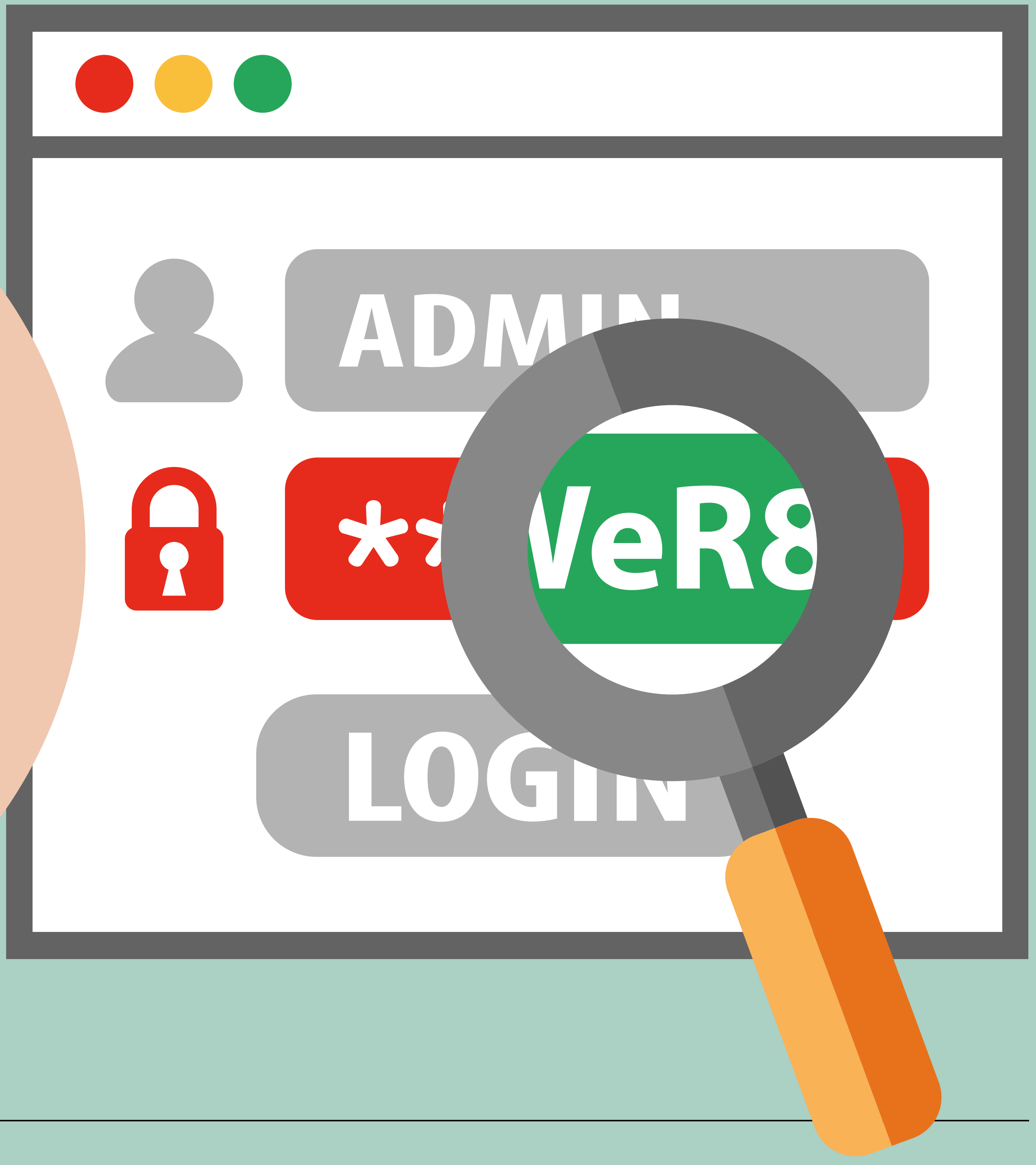
camara-e.net
Câmara Brasileira da Economia Digital

ANTI-FRAUD COMMITTEE OF THE BRAZILIAN CHAMBER OF DIGITAL ECONOMY (2021)

# Security Primer for Digital Consumers

**2021**



How to identify and prevent new Internet scams

# Preface

## Enrico Molinari

*Economist & Journalist, Digital Transformation & Marketing Innovation Officer in FinTech & GovTech Sector | University Professor in Economics, Marketing Innovation, Digital Transformation & Business Technologies | Fintech Insurtech Marketing Top Global Influencer*

Leonardo da Vinci said "the simplicity is the highest degree of sophistication".

May be the Italian scientist, inventor and artist, a man of genius and universal talent of the Renaissance who lived between the fifteenth-sixteenth centuries - would also think the same about the digital Cybersecurity.

In Q3 FY-21, the ransomware attacks increased by 148% globally (source: McKinsey) and Italy became the fourth most affected country in the world by Covid-19-themed cyber threats (source: Trend Micro Research).

All the Digital Consumers are exposed every day to the solid risk of being the victim of cyber-attacks during work or leisure times. Therefore, the use' awareness of fintech and digital & mobile payments tools share thanks to marketing innovation and emerging technologies are strategic to guarantee e-commerce and travels without worries, to make safer money transactions and to have the emotional experience of being connected with our future.

A Gov-Tech Partner like the Brazilian Chamber of Commerce is today an incredible value in the information roadmap for citizens and companies on the risks of Digital Transformation.
«Digito, Ergo Sum!».

camara-e.net
Câmara Brasileira da Economia Digital

# Introduction

## Victims profile

### Gender

Female: 50.8%
Male: 49.2%

### Social Class

Class C: 56.%
Classes A e B: 46,.%

### Age group

25 to 44yo: 51.5%
50+: 16.6%

Victim's average age: 39yo

### Scholarity

High school: 53.6%
University: 25.8%

Source: Report "Financial Frauds in Brazil" - CNDL, SPC Brasil e Sebrae

The social distance caused by the new coronavirus pandemic has contributed not only to an unprecedented growth in the amount of purchases and financial transactions carried out over the Internet since March 2020, but it has also increased the number of scams eCommerce and electronic payments.

According to the survey "Financial Frauds in Brazil", by the National Confederation of Store Managers (CNDL), Credit Protection Services (SPC Brasil) and the Brazilian Micro and Small Business Support Service (Sebrae), 6 out of 10 internet users suffered some financial fraud in the last 12 months in Brazil.

About 16.7 million Brazilians were harmed by virtual scams - a 28% increase over 2019.

Fraudsters continued to apply known scams (such as fake websites) to collect personal and financial information from Internet users, and e-mail with very tempting but false offers. Both are examples of phishing attacks.

However, they found new ways to make victims, taking advantage of the speed and easeness of instant payment transactions, such as PIX and WhatsApp Pay.

In this primer, the Anti-Fraud Committee of the Brazilian Chamber of Digital Economy (camara-e.net) describes these new scams, gives you tips to protect yourself and gives guidance on what needs to be done if you have been a victim of an online fraud.

Good reading!

