22 SETTEMBRE 2026 • 13 MIN DI LETTURA • DANILO GIUDICE

ANATOMIA DI UNA TRUFFA · PUNTATA 2

Finto supporto crypto: come riconoscere chi finge di aiutarti

Il finto supporto non ti prende quando sei distratto: ti prende quando hai già un problema e stai cercando aiuto. Come funziona, i segnali per riconoscerlo e che cosa fare se ci hai già parlato.

PERCHÉ TI RIGUARDA

- Il finto supporto non ti prende quando sei distratto: ti prende **nel momento in cui stai già cercando aiuto**
- Nel 2025 le denunce per finta assistenza arrivate all'FBI sono state **47.794**, per oltre **2,1 miliardi di dollari** di danni
- Chi ti risponde può già sapere il tuo nome e dove hai il conto: quei dati **si comprano**

Scrivi in pubblico che il prelievo è fermo da due giorni. Trenta secondi dopo qualcuno ti risponde. Ha il logo giusto, il tono gentile, la parola «assistenza» nel nome. Tieni a mente quel numero: alla fine dell'articolo ti dirà da solo con chi stavi parlando.

Le difese, in quattro mosse

- **Il canale lo apri tu**: se ti contattano, chiudi e riapri dall'app o dal sito ufficiale
- **Non dettare a nessuno la frase di recupero** o un codice ricevuto: l'assistenza vera non li chiede
- **Prima di firmare o pagare, fermati e verifica altrove**: due minuti, e il dubbio è chiuso
- **Un numero conosciuto sul display non prova niente**: riattacca e richiama tu dal numero che hai salvato

Più sotto: perché funziona anche su chi queste regole le conosce, i segnali che si vedono a mente fredda e che cosa fare se ci hai già parlato.

Questa è la seconda puntata di Anatomia di una truffa, la rubrica di sicurezza di **MoneyViz**. Nella prima abbiamo mappato i nove attacchi che svuotano i portafogli; da qui in avanti ne prendiamo uno per volta. Cominciamo da questo perché è l'unico che non deve inventarsi un pretesto per raggiungerti.

Le altre truffe devono costruirsi un motivo per scriverti: un premio, una scadenza, un conto a rischio. Questa no. Il motivo glielo hai dato tu, in pubblico, ed è un motivo vero. Non ti intercetta mentre sei distratto. Ti intercetta mentre chiedi aiuto.

Perché il finto supporto arriva proprio quando chiedi aiuto?

Perché chi lo pratica non cerca vittime: cerca persone che hanno appena dichiarato di averne bisogno. Ha un nome tecnico, *angler phishing*, e descrive esattamente il gesto: si pesca dove i pesci si sono già radunati.

Il meccanismo è banale e per questo funziona. I messaggi pubblici su una piattaforma sono leggibili da chiunque, comprese le macchine. Un programma che sorveglia parole come «prelievo bloccato», «non riesco ad accedere», «transazione in sospeso» costa poco e non dorme mai. Quando il tuo messaggio compare, la risposta parte prima che tu abbia finito di rileggerlo.

La sequenza è sempre la stessa, e il primo passo lo fai tu senza saperlo. Elaborazione MoneyViz.

La velocità, che sul momento sembra la prova che hai trovato brave persone, è in realtà il primo segnale. Nessuna assistenza vera risponde in trenta secondi a un messaggio pubblico. Ha una coda, ha dei turni, ha un sistema di richieste: ci mette ore, a volte giorni, e quando risponde lo fa dentro il canale che hai aperto tu.

C'è però una ragione più scomoda per cui quella velocità non ti insospettisce: ti fa stare meglio. Quando aspetti una soluzione, una risposta immediata dà sollievo — finalmente qualcuno ti ascolta. E il sollievo ti porta a cercare conferme che la persona sia affidabile, invece delle incongruenze: è il *bias di conferma*, dai più peso a ciò che sostiene quello che speri sia vero. Sapere che sta succedendo è già metà della difesa, perché la rapidità non dimostra chi ti sta rispondendo. Non dimostra niente.

