

26 OTTOBRE 2026 • 14 MIN DI LETTURA • DANILO GIUDICE

Phishing crypto: come riconoscere siti clone, app ed estensioni false

Le copie di oggi sono identiche all'originale, e nel caso più famoso l'indirizzo nella barra era perfino quello giusto. Da dove arrivano, perché i controlli che fai non bastano e la difesa che regge davvero. Puntata 4 di Anatomia di una truffa, la rubrica di sicurezza di MoneyViz.



PERCHÉ TI RIGUARDA

- Gli **episodi** di phishing censiti nel 2026 sono **più che dimezzati**, ma i soldi rubati sono scesi solo dell'11%: meno colpi, ognuno molto più grosso
- Nel primo semestre 2026 **quattro soli episodi** hanno fatto l'85% del bottino: non sei in mezzo a una folla, sei dentro un elenco — e da un elenco **si esce cambiando poche abitudini concrete**, non diventando esperto
- Il controllo che tutti consigliano — guardare l'indirizzo nella barra — è **quello che nel caso più famoso non ha salvato nessuno**
- La difesa che regge non è riconoscere il falso, è **non passare mai dal punto in cui te lo mostrano**
- È la quarta puntata di **Anatomia di una truffa**, la rubrica di sicurezza di **MoneyViz**

LA CHECKLIST, PRIMA DI TUTTO IL RESTO

Quattro gesti che puoi fare **oggi**, senza comprare niente e senza imparare niente di nuovo. Si fanno una volta e valgono da lì in avanti: da soli chiudono la maggior parte di questi attacchi.

1. **Metti nei segnalibri** i servizi dove tieni i soldi, e da domani aprili solo da lì: mai da una ricerca, mai da un link ricevuto.
2. **Fai l'inventario delle estensioni** del browser e togli quelle che non usi più: ogni estensione viva è una superficie viva.
3. **La frase di recupero si digita in un posto solo**: nella tua app o sul tuo dispositivo, quando sei *tu* a ripristinare un portafoglio. Mai dentro una pagina web, mai perché qualcuno te l'ha chiesta — e nessun servizio legittimo te la chiede.
4. **Le app si scaricano dallo store**, arrivandoci però dal sito ufficiale del produttore: guarda il nome di chi pubblica, non quello dell'app, che è la parte facile da copiare.

Se hai già cliccato, vai direttamente a che fare nei primi dieci minuti. E se non sai da dove cominciare o hai un dubbio su un movimento che non ti torna, **chiedi a noi**: è esattamente il tipo di domanda che l'assistenza di **MoneyViz** riceve tutti i giorni. La difesa completa — inclusa quella che regge anche quando il sito è una copia perfetta — la trovi più sotto.

Hai cercato su internet il nome del servizio che usi da anni, hai cliccato il primo risultato e hai fatto quello che fai sempre. Il rischio è che quel primo risultato fosse comprato, che la pagina fosse una copia e che le credenziali o la firma che hai dato siano già altrove. La difesa esiste e non richiede di diventare più bravo a riconoscere i falsi: **smetti di arrivare ai siti che contano passando da una ricerca**. Salvati una volta nei segnalibri e aprili solo da lì. È il gesto che annulla la maggior parte di questi attacchi, e costa trenta secondi oggi.

Il 24 aprile 2018, per circa due ore, chi apriva MyEtherWallet leggeva nella barra degli indirizzi *myetherwallet.com*. Era vero: il dominio era quello giusto. Il browser però segnalava un problema sul certificato, e molti sono andati avanti lo stesso. Tieni a mente quelle due ore: ci serviranno ancora, perché raccontano l'unica cosa che conta davvero di questa puntata.

In **MoneyViz** ricostruiamo storici di operazioni su decine di piattaforme, e il phishing è la categoria in cui il cliente arriva con la frase più difficile da smontare: “ma io ero sul sito giusto”. Spesso è vero. Il problema non è che non guardi: è che guardare, da solo, non basta più da un pezzo.

