bankinter

How can we protect ourselves against cyber attackers?

Being aware of the most common online scams is the first step.

Let us share our knowledge

bankinter

Cyber attackers will try to contact you **via any communication channel**, usually while spoofing the identity of a company you're familiar with, such as your bank.

They'll copy logos and communication styles to make their messages more believable. Then, they'll ask you to carry out a specific action, which is most likely an urgent request, so you don't have time to check the information.

These are some of the **most used channels:**

bankinter

Phishing

Phishing scams consist in **sending emails to users that spoof the identity of public or private companies**, in order to trick the recipients into disclosing personal, professional, or financial information.

In these types of scams, cyber attackers will copy logos and the style of real messages sent by the spoofed company. They'll ask you to carry out a specific action, which is usually urgent.

How to proceed

- **Be suspicious** if you receive an email asking you to **provide** your banking details or passwords.
- **Pay attention to the sender**. If something rings alarm bells, refrain from opening the email.
- If you notice anything strange, **do not reply to the email**.
- **Do not click** on any links or download attachments if the sender asks you to carry out an unexpected action.

bankinter

Smishing

Smishing scams consist in sending **fraudulent SMS messages to users' mobile phones** with the aim of obtaining personal, professional, or financial information. These texts will typically **ask users to click on a link or call a specific phone number** in order to 'verify', 'update', or 'reactivate' a service.

How to proceed

- Avoid hasty actions. **Do not click** on links, attachments, or images without checking the sender and the website address.
- **Do not reply to SMS messages** that ask you for your PIN, the password to your online bank account, or any other security credentials.
- **Bankinter will never ask you** to provide your credentials via text.

QRishing

QRishing scams consist in tricking users into **scanning a malicious QR code** with their mobile phones, which **redirects them to a fraudulent website** that will ask them to enter their credentials or confidential information.

How to proceed

- **Disable** the setting for automatically opening links after scanning QR codes with your mobile phone.
- **Use scanning applications** that allow you to view the URL destination of the QR code before opening it.
- **Look out for signs** that the QR code could have been tampered with.

Vishing

In vishing scams, **attackers call users** in an attempt to steal personal or corporate funds, or to trick them into disclosing sensitive information or granting access to their computer. To convince you that you're talking to a legitimate company, **attackers will use basic information about you that they've found online**.

How to proceed

- **Be suspicious** if you receive an urgent phone call or if you feel the caller is pressuring you.
- **Do not provide sensitive information** over the phone.
- If the caller asks you to download software, click on a link, or open a file, **do not follow their instructions.**
- Bankinter will **never ask you to provide confidential information** over the phone.

Baiting

In baiting attacks, cyber criminals leverage **removable devices, such as USBs, to infect your computer** with malware, which will allow them to gain access to your confidential information.

How to proceed

- **Be suspicious** of removable devices if you're unsure of their source.
- **Always** keep your antivirus software **up to date**.
- **Do not connect** unknown external devices to your computer.

bankinter

Attacks leveraging public Wi-Fi networks

Public Wi-Fi networks are inherently **insecure**, meaning they are more vulnerable to attacks even if they are password-protected.

In high-traffic areas, such as airports, cyber criminals usually give public Wi-Fi networks names that are similar to real networks.

How to proceed

- Do not access your online bank account or confidential information when connected to a **public/passwordless Wi-Fi network**.
- Do not connect to **open** Wi-Fi networks that **do not require log-in credentials**.
- Make sure the **latest versions** of your browser and operating system are installed. In addition, check that your antivirus software is correctly installed.

Online shopping scams

While there are many ways to shop securely online, we're often presented with fake offers that could be a scam.

How to proceed

- **Check whether the URL** begins with “https”.
- **Check whether the online store** has a digital certificate. **Search for information** about the company and customer **reviews**.
- **Pay close attention to the design** of the website to spot any strange elements or mistakes.

Attacks leveraging Bizum

Bizum can be used to send money to recipients using just their mobile number. And while this function is integrated in the bank's application, it can be used for fraudulent purposes.

Cyber criminals have been seen to send **money requests via Bizum** to customers of the service who, without realising, accept the transfer request.

How to proceed

- **Verify** the identity of the user that has sent the request.
- Always **read** messages before carrying out any transactions via Bizum.
- When you receive a Bizum, the amount is immediately deposited in your bank account. You will also receive a notification from your bank informing you that the transfer has been completed.

bankinter

CEO fraud

CEO fraud consists in **spoofing the identity of a senior figure** within a company that manages employees with access to corporate funds, in order to trick them into transferring money to accounts controlled by the cyber criminals. These types of scams are usually carried out over the phone or via email.

How to proceed

- **Be suspicious** of requests involving money transfers, especially if they are unusual or involve foreign bank accounts.
- **Carefully examine** the sender of the message and look out for any grammatical errors.
- When in doubt, contact the sender via a different channel to **confirm their identity**.

Fake news

The term 'fake news' refers to **fictitious news stories that are circulated** in order to divide and manipulate public opinion, usually for political, financial, or social motives.

How to proceed

- **Analyse the media outlet** that posted the news story and cross-check the information.
- **Pay attention to the URL** in case it seems suspicious.
- **Check** publication **dates**.
- **Make sure** there are no grammar or spelling mistakes.
- **Check** for signs that images could have been tampered with.

bankinter

Attacks leveraging payment cards

Payment card fraud occurs when cyber criminals gain access to a victim's card (or their cardholder data) and use the payment service to make purchases or unauthorised cash withdrawals.

How to proceed

- **Never provide your card details** unless you're making a purchase on a legitimate website.
- **Check** the purchase amount before confirming the transaction.
- **Always use two-factor authentication**, even when making small purchases.

And remember:

- Bankinter will never ask you to provide confidential information via email.
- Bankinter will never request your credentials via text.
- Bankinter will never ask a third-party to contact you to request information on our behalf.

If you have been the victim of cyber fraud and need help, contact our **Fraud Assistance Service (900 81 00 62)** or visit your nearest branch.

Knowledge is the key to security.