

# WhatsApp: Learn how to make the mobile app safer!



Brazil is the world champion country in the ranks of frauds involving the messaging app WhatsApp. According to Kaspersky, an antivirus business company, they identify more than 76 thousands scams involving the tool. Fortunately, the users can protect themselves in various ways, using different kinds of resources and functions.

Still, the messaging app offers to their users, some tools that assist them to keep their privacy and security. We can talk about the authentication in two phases, and account recovery, for example. Also, Meta, the business company that owns WhatsApp, Facebook and Instagram, launched, recently, a security center.

The messaging app users can search for tips and strategies to avoid not only scams involving WhatsApp, but the spams in the application software. By the way, Meta has been

worrying about not only offering their users a better experience, but a way to protect their information, data, and privacy.

At the moment, the messaging app is present even more in peoples routine, whether in conversations with friends and family, or in business reunions. Thus, it is essential that WhatsApp try to offer more security and tranquility to their users.

## **WhatsApp security resources**

The two-phase authentication works like a user's verification in two ways. Is an additional function of WhatsApp. The objective here is to prevent the misplacement of the user's account. This tool can be used in situations where the cybercriminals try to break into the messaging app through access code sent to them.

Thus, the software application user can create an optional password requested by WhatsApp. Is worth mentioning that it will be solicited after a confirmation of the telephone number. The messaging app will ask again for access to the user profile in case his cellphone has been robbed. He will receive a message with a confirmation code, through SMS.

The cybercriminal will then be automatically blocked to use the tool. In some cases, the user will receive a verification code in two steps. If he can't access it, that means that the cybercriminal has robbed his account and has activated the function. The user will have to wait for seven days to access his account again. In this case, he will need to click on "Forget the Pin code?" and reconfigure the numerical code through the app.

## **Other security resources**

WhatsApp users with the Android operational system in their cellular phones can activate the option to block the software application. Through this function, the messaging app will

then be liberated to the user using biometric through the mobile device. This way he can choose digital or facial recognition.

In summary, this security resource is activated by the cellular phone configuration. In the case of Apple's users, it is possible to block WhatsApp through the function Touch ID or Face ID. They are present in the mobile device. One can choose the time of the biometry request blocking the phone in a predetermined period.

Another resource that is worth mentioning is a function that allows the user of WhatsApp to protect their photos of unknown people. It's a good option for users that desire to have more privacy in using the messaging app. In short, it is possible to choose the contacts authorized to see the profile photo.

## **Conclusion**

Whatsapp users also can avoid being added to unwanted groups. With this resource, they can indicate the contacts that can't include them in their social groups in the messaging app. It is a great tool when someone tries to add a profile insistently but the user doesn't want to be added and participate.

In conclusion, the WhatsApp central security offers to the messaging app users a great number of tips that can help him to not be involved in scams. Meta is at the moment encouraging people to denounce and block fake accounts that can be involved in frauds and publish invasive contents.