7 SETTEMBRE 2026 • 10 MIN DI LETTURA • DANILO GIUDICE

Anatomia di una truffa, come difenderti dagli attacchi crypto più comuni e avanzati

I nove attacchi che svuotano i portafogli in criptovalute, i segnali per riconoscerli in tempo e le otto regole che li fermano quasi tutti. Apre Anatomia di una truffa, la rubrica di sicurezza di MoneyViz.

PERCHÉ TI RIGUARDA

- A dicembre 2025 una persona ha perso **50 milioni di dollari** copiando un indirizzo dalla cronologia: un gesto che hai fatto anche tu
- Non è una questione di ingenuità: **non vieni ingannato quando non sai niente, vieni ingannato quando l'attacco sembra normale abbastanza a lungo**
- Quasi tutte le perdite partono da un gesto ordinario: un clic dato di fretta, una firma approvata senza leggerla, un indirizzo copiato
- Le regole che chiudono la porta alla maggior parte degli attacchi sono **otto**, non richiedono competenze tecniche, e qui sotto trovi la scheda da ritagliare
- È la prima puntata di **Anatomia di una truffa**, la rubrica di sicurezza di **MoneyViz**: nove attacchi, una puntata ciascuno

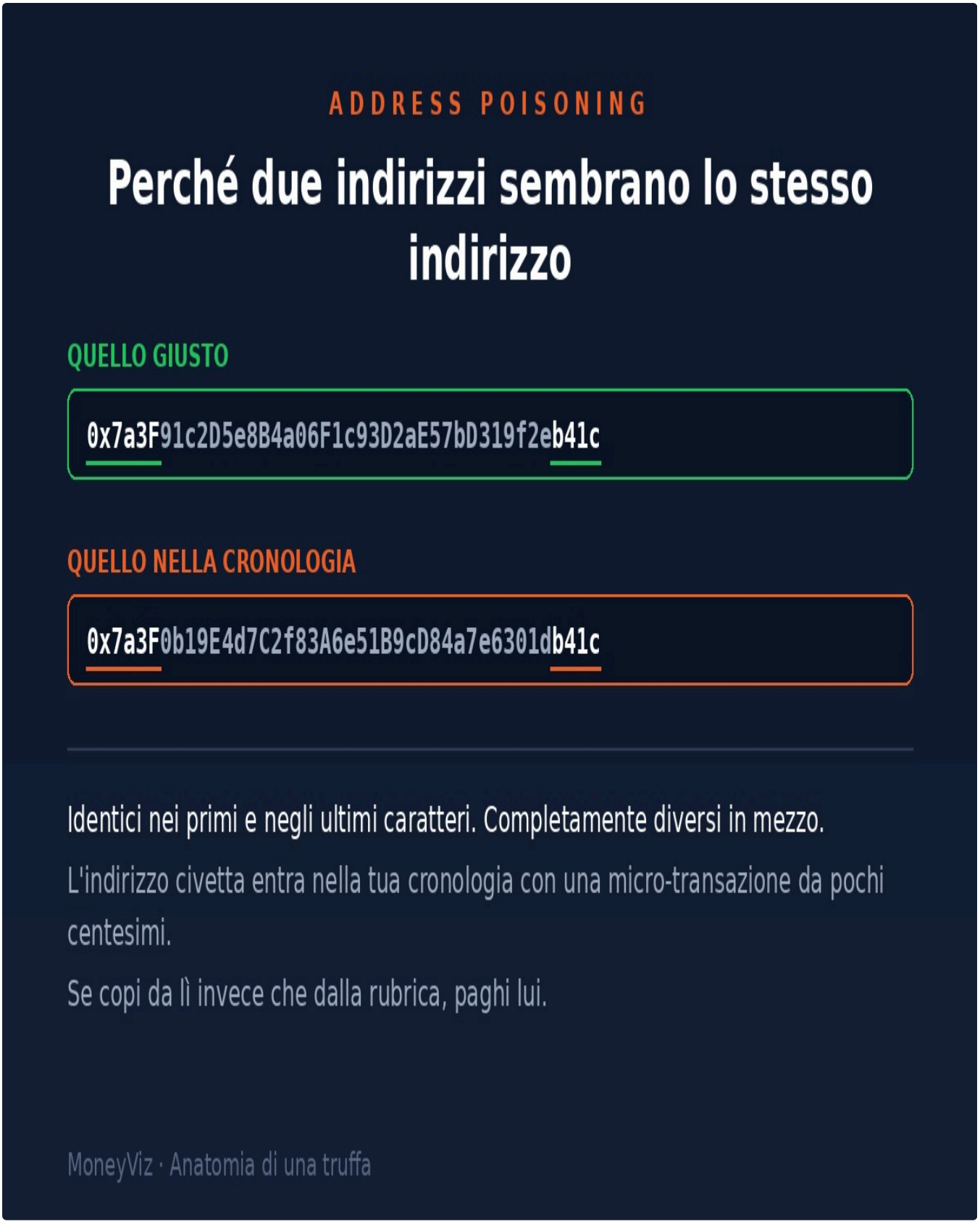
A dicembre 2025 una persona ha perso **50 milioni di dollari** facendo una cosa che probabilmente hai fatto anche tu: copiare un indirizzo dalla cronologia delle transazioni.