Questa puntata smonta il meccanismo: da dove arriva la copia che apri senza sospetti, perché le estensioni del browser sono il punto cieco più grande, che cosa non ti salva nonostante te lo consiglino tutti, e quali cinque abitudini chiudono il problema alla radice.

Perché il phishing è diventato l'attacco più redditizio?

Perché smonta la persona, non il codice. Un difetto in un programma si corregge e sparisce; la fiducia invece si ripresenta ogni giorno, uguale. Per questo il phishing è passato dal quinto posto per danni del 2023 — **203 milioni di dollari** su 55 episodi, secondo il rapporto annuale di CertiK — al primo del 2024, con **1,05 miliardi** su 296 episodi. Nel 2025 è rimasto il vettore con più episodi in assoluto: **248**, per 722,9 milioni.

Il dato che conta però è quello del **primo semestre 2026**, ed è controintuitivo. Gli episodi sono crollati del **52,3%**, da 132 a 63. Le perdite sono scese solo di circa l'**11%**, a 366,3 milioni di dollari. E **quattro soli episodi** hanno prodotto circa l'85% di quelle perdite.

Tradotto: la rete a strascico è stata ritirata. Al suo posto ci sono poche operazioni costruite su misura, che costano di più a chi le prepara e rendono molto di più. La mail scritta male rivolta a un milione di persone era un'epoca; questa è l'epoca in cui qualcuno ha guardato prima che cosa possiedi. Detto così suona come una condanna, e non lo è: **le perdite si concentrano in pochi grandi episodi, e per proteggerti si comincia dalle abitudini che puoi controllare** — le stesse quattro della checklist qui sopra, che valgono uguale che tu sia uno su un milione o uno su dieci.

MENO EPISODI NON VUOL DIRE MENO RISCHIO

È la lettura sbagliata più comune di questi numeri. Attenzione però a che cosa contano: CertiK censisce **episodi** andati a segno, non i messaggi che arrivano nelle caselle. Se gli episodi dimezzano e il bottino quasi non si muove, il bottino medio per episodio è raddoppiato: quello che cresce è la posta in gioco di ogni singolo colpo riuscito, non il numero di esche che ti passano davanti. Sul secondo numero non abbiamo dati, e nessuno li ha. Un attacco riuscito oggi è mediamente molto più preparato di quello che ti arrivava due anni fa. Il calo degli episodi non è una buona notizia per te: è una selezione.

Che cosa è successo il giorno in cui l'indirizzo era quello giusto?

È stata deviata la strada, non falsificata la targa. Il 24 aprile 2018, fra le 11:05 e le 13:03 UTC, un operatore di rete dell'Ohio ha annunciato a internet di avere la via più diretta verso un pezzo dei server che traducono i nomi dei siti in indirizzi numerici — quelli di Amazon Route 53. Internet gli ha creduto, come fa sempre, e per due ore le domande “dove sta myetherwallet.com?” hanno ricevuto in risposta un indirizzo sbagliato.

Chi apriva il sito finiva su una copia ospitata altrove. Nella barra degli indirizzi c'era scritto il nome giusto, perché *era* il nome giusto: a essere stata dirottata era la strada. L'unico segnale rimasto era l'avviso del browser sul certificato di sicurezza, e in molti lo hanno chiuso per andare avanti. In quelle due ore sono stati sottratti circa **150.000 dollari** in ether — le stime delle diverse ricostruzioni oscillano fra i 150 e i 160 mila.

LA RUBRICA E I CARTELLI STRADALI

Due pezzi diversi di internet, che qui si sono rotti insieme. Il **DNS** è la rubrica: traduce *myetherwallet.com* nel numero del server che risponde. Il **BGP** è l'insieme dei cartelli stradali fra i grandi operatori: dice a ogni pacchetto quale strada prendere per arrivare a quel numero. Chi ha condotto l'attacco non ha toccato la rubrica di nessuno: ha piantato un cartello che dichiarava una scorciatoia verso i server della rubrica, e il traffico ha seguito il cartello. Da fuori, per chi digitava, tutto sembrava al suo posto.

