CaixaBank
PAYMENTS & CONSUMER

WHAT ARE THE MOST COMMON INTERNET SCAMS?

Every day, many people receive
scam attempts over the internet.
They are very common and anyone can fall for them
because they look real.

Therefore, you have to be very careful
and take into account all the information
which we explain here.

The three most common scams have strange names,
but here we explain them to you in simple terms.

1. *Phishing*: e-mail scam

It works as follows:

- You get an email that looks like it's from your bank
  or a company you know, but it's fake.
- The message is usually urgent, for example:
  «Your account will be blocked
  if you do not update your details».
- It includes a link and, when you open it,
  it takes you to a fake page that imitates the real one.
- On this page they want you to enter your personal
  or bank details in order to steal them.

Important:
If you receive an email like this, do not open the link or enter personal data.

If in doubt,
exit the message you have been sent
and go to the bank's or company's official website
or call their customer service telephone number.

2. *Smishing*: mobile phone SMS scam

It works as follows:

- You get a text message (SMS) on your mobile phone.
- The message might say: «There's a parcel for you» or «Your account will be suspended».
- It also includes a link or a dummy number for you to open and enter your details.
- If you do, they can steal money from your account or make purchases in your name.

Important:
If you receive an SMS like this, do not open the links.

If you have any doubts,
visit the official website of the bank or company yourself
or call their customer service telephone number.

3. *Vishing*: telephone scam

It works as follows:

- You get a call from somebody pretending to be from a bank, a company's technical service or an official institution.
- They speak convincingly so that you trust them.
- They ask you for your personal data or try to get you to install programmes that damage your computer or mobile phone.

Important:
If someone calls you asking for personal information or access to your equipment, hang up.
It is a scam attempt.

If you have doubts about whether the call is real, go to the official website of the bank or company yourself or call their customer service telephone number.

How can you protect yourself in all cases?

- Don’t share your personal data
  if you don’t know who is asking for it.
- Don’t answer with «yes» when you pick up the phone.
- Check the email address or the number
  from which they write or call you.
- Don’t open suspicious links or download files
  from people you don’t know.

What is two-factor authentication (2FA)?

- Two-factor authentication is an extra security
  feature to protect your accounts.
- In addition to the password,
  you need a second code to log in to your accounts.
- This code is sent to your mobile phone
  or a security application.
- This way, even if someone has your password,
  they will not be able to enter without the code.

Remember:

- Always keep your computer and mobile phone up to date.
- Use antivirus software and update it.
- If you follow these tips, you will be much better protected.
- And, if in doubt, never share your data.

Taking care of your personal information is taking care of your security.