Nessun programma sofisticato. Nessun difetto nel suo portafoglio. Solo un indirizzo che somigliava a quello giusto nelle prime e nelle ultime cifre, e uno sguardo dato di fretta. Tieni a mente le due righe che si somigliavano, perché ci

serviranno ancora.

Il punto è tutto qui, ed è la tesi di questa rubrica: **non vieni ingannato quando non sai niente, vieni ingannato quando l'attacco sembra normale abbastanza a lungo.** L'ingenuità non c'entra. Quella persona sapeva benissimo come si invia una transazione: è proprio per questo che l'ha inviata senza guardarla.

Da oggi apriamo una rubrica dedicata: **Anatomia di una truffa**. Una puntata per ogni tipo di attacco, sempre con lo stesso schema — come funziona, i segnali, come ti difendi, che cosa fare se è già successo. In **MoneyViz** passiamo le giornate dentro gli storici di chi queste cose le ha subite, e la parte difficile del lavoro raramente è tecnica: è spiegare a una persona informata come sia potuto succedere proprio a lei.



I due indirizzi della storia: uguali dove guardi, diversi dove non guardi. Elaborazione MoneyViz.

Perché una rubrica sulla sicurezza, e perché adesso?

Perché il tipo di attacco che colpisce le persone comuni è cambiato. Secondo il rapporto annuale di Chainalysis, nel 2025 le truffe in criptovalute hanno raccolto **almeno 17 miliardi di dollari**. Il dato che conta però non è il totale, è la composizione: le impersonificazioni sono cresciute del **1400 per cento** in un anno, e l'importo medio di ogni pagamento verso un truffatore è passato da 782 a 2.764 dollari. In Italia il fenomeno arriva soprattutto come false piattaforme di investimento: la Polizia di Stato ne ha oscurate **473** in una sola operazione, molte promosse con video creati artificialmente. Si comincia con 250 euro, la piattaforma mostra guadagni che non esistono, e la richiesta cresce.

> **CHE COSA VUOL DIRE IMPERSONIFICAZIONE**
>
> È un attacco in cui qualcuno finge di essere un soggetto di cui ti fidi già: l'assistenza della piattaforma dove tieni i tuoi soldi, il supporto del portafoglio, l'amministratore di un gruppo, perfino un ente pubblico. Non richiede alcuna competenza tecnica: soltanto che tu creda alla prima frase. È il tipo di attacco che cresce più in fretta di tutti.

Le truffe in criptovalute del 2025 in quattro numeri. Fonte: elaborazione MoneyViz su dati Chainalysis e Scam Sniffer, 2026.

Perché “stare attenti” non basta?