# Contents:

camara-e.net
Câmara Brasileira da Economia Digital

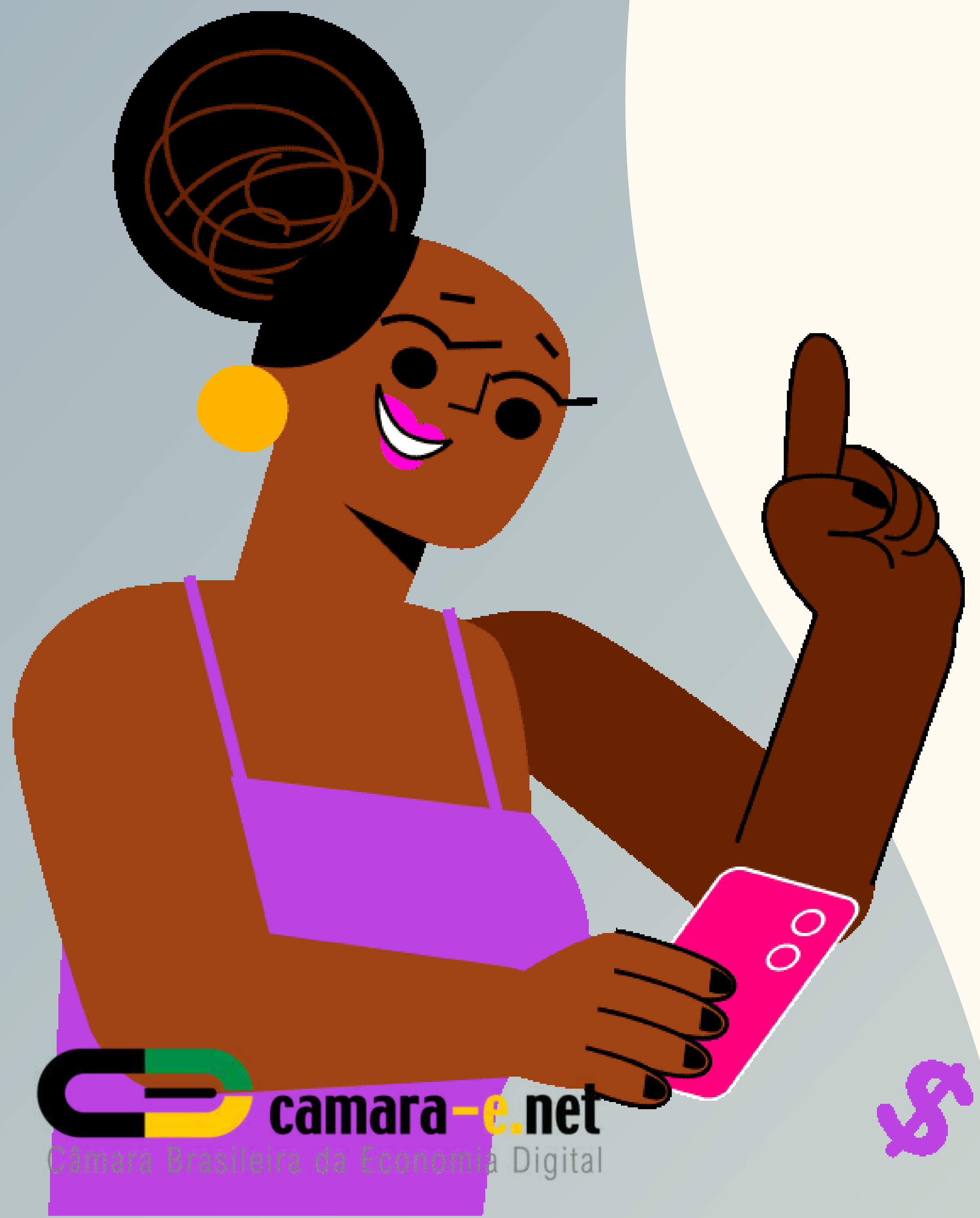
# Instant payment methods

# Fraud mechanic

The fraudster asks the victim, by WhatsApp or phone, to transfer money to a specific account or user via PIX (Brazilian P2P service equivalent to Zelle, Venmo or PayPal) or WhatsApp Pay. Taking advantage of the speed and easiness of these payment services, it uses the following hacking methods

- Creation of a fake WhatsApp account to request money from family and friends of the victim via PIX (Brazilian P2P payment), WhatsApp or any other form of instant payment.
- WhatsApp account hacking to request money from the victim's contact.
- False billing after credit card payment denied on original website.
- Kidnapping to access the Bank application and the PIX on the victim's cell phoneVictim's flash kidnapping in order to access the Bank application and the PIX (Brazilian P2P) on the victim's cell phone to steal his money.
- Scam call center.
- Improper purchase on credit or debit card.

# How to prevent



- When a friend or a relative asks for money through WhatsApp, always be suspicious, even if the story looks real and convincing.
- Call the person to confirm. Do not use the WhatsApp connection to make that call.
- If you receive a phone call from someone claiming to be an employee of a store, bank or public agency asking you to confirm a code sent by SMS, ignore it or hang up. Probably the person is trying to clone your WhatsApp.
- If you receive a call from a person claiming to be a bank or credit card company employee alerting you that your card has been cloned, and therefore you need to transfer your money to a specific account, via PIX (P2P payment), or any other instant payment, ignore it. It's a scam.

camara-e.net
Câmara Brasileira da Economia Digital

# What to do if you've been hacked

Unfortunately in these kind of scam, recovering lost money is very difficult, as the transfer of values is immediate and the destination account is an alias.

Our suggestion is to make a police report, describing the fraud th as detailed as possible, and look for a way to minimize the damage.

In Brazil it is possible to do the police report over the internet. Google it as Boletim de Ocorrência Online.

# Cell phone theft

# Fraud mechanics

With the cell phone assuming a main role in the personal and financial life of its users, the device became a target for thieves and gangs.

In the state of São Paulo (Brazil) alone, from January to July 2021, 160,000 devices were stolen - 1 every 17 hours. The reason is little related to the cost of the device, as its real value is in the information stored on it and in the apps installed.

With the victim's cell phone with personal and financial data in hands, the fraudster can make transfers, purchases, loans, open new accounts, apply for new credit cards and even apply new scams if impersonating the victim.

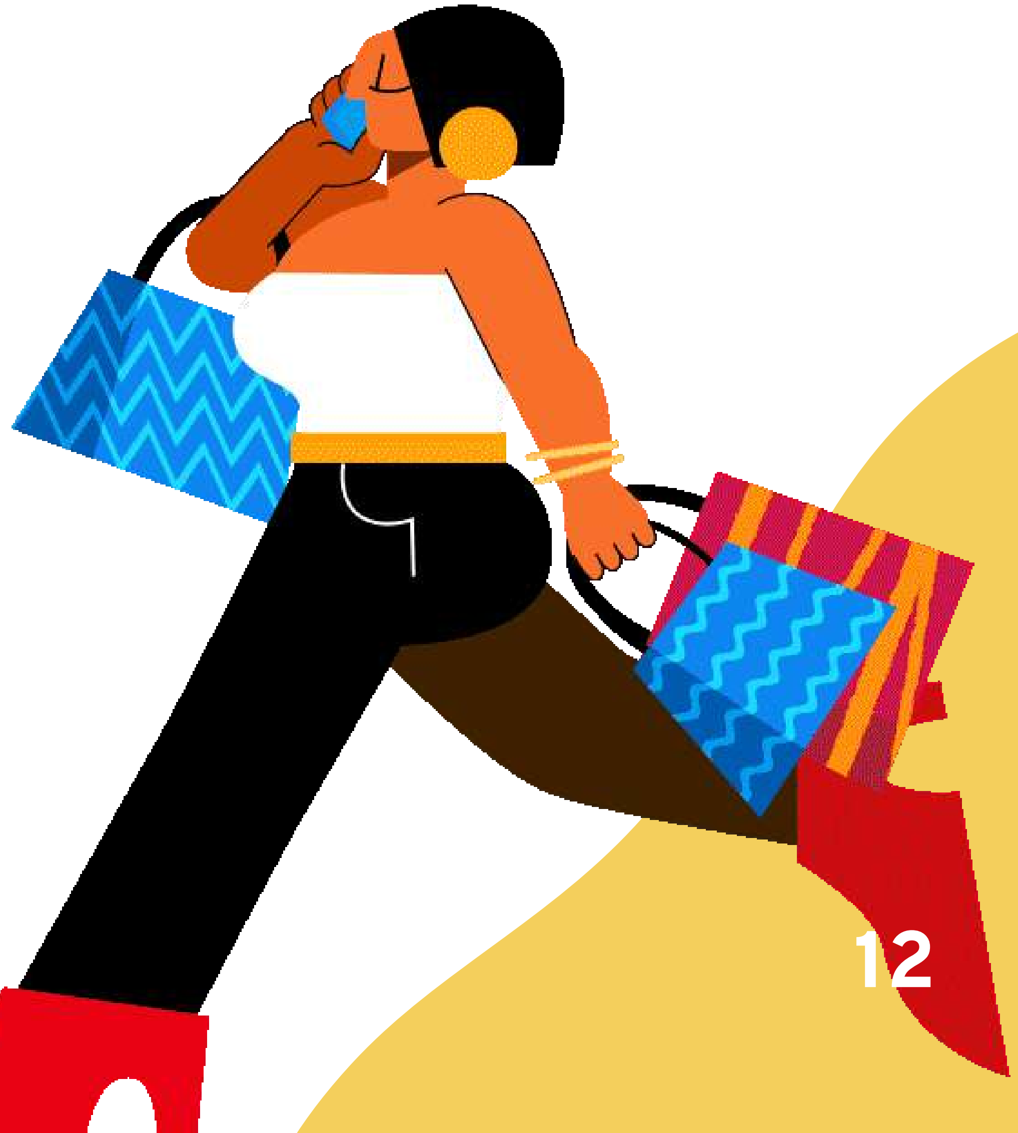
Thefts usually happen when the user is walking on the street, taking photos, stopped at traffic lights, or even inside restaurants, stores, and parks, due to an owner's oversight.

camara-e.net
Câmara Brasileira da Economia Digital

# How to prevent

Cell phone theft is a public safety issue that depends on public policies to be solved. However, it is possible to take some precautions to avoid having the device stolen:

- Avoid using your cell phone on the street and beaches, especially for sending text messages or taking photos or making selfies. In addition to attracting the thief, the practice can lead to accidents.
- If you have to use your cell phone, pay attention to your surroundings. Thieves take advantage of any distraction to commit the crime.
- Avoid carrying your cell phone in your hand or keeping your cell phone in the back pocket of your pants or on the outside of bags and backpacks.
- In the car, drive with the windows closed, especially if you have your cell phone unlocked and connected to the dashboard with Waze app on.
- If possible, use Waze on a “bad guy's mobile”, which is a second, cheaper device that doesn't contain your personal and financial information or banking apps.
- On public transportation, keep your cell phone in a safe place.
- Don't react when approached by a bad guy. Material goods can be replaced. Life doesn't!



