GET INFO FREE · GUIDA GRATUITA 04

Truffe finanziarie: il manuale di difesa

I segnali che si ripetono, gli schemi più diffusi, le verifiche da fare e che cosa fare se è già successo.

GETINFOFREE.CO

EDIZIONE 2026-10

IN QUESTA GUIDA

Le truffe finanziarie colpiscono persone di ogni età, professione e livello di istruzione. Non funzionano perché le vittime sono ingenue: funzionano perché sono costruite bene, da professionisti. Conoscerne gli schemi è la difesa più efficace, ed è l'unico scopo di questa guida.

01 I segnali che si ripetono

02 Gli schemi più diffusi

03 Le verifiche da fare, sempre

04 Se è già successo

05 La scheda da tenere a portata di mano

Contenuto esclusivamente educativo e informativo. Non è consulenza finanziaria, fiscale o di investimento personalizzata e non è un invito ad acquistare o vendere strumenti finanziari. Gli esempi numerici sono ipotetici. Tutti gli investimenti comportano rischi, inclusa la possibile perdita del capitale investito.

01

CAPITOLO 1

I segnali che si ripetono

Cambiano i nomi e le piattaforme, non il copione.

Dietro la varietà delle truffe c'è un numero ristretto di elementi ricorrenti. Riconoscerne anche uno solo è un buon motivo per fermarsi.

Segnale	Come si presenta	Perché deve insospettire
Guadagni alti e sicuri	«Rendimento garantito», «senza rischi», percentuali mensili	Rendimento alto e rischio basso insieme non esistono
Fretta	«L'offerta scade oggi», «ultimi posti»	Serve a impedire di riflettere e di chiedere consiglio
Contatto non richiesto	Telefonate, messaggi, annunci con volti noti	Chi è autorizzato non cerca clienti così
Denaro verso canali insoliti	Conti esteri, portafogli di criptovalute, carte prepagate	Rendono il recupero quasi impossibile
Accesso remoto	Richiesta di installare un programma «di assistenza»	Dà al truffatore il controllo del dispositivo e dei conti
Segretezza	«Non dirlo in banca», «non parlarne in famiglia»	Chi chiede di tacere sa che un terzo riconoscerebbe la truffa

LE SETTE DOMANDE DELLA FCA

L'autorità di vigilanza britannica invita a porsi sette domande davanti a qualsiasi proposta: è inattesa? Mi viene messa fretta? Sembra troppo bella per essere vera? È un'offerta «solo per me»? Stanno cercando di lusingarmi? Mi sento preoccupato o euforico? Parlano con tono di autorità? Avverte inoltre che chi è già stato truffato può essere preso di mira di nuovo. (Fonte: Financial Conduct Authority, pagina aggiornata al 19/01/2026.)

> *Se un'offerta è alta, sicura e urgente, una delle tre cose non è vera. Di solito nessuna.*

02

CAPITOLO 2

Gli schemi più diffusi

Sei copioni che spiegano la grande maggioranza dei casi.

La falsa piattaforma di trading

Un annuncio o una telefonata portano a un «consulente» che propone di iniziare con una piccola somma. Un sito dall'aspetto professionale mostra guadagni che crescono. La persona versa di più. Quando chiede di ritirare, compaiono «tasse» o «commissioni di sblocco» da pagare in anticipo. I guadagni sullo schermo non sono mai esistiti.

Lo schema Ponzi

I rendimenti pagati ai primi partecipanti non vengono da un'attività reale, ma dal denaro dei nuovi. Funziona finché entrano nuove persone, poi crolla. Spesso si diffonde tra amici, colleghi o membri di una stessa comunità, in buona fede.

Il falso recupero

Chi ha già perso denaro viene ricontattato da un sedicente avvocato, da un'«autorità» o da una società che promette di recuperarlo in cambio di un pagamento anticipato. È una seconda truffa, spesso opera degli stessi autori della prima.

La clonazione di soggetti autorizzati

I truffatori copiano nome, logo e numero di autorizzazione di un intermediario vero, cambiando solo i contatti. Per questo il controllo va fatto sul registro ufficiale, e i recapiti vanno confrontati con quelli che lì risultano.

La truffa sentimentale

Una relazione nata online, coltivata per settimane, che a un certo punto porta a un «investimento sicuro» consigliato dalla nuova conoscenza. La fiducia costruita nel tempo abbassa tutte le difese.