Perché l’attenzione si consuma, le abitudini no. Il caso più istruttivo del 2025 non riguarda un utente distratto: a febbraio la piattaforma Bybit ha perso circa 401.000 ether, attorno a un miliardo e mezzo di dollari, perché l’interfaccia usata per approvare l’operazione era stata manomessa. Chi firmava vedeva un’operazione ordinaria e stava autorizzando tutt’altro.

Se succede a professionisti con portafogli protetti da più firme, l’idea che basti “essere svegli” non sta in piedi. Quello che sta in piedi sono abitudini che reggono anche quando non sei lucido: quando hai fretta, quando un’operazione non va a buon fine, quando qualcuno ti scrive che il tuo conto è a rischio.

> **PERCHÉ UNA FIRMA NON È UN CLIC**
>
> Quando approvi una firma nel tuo portafoglio non stai confermando genericamente. Puoi star concedendo a un programma il permesso di spendere i tuoi token, anche in futuro e anche senza limite di importo. Nel 2025 le firme del tipo *Permit* sono state lo strumento più sfruttato in assoluto, e un permesso concesso oggi può restare fermo per mesi prima di essere usato. Per questo revocare le autorizzazioni vecchie è manutenzione ordinaria, non paranoia.

Quali attacchi vedremo, uno per puntata?

Nove tipologie, ognuna con la sua puntata. Tieni da parte questa mappa: nella maggior parte dei casi, per sapere che cosa fare, basta riconoscere in quale riga ti trovi.

ATTACCO	DA DOVE TI ARRIVA	LA DIFESA IN UNA RIGA
Finto supporto	Un aiuto non richiesto, pochi minuti dopo che hai scritto in pubblico di un problema	Nessuna assistenza vera ti contatta per prima
Phishing	Sito clone, applicazione o estensione fasulla, risultato sponsorizzato nei motori di ricerca	Solo segnalibri salvati da te, mai link ricevuti
Frase di recupero esposta	Fotografie, copie nel cloud, note sul telefono, finte pagine di ripristino	La *seed phrase* sta offline e non si digita mai online
Password deboli e secondo fattore aggirato	Credenziali riusate, archivi di password rubate, duplicazione della SIM	Password uniche e codici da app o chiave fisica, mai via SMS
Address poisoning	Una micro-transazione che lascia in cronologia un indirizzo somigliante al tuo	Mai copiare un indirizzo dalla cronologia
Approval phishing	Finto premio, finta migrazione, finto riscatto che ti fa firmare un permesso	Non firmare quello che non capisci, revoca i permessi vecchi
Sandwich attack	Il tuo scambio in attesa, visibile pubblicamente prima di essere eseguito	Tolleranza di prezzo stretta e mercati con scambi profondi
Rug pull	Un progetto che esplode in poche ore e sparisce con i soldi raccolti	Squadra verificabile, fondi vincolati, distribuzione dei token
Honeypot	Un token che puoi comprare ma che non riesci più a vendere	Codice pubblicato e verificato prima dell’acquisto

I nove attacchi che analizzeremo, uno per puntata

Per capire quanto pesano: sul solo address poisoning, due vittime hanno perso 50 milioni e 12,25 milioni di dollari, entrambe copiando un indirizzo dalla cronologia.

Che cosa hanno in comune tutti questi attacchi?

Tre leve, sempre le stesse. La prima è **la fretta**: quasi ogni truffa contiene una scadenza inventata. Se un messaggio ti spinge ad agire in fretta, quella fretta è già parte dell'attacco.

La seconda è **la somiglianza**: un dominio con una lettera diversa, un profilo con lo stesso avatar, un indirizzo identico nelle prime quattro e nelle ultime quattro cifre. Sono le due righe che si somigliavano da cui siamo partiti.