Questo caso è vecchio di otto anni e resta il più istruttivo di tutti, per una ragione sola: **le persone colpite stavano facendo la cosa giusta.** Non avevano cliccato un link in una mail, non erano arrivate da un messaggio privato, non avevano cercato il sito su un motore di ricerca. Avevano digitato l'indirizzo. Il consiglio che si legge ovunque — “controlla sempre l'URL” — quel giorno era soddisfatto, e non è bastato.

24 APRILE 2018

Il nome nella barra era quello giusto

LA BARRA DEGLI INDIRIZZI

myetherwallet.com

corretto

Il dominio non era falsificato. A essere stata deviata era la strada per arrivarci: rotte annunciate verso i server che traducono i nomi.

L'UNICO SEGNALE RIMASTO

⚠ **Il certificato del sito non è valido**

Molti hanno chiuso l'avviso e sono andati avanti.

11:05 → 13:03 UTC

la finestra

~150.000 \$

sottratti in ether

0

controlli dell'utente falliti

MoneyViz · Anatomia di una truffa

Il nome era giusto e i controlli dell'utente erano tutti superati. Elaborazione MoneyViz.

Da dove arriva il sito falso che apri senza sospetti?

Da cinque strade, e nessuna assomiglia alla mail scritta male degli anni scorsi.

- **Il risultato sponsorizzato.** Cerchi il nome del servizio che usi, e la prima posizione è uno spazio comprato. Si può comprare anche per il nome di un servizio che non è il proprio. Chi non clicca mai sui link ricevuti, ma cerca sempre da sé, finisce qui: è il canale che colpisce i prudenti.
- **Il dominio quasi identico.** Una lettera doppia, un trattino in più, .net al posto di .com. Esiste anche la versione più sottile, costruita con caratteri di altri alfabeti che sullo schermo sono indistinguibili dai nostri: una “a” cirillica al posto di una latina. I browser moderni difendono dai casi più evidenti mostrando il dominio in forma estesa, ma la difesa non è completa e non vale ovunque.
- **Il profilo che sembra ufficiale.** Account social con lo stesso nome, la stessa immagine e un seguito comprato, che pubblicano un link. È la stessa leva della seconda puntata, usata per portarti su una pagina invece che in una conversazione privata.
- **L’avviso urgente.** Messaggio o mail che dichiarano un problema sul tuo conto e danno una scadenza: ventiquattro ore, poi perdi l’accesso. La scadenza non esiste e serve solo a impedirti di verificare altrove.
- **Il canale ufficiale violato.** L’account vero di un progetto vero, bucato per qualche ora, che annuncia una migrazione obbligatoria. Qui non c’è niente di falso da riconoscere: il mittente è autentico.

Nota che cosa hanno in comune: in nessuno di questi casi ti viene chiesto di essere disattento. Ti viene chiesto di essere normale.

Perché le estensioni del browser sono il punto cieco più grande?

Perché stanno dentro la pagina, dopo ogni controllo che potresti fare. Il lucchetto, il certificato e il dominio riguardano il viaggio fra te e il server. Un’estensione lavora a viaggio finito, sulla pagina già aperta davanti a te, e ha il permesso di riscriverla. Può sostituire un indirizzo di destinazione nel momento in cui lo incolli, cambiare una cifra, aggiungere un campo che chiede qualcosa che quel sito non chiede mai.

Il passaggio che quasi nessuno considera è il **cambio di proprietario**. Un’estensione onesta, con anni di recensioni buone, viene venduta o ceduta; l’aggiornamento successivo arriva in automatico e in silenzio, e non è più la stessa cosa che avevi installato. Tu non hai fatto niente di nuovo: è cambiato sotto di te qualcosa che avevi già approvato.