I falsi testimonial

Video e articoli in cui personaggi noti sembrano raccomandare un investimento. Sono montaggi o contenuti generati artificialmente: l'uso di un volto famoso è, di per sé, un segnale d'allarme.

03

CAPITOLO 3

Le verifiche da fare, sempre

Cinque minuti che valgono più di qualsiasi promessa.

1. Cerca da solo il sito dell'autorità di vigilanza del tuo paese: non usare il link che ti è stato dato.
2. Verifica nel registro che il soggetto sia autorizzato a prestare servizi di investimento.
3. Confronta sito, email e telefono con quelli indicati nel registro: devono coincidere.
4. Controlla gli avvisi pubblicati dall'autorità sui soggetti non autorizzati.
5. Parlane con una persona di fiducia o con la tua banca prima di versare qualsiasi somma.

CHE COSA NON PROVA NULLA

Un sito elegante, un numero di licenza a piè di pagina, un indirizzo in una capitale finanziaria, recensioni entusiaste, un contratto con timbri e firme, una piccola somma restituita all'inizio per conquistare fiducia.

TRE COSE DA NON FARE MAI

Non installare programmi di controllo remoto su richiesta di qualcuno. Non comunicare codici, password o codici ricevuti per messaggio. Non versare denaro su conti intestati a persone fisiche o a società diverse dall'intermediario.

04

CAPITOLO 4

Se è già successo

Agire subito aumenta le possibilità e limita i danni.

1. Interrompi ogni contatto e ogni pagamento, anche se ti viene detto che serve per «sbloccare» il denaro.
2. Chiama subito la tua banca: in alcuni casi un bonifico recente può essere bloccato o richiamato.
3. Cambia password e codici, e fai controllare i dispositivi su cui hai installato programmi.
4. Raccogli tutto: messaggi, email, ricevute, indirizzi dei siti, numeri di telefono.
5. Sporgi denuncia alle forze dell'ordine e segnala il caso all'autorità di vigilanza.
6. Diffida di chiunque ti contatti promettendo di recuperare il denaro a pagamento.

Molte vittime non denunciano per vergogna. È un errore comprensibile, ma è un errore: la denuncia è la condizione per qualsiasi tentativo di recupero, e ogni segnalazione aiuta le autorità a bloccare lo stesso schema prima che colpisca altri.

> *La vergogna è il miglior alleato dei truffatori. Parlarne è il primo modo di difendersi.*

05

CAPITOLO 5

La scheda da tenere a portata di mano

Da rileggere ogni volta che qualcuno propone un investimento.

- [ ] Chi mi propone l'investimento è nel registro dell'autorità di vigilanza? L'ho verificato io, partendo dal sito ufficiale?
- [ ] I recapiti coincidono con quelli del registro?
- [ ] Mi è stato promesso un guadagno alto, sicuro o rapido?
- [ ] Mi viene messa fretta o chiesto di non parlarne con nessuno?
- [ ] Mi viene chiesto di versare su un conto estero, in criptovalute o a una persona?
- [ ] Mi viene chiesto di installare un programma o di comunicare dei codici?
- [ ] Ho capito in che cosa consiste l'investimento, tanto da saperlo spiegare?
- [ ] Ne ho parlato con qualcuno di cui mi fido?

Se la risposta a una delle domande dalla terza alla sesta è sì, o a una delle altre è no, la cosa giusta da fare è fermarsi. Un'opportunità vera può sempre aspettare il tempo di una verifica.

PER CONTINUARE

Tutti i corsi, il glossario e i calcolatori sono liberamente consultabili su getinfofree.co, senza registrazione.

Fonti istituzionali per approfondire

- CONSOB — Educazione finanziaria — https://www.consob.it/web/investor-education
- ESMA — Investor Corner — https://www.esma.europa.eu/investor-corner
- Banca d'Italia — L'Economia per tutti — https://economiapertutti.bancaditalia.it/

Fonti consultate per questa guida

- 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

---

Contenuto esclusivamente educativo e informativo. Non è consulenza finanziaria, fiscale o di investimento personalizzata e non è un invito ad acquistare o vendere strumenti finanziari. Gli esempi numerici sono ipotetici. Tutti gli investimenti comportano rischi, inclusa la possibile perdita del capitale investito.
© 2026 Get Info Free — getinfofree.co