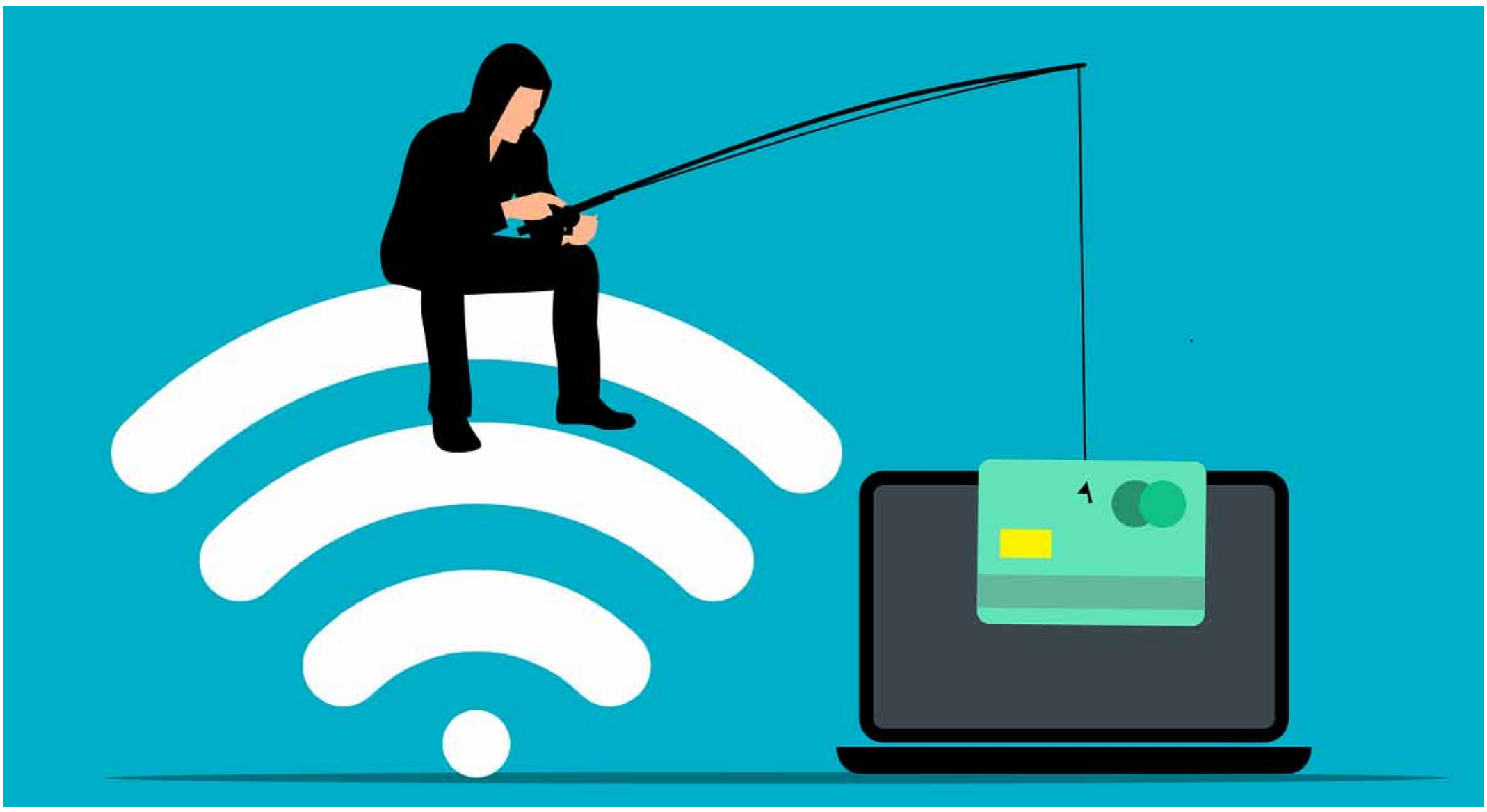
el Periòdic News

CYBER SCAMS

PIXABAY



It is important to be alert and use security measures such as two-factor authentication.

Understanding phishing: tips and prevention

Some entities in the Principality have publicly reported being the victims of an attempted scam.

