Protect yourself from identity theft on WhatsApp

Reading time: 7 min | 1,276 words

Content

1. What happens if your identity is stolen on *WhatsApp*?

Identity theft on *WhatsApp* can be a real headache. Criminals impersonate you to scam your contacts, ask for money or collect your personal information. This not only affects your personal and professional relationships, but can also have serious financial consequences. According to TransUnion’s latest report, digital fraud will increase 140% in the region by 2024.

Dealing with the uncertainty and consequences of this is stressful and exhausting. Regaining control of your *WhatsApp* account and mitigating the damage can take considerable time and effort.

RISCCO

2. How can you prevent identity theft?

It is important to protect your *WhatsApp* account. The following best practices and security tips will help prevent you from becoming a victim:

1

Enable the two-step verification option in *WhatsApp*.

Available in your *WhatsApp* account settings, this feature requires a PIN code to register your account on another mobile phone. This PIN is a 6-digit number that you create and must remember in order to add your *WhatsApp* account to a mobile phone. You can enable it (on both Android and iOS) in **Settings > Account > Two-step verification.**

2

Do not share your unique *WhatsApp* verification code:

This 6-digit code is provided by *WhatsApp* via text message (SMS) when you add your phone number and is randomly generated. The SMS begins as follows (on both Android and iOS): "<#> WhatsApp code: [code]". Do not share this code with anyone. If someone asks you for it, it is a clear attempt to take control of your *WhatsApp* account.

3

3. Associate your email with *WhatsApp*:

Add your email address to make it easier to regain access to your *WhatsApp* account if you don’t remember or have the two-step verification PIN. If an attacker tries to access your *WhatsApp* account, they will also have to go through this security check, in addition to the code sent via SMS and two-step verification. This would make it even more difficult for the attacker to access your account. You can associate your email (on both Android and iOS) in **Settings > Account > Email address**.

4

Back up your *WhatsApp* conversations regularly:

Enable automatic backup of your chats to the cloud to protect and retrieve your conversation history. Set this up (on both Android and iOS) in **Settings > Chats > Backup**. This option allows you to back up to Google Drive on Android or iCloud on iOS.

5

Limit who can see your information in *WhatsApp*:

In WhatsApp's privacy settings, limit who can see your profile picture, status, and last connection. Choose "My contacts" or "My contacts except..." for more privacy.

RISCCO

3. What to do if you are already a victim?

Regardless of whether or not you have already regained access to your *WhatsApp* account or not, the first thing you should do is to inform your important contacts via other means such as social networks, email or phone calls, warning them that your *WhatsApp* account has been compromised and that they should not trust any messages sent from your account.

Here are some recommendations in case you did not follow the precautions mentioned in Section 2 of this article and gave the SMS verification code to the attacker:

