Basic Text Safeonweb 2025 Campaign

Don't get fooled by investment fraud: recognise the signs and protect yourself

Investing can be a smart way to grow your money, but unfortunately there are also fraudsters who take advantage of your trust. Investment fraud is increasingly common, especially online, and can result in significant financial losses. For the victims, the emotional and psychosocial consequences are not to be underestimated either.

What is investment fraud?

Investment fraud involves scams where criminals try to convince you to invest money in non-existent or fake financial products (crypto, forex, etc.). They often promise high returns with little risk, but it is actually a trap to steal your money. After receiving your money, these fraudsters often disappear without a trace.

How can you recognise investment fraud?

Watch out for the following warning signs:

- **Unsolicited contact:** You are contacted by phone, email or social media.
- **Promises too good to be true**: High profits are promised without any risk.
- **Pressuring to decide quickly:** You are pressured to invest quickly.
- **No transparency:** Little to no information is given about the product or provider. The provider is not licensed.
- **Unusual payment requests:** You are asked to transfer money to foreign accounts or through unusual payment methods, such as crypto.

How can you avoid investment fraud?

- **Check the provider:** Check whether the firm is licensed with the FSMA (https://www.fsma.be/en/check-your-provider). Also check if the name appears on the list of untrustworthy companies (List of companies operating unlawfully in Belgium | FSMA). If you have any doubts about the provider who has contacted you, please contact the FSMA using the contact form.
- **Be critical**: Has a nice investment opportunity appeared out of the blue? Then be critical and don't accept it straight away. Always take time to eliminate any doubt or suspicion.
- **Ask for clear and understandable information** from the provider. Don't invest in a financial product if you don't understand exactly what it entails.
- **Don't make any hasty payments:** Take your time to research the offer and don't be pressured.
- **Protect your personal information:** Never just share information about your identity, bank account details or other personal information.
- **Check in just a few minutes if you're dealing with a scammer.** Take the fraud test: https://www.fsma.be/en/have-i-been-victim-fraud Even if you think you know the

provider, double check and also check the contact details of the company who has contacted you. Many scammers fraudulently use the name of a familiar company that is licensed. Find more information here.

How do these scammers approach you?

Investment fraudsters use a variety of ways to make contact with their victims. Some commonly used methods include:

- **Social media and ads**: They advertise on Facebook, Instagram or YouTube with professional videos or famous faces (without the latter's permission) or they approach you through a personal message on one of your social media channels. It also happens that influencers advertise fraudulent investments.
- **Fake websites or platforms**: They create professional, fake websites that appear legitimate, including fake reviews.
- **Emails**: You receive an email with an exclusive invitation to take part in a promising investment.
- **Dating websites and apps**: They first build a bond of trust through a dating platform and then subtly shift the conversation to investment (known as *pig butchering*).
- **WhatsApp or text**: They sometimes pretend to be a friend, family member or "investment coach" via messages.
- **Telephone**: You get an unsolicited call with a supposedly interesting investment offer.

How does the actual scam work?

Investment fraud often proceeds via a well-constructed step-by-step plan. This is how scammers usually go about it:

1. **You are approached with an attractive offer**
   via social media, email, phone or an advertisement, you receive an offer to invest in crypto, stocks or an "innovative" platform.
2. **You are contacted**

   Once you express interest or leave your details, you are contacted by phone by a "personal account manager." You create a bond of trust with the scammer and they encourage or pressure you to invest.

3. **You are redirected to a very professionally produced trading platform**
   This platform seems reliable, with dashboards, charts and often even a personal "account manager".

4. **You are asked to make a small initial investment**
   The amount is often €250. Everything seems professional and you see results straight away on the platform.
5. **You see fictive profits in your account**
   The platform shows charts and figures showing that your investment is rising in value. That reassures you.
6. **Sometimes you can withdraw a small amount**
   This is a deliberate trick: it convinces you that the platform is legitimate, so you are more likely to invest larger amounts.
7. **You are encouraged to invest more**
   The "account manager" or the platform encourages you to deposit larger amounts for higher gains or exclusive opportunities.
8. **At some point everything goes wrong**
   You want to withdraw your money, but suddenly your account is locked, there are "technical problems," or you have to pay taxes or additional fees first.
9. **Eventually the scammer or platform disappears**
   You lose all access and your money is gone. There is often no longer any trace of the website, and it's impossible to contact them.

When does it end?

If you've already fallen victim to investment fraud, chances are you'll be approached again - this time by scammers claiming they can help get your money back. This is referred to as *recovery room fraud*.

This is their approach:

- **They pretend to be an official agency**
  They use official language, fake documents, pretend to be lawyers or banks, or claim to work together with the FSMA, Europol or pretend to be other official bodies such as financial regulators.
- **They seem to know about your previous investment**
  They use information you have previously shared, which makes it seem credible. They are often linked to the original scammers, or your data is resold to other criminals.
- **They ask for money again**
  For "releasing your funds," "administration fees," or "taxes," you first have to pay another amount.
- **They string you along**
  After you make the payment, they keep promising that the money is on its way, but keep delaying it.
- **You have lost your money again**
  In the end, these fraudsters also disappear with your second payment, and you have lost twice the amount.

Important: genuine agencies will never contact you to ask for money to recover lost investments.

What should you do if you are a victim of investment fraud?

- **Stop all contact with the scammers**: Block their calls.
- **Stop paying**: Don't transfer any additional funds, even if you are promised that you will then get your investment back.
- **Inform your bank:** Contact your bank immediately to try to block the transfer or prevent further losses.
- **Block your means of payment**: If you have shared bank information, contact Card Stop (078 170 170) to block your cards.
- **File a complaint with the police:** File a report at your local police station or at www.politie.be.
- **Report the fraud (Dutch/French only):** via ConsumerConnect > Consumentenbedrog > Verdachte beleggingen or via safeonweb.be
- **Beware of 'recovery rooms':** Some scammers approach victims a second time with the promise of recovering lost money, but charge more money to do so.

How are governments and partner organisations tackling online fraud?

Several governments and partner organisations, such as Safeonweb, the FSMA (Financial Services and Markets Authority) and the FPS Economy, have joined forces to prevent even more people from becoming victims of online fraud. They have various approaches in this regard:

Raising public awareness

The FSMA, Safeonweb, FPS Economy, Febelfin, the Cyber Security Coalition and local prevention advisers run joint campaigns to warn people about investment fraud.

- View the Safeonweb campaign:
- Long video

Information and resources

Safeonweb and the FSMA offer a fraud test and extensive information to help citizens recognise fraud.

More info on Wikifin.

Dedicated reporting point

There is a dedicated reporting point where consumers can report fraud or request information.

Reporting point via Consumer Connect

Active detection and monitoring of fraudsters

The FSMA plays a key role in this regard:

- It publishes warnings against fraudulent companies.
- It reports suspicious cases to the judicial authorities.
- It collects information on financial flows, including through collaboration with other supervisory authorities.
- It uses reports from consumers to identify new fraud trends.
- Provides a personalised response to all consumers who submit direct enquiries or reports to the FSMA.

Swift action against fraudulent platforms

Government agencies, including the FPS Economy and the FSMA, work with trusted partners within the BAPS system of the Centre for Cybersecurity Belgium, to quickly detect fake trading platforms and take them offline.

Learn more about BAPS and trusted partners.

More information and help

For more tips and information on how to protect yourself from investment fraud, visit the Wikifin website (French/Dutch only), where you can find independent, reliable and practical information on money matters.

Stay vigilant and don't be fooled by promises that are too good to be true. If in doubt, always contact the FSMA or your bank before investing.