Da dove ti arriva?

Da qualunque canale in cui qualcuno può parlarti per primo. Cambia la superficie, non il copione:

- **La risposta pubblica** sotto il tuo messaggio, da un profilo che ha il logo, il nome quasi giusto e qualche migliaio di follower comprati
- **Il messaggio privato** che arriva subito dopo, «così non intasiamo il thread»
- **Il gruppo di assistenza** su una chat, dove chi ti scrive ha il badge di amministratore che si è messo da solo
- **La telefonata**, con un numero che sul display sembra quello della tua banca o della piattaforma
- **Il risultato sponsorizzato** in cima ai motori di ricerca quando cerchi «assistenza» insieme al nome del servizio

- **Il finto numero verde** pubblicato su una pagina costruita apposta per essere trovata da chi ha fretta

In Italia la versione telefonica è talmente diffusa che la Polizia Postale le ha dedicato avvisi ripetuti. Il meccanismo è sempre lo stesso: centralini che permettono di «clonare» il numero che compare sul display. Chi chiama si presenta come operatore della banca o delle Poste, e la richiesta è sempre la stessa: spostare i soldi su un conto «sicuro». Nella variante più sfacciata si spacciano per la Polizia Postale stessa, usando i numeri veri delle questure.

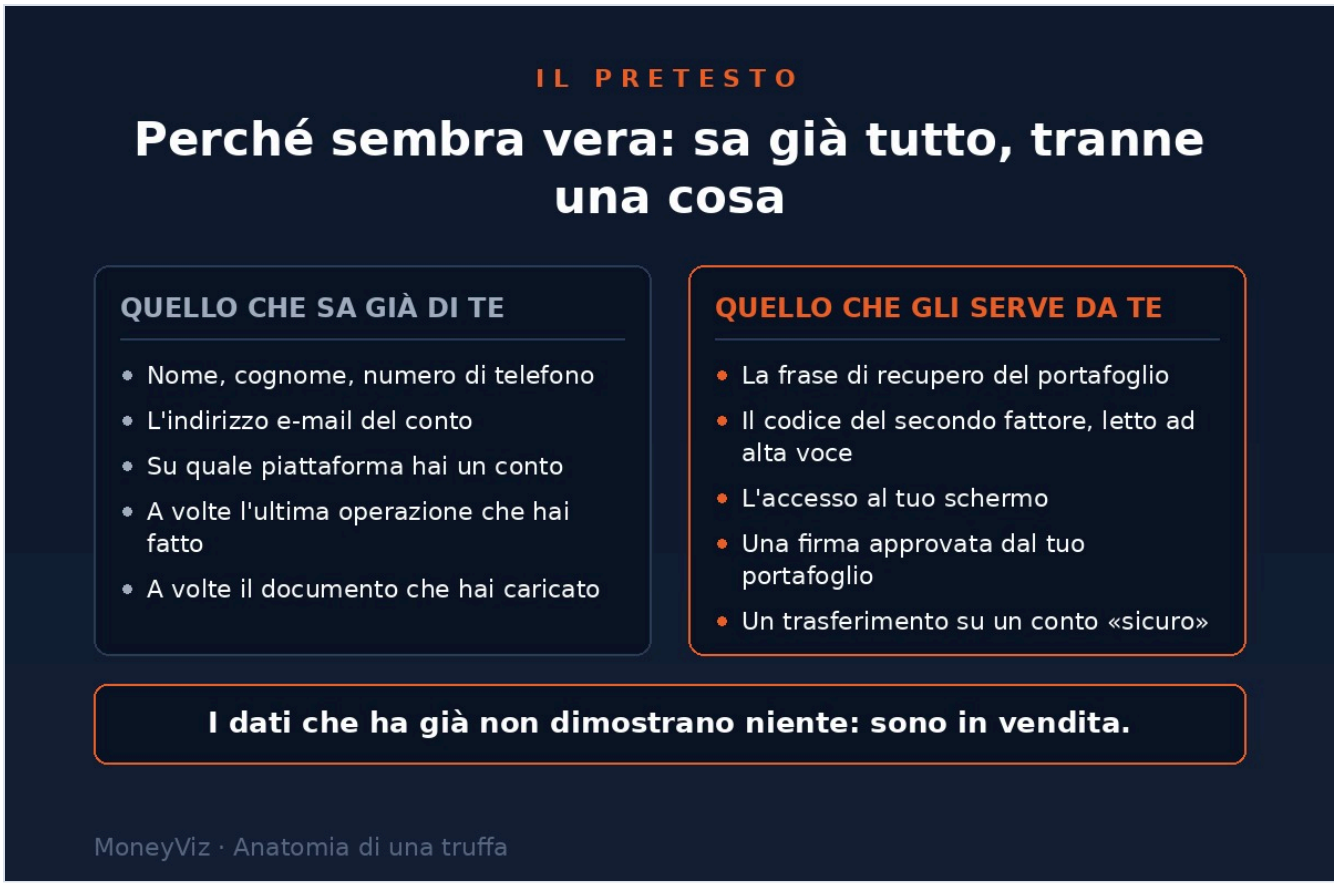
> **Il numero sul display non è una prova**
>
> La tecnica si chiama *spoofing* del chiamante: chi chiama decide quale numero far comparire sul tuo telefono, e può scegliere quello stampato sul retro della tua carta. Funziona perché la rete telefonica non è stata progettata per verificare chi chiama, allo stesso modo in cui la posta elettronica non verifica il mittente. Un numero conosciuto, da solo, non dimostra nulla: è solo un'etichetta che il chiamante ha scelto.