DOVE GUARDANO I TUOI CONTROLLI

L'estensione lavora dopo l'ultimo di essi



I due controlli che puoi fare stanno in mezzo alla catena. Ai due estremi — la strada e l'estensione — non arrivi, ed è lì che passano gli attacchi riusciti.

MoneyViz · Anatomia di una truffa

I tuoi due controlli stanno in mezzo alla catena. Gli attacchi riusciti passano dagli estremi. Elaborazione MoneyViz.

LE TRE DOMANDE DA FARE A UN'ESTENSIONE

Che permessi ha? “Leggere e modificare tutti i dati sui siti che visiti” è il permesso massimo: giustificato per pochissimi strumenti, sospetto per tutti gli altri. **Mi serve ancora?** Quelle installate per una cosa sola, mesi fa, vanno rimosse: ogni estensione viva è una superficie viva. **Chi la mantiene oggi?** Non chi l’ha scritta: chi pubblica gli aggiornamenti adesso.

Come fa una copia di un’app a passare i controlli?

Non li passa: li aggira, facendotela installare da fuori. La ricerca più citata su questo schema è di [Trend Micro](#) e risale al **gennaio 2022** — la cito per il meccanismo, non per le cifre, che hanno quattro anni: 249 applicazioni che

imitavano portafogli molto diffusi, per oltre 4,3 milioni di dollari sottratti.

Il meccanismo è invecchiato bene, purtroppo. Quelle copie vivevano quasi tutte fuori dagli store ufficiali: su pagine di download raggiunte da un messaggio, da una mail che annunciava un aggiornamento necessario, o da una telefonata di una finta assistenza. È l'origine più comune, non l'unica: copie che superano la revisione e finiscono negli store ufficiali esistono — [Trezor ne ha documentata una sull'App Store](#) che portò via 17 bitcoin. Lo store riduce il rischio, non lo azzerà: il controllo che resta è arrivare alla pagina di download dal sito ufficiale del produttore e guardare chi pubblica. E la parte peggiore è il tempo: diverse di quelle applicazioni funzionavano normalmente, catturavano la frase di recupero durante la configurazione e restavano ferme per settimane prima di svuotare il portafoglio. Quando succedeva, nessuno collegava più le due cose.

Che cosa non ti salva, anche se te lo consigliano tutti?

Quattro controlli che funzionano meno di quanto credi. Non sono inutili: sono parziali, e il guaio è che danno la sensazione di aver chiuso il problema.

QUELLO CHE FAI	CHE COSA FERMA DAVVERO	DOVE NON ARRIVA
Controllare l'indirizzo nella barra	I domini sbagliati di una lettera, se li noti	Al caso del 2018: l'indirizzo era corretto. E a un account ufficiale violato, dove il mittente è autentico
Cercare il lucchetto e l'HTTPS	Che qualcuno legga il traffico lungo la strada	A chi ha allestito il sito: un certificato valido si ottiene gratis in pochi minuti, anche per un dominio appena registrato
Cercare il servizio su un motore di ricerca invece di cliccare i link	I link ricevuti per messaggio	Al risultato sponsorizzato in cima, che è uno spazio comprato: è proprio il canale che intercetta chi fa così
Fidarti di un'app perché la usi da mesi e funziona	Niente	Le copie spesso funzionano: prendono la frase di recupero all'inizio e aspettano. Il tempo che passa è parte del progetto

I controlli più consigliati e dove si fermano

Il filo che li unisce è lo stesso delle due ore del 2018: sono tutti controlli *percettivi*, cioè chiedono a te di accorgerti di qualcosa. Funzionano finché c'è qualcosa da notare. Il giorno in cui non c'è, non resta niente sotto. Il che non vuol dire che non ci sia difesa: vuol dire che **la difesa sta un gradino più in là**, e non ti chiede di accorgerti di niente.