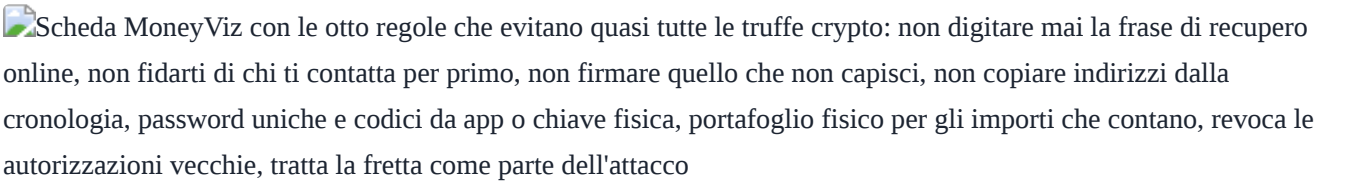
La terza è **la fiducia**, e non è un difetto tuo: chiedere aiuto quando qualcosa non funziona è normale, ed è esattamente il momento in cui i truffatori si presentano. La regola non è "non fidarti di nessuno", ma "sei tu che apri il canale, non chi ti scrive".

Le tre leve che ritroverai in ogni puntata della rubrica. Elaborazione MoneyViz.

Quali sono le otto regole che ti evitano quasi tutte le truffe?

Otto, e nessuna richiede competenze tecniche. Prima ancora del dettaglio dei singoli attacchi, riducono il rischio in quasi tutti gli scenari che vedremo.

1. **Non digitare mai la frase di recupero online.** Nessun servizio legittimo ne ha bisogno: se qualcuno la chiede, la conversazione finisce lì.
2. **Non fidarti di chi ti contatta per primo.** Nell'aiuto non richiesto sta la trappola più antica del settore.
3. **Non firmare quello che non capisci.** Se la richiesta non corrisponde a quello che volevi fare, non firmare.
4. **Non copiare mai indirizzi dalla cronologia.** Somigliante non vuol dire uguale.
5. **Password uniche e secondo fattore robusto.** Gestore di password e applicazione di autenticazione, o meglio una chiave fisica, al posto degli SMS.
6. **Un portafoglio fisico per gli importi che contano.** Per cifre significative è la scelta di partenza, non un optional.
7. **Rivedi e revoca le autorizzazioni.** Un permesso vecchio è comunque un permesso attivo.
8. **Tratta l'urgenza come un segnale d'allarme.** Chi ti mette fretta ha un motivo, e non è il tuo interesse.