Perché chi ti contatta sa già tutto di te?

Perché i tuoi dati non li ha indovinati: li ha comprati. È la parte che nel racconto delle vittime torna sempre, ed è quella che spinge ad abbassare la guardia: «sapeva il mio nome, sapeva che avevo un conto lì, sapeva persino l'ultima operazione».

Nel maggio 2025 Coinbase ha comunicato alle autorità di mercato di aver subito un furto di dati: non un'intrusione nei sistemi, ma alcuni operatori dell'assistenza in outsourcing pagati per estrarre le informazioni dei clienti. Sono finiti fuori nomi, recapiti, indirizzi e storici delle operazioni di meno dell'1% degli utenti attivi, circa 69.000 persone. Nessuna password, nessuna chiave privata, nessun fondo toccato direttamente. Eppure la richiesta di riscatto, 20 milioni di dollari, è stata rifiutata. Il conto della vicenda, invece, la società stessa lo ha stimato tra i 180 e i 400 milioni di dollari, tra rimedi e rimborsi.

Quei dati non servivano ad accedere ai conti. Servivano a far sì che, al telefono, le prime tre frasi fossero tutte vere: il tuo nome, la piattaforma su cui hai il conto, l'ultima operazione che hai fatto. Dopo tre frasi vere, la quarta la ascolti.



Tutto quello che sa lo può avere comprato. Tutto quello che chiede, invece, può darglielo solo tu. Elaborazione MoneyViz.

I dati che ha già non dimostrano niente

Nome, e-mail, numero di telefono e perfino l'ultima operazione possono essere stati comprati. Non sono una credenziale: sono un biglietto da visita che chiunque può stampare. L'unica cosa che conta, in quella conversazione, è che cosa ti sta chiedendo di fare.

Quali sono i segnali che stai parlando con il finto supporto?

Il primo e più affidabile: il contatto è partito da lui. Gli altri li riconosci a mente fredda, questo lo riconosci subito.

Sei segnali che convivono nello stesso messaggio: chi ha aperto il contatto, il nome quasi giusto, la spunta disegnata, lo spostamento in privato, la scadenza inventata e la richiesta finale. Elaborazione MoneyViz.

