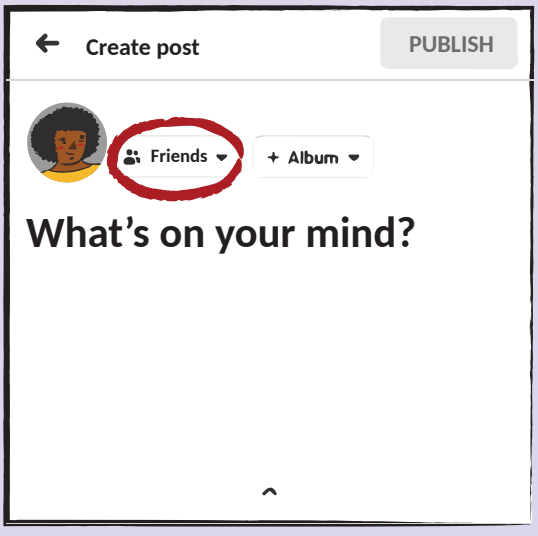
On social networks like Facebook and Instagram you can have a private account, this is a setting that makes your content visible only to your friends and still lets you accept or not a request from someone to follow you. You may even consider keeping a more private profile, to interact with people closer to you, and another audience to address work issues, for example. In your personal profile add only people you know.



You can also set up an alert so Facebook will notify everytime it considers suspect a login into our account:



You can also choose who sees what you post, so that you already set up who interacts with your posts, and limit who views those posts.



To reflect:

Increasing your security on Whatsapp

It is no secret to anyone that Whatsapp is part of the life of most Brazilian men and women. No matter what region of the country they are in, if there's internet, there are people using it to communicate with.

Now, can you imagine if our Whatsapp could talk? What would it say about us? Would it be able to tell a lot of your secrets or things about your privacy? If we think about it, yes, Whatsapp could say a lot about us, including to people who we don't even speak to.

Just add a person, even without their permission, and you can now see their profile picture, name, a message, your status.

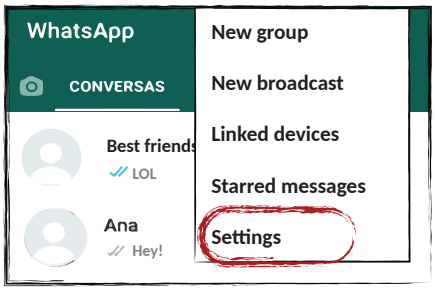
To have more security in Whatsapp, we first invite you to think:

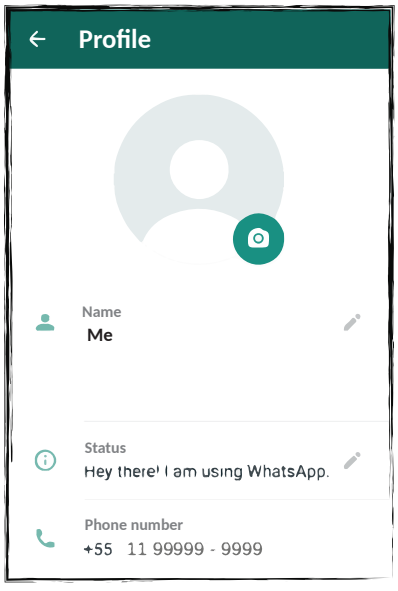
What can people know about you just by looking at your public information on Whatsapp?

Profile picture, status photos, voice messages, phone number...

How much of this information together exposes you?

To modify your personal information, go to:
Menu> Settings> Account > Privacy





Important: Your phone number is the only information here that you can't change or withdraw, so it will always be seen by other people! Remember that.

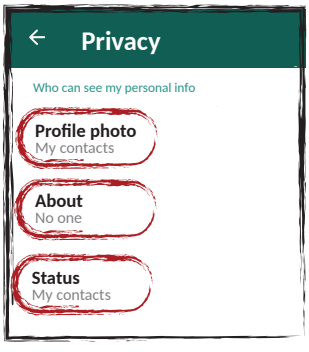
Safety on WhatsApp groups

Everyday we are added to a new group. Let's think about some questions?