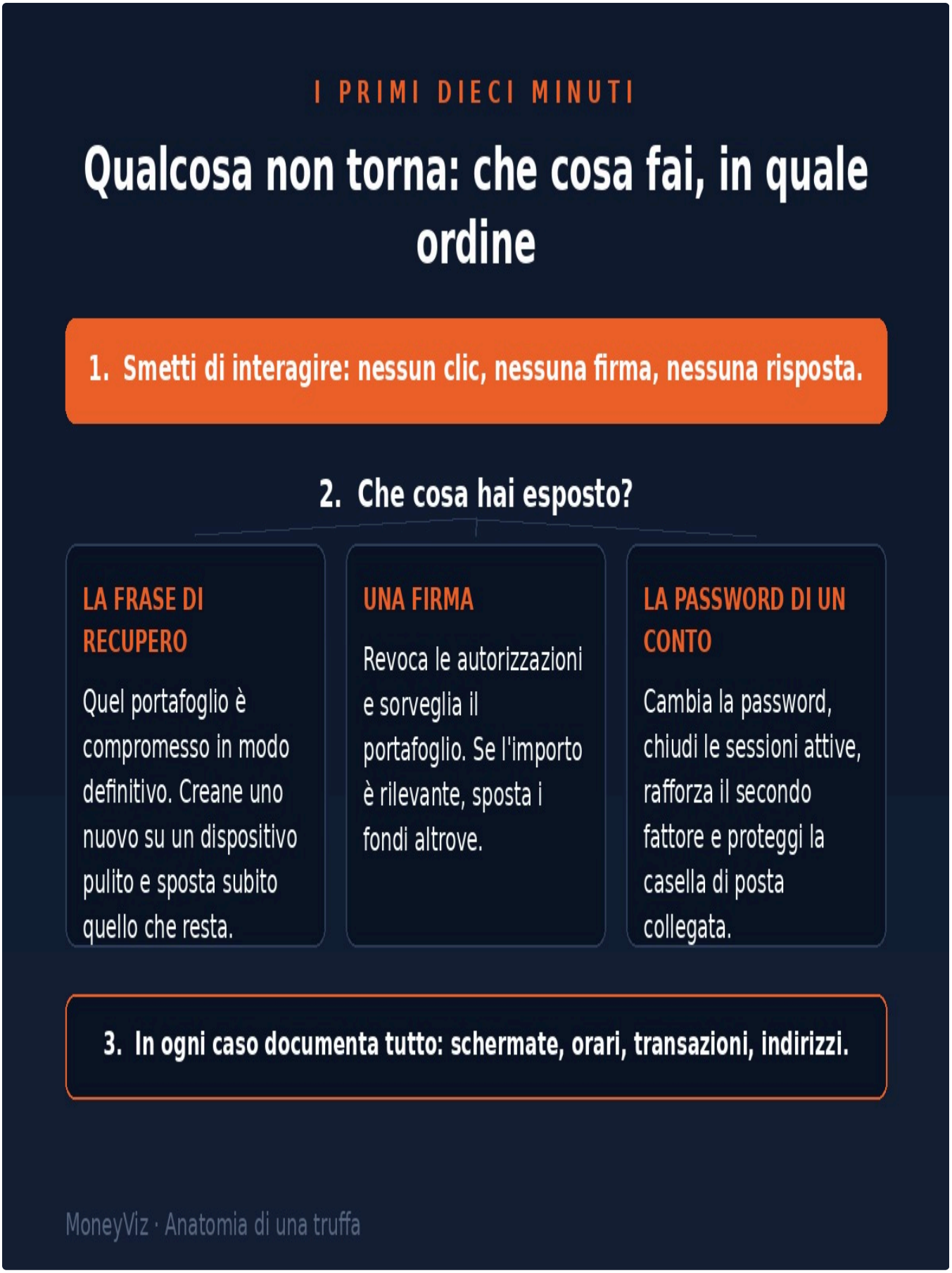

Scheda MoneyViz con le otto regole che evitano quasi tutte le truffe crypto: non digitare mai la frase di recupero online, non fidarti di chi ti contatta per primo, non firmare quello che non capisci, non copiare indirizzi dalla cronologia, password uniche e codici da app o chiave fisica, portafoglio fisico per gli importi che contano, revoca le autorizzazioni vecchie, tratta la fretta come parte dell'attacco

Le otto regole in una scheda sola. Scaricala, stampala e ritagliala lungo il bordo tratteggiato: sta accanto al computer o dentro il portafoglio vero.

Che cosa fai nei primi dieci minuti se qualcosa non torna?

La velocità conta, ma solo se ti muovi nell'ordine giusto. Questa è la sequenza generale; nelle puntate la adatteremo a ogni attacco.

1. **Smetti di interagire.** Nessun altro clic, nessun'altra firma, nessuna risposta.
2. **Capisci che cosa hai esposto.** Una password, la frase di recupero o una firma: sono tre scenari con tre risposte diverse.
3. **Frase di recupero esposta:** quel portafoglio è compromesso in modo definitivo. Creane uno nuovo su un dispositivo pulito e sposta subito quello che resta.
4. **Firma sospetta:** revoca le autorizzazioni e sorveglia il portafoglio; se l'importo è rilevante, sposta i fondi altrove.
5. **Conto su una piattaforma:** cambia la password, chiudi le sessioni attive, rafforza il secondo fattore e proteggi la casella di posta collegata.
6. **Documenta tutto.** Schermate, orari, identificativi delle transazioni, indirizzi: servono per la denuncia e per ricostruire la posizione.



La sequenza dei primi dieci minuti, in un colpo d'occhio. Elaborazione MoneyViz.

E se la truffa è già successa, che cosa resta da fare?

