SEDENA

SECRETARÍA DE LA DEFENSA NACIONAL

SECURITY RECOMMENDATIONS FOR USING WHATSAPP

Target of WhatsApp account theft

Account theft is a modus operandi used to extort or defraud victims' contacts and obtain other numbers to do the same.

How is account theft possible?

The ways in which cybercriminals can steal your account are very diverse:

Some cybercriminals can steal your account through suspicious text chains, or by sending you messages to advertise contests, where they claim you could win a prize.

It has also been detected that in the context of the COVID-19 pandemic, cybercriminals make phone calls posing as health personnel conducting surveys.

At the end of the questions, the offender asks for a code that the victim will receive via SMS supposedly to register his participation and avoid being called again.

In reality, the code is the one that WhatsApp sends in order to activate the application on a new phone with the victim's account.

The cybercriminals also impersonate technical support staff of the application by performing the described procedure.

Techniques used to circumvent two-step verification.

Two-step verification has become one of the most widely used account protection measures nowadays, although it is a method that clearly reinforces the security of our profiles on social networks, cybercriminals have devised methods to breach it.

One way that cybercriminals use to obtain the codes is to request them via SMS. To do this, they perform a "Sim Swapping" (duplication or impersonation of the SIM card) by contacting the victim's telephone company to convince them that they are the owners of the line and request that the number be changed to another device.

The cybercriminals publish malicious applications with permissions to access the SMS on the device which would allow them to view the verification codes and steal the victim's account, most of the malicious applications are found on unofficial sites, but it is not ruled out that they are also found on Google Play or AppleStore.

Recommendations

To avoid becoming a victim of cybercriminals on WhatsApp, perform the following actions:

A. Enable two-factor authentication (six-digit code) on WhatsApp by following the configuration steps in the application.

B. Do not open your account on shared computers and frequently check on which devices your initiated WhatsApp Web sessions appear.

C. The application never asks users for information via calls, WhatsApp messages or text messages (SMS).

D. At the moment you have to receive any verification code, avoid sharing it with more people even friends or family.

E. Whenever you receive text messages from unknown numbers, block them without replying or giving personal information.

F. Close all open sessions on WhatsApp Web, this is often a source of information leakage and usurpation in the messaging system.

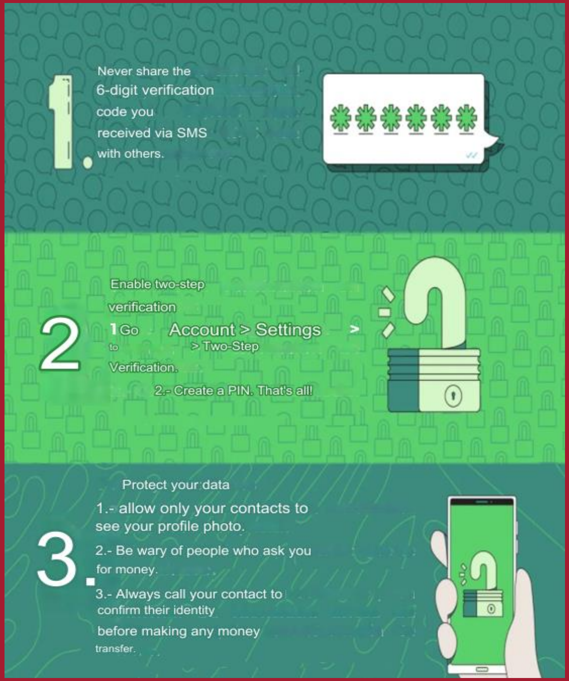
G. Request that your phone number be removed from lists of caller ID applications, scammers can use these lists to find your number from your name.

If you think someone stole your WhatsApp account, the steps to follow are:

- Send an email to support@whatsapp.com containing your full phone number (including country and area code), describe what happened.

- Notify your family and friends as the attacker could impersonate you in your individual and group chats.

With these simple steps you can avoid becoming a victim of account theft.



1. Never share the 6-digit verification code you received via SMS with others.

2. Enable two-step verification
1 Go to Account > Settings > Two-Step Verification.
2.- Create a PIN. That's all!

3. Protect your data
1.- allow only your contacts to see your profile photo.
2.- Be wary of people who ask you for money.
3.- Always call your contact to confirm their identity before making any money transfer.

References

- ➢ https://noticieros.televisa.com/videos/hackeo-a-whatsapp-la-paparrucha-del-dia/
- ➢ https://latam.kaspersky.com/blog/robo-de-cuentas-en-whatsapp-al-burlar-la-doble-autenticacion/21962/
- ➢ https://faq.whatsapp.com/general/account-and-profile/stolen-accounts/?lang=es_pe