PRODOTTO 01 / GUIDA PRATICA

Riconoscere e comprendere le truffe

Schemi, indicatori, casi realistici e procedure di reazione per trattative tra privati.

Su una piattaforma che facilita l'incontro tra persone e imprese possono apparire proposte legittime, progetti incerti e tentativi deliberati di frode. Non tutto ciò che è rischioso è fraudolento; ma nessun progetto merita fiducia automatica. La difesa migliore è fermarsi, chiedere prove e usare canali verificabili.

1. Rischio commerciale, errore e frode: non sono la stessa cosa

Situazione	Cosa significa	Comportamento
Rischio di business	La società può fallire anche se le dichiarazioni sono sincere.	Esaminare numeri, scenari e perdita potenziale.
Dati incompleti	Mancano documenti o l'ipotesi è troppo ottimista.	Chiedere evidenze e sospendere il giudizio.
Segnale di frode	Si usano inganni, pressioni e pagamenti o identità non verificabili.	Interrompere scambi sensibili, preservare prove e segnalare.

Una singola incongruenza non prova una truffa. Tuttavia rifiuti persistenti di documentare identità, poteri di firma o destinazione dei fondi sono motivi sufficienti per non procedere.

2. Otto schemi da conoscere

Finto investitore con costo di sblocco

Promette capitale, ma prima chiede una «commissione di verifica», una cauzione o una spesa notarile su un conto non verificato.

Finto founder e documenti inventati

Presenta fatturato, clienti o brevetti non confermabili; usa loghi, testimonianze o fotografie di altre imprese.

Finta due diligence

Chiede copie di documenti personali, credenziali, account bancari o materiale societario prima di spiegare finalità e garanzie.

Furto di identità e profili clonati

Usa nome e foto di un vero professionista o di una vera società, ma comunica tramite un profilo o un canale non verificato.

Falsa garanzia di rendimento

Promette capitale protetto, ritorni fissi e risultati «certificati», senza documentazione adeguata o con richiami a enti inesistenti.

Pagamento urgente per un posto esclusivo

Crea scarsità fittizia: «versi oggi o perdi il diritto», impedendo consulenza e verifica.

Truffa del cambio IBAN

A ridosso di un accordo viene comunicato un conto bancario diverso, usando una falsa identità o una comunicazione contraffatta.

Link e file malevoli

Invia presunti contratti o piattaforme di firma che chiedono password, OTP, installazione software o accesso remoto.

3. Dodici segnali d'allarme: cosa osservare

- Richiesta di denaro prima di esibire contratto, ruoli e documentazione.
- Garanzia di rendimenti o assenza dichiarata di rischio.
- Sollecitazione a decidere nello stesso giorno.
- Informazioni economiche che cambiano tra pitch, visura e bilanci.
- Nome della persona non compatibile con ruolo, delega o firma.
- Contatti non coerenti con quelli reperibili da fonti indipendenti.
- Rifiuto di un incontro video o di controlli minimi ragionevoli.
- Richiesta di spostarsi subito fuori dai canali previsti dalla piattaforma.
- Richiesta di OTP, password, accesso remoto o dati di pagamento.
- Richiesta indiscriminata di passaporto, carta d'identità o dati di terzi.
- Pressione per nascondere l'operazione a soci, consulenti o familiari.
- «Badge verificato», autorizzazioni o certificazioni presentati come garanzia totale.

Regola pratica: 1 richiesta critica basta a fermarsi

Se ti viene chiesto di consegnare credenziali bancarie, OTP o denaro non giustificato, non serve accumulare altri indizi per sospendere il contatto.

4. Quattro casi realistici e la risposta corretta

Caso	Messaggio ricevuto	Risposta sicura
A / Investitore	«Prima di inviare i 30.000 €, anticipa 750 € per attivare il deposito».	Non pagare. Chiedi identità e basi giuridiche; usa «Segnala».
B / Fondo estero	«Il nostro manager ti manda un link: registrati con SPID e carica il documento».	Non aprire il link. Verifica il soggetto su fonti ufficiali.
C / Cofounder	«Ti cedo il 40%, ma prima inviami tutte le credenziali del gestionale».	Mai condividere credenziali. Definisci per iscritto gli accessi necessari.
D / Acquirente	«Trasferisci l'acconto al nuovo conto comunicato via chat».	Sospendi e verifica l'identità e le istruzioni tramite una procedura indipendente.

5. Come verificare una dichiarazione sospetta

1. Identifica la dichiarazione in una frase: «La società X ha raccolto 500.000 €»; «Y è amministratore».
2. Individua la fonte primaria pertinente (Registro Imprese, documento originale, autorità di vigilanza se applicabile).
3. Confronta denominazione, codice fiscale, incarico, date e modalità di contatto.
4. Annota ciò che la fonte dimostra e ciò che NON dimostra. Un nome reale può essere usato abusivamente.
5. Non usare un solo elemento a conferma. Un sito web curato o una videochiamata non sostituiscono i controlli.

6. Cosa fare subito se qualcosa non torna

1. Non eseguire nuovi versamenti e non inviare altri documenti o informazioni riservate.
2. Non aprire file o collegamenti sospetti; non installare software indicato dalla controparte.
3. Conserva i messaggi già disponibili, le date, i riferimenti dei profili e i documenti ricevuti senza modificarli.
4. Usa il pulsante «Segnala» su profilo o annuncio, oppure la pagina Contatti di ImprendereOra.
5. Se hai già pagato, contatta immediatamente la banca o il prestatore di servizi di pagamento per valutare blocco e recupero: l'esito non è garantito.
6. Se hai comunicato credenziali, cambia password su un dispositivo affidabile, attiva l'autenticazione multifattore dove disponibile e contatta gli operatori coinvolti.
7. Se temi un reato, rivolgiti alle forze dell'ordine. Pericolo immediato: chiama il 112.

7. Prevenzione quotidiana: un protocollo di cinque minuti

Prima di rispondere	Prima di documenti riservati	Prima di firmare o pagare
Leggo il profilo, cerco incongruenze e non esco dalla piattaforma.	Verifico ragione sociale, ruolo, finalità e condizioni di accesso.	Controllo gli originali e richiedo una revisione professionale.
Non invio documenti personali non necessari.	Condivido solo materiale pertinente, per fasi e con accessi limitati.	Confermo beneficiario, dati e causale tramite canale indipendente.

8. Errori comuni e falsi miti

- «Ha una società iscritta, quindi è affidabile». No: l'iscrizione non certifica la bontà di un investimento.
- «C'è scritto investitore verificato, quindi posso pagare». No: un badge non elimina la necessità di verifiche.
- «Mi ha mostrato un documento in videochiamata». La sola immagine di un documento può essere falsa o sottratta.
- «Se denuncio alla piattaforma, ho denunciato alla Polizia». No: sono procedure differenti.
- «Se non ho perso denaro, non devo segnalare». Anche un tentativo può essere rilevante per la sicurezza di altri utenti.

Fonti per approfondire

- ImprendereOra: FAQ (imprendereora.com/faq) e Contatti (imprendereora.com/contatti).
- CONSOB: sezione «Occhio alle truffe!» e avvisi sull'abusivismo (consob.it).
- Banca d'Italia: albi ed elenchi dei soggetti vigilati (bancaditalia.it).
- Polizia di Stato: consigli antifrode e Denunce Online (poliziadistato.it).
- Garante Privacy: principi fondamentali del trattamento dei dati (garanteprivacy.it).

ImprendereOra offre strumenti informativi e di comunicazione. I modelli non costituiscono consulenza legale, finanziaria o un impegno contrattuale automatico.