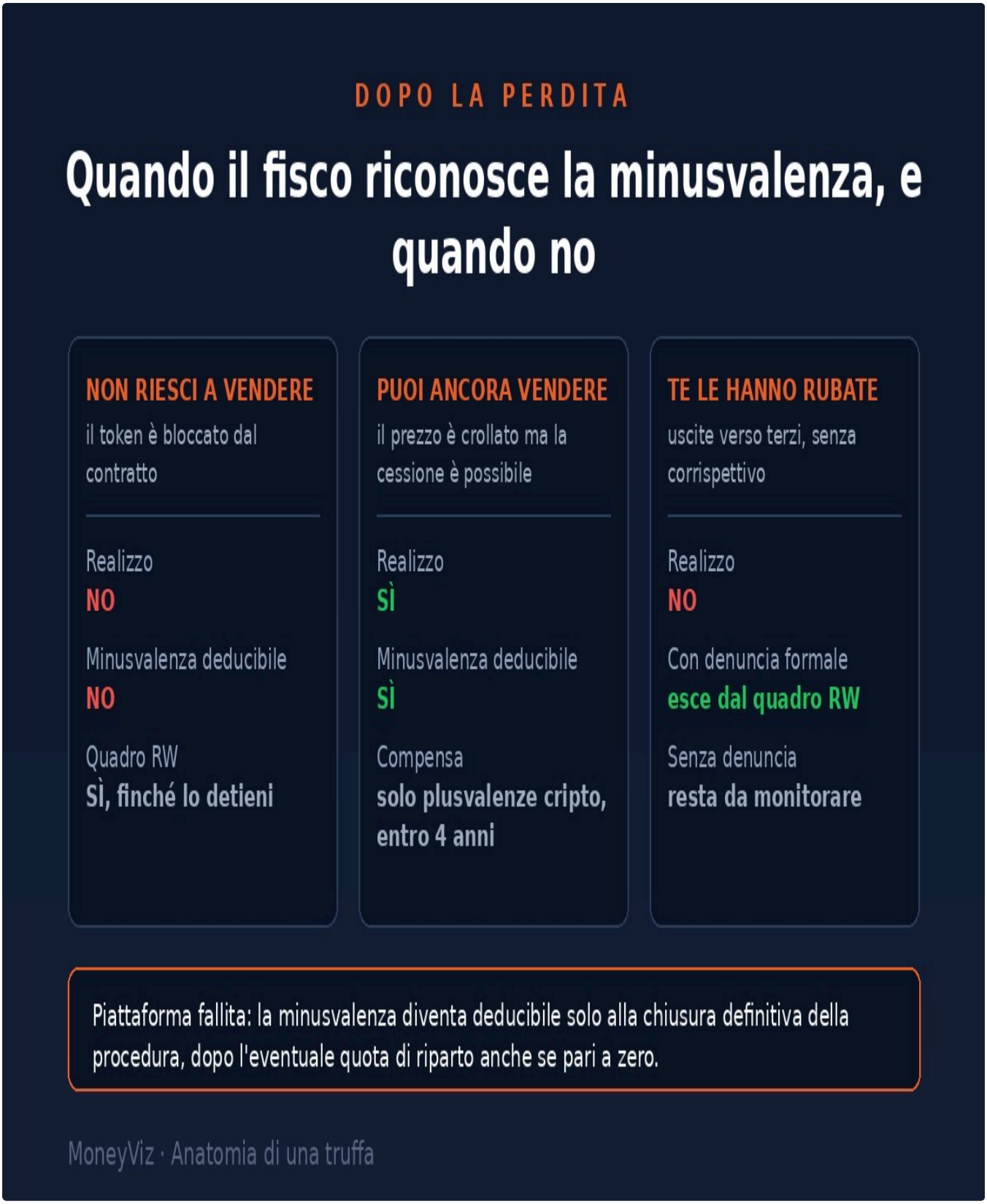
Prima la denuncia, poi la ricostruzione, e diffidenza assoluta verso chi promette di recuperare i soldi. I trasferimenti su un registro pubblico sono di norma irreversibili: nella maggior parte dei casi i fondi non tornano indietro, e chi garantisce il contrario in cambio di un pagamento anticipato sta costruendo una seconda truffa sopra la prima. Solo negli Stati Uniti, nel 2025, le truffe del finto recupero hanno prodotto oltre **1,4 miliardi di dollari** di danni. La denuncia va presentata alla Polizia Postale con ogni evidenza raccolta.