# What to do if your cellphone is stolen

- Search for a computer or other cell phone as soon as possible and erase all data and applications from your device. For Android devices, go to android/find website, login using your Google account data and click on “Clean device” option. For iOS devices, go to icloud.com, log in, click on “Find Device” option, and then on “Erase Device”.

- Once this is done, contact the telephone operator and block the SIM card, also informing the device's IMEI. The IMEI is a kind of ID for the phone.

- Contact the banks whose apps are installed on the device to report the theft and request that your account and all your cards be blocked.

- Change passwords and authentication settings for accounts of stores and services whose apps are installed on your mobile. This includes social media, emails, food and goods delivery services and transport apps.

- Call the police and register a police report. In Brazil, theres is a Cybercrime Department you can ask for help.

# WhatsApp frauds

# The newest WhatsApp frauds

WhatsApp has over 2 billion active users worldwide -110 million of them in Brazil alone. The country is the second in the world ranking of users.

In Brazil, the app is used for everything: from exchanging messages with friends, family, customers, and companies, to make business, video conferences, and phone calls. More recently, WhatsApp has also incorporated a payment function in many countries. The service is called WhasApp Pay.

The app's popularity and new functionality have made the tool the favorite target of fraudsters, who have created scams like Account Cloning and Fake Profile. The goal: take money from the victim's contacts.

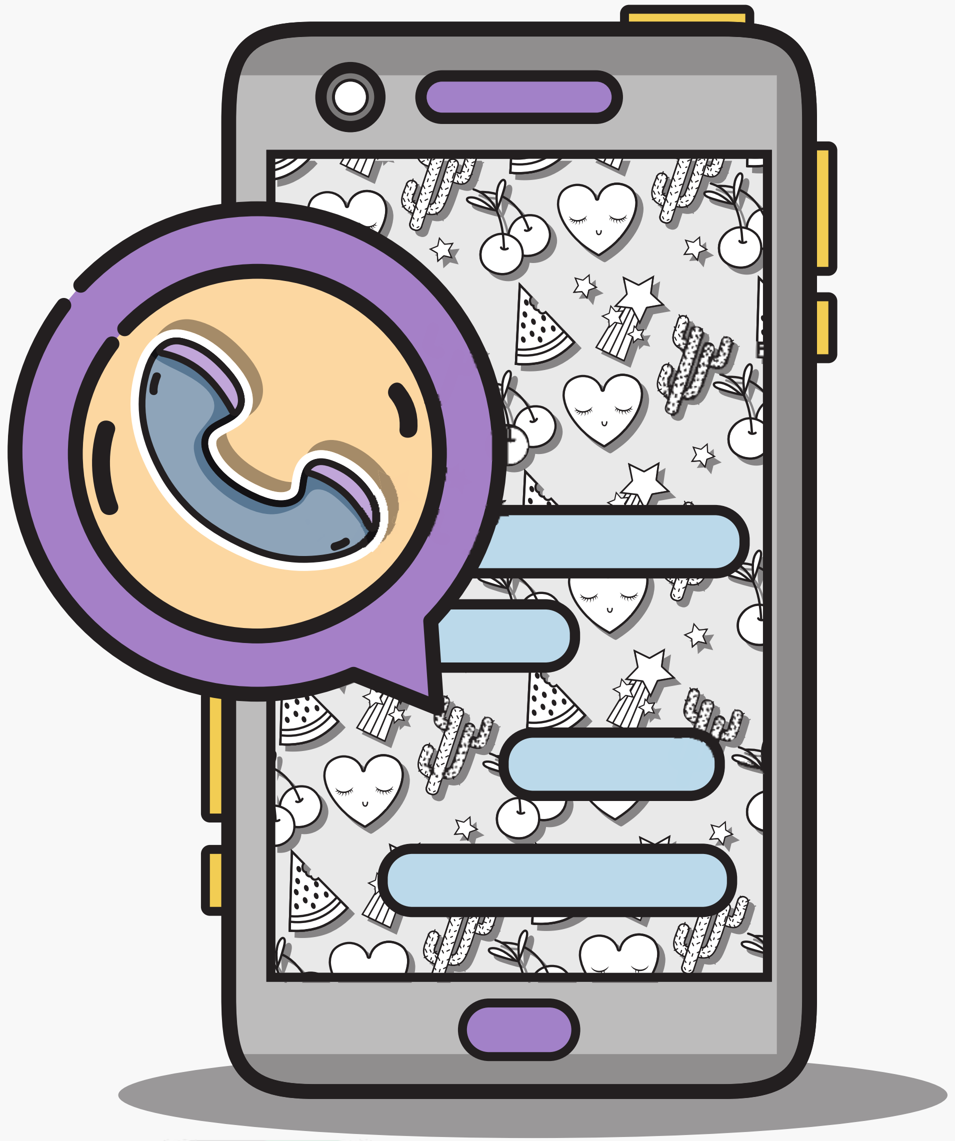
# WhatsApp account cloning mechanics

WhatsApp cloning is becoming popular among fraudsters. With the victim's phone number and name in hand (usually purchased from leaked databases), the scammer logs into WhatsApp after obtaining the account verification code.

On another device, he can replicate the account and have access to conversation and contact history.

With the cloned account, the fraudster sends a message to the victim's contacts, advising that the phone number has changed and that the "old" one can be deleted from the phonebook. From there, he tries to fraud victim's contacts.

A WhatsApp account can be cloned in two ways: through unauthorized login or through access to the app's verification code.



To obtain the verification code, the scammer calls the victim pretending to be the call center of a store, bank or even a public agency such as the Ministry of Health doing research on Covid.

At a certain point in the conversation, the fraudster tells the victim that he/she has to confirm a code that was just sent via SMS to the cell phone and that it will be necessary to update the registration data.

By entering this code, the criminal has access to the victim's WhatsApp account, with all contacts and message history.

Keep in mind that fraudsters will use any and all means to obtain confidential details: from creating a compelling story to get the victim to enter the activation code, to sending a message via SMS or WhasApp with an unsolicited OTP (One-Time Password), so that a certain information is confirmed.

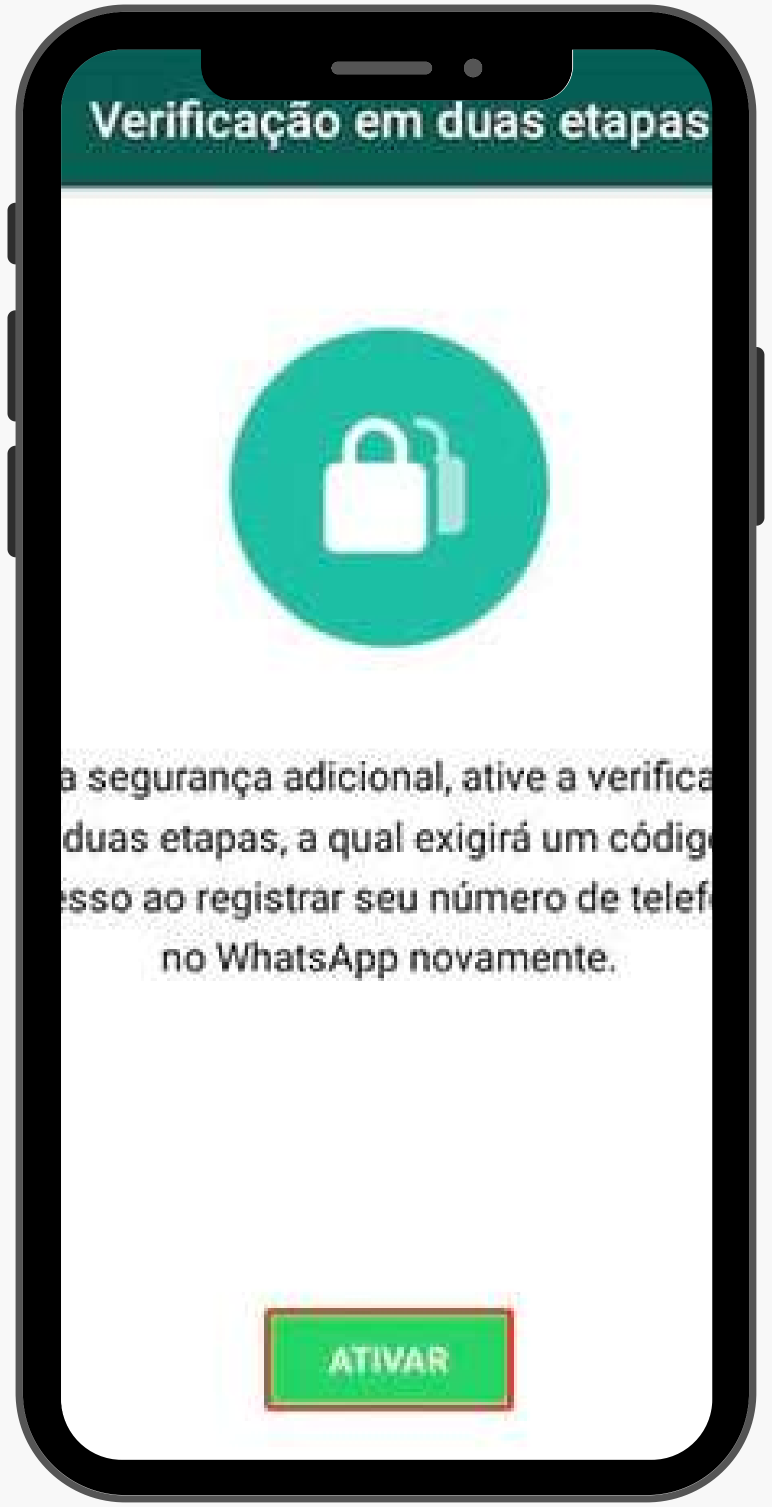
# How to prevent

- Do not click on links or respond to unsolicited one-time password messages via SMS or WhatsApp.

