

Tip 4: Be wary of fraud through Internet and social networks

- Non-registered entities may have sophisticated and fast websites.
- The anonymity of social networks plays into the hands of those who wish to commit fraud.
- Be wary of unsolicited investment offers.
- On social networks, groups of people who share interests can be the victims of fraud.
- Protect your personal data online.

Warning signs:

1. ***“Do not allow yourself to be deceived by sophisticated and fast websites”***

“Boiler rooms’ usually operate through websites that appear technically high-quality and to have an impressive design: do not be dazzled by that appearance; check that behind these sites there is an entity registered with CNMV. Whether we are interested or not, we know that they have obtained our data legitimately and that if our answer is negative they will accept it without insisting.”

2. ***“Be careful when using social networks as an investment tool”***

“Social networks can enable fraudsters to contact a large number of people at a relatively low cost. It is also easy for them to create a website, e-mail accounts and social networks to contact their potential victims through direct messages, posing as a legal and regulated business. This appearance of legality is what convinces investors to entrust their money. It is difficult to trace and identify the real people behind fake accounts. Anonymity plays into the hands of fraudsters.”

3. ***“Be wary of unsolicited investment offers”***

“Potential fraudsters target victims on social networks, chat rooms and virtual forums. If you see a post on your wall, a tweet that mentions you, a direct message, or an e-mail you have not requested, you should be extremely careful about responding.

Many scams use 'spam' or unsolicited bulk mail to reach potential victims. The concepts 'opportunity', 'guaranteed return', 'high profitability' or similar abound in these messages that seek to attract investors.”

4. ***“Suspicion of affinity fraud”***

“One of the techniques used by those who seek to promote scams on social networks is 'affinity fraud', which consists of capturing the interest of a virtual group who are willing to make an investment. The goal is to capture members from identifiable groups, such as elderly groups or professionals.

As some members agree to make the investment, the rest will be trusting and tend to follow the advice of someone from the same group. Sometimes these influential people are part of the scam and try to convey security in the business they recommend.”

5. ***“Be careful about your privacy and security settings”***

“Those who use social networking as an investment tool should be aware of whether these sites protect their privacy and prevent fraudulent actions.

You should be aware that if you do not protect your personal information, it is possible that fraudsters will try to access this data.”

And always remember, should you have any doubts, to consult CNMV's investor assistance office (900 535 015) or send a query via the [form](#) found in CNMV's Investor Section.

Go to the complete [Investor Decalogue](#).