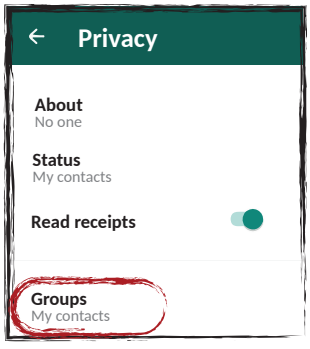
- How do you choose the groups you're in?
- Who added you? Did you authorize them?
- How does this person know your number?
- How frequently do you use those groups? Why are you there?
- Are you in groups with people you don't know?
- Are you sure everyone really is who they claim to be?

To reflect:

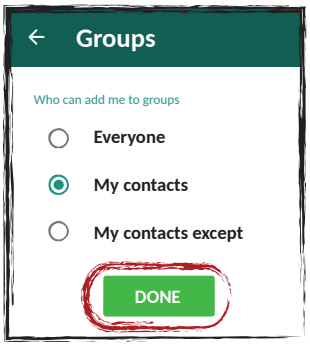
Consider leaving groups that you realize you no longer need to be in, that don't interest you anymore, and especially if there are people you don't know and don't trust, or if the exchanged issues don't interest you. That way your phone number won't be exposed in a place where you have no control of who comes and goes. If you think you need or want to continue in these groups, choose to set up Whatsapp to make your personal information visible only to your contacts.



You can use the following steps to modify these settings and allow only your contacts, saved on your phone, to see your information.
Settings > Account > > Privacy



Then click the "Groups" option and select "My contacts."



Do not forget to click the Save button after changing the settings, this will ensure your new settings are saved. You can configure so that only your contacts can view your information.

To reflect:

Whatsapp Status is, by default, an open place where anyone can view the information, but this can be different, just change the settings. But don't forget that even by adjusting these settings for safer options it's important to remember that in the day-to-day rush, sometimes we add people with whom we don't have any intimacy, people with whom we need to resolve things with punctually and quickly, and who we have a more formal relationship with, such as work contacts.

With that in mind, it is worth reflecting whether the Status should be a place to share information about our personal lives and what kind of information it should be.

Many people like to use this place to leave indirect messages, family photos or parties with friends which ends up exposing your personal life. This way it might be interesting to set up so that only your contacts can view it. You shouldn't stop posting what you like, but it's important to reflect on this type of use.

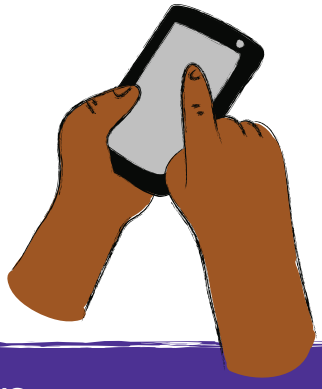
Beware of the links out there...

Since the internet became popular, the use of fake links are a common way to apply scams. They are also used to spread viruses, steal personal information and, with the advent of Whatsapp's success, it has also become a common place for cloning scams.

Beware of links with very attractive advertisements, great offers, discounts and in particular, prizes and gifts that come from nowhere! They are made precisely to convince us that they are harmless, it is very easy to get confused, so try not to click on everything you receive or see out there.

If you can, check before clicking:
Do not click on links sent by strangers.
If you receive something from someone you know, ask them about it and confirm that the person sent you that information.
Just click to open if you feel safe, you are not obliged to open everything you are told to!

If you're in doubt, ask someone you trust for help.



Fake News

Also beware of links with dubious content, false information, misinformation or as we popularly call "fake news":

Be wary of sensationalist content.

Look for the source of that information and see if it is from a trusted media or channel.

When possible, search other sites and see if that information or news has been published on other reliable sites.

And avoid sharing content that you are not sure about the veracity or its origin avoid collaborating in the dissemination of fake content on the networks!