- Do not inform any verification code received by SMS to third parties, especially for those who order it over the phone and are waiting on the phone.

- Activate the "two-step verification" function in your WhatsApp. This feature creates a unique identity for your account, which is accessible only by a passcode defined by you.

- See how to enable two-step verification on the next page:

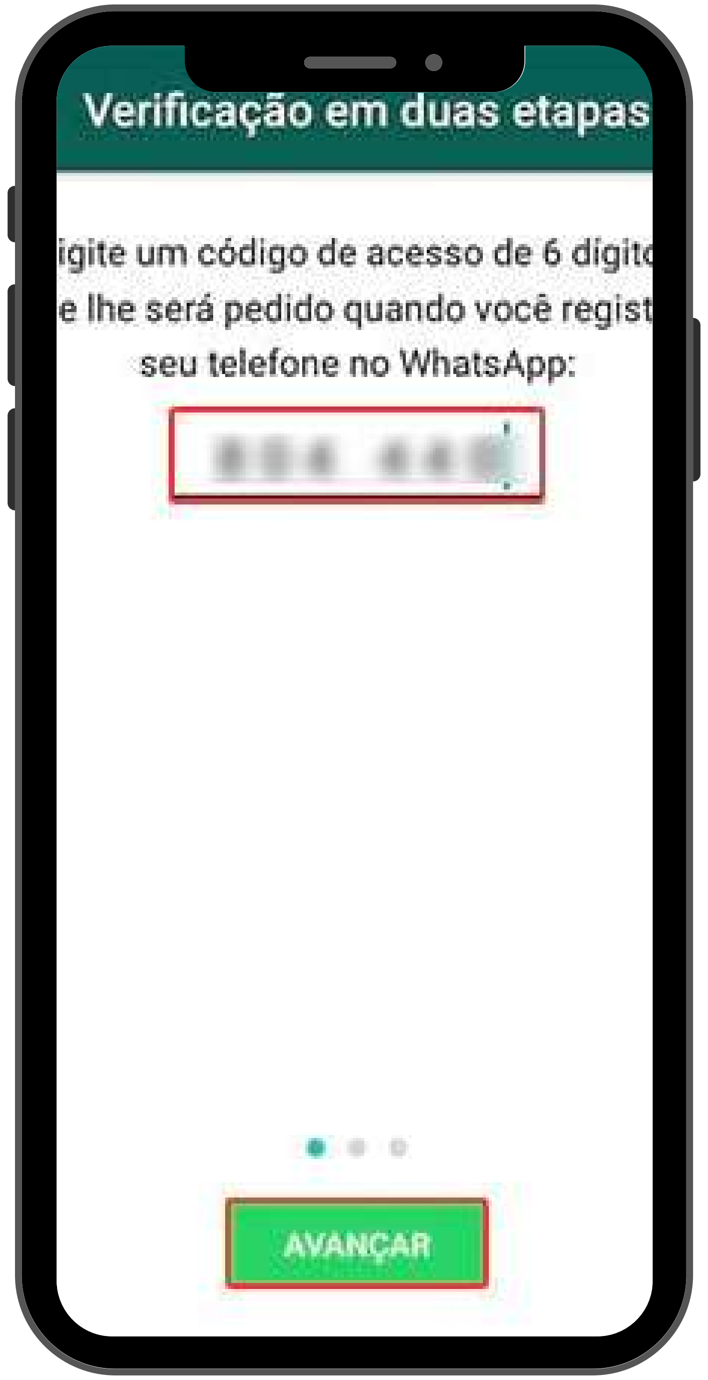


Verificação em duas etapas

a segurança adicional, ative a verifica
duas etapas, a qual exigirá um códig
esso ao registrar seu número de telef
no WhatsApp novamente.

# How to setup two-step verification

1. Open the app. In the upper right corner, click on the three dots;
2. Click on "Settings" and then on "Account";
3. Click on  "Two-step Verification" and then on "Next";
4. Click on the "Enable" button;
5. Enter a 6-digit passcode (choose a combination you won't forget). Then click on "Next";
6. Confirm the passcode by entering it again and click on  "Next";
7. Enter an e-mail address to retrieve your access code in case you forget it. Then click on "Next";
8. Confirm your email address by entering it again and then click "Save".  Two-step verification is enabled.

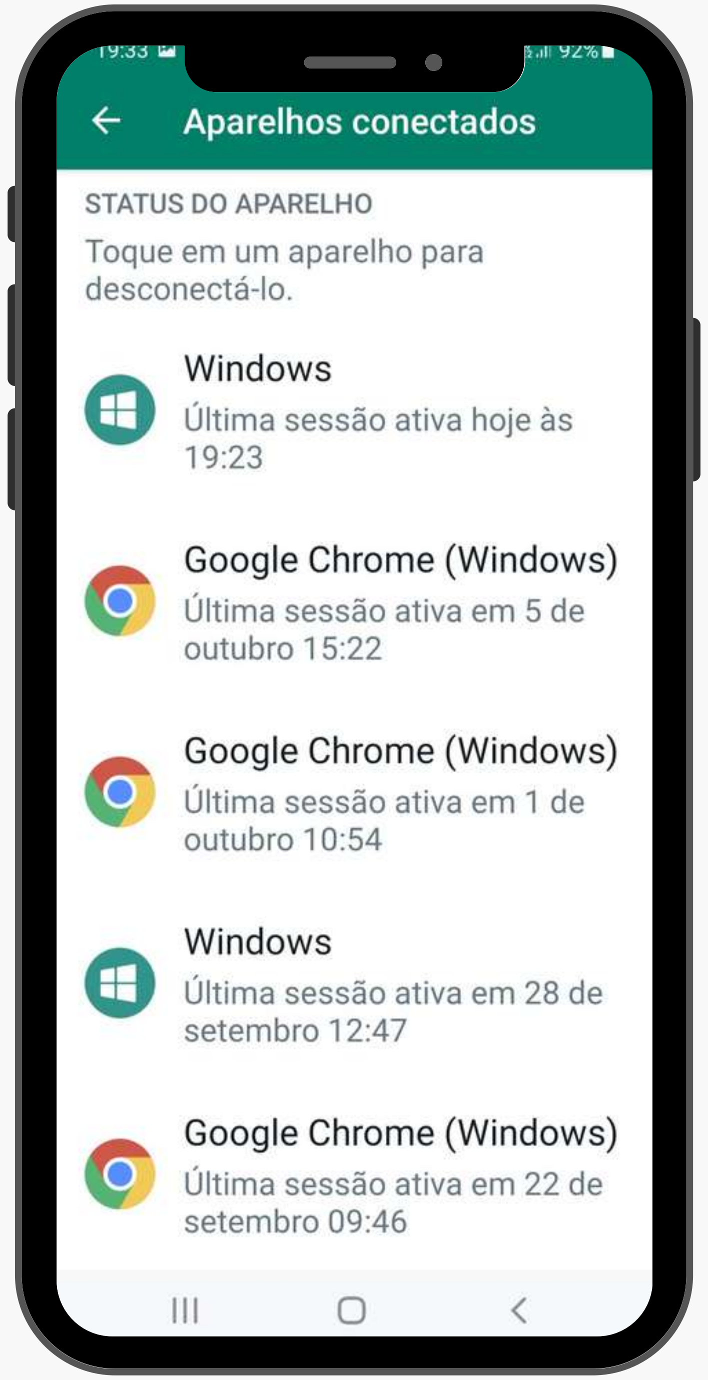


Verificação em duas etapas

igite um código de acesso de 6 dígito
e lhe será pedido quando você regist
seu telefone no WhatsApp:

camara-e.net
Câmara Brasileira da Economia Digital

# What to do if your WhatsApp is hacked



19:33 92%

Aparelhos conectados

STATUS DO APARELHO

Toque em um aparelho para desconectá-lo.

