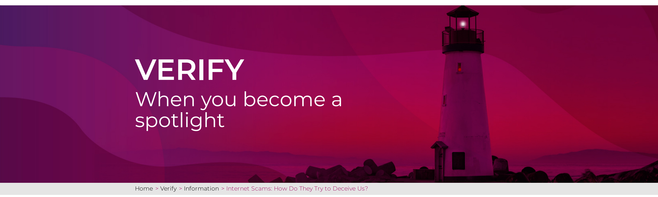


VERIFY
When you become a spotlight

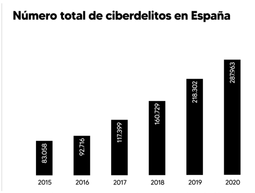
Internet Scams: How Do They Try to Deceive Us?

Email, WhatsApp, and social media are increasingly popular channels for cybercriminals to carry out scams. These are platforms where we receive all kinds of messages, from personal and professional communications to promotional messages, leading us to often perceive them as safe and trustworthy spaces. However, in 2022, law enforcement agencies recorded 375,506 criminal offenses through these channels, a 72% increase compared to 2019, according to data from the Ministry of the Interior.

Posted by Susana Pérez Soler | 05.12.2024 Share:

This rapid rise underscores the growing challenge of identifying and preventing scams in digital communication channels we frequently use and trust.

As a result of the pandemic, online transactions and shopping have increased exponentially, as has cybercrime: currently, one in five crimes is committed online.



Evolución de los ciberdelitos en España. Fuente: Ministerio d

In Catalonia, last year, the Mossos d'Esquadra received more than 92,000 reports of this type of crime. And despite the astronomical figure, it may still be far from reflecting the reality, because according to the Mossos, there would be many more cases, as most victims of fraud never file a report with the police.

Most Common Types of Cybercrimes

All **digital scams** have one thing in common: they stem from a fictional story or scenario in which the attacker tries to get the **victim to share information they would otherwise not disclose**. "This is called social engineering, which involves persuading the user to take an action and click on a link, whether to **access their data, damage their device, or spy on them**," explains Jorge Chinea, head of cybersecurity at the National Cybersecurity Institute (INCIBE).

Phishing

Phishing is one of the most widespread digital frauds. The attacker tries to deceive the victim through email to take an action against their best interests. For example, they might trick the victim into revealing their banking credentials, granting access to personal information, downloading malicious software, or visiting websites that compromise their devices.

Smishing

Smishing is a variant of phishing, but in this case, the scam is carried out through SMS text messages. Smishing is actually a compound word referring to SMS and phishing. Users often fall for this type of fraud because they don't expect to be tricked through this channel.

Vishing

Another rising type of crime is called vishing. In this case, the scam is carried out through a phone call where the caller impersonates the identity of a company, organization, or trusted individual. As with the previous cases, the attacker tries to access the victim's personal data to use it for their own benefit.

Baiting

In this case, the scammer presents a tempting opportunity to the victim. Unlike phishing and its variants, this is not a mass, indiscriminate attack via email, SMS, or a phone call. Instead, the attacker designs a customized bait and waits for the victim to fall into the trap. For example, if the attacker targets university professors, they study their browsing habits and might determine they are particularly interested in acquiring books. The scam might involve offering a free book in exchange for personal data or allowing them to download a file containing one, which actually infects the device.

Quid pro quo

Quid pro quo attacks are based on psychological manipulation and the creation of trust to obtain information from the victim. Unlike baiting, where the attacker expects the victim to fall into the trap by clicking on a link, the scammer offers a service in exchange for the victim's data. The term ***quid pro quo*** literally means "something for something," and this type of attack often works by appealing to the psychological principle of reciprocity, where when someone does something for us or gives us a favor, we feel compelled to return the favor.

Five Tips to Detect and Prevent Cyberfraud

Protecting Our Digital Identity

"Our information has value that can be exploited positively or negatively," explains **Joana Marí Cardona**, Data Protection Officer and Strategic Projects Manager at the Catalan Data Protection Authority. "To protect ourselves from any cyber scam, the first thing **we must do is become aware of the value our data holds** for cybercriminals and protect the information we share, both on social networks and through email or WhatsApp. Profile pictures, usernames, age, marital status, the school we attended, the job we have... everything can be used by a criminal to create a fictitious scenario. It's not about having things to hide, but about becoming aware of what we want to share and what we don't," she adds.

Pay Attention to the Details of the Message

Spelling mistakes, the type of font used, or the sender are some of the elements worth paying attention to when determining if the message we receive is genuine or an attempt at fraud. "It's essential to ignore messages claiming we have a package arriving that we didn't order, and be suspicious of any message offering things for a ridiculously low price. Digital scams are just old-fashioned scams applied in the digital environment," explains Chinea. We should carefully check the sender, as identity theft is sometimes revealed by small changes in the web address, username, or email.

Contact the Alleged Sender and Be Wary of Urgency

If you suspect that you are dealing with a scam, it's best to stop the communication and **contact the company or organization requesting your data or asking you to click on a link or download a file**. Special **caution should be taken if the sender urges you to act immediately**. The 017 is a free and confidential phone line offered by INCIBE for people with questions about cybersecurity, digital fraud, safe internet use, and privacy.

Do Not Click on Any Link or Provide Personal Information

No company or institution will ever ask for personal data via email or SMS, nor will they request credentials to access your information. If you have already provided them, it's crucial to contact the company as soon as possible to protect yourself from potential identity theft. Any incident that could constitute a data protection violation can also be reported to INCIBE.

Protect Your Devices

"Often, attacks are carried out due to **weaknesses in a system that may allow the attacker to access the device's information,**" explains Chinea. "One of the most commonly used passwords today is still '1234,'" he exemplifies. To avoid such cases, experts recommend basic cybersecurity advice, such as **using strong passwords and regularly updating them, not always having geolocation active, avoiding public Wi-Fi** networks, regularly updating your system and applications, and uninstalling apps you don't use.

You may also like:

disinformation: when to be suspicious

The keys to verifying information

DISINFORMATION
HOW TO COMBAT IT

Sources: how to know if they are reliable

There are no comments

Comment *

Name *

E-mail*

Acepto la política de privacidad y el aviso legal

Post Comment