GET INFO FREE · FREE GUIDE 04

Financial scams: a defence manual

The recurring signs, the most common schemes, the checks to make and what to do if it has already happened.

GETINFOFREE.CO

EDITION 2026-10

IN THIS GUIDE

Financial scams hit people of every age, profession and level of education. They do not work because victims are naive: they work because they are well built, by professionals. Knowing their patterns is the most effective defence, and that is the sole purpose of this guide.

01 The recurring signs

02 The most common schemes

03 The checks to make, always

04 If it has already happened

05 The card to keep at hand

Educational and informational content only. It is not personalised financial, tax or investment advice, and it is not an invitation to buy or sell financial instruments. Numerical examples are hypothetical. All investments involve risks, including the possible loss of invested capital.

01

CHAPTER 1

The recurring signs

Names and platforms change; the script does not.

Behind the variety of scams lies a small number of recurring elements. Recognising even one of them is a good reason to stop.

Sign	How it appears	Why it should raise suspicion
High and safe gains	"Guaranteed return", "risk-free", monthly percentages	High return and low risk do not exist together
Haste	"The offer ends today", "last places"	It is meant to stop you thinking and asking for advice
Unsolicited contact	Calls, messages, adverts with famous faces	Authorised firms do not look for clients this way
Money through unusual channels	Foreign accounts, crypto wallets, prepaid cards	They make recovery almost impossible
Remote access	A request to install a "support" program	It gives the scammer control of your device and accounts
Secrecy	"Don't tell your bank", "don't mention it at home"	Whoever asks for silence knows a third party would spot the scam

THE FCA'S SEVEN QUESTIONS

The UK supervisory authority suggests asking seven questions about any offer: Is it unexpected? Do you feel pressured to act quickly? Does it sound too good to be true? Is the offer exclusively for you? Are they trying to flatter you? Are you feeling worried or excited? Are they speaking with authority? It also warns that people who have been scammed may be targeted again. (Source: Financial Conduct Authority, page updated 19/01/2026.)

> *If an offer is high, safe and urgent, one of the three is not true. Usually none of them is.*

02

CHAPTER 2

The most common schemes

Six scripts that explain the great majority of cases.

The fake trading platform

An advert or a call leads to an "adviser" who suggests starting with a small sum. A professional-looking site shows gains that keep growing. The person pays in more. When they ask to withdraw, "taxes" or "release fees" to be paid in advance appear. The gains on screen never existed.

The Ponzi scheme

The returns paid to early participants do not come from a real business but from the money of new ones. It works as long as new people join, then collapses. It often spreads among friends, colleagues or members of the same community, in good faith.

The fake recovery

Someone who has already lost money is contacted again by a self-styled lawyer, an "authority" or a firm promising to recover it in exchange for an upfront payment. It is a second scam, often by the same people as the first.

Cloned authorised firms

Scammers copy the name, logo and authorisation number of a genuine firm, changing only the contact details. That is why the check must be made on the official register, and contact details compared with those shown there.

The romance scam

A relationship started online, cultivated for weeks, which at some point leads to a "safe investment" recommended by the new acquaintance. Trust built over time lowers every defence.

Fake endorsements

Videos and articles in which well-known figures appear to recommend an investment. They are edited or artificially generated: the use of a famous face is, in itself, a warning sign.

03

CHAPTER 3

The checks to make, always

Five minutes worth more than any promise.

1. Find the website of your country's supervisory authority yourself: do not use the link you were given.
2. Check on the register that the firm is authorised to provide investment services.
3. Compare website, email and phone number with those shown on the register: they must match.
4. Look at the warnings the authority publishes about unauthorised firms.
5. Talk to someone you trust, or to your bank, before paying in any sum.

WHAT PROVES NOTHING

A polished website, a licence number in the footer, an address in a financial capital, glowing reviews, a contract with stamps and signatures, a small sum returned early on to win trust.

THREE THINGS NEVER TO DO

Do not install remote-control software at someone's request. Do not share codes, passwords or codes received by message. Do not pay money into accounts held by individuals or by companies other than the firm itself.

04

CHAPTER 4

If it has already happened

Acting at once improves the chances and limits the damage.

1. Stop all contact and all payments, even if you are told one is needed to "release" the money.
2. Call your bank immediately: in some cases a recent transfer can be blocked or recalled.
3. Change passwords and codes, and have the devices on which you installed software checked.
4. Collect everything: messages, emails, receipts, website addresses, phone numbers.
5. Report it to the police and notify the supervisory authority.
6. Be wary of anyone contacting you with a paid offer to recover the money.

Many victims do not report out of shame. It is an understandable mistake, but a mistake: a report is the precondition for any attempt at recovery, and every notification helps the authorities stop the same scheme before it hits others.

> *Shame is the scammers' best ally. Talking about it is the first way to defend yourself.*

05

CHAPTER 5

The card to keep at hand

To be reread whenever someone proposes an investment.

- [ ] Is the person offering the investment on the supervisory authority's register? Did I check it myself, starting from the official website?
- [ ] Do the contact details match those on the register?
- [ ] Was I promised a high, safe or quick gain?
- [ ] Am I being rushed, or asked not to tell anyone?
- [ ] Am I asked to pay into a foreign account, in cryptocurrency, or to an individual?
- [ ] Am I asked to install a program or to share codes?
- [ ] Have I understood the investment well enough to explain it?
- [ ] Have I talked about it with someone I trust?

If the answer to any of questions three to six is yes, or to any of the others is no, the right thing to do is to stop. A genuine opportunity can always wait for the time a check takes.

TO CONTINUE

All courses, the glossary and the calculators are freely available at getinfofree.co, with no registration.

Institutional sources for further reading

- Financial Conduct Authority (UK) — Consumers — https://www.fca.org.uk/consumers
- ESMA — Investor Corner — https://www.esma.europa.eu/investor-corner
- Autorité des marchés financiers (France) — https://www.amf-france.org/en
- CNMV (Spain) — https://www.cnmv.es/portal/home.aspx?lang=en
- FINMA (Switzerland) — https://www.finma.ch/en/
- Finansinspektionen (Sweden) — https://www.fi.se/en/
- Finanssivalvonta (Finland) — https://www.finanssivalvonta.fi/en/

Sources consulted for this guide

- Financial Conduct Authority — «Protect yourself from scams» (agg. 19/01/2026) — https://www.fca.org.uk/scamsmart/how-avoid-investment-scams
- ESMA — Investor Corner — https://www.esma.europa.eu/investor-corner

---

Educational and informational content only. It is not personalised financial, tax or investment advice, and it is not an invitation to buy or sell financial instruments. Numerical examples are hypothetical. All investments involve risks, including the possible loss of invested capital.
© 2026 Get Info Free — getinfofree.co