Windows
Última sessão ativa hoje às 19:23

Google Chrome (Windows)
Última sessão ativa em 5 de outubro 15:22

Google Chrome (Windows)
Última sessão ativa em 1 de outubro 10:54

Windows
Última sessão ativa em 28 de setembro 12:47

Google Chrome (Windows)
Última sessão ativa em 22 de setembro 09:46

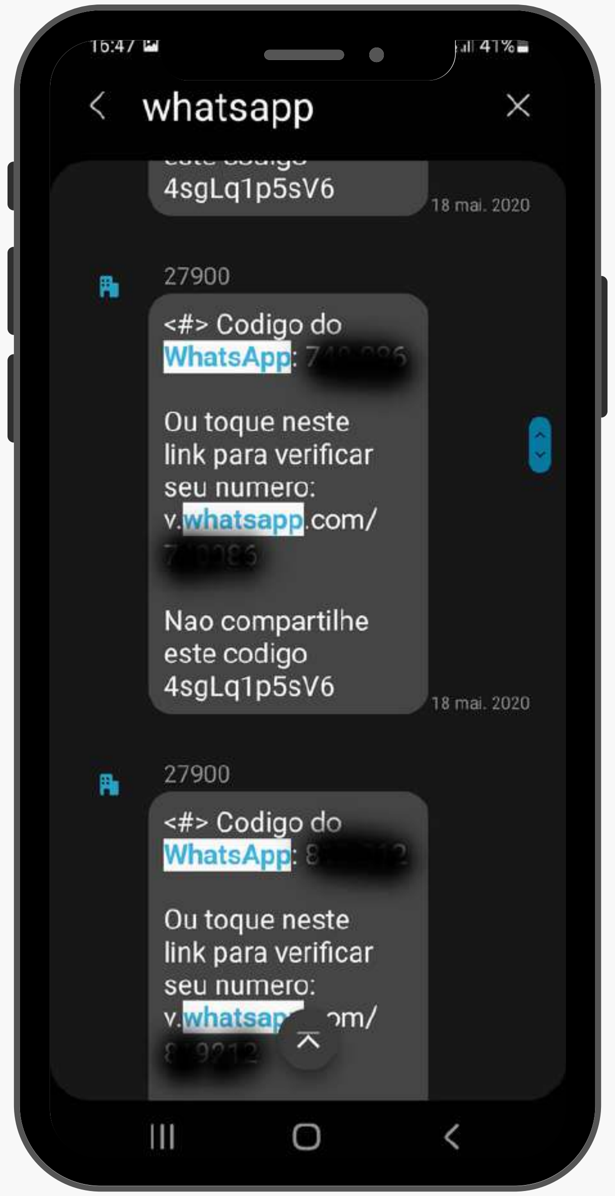
**Scenario 1: You accessed your WhatsApp on another device (a third-party computer, for example) and forgot to log out when you finished. The fraudster is using the app without your permission.**

The fraudster will be able to read messages, access your contacts, and even start new conversations, but he/she will not be able to change the security settings.

However, he/she can steal confidential information while chatting with your contacts to defraud your friends and acquaintances on your behalf. If that happens:

- Access WhatsApp from your cell phone, click on the three dots in the upper right corner and click on "Connected Devices and then Devices";
- Then, under Device Status, disconnect one by one the devices that appear in the list. In older versions of the app and on the iPhone, it is possible to disconnect them all at once by clicking "Disconnect All".

# What to do if your WhatsApp is hacked



15:47

whatsapp

4sgLq1p5sV6

18 mai. 2020

27900

<#> Codigo do WhatsApp: [redacted]

Ou toque neste link para verificar seu numero:
v.whatsapp.com/
[redacted]

Nao compartilhe este codigo
4sgLq1p5sV6

18 mai. 2020

27900

<#> Codigo do WhatsApp: [redacted]

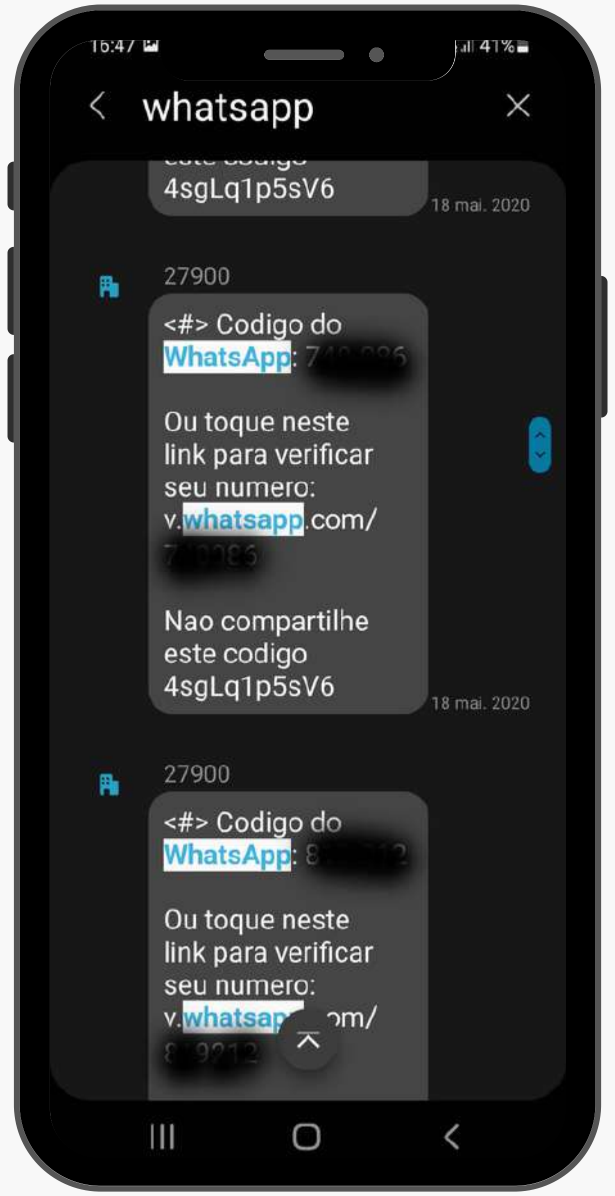
Ou toque neste link para verificar seu numero:
v.whatsap om/
[redacted]

## Scenario 2: You have not activated two-step verification and someone has stolen your account.

- Let friends and relatives know that your WhatsApp has been hacked.
- Enter WhatsApp with your phone number and confirm it with the six-digit code you will receive via SMS.
- Once you enter the code received through SMS, the person using your account will be logged out automatically.
- You may also need to enter a two-step verification code. If you don't know this code, it's possible that the person using your account has activated this feature.
- As you don't have the code, you will have to wait 7 days before logging in without the two-step verification code.
- After this period, log back into WhatsApp.
- Enter the six-digit code sent by SMS.
- Enter the app and change your settings.

camara-e.net
Câmara Brasileira da Economia Digital

# What to do if your WhatsApp is hacked



16:47 41%

whatsapp

4sgLq1p5sV6 18 mai. 2020

27900

<#> Codigo do WhatsApp: 7[redacted]

Ou toque neste link para verificar seu numero: v.whatsapp.com/ 7[redacted]

Nao compartilhe este codigo 4sgLq1p5sV6 18 mai. 2020

27900

<#> Codigo do WhatsApp: 8[redacted]

Ou toque neste link para verificar seu numero: v.whatsap om/ [redacted]

**Scenario 3: You've turned on the two-step verification, but you were misled to inform the verification code and someone is trying to register r account on another device.**

In this situation, the fraudster will not be able to read previous WhatsApp messages due to end-to-end encryption, but will be able to start new chats with your contacts.

What to do to recover the account:

- The moment he/she activates your account on another device, you will receive a notification alerting that your WhatsApp is being used on another device.
- Log out of WhatsApp and log in again using your phone number.
- A six-digit code will be sent to your phone number via SMS. Enter the code (see photo on the left).
- This logs you into your account immediately, and automatically logs out the hacker.

camara-e.net
Câmara Brasileira da Economia Digital

# Fake profile scam mechanics

The fake WhatsApp profile scam victimizes two ends: the user who has the account copied and the victim's contacts, who are deceived by the crook.

The fraudster has access to the victim's information (phone number and personal data) by purchasing a leaked database, and by using the person's public profile photo in the app.

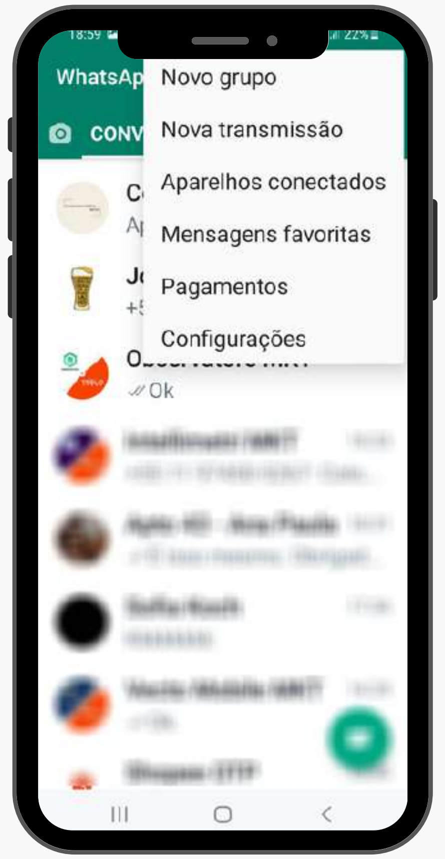
He creates a new WhatsApp account with the victim's photo and information, looks for additional information on social media to identify his friends and relatives, and sends a message "informing" the new phone number and asking that the old one be deleted from the phonebook.