Two-Step Verification or Two-Factor Authentication

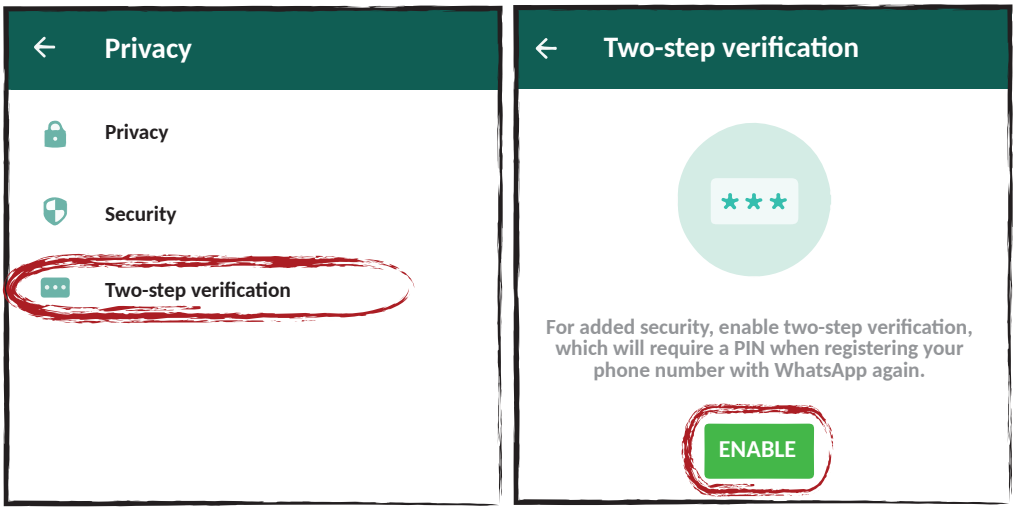
The scams through Whatsapp have become so popular that nowadays everyone knows someone who has been a victim. The most common of these is a cloning of the application but there is a security measure that can help prevent this type of scam in various applications and even Whatsapp, and it is called "Two-step verification".

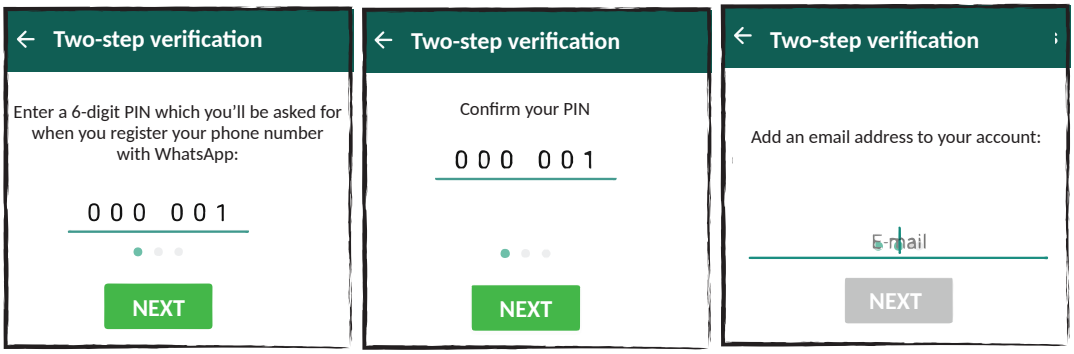
What's it for?

It prevents third parties from activating your account on another device.

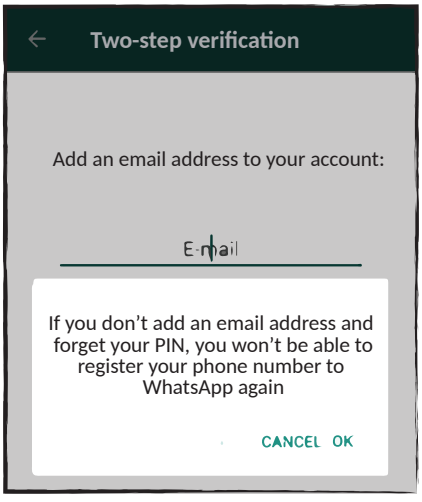
How does it work?

In any attempt to access your account using other devices and/or through third parties, you will be asked to confirm a code, sent at the time of access or a code you can register in advance. If someone tries to use your Whatsapp on another phone, such as in the cases of cloning, they will be asked to enter these codes. Because only you will know the code you created, this will prevent the person from being able to finish installing Whatsapp on another device using your number.



