Truffa crypto o falso investimento online: cosa salvare subito

Checklist operativa per conservare prove digitali, pagamenti, wallet, piattaforme, chat e richieste di ulteriori versamenti. Documento informativo generale, non sostituisce consulenza legale sul caso concreto.

Prima regola: non pagare ancora.	Richieste di “tasse”, “commissioni”, “sblocchi”, “verifiche fiscali” o costi per recuperare crypto sono spesso parte della stessa frode o di una seconda truffa.

1. Chat, profili e canali di contatto

- Conversazioni WhatsApp, Telegram, Instagram, email, dating app e social network.
- Numeri di telefono, username, nickname, ID utente, link profilo e foto profilo.
- Messaggi vocali, promesse di guadagno, istruzioni operative, richieste di pagamento.
- Non cancellare nulla prima di avere una copia ordinata.

2. Piattaforma, sito o app utilizzata

- URL completo del sito e schermate dell’area personale.
- Saldo visibile, presunti profitti, storico operazioni e richiesta di prelievo.
- Richieste di “tasse”, “commissioni”, “sblocchi” o verifiche fiscali.
- Email ricevute dalla piattaforma, termini, contratti, account manager, dati societari dichiarati.

3. Pagamenti bancari o con carta

- Contabili di bonifico, IBAN beneficiario, causale, data, importo e banca utilizzata.
- Estratti conto e movimenti carta collegati ai versamenti.
- Eventuali richieste di recall, reclami o comunicazioni già inviate alla banca.
- Nomi di beneficiari, società, conti esteri o intermediari indicati.

4. Crypto, wallet, exchange e transazioni

- Asset trasferito: USDT, BTC, ETH o altro.
- Rete utilizzata, quantità, data, tx hash e wallet destinatario.
- Exchange utilizzato per acquistare o trasferire crypto.
- Screenshot dell’operazione e ricevute dell’exchange.

5. Cronologia minima dei fatti

- Data del primo contatto.
- Data del primo pagamento.
- Date e importi dei versamenti successivi.

- Data della richiesta di prelievo e del blocco.
- Data delle ulteriori richieste di denaro.

6. Documenti personali e rischio identità

- Documento di identità, selfie, prova di residenza o altri dati caricati sulla piattaforma.
- Eventuali firme digitali, contratti o moduli KYC.
- Ogni messaggio in cui il soggetto chiede nuovi documenti o accesso remoto al dispositivo.

Errore da evitare

Non affidarti a soggetti che promettono recuperi certi, chiedono anticipi per “sbloccare” fondi o pretendono accesso remoto al computer/telefono. Prima va costruito un fascicolo ordinato: fatti, prove, flussi, wallet, piattaforme, pagamenti e allegati.

Avv. Gerardo Di Maria
Piazza Umberto I, n. 1 - 84121 Salerno
gerardo@avvocatodimaria.com · +39 328 607 3439
www.avvocatodimaria.com