From there, he/she starts talking to the victim's contacts until, at a certain point, he/she asks for money, making an excuse, and giving information of an alias account to wiretransfer.

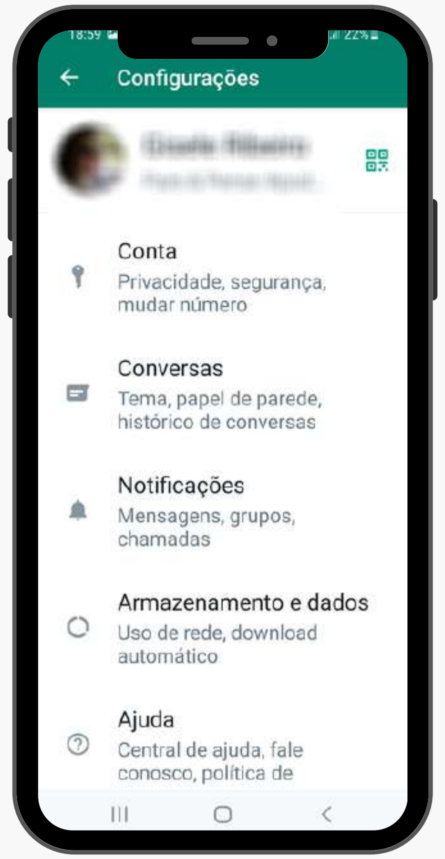
They usually ask for the transfer to be made by PIX (Brazilian P2P) or WhatsApp Pay.

# How to prevent

- Make your WhatsApp profile picture visible to your contacts only: In Whatsapp, go to Settings > Account > Privacy > Profile picture > My contacts.



WhatsApp
CONV
Novo grupo
Nova transmissão
Aparelhos conectados
Mensagens favoritas
Pagamentos
Configurações



Configurações

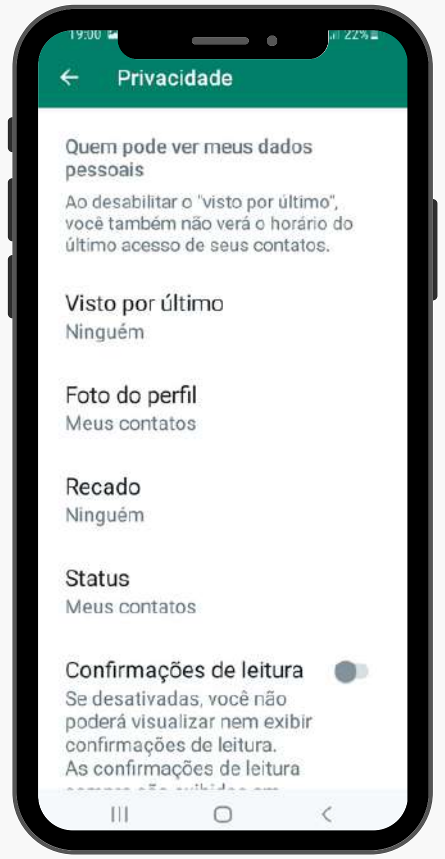
Conta
Privacidade, segurança, mudar número

Conversas
Tema, papel de parede, histórico de conversas

Notificações
Mensagens, grupos, chamadas

Armazenamento e dados
Uso de rede, download automático

Ajuda
Central de ajuda, fale conosco, política de



Privacidade

Quem pode ver meus dados pessoais
Ao desabilitar o "visto por último", você também não verá o horário do último acesso de seus contatos.

Visto por último
Ninguém

Foto do perfil
Meus contatos

Recado
Ninguém

Status
Meus contatos

Confirmações de leitura
Se desativadas, você não poderá visualizar nem exibir confirmações de leitura. As confirmações de leitura

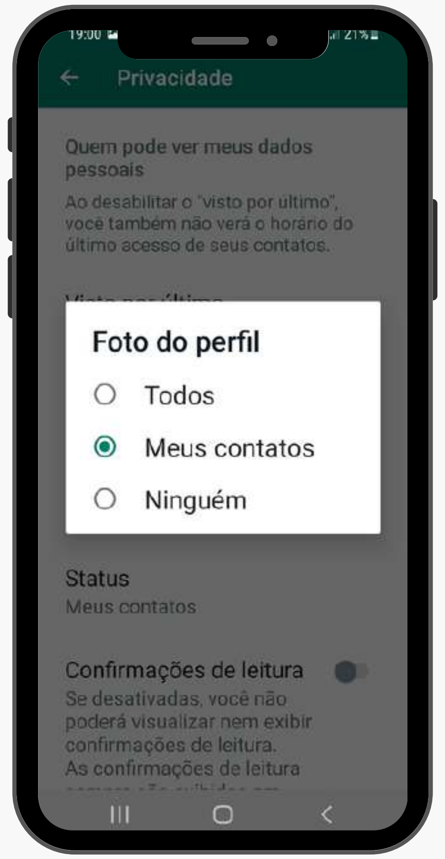


Foto do perfil
○ Todos
● Meus contatos
○ Ninguém

- Pay attention to what you post on social networks, so that you don't give scammers clues about your lifestyle or pass on information that can be useful for scamming your friends and relatives.

camara-e.net
Câmara Brasileira da Economia Digital

# What to do if your profile is spoofed

## If you notice that your profile has been spoofed:

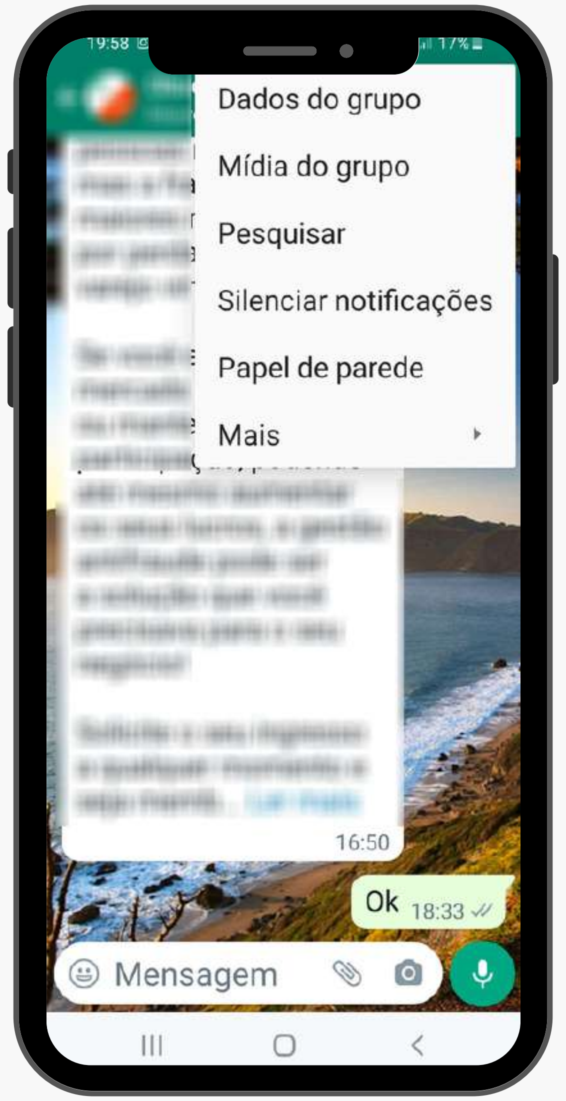
- Let your contacts know that your WhatsApp has been hacked, you haven't changed your phone, and they should NEVER lend money to anyone who asks them claiming to be you.

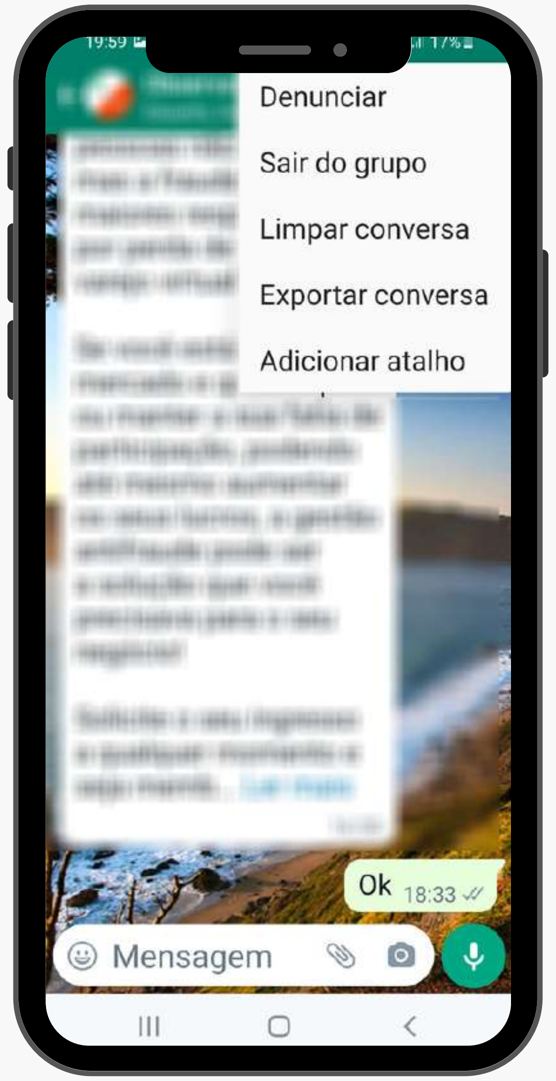
- Ask them to report the number to WhatsApp/Facebook, and block the fake contact.

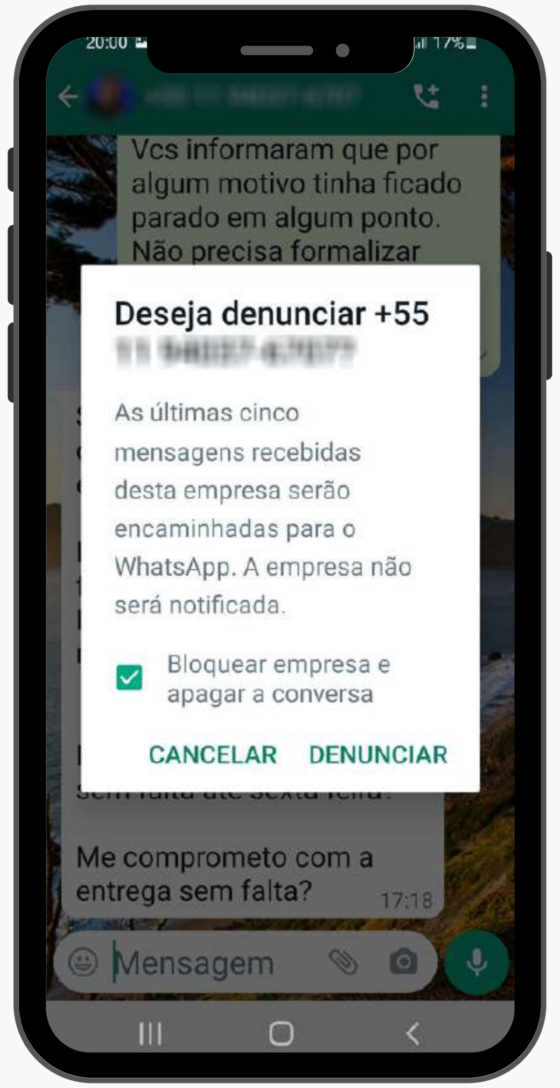
- Register a Police Report.

## If you notice that you are talking to a fake profile:

- In the suspicious contact window, click on the three dots in the upper right corner, then on "More", "Report" and then on the "Report" button.







Vcs informaram que por algum motivo tinha ficado parado em algum ponto. Não precisa formalizar

Deseja denunciar +55 [redacted]

As últimas cinco mensagens recebidas desta empresa serão encaminhadas para o WhatsApp. A empresa não será notificada.

☑ Bloquear empresa e apagar a conversa

CANCELAR DENUNCIAR

Me comprometo com a entrega sem falta? 17:18

camara-e.net
Câmara Brasileira da Economia Digital

# Account Takeover (ATO)

# Fraud mechanics

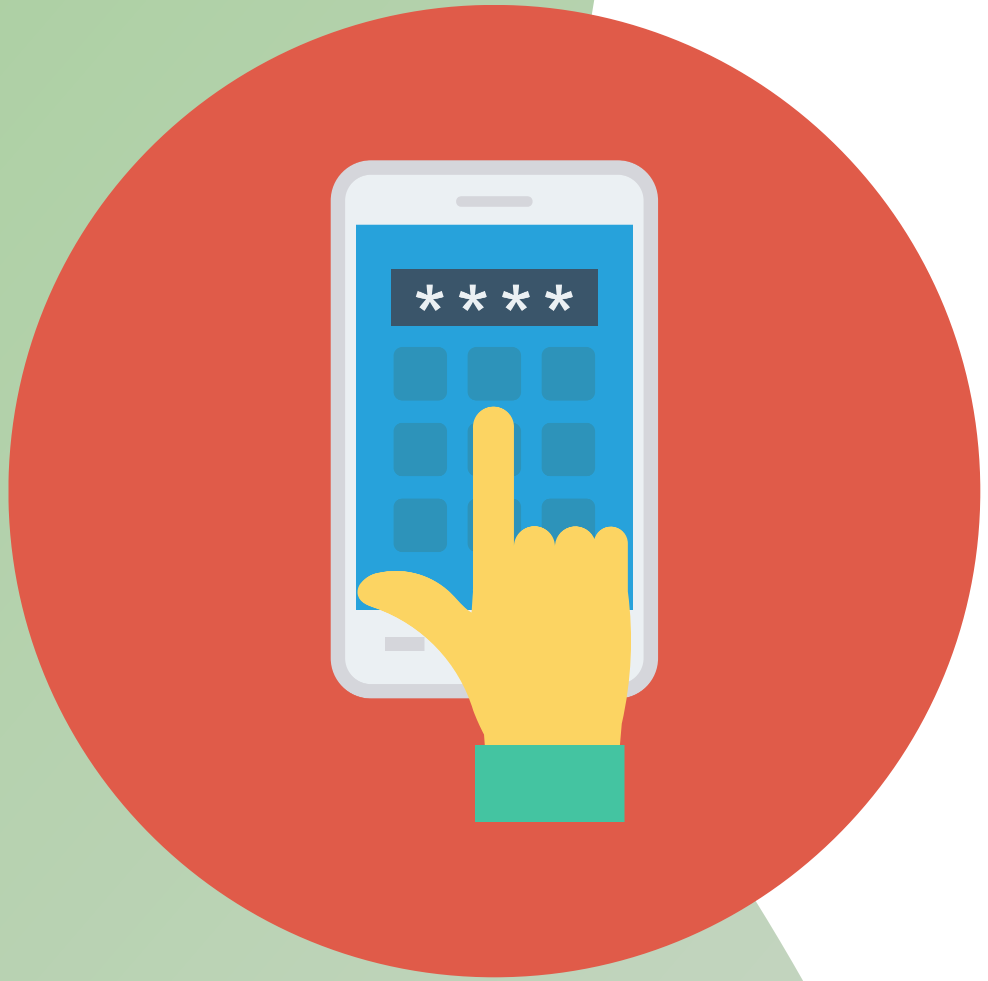
Account takeover (ATO) fraud occurs when a cybercriminal gains access to victim's login data to steal money or information.

Using techniques such as phishing, malware and man-in-the-middle attacks (when someone, inside of the online service, gives the information to the scammer), the fraudsters digitally hack a financial account to control it.

This type of scam, which is often referred to as identity theft or impersonation (depending on what the intruder uses), is one of the main threats to banks, financial institutions, and their customers due to the efforts involved to avoid million-dollar losses.

Fraudsters can take control of existing accounts such as bank, credit card and e-commerce.

# How to prevent



- Use multifactor authentication. This can include biometrics. Fingerprint or face biometrics, for example, are difficult to copy or simulate.

- Enable your two-factor authentication (2FA) on all accounts: banks, stores, shopping apps, messaging apps, networks social etc.

- Activate the security PIN on everything, especially on WhatsApp. The PIN is more important than the second authentication factor since it is required from time to time and every each new login.

- Do not repeat passwords on different accounts or choose a password that makes obvious references, such as birthdays or telephone numbers.

- Use a password manager to make it easier to remember and store it safely (Hint: LastPass).

# What to do if you've been hacked

Account takeover (ATO) can be difficult to detect because the fraudsters can hide behind a customer's positive track record and mimic normal login behavior.

Continuous monitoring provides the ability to detect signals from this kind of fraud before it starts.

If you notice that your account has been accessed by someone else or worse, that it has been completely taken over, whether from financial institutions or from online stores or services, follow the steps below:

- Call your bank, and block accounts and cards. This will prevent the fraudster to perform any action on the account, such as changing the password or make a purchase.
- If the password has already been changed, try forcing the reset password function.
- Call the police.

# Fake contact center

camara-e.net
Câmara Brasileira da Economia Digital

# Fraud mechanics

This is a scam that victimizes consumers of all ages and social classes.

The fraudster contacts the victim pretending he is an employee of the bank or an anline company, with which the victim has an active relationship, informing that his account was hacked, cloned or that there is any other problem. From there, he requests the victim's personal and financial data.

To give credibility to the speech, the scammer even asks the victim to call the Bank's contact center, calling the number that appears on the back of the card, but remains on the line to simulate the call center. This way, the fraudster can request victim's account data, the number of his/her credit card and, most importantly, figures out his password, using a keylogger to steal it while the victim types it on the phone keyboard.

Instant payment methods made this fraud easier for the scammer. In this case, he has just to ask the victim to make an account wiretransfer to a "secure (alias) account" until the issue is solved. When the victim realizes that it was a scam, the transfer has already been made and the money has been lost.

camara-e.net
Câmara Brasileira da Economia Digital

# How to prevent

- If you receive this kind of contact, be aware right away! Because somehow the bad guys have had access to your data and maybe already know your credit card number. They can even simulate a purchase denial, sending an SMS as if they represent the credit card company.

- Hang up the phone and call the financial institution or the store using official contact channels, preferably by cell phone or by the official apps to check if something wrong happened to your account.

- Keep in mind that the bank never calls the customer asking for a password or card number or to ask for a money transfer or any other type of payment.

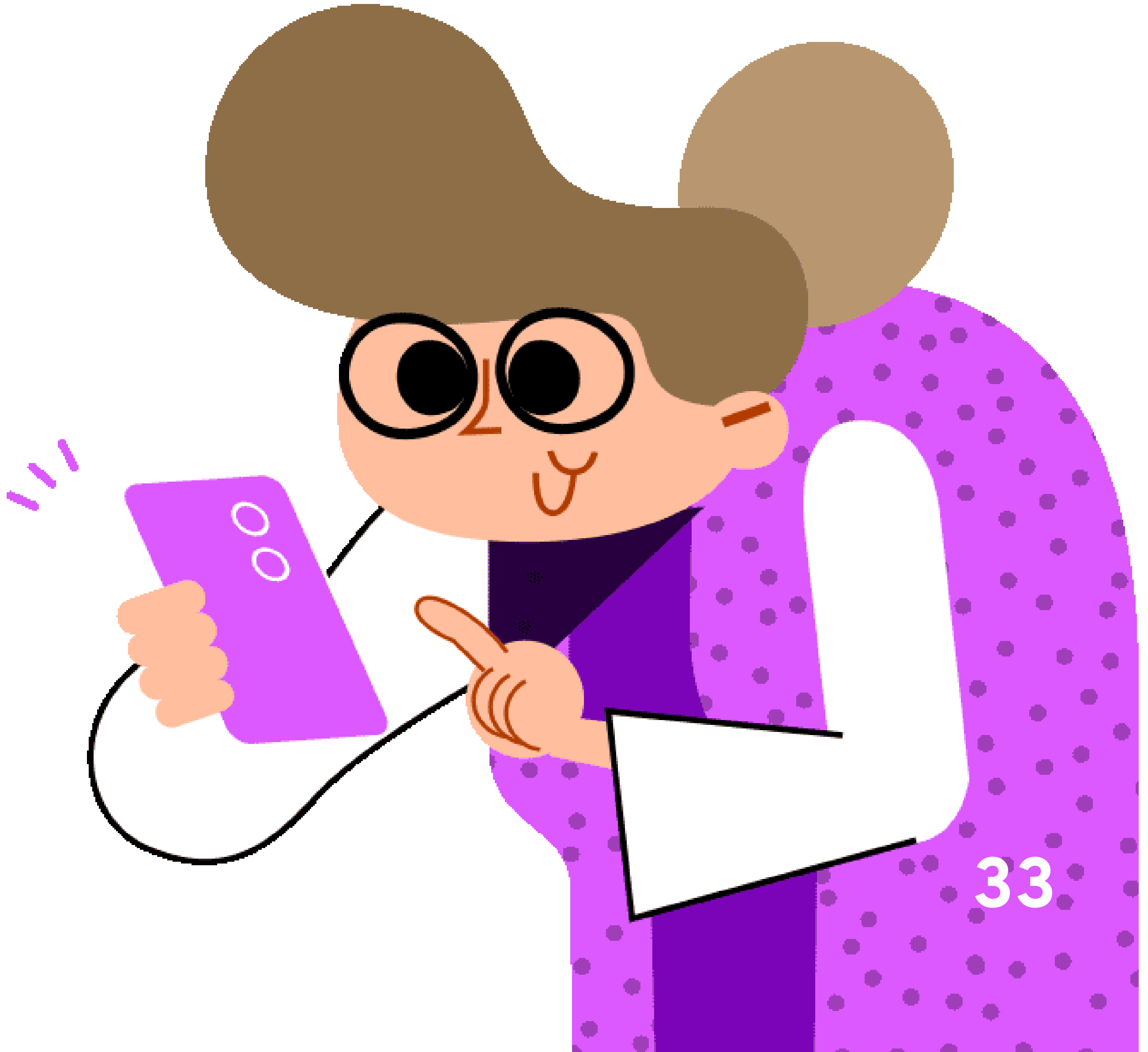
# What to do if you've been scammed

- Contact the bank informing that you were victim of a scam and ask them to block your account and cards.

- Change your passwords.

- Gather as much information as possible by writing down names, protocol numbers, time and date.

- Register a police report.



# Fake job posting

# Fraud mechanics

Taking advantage of the wave of unemployment caused by the pandemic, fraudsters created a new scam to get personal and financial information and quick money from their victims: the fake job posting. Acoording to dfndr lab, about 345,000 people in Brazil were scammed between January and May 2021.

Fake job postings instruct victims to fill in forms with personal details such as name, social security number, address, telephone, and bank information. This data can be used for a number of malicious actions, such as opening fraudulent bank accounts and making purchases or loans in the victim's name.

In some cases, criminals even get a person's login and password from email and social networking services, a situation that opens up the attacker to impersonate the victim and apply other scams.

In a variation of this fraud, the fraudster posing as a representative of the company offering the vacancy gets in touch with the candidate and says that he/she has been selected for the position, but in order to expedite the hiring process, it will be necessary to pay a fee. And then the money is lost.

# How to prevent

- Note if the job ad is posted on a not credible website with irregular formatting. Reputable companies often post opportunities on job sites or recognized job platforms.
- Observe if the job description is generic, without important information about the position, but with a lot of emphasis on salary and benefits. Remember: there is no free lunch!
- Ads that describe large numbers of vacancies or highlight the urgency of filling them are also suspect.
- Be wary of guaranteed vacancy offers.
- When contacting the company to request more information about the job, do not proceed if: document data is required prior to hiring, questions about the position are not properly answered, or if you are instructed to make payments to get the alleged job.

# What to do if you've been scammed

- Contact the real company and report the fraud.
- Gather as much information as possible and make a detailed police report.

camara-e.net
Câmara Brasileira da Economia Digital

# Basic Digital Security Tips and Helpful Websites

# Basic Digital Security Tips

- Take good care of your passwords - don't share them with friends and family or forward them via e-mail or message apps.

- Use strong passwords - Choose one of eight or more characters made up of a combination of uppercase, lowercase, numbers and special symbols.

- Use different passwords - Don't use the same password for multiple accounts. It may be easier to remember, but also easier to defraud.

- Change passwords - At least every three months, change the passwords used in your e-mail accounts, apps and online stores.

- Watch out for calls - If you receive contact on behalf of the bank or credit card to call the Service Center, at the number on the back of the card, dial from another device. This way you prevent the scammer from diverting the call to a false customer service.

# Basic Digital Security Tips

- Watch out for e-mails - If you receive an email saying that your purchase at a certain store was denied and asking you to contact the Customer Service Center, at the number on the back of the card, delete the message. It's a scam.

- Beware of links of unknown origin - Never click on links sent by SMS, messaging apps and unknown e-mails. Even if it is an unmissable offer or they ask for data synchronization, token and app maintenance or registration update. The bank never sends e-mails informing you that your account has been hacked and asks you to send your details.

- Enable dual factor authentication on your internet accounts: e-mails, apps and social media.

- Be careful of what you share on social media. Many scammers use social engineering to choose their victims. This includes looking at their profiles and knowing their lifestyle, and who their family and friends are.

# Useful websites

- To find out if your data has been leaked, the Brazilian Central Bank's Registrato tool allows Brazilians or residents to monitor their CPF, consult Pix key reports, and verify if their data has not been used by fraudsters to open bank accounts or make loans: https://www .bcb.gov.br/cidadaniafinanceira/registrato

- The "Have I Been Pwned" website shows e-mails and passwords that have already been leaked and where they were leaked: https://haveibeenpwned.com/

- The Cadastro Pré tool allows the Brazilians to check if your their CPF is being used improperly to open accounts with telephone operators: https://cadastropre.com.br/#/consulta

- The Lock & Unlock tool, by Serasa AntiFraude, allows Brazilians and residents to monitor their CPF and know if it is being used improperly.

# Useful websites

- CertBr Internet Security Primer - Set of documents with recommendations and tips on how Internet users should behave to increase their security and protect themselves from possible threats: https://cartilha.cert.br/

- Internet Segura - Brings together initiatives to raise awareness about security and responsible use of the Internet in Brazil, helping Internet users to find information of interest and encouraging safe use of the Internet: https://internetsegura.br/

- Pare & Pense #PodeserGolpe - Febraban's initiative to raise awareness about financial scams and how to prevent them: https://bityli.com/PW1pYN

- Beware of scams on the Internet - Primer of the Secretariat of Public Security of the State of São Paulo warning of scams applied on the internet. Download link: https://bityli.com/kHQjqj

# Acknowledgments and copyright

## We'd like to thank our sponsors:

www.olx.com.br/seguranca

www.observatore.org

## Copyright:

The "Security Primer for Digital Consumers - How to indentify and prevent new online frauds" was created and produced by Gerson Rolim and Gisele Ribeiro for the Antifraud Committee of Brazilian Chamber of Digital Economy (camara-e.net). Its content can be used free of charge since the source credits are given.