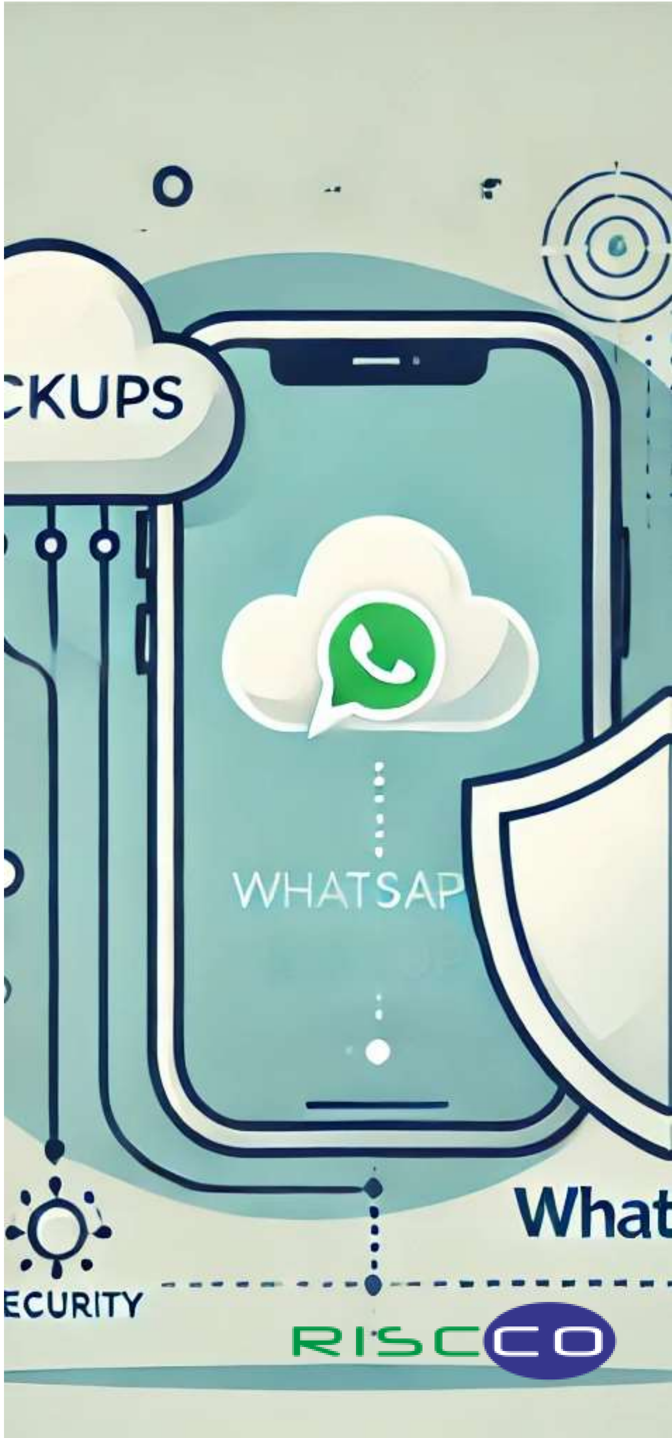
1 Recover your *WhatsApp* account:

From your mobile phone, you will need to open the *WhatsApp* application that you have already installed, enter your phone number, and request the verification code that you will receive via SMS and enter it into the *WhatsApp* application to access your account. This will also close any active sessions of your account on other devices (the attacker's phone or *WhatsApp* Web).

If *WhatsApp* asks you for an additional PIN after you enter the SMS verification code, it means that the attacker has enabled two-step verification. The "Forgot your PIN?" option will appear on your phone screen. If you select this option, *WhatsApp* will send you a link to the email associated with the account to disable the two-step verification PIN.

However, if there is no associated email or the attacker added their own email, you will not be able to deactivate the PIN at that time. In this case, you will have to wait 7 days for *WhatsApp* to automatically deactivate the two-step verification PIN. *WhatsApp* implemented this period to protect its users from improper access, giving them time to recover their account in situations where an attacker set up an email.

In such a case, if the attacker receives the link in their email and accesses the link, this would only disable the two-step Verification that the attacker set up, making it easier for you to recover your *WhatsApp* account.



During these 7 days, neither you nor the attacker will be able to access the account. After this time, you can enter your phone number into *WhatsApp*, which will generate a new SMS, the code of which you will have to enter into the application, and this time you will not be asked for the PIN, which will allow you to recover your *WhatsApp* account.

2 Notify your contacts that you have recovered your *WhatsApp* account:

Once you have recovered your account, immediately notify your contacts that the problem has been resolved. Ask them to ignore any suspicious messages sent while your account was compromised.

3 Follow preventive measures:

Once you have regained access to your *WhatsApp* account, it is important that you follow the recommendations in Section 2 of this article to protect your account from future attempts at identity theft through *WhatsApp*.

RISCCO

Contacts

Antonio Ayala I.
aayala@riscco.com

Rubén Fernández
rfernandez@riscco.com

Roberto Delgado
rdelgado@riscco.com

riscco.com

It is an independent international company dedicated exclusively to helping organizations meet their challenges in GRC (Governance, Risk & Compliance) and ESG (Environmental, Social & Governance); composed of professionals with the knowledge and credibility necessary to translate very technical aspects into a simple language with business sense. With fifteen (15) years of having started operations, RISCCO has in its client portfolio private companies and Government Institutions in the region leaders in their field.