# Types of financial fraud and scams (and how to avoid them)

## What is a financial scam?

Financial scams are deceptive actions carried out for profit by individuals or businesses, causing economic loss to others.

**"Boiler rooms"** or **"financial fraud schemes"** are informal terms for individuals or firms offering and providing investment services without the required authorization.

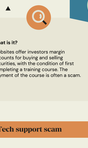
Boiler rooms are not registered investment firms and are not subject to the regulations and control of financial market supervisors.

**The best way to protect yourself against financial fraud is to recognize a scam when you see one.** You can check to see if an investment firm is registered on the website www.cnmv.es or by calling 900 535 015.

CNMV

# Nine types of financial scams (and how to avoid them)

## 1. Impersonation of authorized firms (clone firms)




**What is it?**

Fake companies or individuals copy the name, logo and details of authorized firms registered with the CNMV, making investors believe they're dealing with a legitimate business.

**How to avoid it?**

- Reject any unsolicited investment offers from firms that are not on the list of firms registered with the CNMV.
- Before signing any financial contract, verify the firm's identity and information name, brand, website address and domain, headquarters, telephone and email address, registration number with the supervisory agency.

## 2. Brokerage accounts linked to training courses

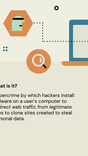
**What is it?**

Websites offer investors margin accounts for buying and selling securities, with the condition of first completing a training course. The payment of the course is often a scam.

**How to avoid it?**

- Be aware of the risk of fraud related to such training courses. Neither the courses or the access to margin accounts falls under the regulation and supervision of the CNMV.

## 3. Tech support scam



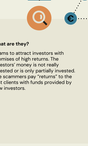
**What is it?**

Fraudsters try to pass as tech support personnel so investors will allow them to install applications and connect remotely to their computer or device. Once connected, they can steal personal data and make trades using the investor's brokerage account without authorization.

**How to avoid it?**

- Don't share login information for bank or brokerage accounts with others.
- Don't allow remote access to your computer or devices.
- Never log into your bank or brokerage accounts if a third party is connected.

## 4. Phising, smishing and vishing



**What are they?**

Three related scams (email, SMS and voice) for acquiring a person's login information to access their bank or brokerage accounts, operate with them and use the funds.

**How to avoid them?**

- Never respond to emails, text messages or telephone calls requesting confirmation of personal or confidential information. Hang up or delete the message and never open any attached files.
- Don't access your online bank or brokerage account by clicking on a link in an email or text message. Type the address for to type in the authentic URL.
- Use strong passwords with a combination of numbers, upper and lower-case letters, special characters.
- Remember that no authorized financial institution will ever ask a client for their personal data or full password.

## 5. Pharming

**What is it?**

Cybercrime by which hackers install malware on a user's computer to redirect web traffic from legitimate sites to clone sites created to steal personal data.

**How to avoid it?**

- Install and update antivirus and antimalware software on your devices. Use a password manager.
- Distrust any website that appears strange, if the URL is different or if the page contains an unusual request for information.
- Verify that you're using a secure connection the URL should start with "HTTPS" (not just "HTTP") and there should be a padlock icon in the address bar.

## 6. Pyramid or Ponzi schemes

**What are they?**

Scams to attract investors with promises of high returns. In reality, investors' money is not really invested or is only partially invested. The scammers pay "returns" to the first clients with funds provided by new investors.

**How to avoid them?**

- Always distrust the scam's number one enticement: unusually high returns compared to what the market offers.
- Never base investment decisions solely on recommendations of friends or family members.
- If you want investment advice, use the services of authorized professionals or firms.

## 7. Fraud related to cryptoassets

**What is it?**

Fake offers to invest in cryptoassets from scammers who promise extraordinarily high returns in little time and with no risk. The scammers pressure investors into making quick decisions and "not miss out on the opportunity".

They advertise aggressively on social media and by email and text messages.

**How to avoid it?**

- Never invest in anything you don't understand.
- Never trust promises of extraordinarily high returns in a short time with no risk. If it sounds too good to be true, it probably is.
- Be skeptical of investment offers that use technical or hard to understand language.
- Distrust anyone who tries to pressure you into making hurried investment decisions.

## 8. Fraud on social media



**What is it?**

Numerous fraudsters use social media in different ways: by creating fake profiles, impersonating legitimate firms or spreading false rumors or misleading information about companies to affect their stock price.

**How to avoid it?**

- Be skeptical of unsolicited investment offers through social media.
- Be sure to verify the source of any investment information you find on the internet.
- Never make investment decisions based solely on celebrity recommendations.
- Seek the advice of an authorized intermediary for personalized recommendations that fit your investor profile, financial objectives and risk tolerance.

## 9. Recovery room scam



**What is it?**

Companies target financial fraud victims, claiming to help them recover their losses. These are scams following previous scams.

**How to avoid it?**

- Always be wary if you're contacted about getting back money you may have lost. Don't pay an advance fee or to purchase stock, in exchange for an upfront fee or tax.
- Do not trust anyone who contacts you by phone, email or SMS offering to help recover financial losses. The CNMV never contacts fraud victims directly and does not authorize the use of its name or corporate identity.

## If you've been scammed:

Contact the CNMV and file a report with the police, Civil Guard or corresponding district court.