- **Ti ha scritto o chiamato per primo.** L’assistenza vera risponde, non cerca
- **Ti sposta subito altrove**: dal thread pubblico al messaggio privato, dalla chat alla telefonata, dalla telefonata alla condivisione dello schermo
- **Ha fretta, e te la passa**: il conto verrà sospeso, la finestra è di ventiquattr’ore, bisogna intervenire adesso
- **Ti manda un «modulo di verifica»** o una pagina di ripristino dove si digita la frase di recupero. Nessun modulo legittimo la chiede
- **Ti chiede di leggere ad alta voce un codice** ricevuto via SMS o dall’app: quel codice sta autorizzando un’operazione mentre parlate

- **Ti propone di spostare i fondi su un conto «sicuro»**, che è semplicemente il suo
- **Il dominio è quasi giusto**: una parola in più, un trattino, un'estensione diversa da quella che usi da sempre

Non sempre la richiesta pericolosa arriva subito. Prima ti chiedono di descrivere il problema, poi di aprire una pagina, infine di autorizzare un'operazione: è la tecnica del *piede nella porta*, una sequenza di piccoli sì che prepara quello impegnativo. Nel frattempo hai investito tempo e vuoi arrivare alla soluzione, e fermarti può sembrarti uno spreco. Non lo è: aver seguito le prime istruzioni non ti obbliga a seguire la successiva. Puoi interrompere in qualsiasi momento, anche a metà, anche dopo aver detto sì tre volte.

C'è un motivo per cui tutti questi segnali convivono nello stesso copione: il tempo. Chi conduce la conversazione sa che se ti lascia riflettere, verifichi. Quindi non te lo lascia. I trenta secondi dell'inizio non erano premura: erano l'inizio di un conto alla rovescia. Da lì in poi, ogni cosa che ti chiede serve a non farti fermare.

Che cosa non fa mai l'assistenza vera?

Non ti scrive per prima, non ti chiede le chiavi e non ti mette fretta. Non è una buona pratica che qualcuno ogni tanto disattende: è scritto nero su bianco dalle piattaforme stesse.

MetaMask, per esempio, mette in fila tutte le negazioni sul proprio sito di assistenza: «non abbiamo un numero di telefono, non parleremo mai con te al telefono», «non ti scriveremo mai in privato per offrirti supporto», «non ti chiederemo mai la tua frase di recupero». Coinbase, dopo l'ondata di telefonate del 2025, ha pubblicato un promemoria ancora più diretto per i propri clienti: riattacca. E la Polizia Postale, sul versante bancario, ripete la stessa cosa da anni: non si comunicano a nessuno, né al telefono né via e-mail, password, PIN o codici di accesso.

	ASSISTENZA VERA	FINTO SUPPORTO
Chi apre il contatto	Tu, dall'app o dal sito ufficiale	Lui, subito dopo un tuo messaggio pubblico
Dove si parla	Dentro la richiesta che hai aperto tu	In privato, in un gruppo, al telefono
Che cosa chiede	Dati dell'operazione: data, importo, identificativo	Frase di recupero, codici, accesso allo schermo
Quanto tempo ti dà	Quello che serve, anche giorni	Pochi minuti, con una scadenza inventata
Come si verifica	Richiudi tutto e riapri dal canale ufficiale: la trovi lì	Se richiudi e riapri dal canale ufficiale, sparisce

Cinque differenze che si notano prima di aver perso qualcosa

L’ultima riga è la più utile, perché è l’unica che puoi usare senza saper riconoscere niente: chiudere e riaprire dal canale ufficiale costa due minuti e distingue i due casi in modo definitivo. Due minuti contro i trenta secondi che sono bastati dall’altra parte: è l’unico scambio di tempo che conviene a te.

Come ti difendi, in pratica?

Con una regola che non ha eccezioni: il canale lo apri tu. Tutto il resto discende da qui.

La stessa regola, nelle tre situazioni in cui serve davvero. Elaborazione MoneyViz.