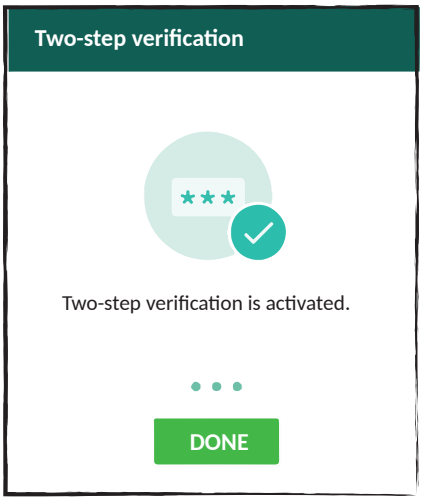


In the case of WhatsApp, when you enable two-step verification, you will have to register a six-digit code, which is called PIN (attention, this is not your phone PIN, it is a code that you will create on the spot, it is the WhatsApp PIN).



Don't forget to click the "Done" button to save your new settings. And don't be alarmed if the next time you open WhatsApp it asks you to type the PIN, as we said earlier, it does this to help you memorize those 6 digits.

You have the option to also register an email to redeem this code if you forget it and more, Whatsapp will ask you to confirm the PIN code, so you need to memorize the 6 digits, ok?



However, there are some details which you need to be aware to don't have problems:

1. When you need to install your Whatsapp on another phone, such as when you buy a new handset, you should use the same PIN code, so you need to memorize it and never forget it! If you forget this code, you will not be able to use Whatsapp again with your number on another device.

2. If you do not have an email to register or prefer not to use this option is still possible to enable two-step verification, but make sure you will not forget this code. Write it down somewhere safe and destroy the note when you're sure you have memorized it.

3. Finally and very important: do not give this PIN code to anyone, especially if you receive any message, text, call or email requesting this code, even if it appears to be a genuine message distrust it, do not inform the PIN to anyone. An operator will never ask you for this information, neither your bank nor any store. It's a common scam, so stay alert!

Curiosity

How do most common WhatsApp cloning scams work:

You may have heard of people who receive messages with a code that they didn't request, and then they receive another message or call from a person identifying themselves as someone who works for their phone provider, for example, they might say they sent the code to the wrong person, so they ask the victim to tell them the code they received a few minutes before. At that moment the person who is scamming gets the code and can install the application on another phone using the victim's number, and just like that their Whatsapp is cloned! This is especially true for those who do not have a two-step verification enabled. So, stay alert!

The internet is, yes, WONDERFUL! It is a great tool that can help us with many different things: with communication, at work, in militancy, to inform us, to make purchases and sales, have fun and much more... But we need to be alert to some details... such as the tips given in this booklet.

Although online life sometimes seems easier, after all, we can do pretty much everything without leaving home, keeping our relationships out of digital spaces also keeps us strong, so we need to find a balance. Use the internet but don't undermine the importance of eye-to-eye connection and conversations.

To dedicate our time to taking care of our health, our nutrition, our homes, and our families are all activities that need our care and attention too, pleasurable activities we must rescue and remember the things we like to do in groups or even alone outside the internet. There's a lot of fun to be had also outside of video games and social networks and when we're happy we have so much more to share and show our loved ones and the world!

This publication was developed as part of the project “Action-research on Feminist Autonomous Networks”, supported by the Feminist Internet Research Network (FIRN) led by the Association for Progressive Communications (APC), and funded by the International Development Research Centre (IDRC).

The project was coordinated by Bruna Zanolli and Débora Prado and had the collaboration of a working group also joined by Carla Jancz, Daiane Araujo dos Santos, Glaucia Marques and Natália Santos Lobo. More information is available at firn.genderit.org/research/action-research-feminist-autonomous-networks

With special thanks to the residents of the Barra do Turvo quilombos, in Brazil, and to the women and partners of the Sempreviva Organização Feminista (SOF), the Rede Agroecológica de Mulheres Agricultoras (RAMA) and the MariaLab. The production of this zine was based on information from the action-research project and had the collaboration of Violeta Cunha and Helena Zelic. It was translated to English by Silvia Leal

Partners:

Supporters: