#LEARNWITHASUFIN

Cyber fraud

· Trends 2022 ·

MINISTERIO DE CONSUMO

This project has been subsidized by the Ministry of Consumer Affairs, its content being the exclusive responsibility of ASUFIN.

asufintech

Finanzas Para Todos

www.tech.asufin.com

Carried out within the framework of the 2022 Financial and Digital Education program

Threats and Financial Fraud

In a society increasingly dependent on electronic devices, the increase in threats in the digital world is increasing and transforming, with the aim of taking advantage of any technological weakness to obtain sensitive data and exercise all kinds of attacks and thefts.

The mobile phone is the main attack vector, due to all the personal information it possesses. However, it is not the only one: computers, tablets, videoconferencing cameras, smartwatches or drones, among others, are sensitive to being hacked for fraudulent purposes.

The Spanish National Cybersecurity Institute (INCIBE) is the organization that works to strengthen digital trust, increase cybersecurity and contribute to the safe use of cyberspace in Spain. If you have any questions, you can contact them by dialing 017.

Cyberattacks related to identity theft and financial fraud with the highest incidence this year are:

01. **SIM swapping or duplicate mobile cards**

02. **Malware, hostile or intrusive software**

03. **Phishing, smishing and vishing**

04. **Fake apps**

05. **Ransomware or data hijacking for money**

SIM swapping or duplicate mobile cards

The SIM swap scam consists of duplicating the SIM card from a mobile phone to access all the information stored on it.

When a cybercriminal manages to duplicate a SIM card, they not only access the victim's contacts, but, thanks to multifactor authentication, they can also open their social networks (and, therefore, spread the virus to infect and "hijack" other devices or obtain confidential information) and, what is worse, they can obtain the access or authorization key of a banking operation via SMS and transfer money, request a loan, etc.

Sometimes, it is enough to just make a phone call to duplicate the SIM, which makes this type of scam easier.

Tips

1. **Be cautious of what you share on the Internet.** The less personal information there is, the harder it will be for cybercriminals to get sensitive information.
2. **Configure two or more-step authentication that does not involve SMS** (facial recognition, voice recognition, additional pin, etc.).
3. **Call your mobile operator** to strengthen its security systems in the case of duplicates on SIM cards.
4. **Install an antivirus or security tool** that facilitates the protection of the SIM card.

How do you know if you have been a victim of this type of attack?

- Once cybercriminals have access to the duplicate SIM card, the user's card will be automatically deactivated and only the criminal's card will work. Therefore, if you don't have coverage and can't make phone calls or send text messages, maybe the SIM card has been duplicated.
- The phone provider will notify you that the SIM card has been activated on another device.
- Another clue is the inability to access accounts and/or bank cards online with your usual passwords.

If you think this has happened to you, ASUFIN can help you.

Malware, hostile or intrusive software

Malware or malicious software is a hostile or intrusive program that is harmful to the operating system, intended to invade, damage or disable it. This is commonly known as a computer virus.

The objective of malware is to access the device, being able to steal, encrypt, spy, alter and/or delete the data found in the system.

The most common way to get infected is by downloading any malicious file (music, movies, email attachments, USB, etc.).

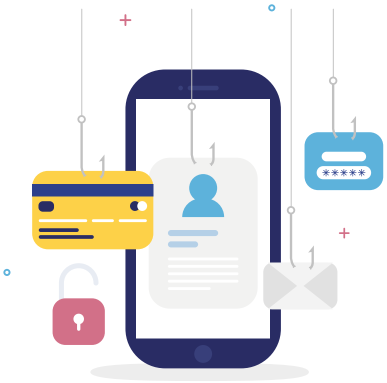
Tips

1. Use **antivirus software** to keep your computer protected.
2. **Do not download files from strangers** that lead you to think they are tampered with. If an email, website or removable drive (USB) is not reliable, it should not be downloaded.
3. **Download** programs and files from official websites.
4. **Keep your computer up to date** with the latest version to keep it safe.

How do I know if I have malware on my computer?

- **The computer slows down.** The speed of the operating system will decrease, resource utilization will increase, and the equipment fan will run at full speed.
- **Advertising and pop-up ads are constantly appearing.** Therefore, if you receive a message like “YOU WON AN IPHONE 13!”, your device may have a virus.
- **The system locks-up constantly** or displays a blue screen indicating that it has encountered a serious error.
- **The browser is filled unexpectedly with new toolbars,** extensions, or add-ons.

Phishing, smishing and vishing



Phishing, vishing or smishing are some of the scams used to steal private data. The aim is to deceive the victim by impersonating a trusted third party, who seeks to obtain personal data to replace the user's personality and steal their data.

When the cybercrime reaches the device via **email**, it is called **phishing**, and if it does so via **SMS, smishing**. There is a third form of fraud, **vishing**, which is committed through a **telephone call**.

If you suspect that you have been the victim of this type of scam, you should access your accounts (email, digital wallet, social networks...) to change the passwords and confirm that the attacker has not altered the access settings (check if the password recovery address, security questions, phone, etc. have been modified).

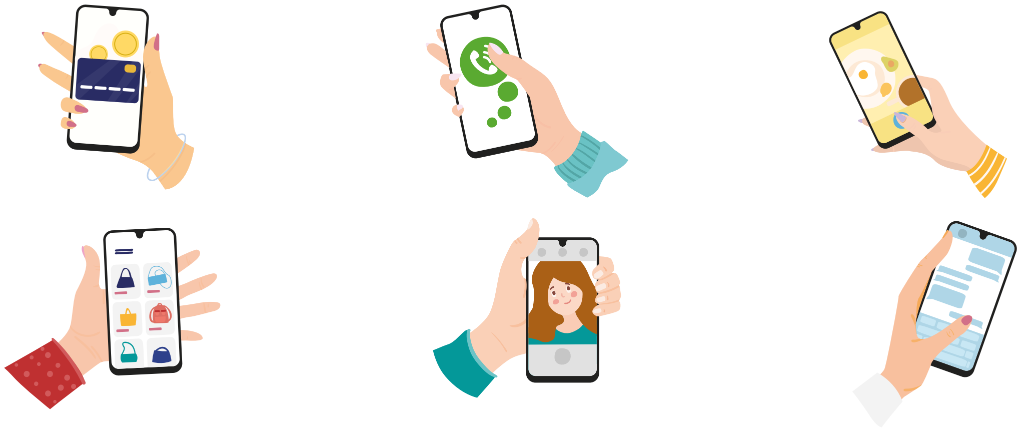
Tips

1. **Configure logon using multifactor authentication** (MFA). This method requires testing the identity of users through two or more tests.
2. **Use secure connections** and check that the website displays a lock or key and that its URL starts with "https".
3. **Do not provide sensitive data** over the internet and/or telephone, unless required by trusted sites or individuals.
4. **Be wary of SMS, calls, or emails** that indicate that you have won a draw in which you have not participated.

How do you know if you are a victim of this type of fraud?

- Understand that providers of any platform will never ask for your personal access passwords.
- Suspect poorly worded emails, misspellings or formatting errors.
- In this type of fraud, it is common to establish urgent deadlines to resolve the incident without serious consequences. This type of technique is carried out so that you react immediately.

Fake "apps"



Another of the main access routes for malware to devices, especially smartphones, are fake applications, which contain a specific code for the theft of sensitive data. The appearance and operation mimics that of the legitimate and official application, and its objective is for users to download it in order to access content and personal data without the user's consent. The appearance of these apps confuses the user, since their operation perfectly mimics that of an official application.

Tips

1. **Verify the authenticity** of an application before starting a download.
2. Pay attention to **other users' comments.**
3. **Confirm** what **permissions** are being requested.
4. **Acquire** a good **antivirus** product and make **frequent backups**.

How do I know if a fake application has been installed?

If a fake application has been installed, you may experience the following problems:

- A false warning for law enforcement requiring a fine/fee to be paid.
- A message from a fake antivirus.
- Redirecting to a website or downloading an unwanted application.

Ransomware or data hijacking for money

Ransomware. The aim is to hijack access to the user's sensitive data, preventing them from entering the system or personal files in exchange for a payment, usually in cryptocurrencies or credit cards.

Like any malware, the infection can come through opening email attachments from strangers, clicking on corrupt web links, using infected removable drives (USB flash drive), etc.

Tips

1. Avoid installing **unknown programs** on devices.
2. **Regularly update** the operating system, browser, antivirus, and other programs.
3. If the device has been infected and a ransom is requested for the information, it must never be paid and **INCIBE must be contacted at 017.**
4. **Secure duplicates of important files** and verify that the **backup** is not corrupt.

How to know if you have been a victim of ransomware?

Two levels of ransomware or rescue malware can be distinguished depending on the attack:

- On the one hand, **only certain text documents, images or other files may be affected,** which will be blocked until they are released for financial charges.
- On the other hand, in a more massive attack, **equipment can be completely blocked,** such as a computer or mobile phone, preventing general access to the system and all files.

Contact

Let's talk!

TELEPHONE
91 532 75 83

EMAIL
info@asufin.com

ADDRESS
Plaza de las Cortes 4, 4°D
28014 - Madrid

OPEN HOURS
De 09:00 a 18:00h.

asufintech

www.tech.asufin.com