In pratica sono tre gesti, sempre gli stessi: chiudi quello che ti è arrivato, apri tu l’app o il sito che usi da sempre, e scrivi lì la tua richiesta. Se l’assistenza ti stava cercando davvero, la ritrovi in quel canale.

Intorno alla regola ci sono quattro abitudini che riducono la superficie esposta, e nessuna richiede competenze tecniche:

1. **Non raccontare il problema in chiaro.** Se devi chiedere aiuto in pubblico, evita di scrivere quale piattaforma, quale importo e quanto sei bloccato: è esattamente l’insieme di informazioni che seleziona i messaggi da colpire
2. **Salva i canali ufficiali una volta sola.** Il sito dell’assistenza nei segnalibri, l’app installata dallo store, il numero preso dal sito e non dal motore di ricerca. La prossima volta che hai fretta, li hai già
3. **Diffida dei risultati sponsorizzati.** Quando cerchi «assistenza» insieme al nome di un servizio, le prime posizioni sono spazi comprati, e si comprano anche da chi non è quel servizio
4. **Tieni separata la casella di posta del conto.** Un indirizzo che non usi per i forum e per gli acquisti è un indirizzo che finisce in meno elenchi

In **MoneyViz** queste storie le vediamo dal lato che nessuno racconta: mesi dopo, con davanti un elenco di movimenti da rimettere in ordine e una dichiarazione da chiudere. Tocca ricostruire che cosa è uscito, quando e verso dove. La sequenza è quasi sempre la stessa, e comincia da un messaggio di aiuto scritto in pubblico.

Mesi dopo, però, si sistemano i conti, non la perdita. Se la conversazione è ancora aperta adesso, il margine c'è.

Che cosa fai se ci stai parlando adesso?

Interrompi, e verifica da un'altra parte. Nell'ordine:

1. **Non completare l'operazione in corso.** Nessuna firma, nessun codice letto ad alta voce, nessun modulo compilato, nessuna schermata condivisa
2. **Chiudi la conversazione o riattacca.** Non serve spiegare, non serve essere gentili: una conversazione legittima sopravvive benissimo a una telefonata interrotta
3. **Apri tu il canale ufficiale** e chiedi se ti hanno contattato. È la verifica che chiude il caso in entrambi i sensi
4. **Se hai già condiviso lo schermo**, interrompi la condivisione, chiudi il programma con cui l'hai fatta e disinstallalo
5. **Documenta tutto**: schermate della conversazione, numero chiamante, orari, nomi dei profili. Serve alla denuncia e serve alla piattaforma per far chiudere l'account falso

E se hai già dato qualcosa, che cosa resta da fare?

Dipende da che cosa hai dato, e la differenza è netta. Una password si cambia, e il conto resta tuo. Una frase di recupero non si cambia: il portafoglio che protegge smette di essere solo tuo.

- **La frase di recupero.** Quel portafoglio è compromesso in modo definitivo, anche se adesso sembra intatto. Creane uno nuovo su un dispositivo pulito e sposta subito quello che resta: chi ha la frase può svuotarlo quando vuole
- **Una firma approvata.** Revoca le autorizzazioni concesse e sorveglia il portafoglio. Un permesso può restare fermo per settimane prima di essere usato — è il tema della settima puntata
- **La password o un codice del secondo fattore.** Cambia la password, chiudi tutte le sessioni attive, sostituisci il secondo fattore e proteggi la casella di posta collegata, che è la chiave di tutto il resto
- **Un trasferimento già partito.** Se è un bonifico, contatta subito la banca: entro poche ore a volte si blocca. Se sono criptovalute, l'operazione è irreversibile, e quello che resta da fare è conservare le prove

In ogni caso presenta denuncia. In Italia si fa alla Polizia Postale, anche dal portale del Commissariato di PS, allegando schermate, ricevute e orari. E diffida di chi, poco dopo, si offrirà di recuperare i fondi dietro pagamento anticipato: è la truffa successiva, e colpisce quasi solo chi ha già subito la prima.

Dal punto di vista fiscale, quella perdita conta?

Il furto non è una cessione, quindi non genera né plusvalenza né minusvalenza. Non c'è un corrispettivo, non c'è un realizzo: fiscalmente non è un'operazione. La conseguenza pratica riguarda il monitoraggio: con una denuncia formale il bene sottratto esce dal quadro RW, perché non lo detieni più; senza denuncia, formalmente, risulta ancora tuo.

> **Che cosa cambia in dichiarazione**
>
> Se invece hai venduto in perdita — non ti hanno rubato niente, hai solo ceduto a un prezzo più basso — la minusvalenza esiste e si può usare, ma dentro un recinto preciso: le minusvalenze su cripto-attività realizzate dal 2023 in poi riducono soltanto plusvalenze da cessione di altre cripto-attività, non quelle su azioni, ETF o altri strumenti finanziari, e si riportano nei quattro anni successivi, dopodiché scadono. Per le perdite più vecchie, fino al 2022, vale ancora la regola precedente, che le tiene insieme agli strumenti finanziari tradizionali. Monitoraggio e tassazione viaggiano poi su due binari distinti: il possesso si dichiara nel quadro RW, mentre plusvalenze e perdite da riportare stanno nel quadro RT, nella sezione dedicata alle cripto-attività. Nelle guide di **MoneyViz** trovi la compilazione passo per passo di entrambi.

Che cosa vediamo nella prossima puntata?

Il phishing: i siti clone, le applicazioni e le estensioni fasulle, i risultati sponsorizzati che portano su una copia perfetta della pagina che usi ogni giorno. È il seguito naturale di questa puntata, perché il finto supporto quasi sempre finisce lì: su un indirizzo che sembra quello giusto.

Torniamo ai trenta secondi dell'inizio. Non sono un dettaglio di colore, sono la diagnosi: l'unica assistenza che risponde in trenta secondi è quella che non esiste. Quando hai un problema e qualcuno arriva subito, la fretta che senti non è tua — è il suo strumento di lavoro.

Per questo la regola va decisa adesso, mentre non ti serve: se qualcuno mi contatta e mi chiede di agire sul conto o sul portafoglio, interrompo e verifico dal canale ufficiale. Una regola già pronta è più facile da seguire quando hai fretta, paura o semplicemente voglia di risolvere — cioè esattamente quando non sei nelle condizioni di deciderla.

Le puntate di Anatomia di una truffa

1. Come difenderti dagli attacchi crypto
2. **Il finto supporto** — questa puntata
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, per leggerla con calma o girarla a chi ti ha chiesto aiuto.

Fonti

- FBI — Internet Crime Report 2025: 47.794 denunce per finta assistenza e 2,13 miliardi di dollari di danni (PDF)
- FBI IC3 — archivio dei rapporti annuali sulle frodi online
- MetaMask — quali sono i canali ufficiali di assistenza e che cosa non chiedono mai
- Coinbase — riattacca: come riconoscere le finte telefonate dell'assistenza
- The Register — Coinbase conferma il furto di dati tramite operatori corrotti (maggio 2025)
- Halborn — ricostruzione tecnica dell'estorsione a Coinbase e dell'uso dei dati rubati
- Polizia di Stato — attenzione al vishing: le finte telefonate dell'operatore
- Polizia di Stato — truffe tramite spoofing del numero chiamante
- Polizia Postale — falsi operatori di banche o di Poste Italiane
- Questura di Milano — false telefonate a nome della Polizia Postale
- Scam Sniffer — rapporto annuale 2025 su phishing e svuotamento dei portafogli
- Chainalysis — Crypto Crime Report 2026, capitolo sulle truffe
- Consob — educazione finanziaria: come riconoscere le truffe
- MoneyViz — Anatomia di una truffa, puntata 1: i nove attacchi e le otto regole
- MoneyViz — quadro RW crypto 2026: guida completa alla compilazione