LAURA GÓMEZ RODRÍGUEZ
ESCALDES-ENGORDANY

Cybersecurity is not just a concern for businesses or institutions, but for anyone who uses the internet. Cybercrimes, such as phishing, are increasingly sophisticated and frequent. Therefore, it is essential to understand how these threats work and how we can protect ourselves. From the Andorran Police, they maintain the objective of educating society on this issue, for this reason they have shared key information to be safer online.

PHISHING: WHAT IT IS AND HOW IT WORKS // Phishing is one of the techniques most used by cybercriminals to deceive people and obtain personal information, such as passwords or bank details. These attacks often appear as emails that appear to come from a legitimate source, such as a bank or parcel company. «These are the techniques used to deceive someone. He pretends to be someone legitimate, a company, a mail service, a supermarket, a bank,» explain the agents.

A common example is receiving an email pretending to be from a shipping company informing you that you have a package waiting to be picked up and asking you to click on a link to see the delivery status. If the user falls for the trap, they could end up revealing their password or other sensitive data.

VARIANTS OF PHISHING // Phishing is not limited to emails only. There are several variants of this attack that can be presented in different ways:

Smishing: It is a variant of phishing that arrives by SMS. The user receives a text message that appears to come from a trusted source, such as a bank, and contains a link or a request for personal information. «They always have

patterns that are always the same. There is a reason for urgency in the middle», say the agents, warning that these messages often try to create a sense of urgency or fear so that the user acts without thinking.

Phishing web: In this case, cybercriminals create fake websites that imitate legitimate ones, with the aim of tricking the user into entering their personal information. «Directly you find a web game that simulates the legitimate web game», they warn. It is important to always verify that the website URL is correct and starts with HTTPS, which indicates that the connection is secure.

Spear phishing: This technique involves a more targeted attack, in which cybercriminals gather information about their victim to make the deception more believable. For example, they can impersonate a superior in a company and send an email to employees asking them to make a wire transfer to a fake account.

Telephone spoofing: This variant involves impersonating the telephone number of a legitimate entity. When you receive the call, the number that appears on your device looks legitimate, but it's actually a scam. «The basic recommendation here is to ignore the beginning of what they tell you and call directly to the place from where they say they are calling you», point out the agents, emphasizing the importance of always verifying the information before acting.

HOW TO AVOID FALLING FOR PHISHING AND OTHER CYBERCRIMES // Avoiding being a victim of phishing or other cybercrimes requires a combination of preventive measures and common sense. Officers recommend a series of steps that everyone should take to protect themselves:

If the user falls for the trap, they could end up revealing their password or other sensitive data

Phishing has several variants that can be presented in different ways

Don't click on suspicious links: If you receive an email or text message with a link you didn't expect, don't click on it. Instead, go directly to the company's official website by typing the URL into your browser.

Use two-factor authentication: This measure adds an extra layer of security, making it much harder for cybercriminals to access your accounts even if they get your password. «I have it in all the accounts. In all my accounts I have the double factor», comments one of the agents, highlighting the importance of this step.

Check website security: Whenever you enter personal or financial information on a website, make sure the address starts with HTTPS. This indicates that the connection is encrypted and more secure.

Educate yourself and others: The more knowledge you have about how these attacks work, the better you can protect yourself. Talking to friends and family about these threats is also a good way to help prevent others from falling into the same traps.

Prevention is key to avoid becoming a victim of cybercrimes such as phishing. As Andorran police officers emphasize, it is important to be alert, use security measures such as double factor authentication, and stay informed about the latest techniques used by cybercriminals. «If you are doubting, inaction», is the advice they give to avoid falling into these traps. Remember, cyber security is a shared responsibility that requires attention and caution at all times.

SOME CASES // In recent months, the Principality has witnessed several phishing attempts that have affected different entities. On August 19th, Andorra Telecom warned of a phishing attack using the andorra.ad email address. The entity communicated through a tweet on X (formerly Twitter) that it was working to deregister the fraudulent website and block its access from browsers.

Previously, on August 6th, the University of Andorra warned of an attempted online scam circulating through false advertisements about courses supposedly taught by the university. The entity reminded that registrations can only be made through its official page and that the dissemination is always carried out in Catalan and through its official profiles.

Also, on May 24th, MoraBanc issued an alert on social networks about an attempt, in this case Smishing, in which confidential customer data was requested. The entity stressed that it never requests personal information through links in text messages or WhatsApp, warning users of the risk of falling for this type of fraud.

However, these incidents underline the importance of maintaining vigilance and following the safety recommendations we must have on the net to avoid being victims of this type of scam.●