E dal punto di vista fiscale, che cosa succede alla perdita?

La perdita peggiore è spesso quella che non puoi nemmeno dedurre. In Italia una minusvalenza su cripto-attività esiste, ai fini fiscali, solo a fronte di una cessione a titolo oneroso, di una permuta o di un rimborso: in una parola, di un realizzo. Finché tieni il token in perdita senza venderlo, la perdita resta latente e per il fisco non c'è. L'honeypot è il caso limite: compri un token, il prezzo va a zero e il contratto ti impedisce di venderlo. Non hai ceduto nulla, quindi non hai una perdita fiscalmente rilevante: hai una cripto-attività che vale zero e che, finché la detieni, continua a rientrare negli obblighi di monitoraggio del quadro RW.

All'estremo opposto, se il token è ancora vendibile a un prezzo non nullo, la cessione esiste: la minusvalenza è realizzata e compensa — solo dentro il comparto delle cripto-attività — le plusvalenze dei quattro periodi d'imposta successivi. Il furto puro invece non è un realizzo: le cripto escono verso un indirizzo di terzi senza corrispettivo, quindi non nasce né una plusvalenza tassabile né una minusvalenza automaticamente deducibile. Qui conta la denuncia: con una denuncia formale quel token esce dal quadro RW, senza denuncia resta formalmente tuo e va comunque monitorato.

È qui il classico cornuto e mazziato: la perdita è reale, ma per il fisco conta solo se viene realizzata, e finché quel token resta nel portafoglio va comunque monitorato nel quadro RW senza dare diritto ad alcuna deduzione. Con una piattaforma fallita la minusvalenza diventa deducibile solo alla chiusura definitiva della procedura, dopo l'eventuale quota di riparto anche se pari a zero.



Le tre situazioni a confronto: quando la perdita conta per il fisco e quando no. Elaborazione MoneyViz.

> **UNA TRUFFA LASCIA TRACCE ANCHE IN DICHIARAZIONE**
>
> Un portafoglio svuotato, una firma che ha spostato token verso un indirizzo sconosciuto, un token comprato e mai più vendibile restano tutti nel tuo storico, e qualcuno dovrà spiegarli. È la parte che vediamo più spesso: non la truffa in sé, ma i mesi dopo, quando bisogna rimettere in ordine le operazioni di dieci piattaforme diverse e capire quali movimenti sono tuoi e quali no. Con **MoneyViz** ogni riga resta tracciabile fino alla singola transazione che l'ha generata. Per la parte fiscale: la guida al quadro RW e come si compila il quadro RT.

Da dove cominciamo?

Dal finto supporto, l'attacco cresciuto più in fretta nell'ultimo anno e quello che intercetta le persone nel momento peggiore: quando hanno già un problema e stanno cercando aiuto. Poi seguiremo l'ordine della tabella.

Torniamo alle due righe che si somigliavano. Per portare via cinquanta milioni non è servito violare niente: è bastato che, per due secondi, un indirizzo sbagliato sembrasse quello giusto. La sicurezza non è una cosa che si sa, è una cosa che si fa — ogni volta, soprattutto quando sembra superfluo.

> **LE PUNTATE DI ANATOMIA DI UNA TRUFFA**
>
> 1. **Come difenderti dagli attacchi crypto** — questa puntata
> 2. Il finto supporto — in arrivo
> 3. Phishing: siti, applicazioni ed estensioni clone — in arrivo
> 4. La frase di recupero esposta — in arrivo
> 5. Password deboli e secondo fattore aggirato — in arrivo
> 6. Address poisoning — in arrivo
> 7. Approval phishing — in arrivo
> 8. Sandwich attack — in arrivo
> 9. Rug pull — in arrivo
> 10. Honeypot — in arrivo
>
> Ogni puntata è raccolta sotto il tag **anatomia-di-una-truffa**. Questa la puoi anche scaricare in PDF, insieme alla scheda delle otto regole.

