Find out how cybercriminals can impersonate your bank

- ***Cybercriminals use techniques such as vishing (fraudulent calls) to deceive customers and request confidential information***

- ***In safe situations, the bank can contact the customer to verify transactions and protect the account against fraud***

31 May 2024

It is crucial to **be cautious when receiving calls from unknown numbers, as they may be fraudulent**. Nevertheless, sometimes banks contact their customers for various reasons, such as notifying them that a card has been requested and is pending collection at a branch.

Another reason could be to verify when transactions are carried out through online banking, in order to confirm the safety of these. This could also be to summon the customer for a face-to-face interview at the retail branch.

These are some of the most common situations in which the bank may contact its customers to provide them with relevant information or verify the authenticity of transactions for security reasons. However, you should always exercise caution and verify the legitimacy of incoming calls.

Is it possible for someone to impersonate a bank employee and call you?

Fraudulent calls (known as vishing) are an increasingly common reality in the digital age. Cybercriminals are continually improving their techniques to trick their victims.

Cybercriminals are constantly refining their techniques to deceive customers. Among the most commonly used, a broad and deep **knowledge of online banking**, enables them to guide customers through the processes needed to obtain their personal information. Spoofing is another technique they use, where they manipulate caller ID to make the victim believe that the call is coming from the bank's official number. They also **use compelling arguments** to gain the trust of customers and offer to help resolve false problems with their accounts.

It is essential to remember that, even if the call seems legitimate, customers should **never give out personal information over the phone** unless they are confident about who they are providing the information to.

The most recurrent scams among cybercriminals are the following:

Requesting **confidential** data such as card numbers or login credentials to online banking on the premise of supposedly refunding money.

External Communication Department
prensa@caixabank.com
www.caixabank.com/comunicacion

It is common for them to **use immediate payment systems** such as BIZUM or to request a **cash withdrawal from an ATM** using a personal code. CaixaBank allows cash withdrawals through an ATM, using a personal code, which offers great security advantages, but can become a common pretext for cybercriminals to carry out this type of scam.

A common pretext used is that someone else is making a withdrawal at an ATM and that, in order to cancel it, they must follow the steps indicated by the fraudsters, who will guide the customer to complete the cash withdrawal.

CaixaBank will never request by phone, SMS or email, information about passwords, personal data or codes. The bank works continuously to provide security information to its customers by keeping the security section of its website updated. In the event of any suspicious request, customers are advised to immediately contact the CaixaBank Customer Service number (900 40 40 90).