Fonti

- Chainalysis — Crypto Crime Report 2026, capitolo sulle truffe (dati 2025)
- Chainalysis — Crypto Crime Report 2026, rapporto completo
- Scam Sniffer — rapporto annuale 2025 su phishing e svuotamento dei portafogli
- FBI — Internet Crime Report 2025, dati sulle denunce e sulle truffe del finto recupero (PDF)
- Ministero dell'Interno — 473 siti di false piattaforme di trading oscurati
- Polizia Postale — che cosa fare in caso di truffa da trading online
- NCC Group — analisi tecnica dell'attacco a Bybit del febbraio 2025

- Halborn — ricostruzione dell’attacco a Bybit e del ruolo della firma cieca
- Coinbase — come riconoscere le finte telefonate dell’assistenza
- Consob — sezione di educazione finanziaria sulle truffe
- MoneyViz — quadro RW crypto 2026: guida completa alla compilazione
- MoneyViz — come compilare il quadro RT crypto 2026

Domande frequenti

Che cos’è la rubrica Anatomia di una truffa?

È la rubrica di MoneyViz dedicata alla sicurezza delle criptovalute. Ogni puntata analizza un singolo tipo di attacco — dal finto supporto all’address poisoning — con lo stesso schema fisso: come funziona, da dove ti arriva, quali sono i segnali di allarme, come ti difendi e che cosa fare se è già successo. Le puntate previste sono nove, più questo articolo di apertura.

Qual è l’errore più comune che porta a perdere criptovalute?

Conservare la frase di recupero del portafoglio in un posto raggiungibile da internet: fotografie, copie nel cloud, note sul telefono, file di testo. Non serve alcun attacco sofisticato per sfruttarlo, ed è la causa di una quota molto rilevante delle perdite definitive. La frase di recupero va tenuta offline e non va mai digitata online, per nessun motivo.

L’assistenza di una piattaforma può chiedermi la frase di recupero?

Mai, in nessuna circostanza. Nessun servizio legittimo ha bisogno della tua frase di recupero per assisterti. Qualunque richiesta in tal senso è una truffa, indipendentemente da quanto il profilo, il logo o il tono del messaggio sembrino credibili. Vale la stessa regola per le chiavi private e per i codici del secondo fattore.

Se ho firmato un’autorizzazione sospetta, i fondi spariscono subito?

Non necessariamente, ed è proprio questo che rende insidioso l’approval phishing. Un’autorizzazione concessa può restare inattiva per settimane o mesi prima di essere sfruttata. Per questo conviene revocare con regolarità i permessi non più necessari, senza aspettare che accada qualcosa: nel 2025 le firme del tipo Permit sono state lo strumento più usato in assoluto.

Posso recuperare le criptovalute inviate a un indirizzo sbagliato?

I trasferimenti su blockchain sono di norma irreversibili, quindi nella maggior parte dei casi no. Conserva ogni evidenza, verifica dove sono finiti i fondi e presenta denuncia alla Polizia Postale. Diffida di chi promette il recupero dietro pagamento anticipato: solo negli Stati Uniti, nel 2025, le truffe del finto recupero hanno prodotto oltre 1,4 miliardi di dollari di danni.

Un portafoglio fisico mi mette al sicuro da tutto?

Protegge molto bene le chiavi private dal furto, ma non ti protegge da una firma che autorizzi tu. L’attacco a Bybit del febbraio 2025 lo dimostra: i fondi erano su portafogli protetti da più firme, e l’operazione è stata comunque approvata perché chi firmava non vedeva il contenuto reale. Il dispositivo aiuta, l’abitudine di verificare resta indispensabile.