Come ti difendi, allora?

Spostando la difesa dall'occhio alla porta. Se il problema è che il falso può essere perfetto, l'unica mossa che regge è non passare dal posto in cui te lo mostrano.

1. **I segnalibri sono l'unica porta.** Salva una volta sola gli indirizzi dei servizi che contano, e da lì in poi aprili solo da quelli: mai da una ricerca, mai da un link ricevuto, mai dalla cronologia. Questo gesto chiude il canale del risultato sponsorizzato e quello del dominio quasi identico, che sono la stragrande maggioranza dei casi.

Non chiude però il caso del 2018: quando a essere dirottata è la strada, il segnalibro porta allo stesso nome e quindi allo stesso server finto. Lì l'unico avviso che arriva è quello sul certificato — ed è il motivo della regola qui sotto.

2. **L'avviso sul certificato non si scavalca mai.** È la riga che hanno cliccato via in migliaia quel 24 aprile. Su un sito dove tieni dei soldi quell'avviso non è un fastidio da superare: è l'unico momento in cui un dirottamento di rotta diventa visibile. Si chiude la scheda e si riprova più tardi.
3. **La firma su un portafoglio fisico.** Il dispositivo mostra l'operazione sul proprio schermo, che la pagina non può riscrivere: se quello che leggi sul computer e quello che leggi sul dispositivo non coincidono, hai appena visto l'attacco. Attenzione però a che cosa protegge davvero: mette al riparo le chiavi, **non ti protegge da una firma che autorizzi tu.** Se la copia ti fa firmare un'autorizzazione, il dispositivo mostra esattamente quell'autorizzazione e tu la confermi: è la terza puntata, e lì la difesa è leggere che cosa stai firmando.
4. **La frase di recupero si digita solo dove l'hai decisa tu.** C'è un caso legittimo, ed è uno: ripristinare il tuo portafoglio nella sua app, su un dispositivo che controlli, in un momento che hai scelto tu. Fuori da lì, nessun servizio legittimo la chiede: né per “verificare”, né per “sbloccare”, né per migrare. Una pagina web che la chiede ti ha già detto tutto quello che serve sapere su di lei, qualunque nome abbia nella barra.
5. **Le app dallo store, arrivandoci dal sito ufficiale.** Mai da una pagina di download raggiunta da un messaggio. Il nome giusto non basta: conta il nome di chi pubblica, che negli store si vede. E lo store non è una garanzia: il link allo store prendilo dal sito ufficiale del produttore, non da una ricerca.

UNA PORTA SOLA

Come arrivi al sito conta più di come lo guardi

✗ **La ricerca su internet**
il primo risultato è uno spazio comprato

✗ **Il link ricevuto**
messaggio, mail, post: non lo hai scelto tu

✗ **La cronologia**
ci finisce anche il sito sbagliato di ieri

✓ **Il segnalibro salvato una volta**
l'unico che hai verificato tu, quando eri tranquillo

MoneyViz · Anatomia di una truffa

Tre porte da chiudere, una da tenere. Elaborazione MoneyViz.

IL PROFILO SEPARATO DEL BROWSER, SE VUOI FARE SUL SERIO

Un secondo profilo del browser usato **solo** per le operazioni che contano: nessuna estensione installata, nessuna sessione social aperta, solo i segnalibri dei servizi che usi. Non è da esperti e non costa niente: toglie di mezzo in un colpo sia il punto cieco delle estensioni sia i canali che ti raggiungono mentre stai facendo altro. Il profilo di tutti i giorni resta quello che era.

Che fare nei primi dieci minuti, se hai già cliccato?

Conta che cosa hai lasciato sulla pagina, perché da lì dipende tutto il resto.

1. **Chiudi e non toccare altro.** Niente altri clic, nessun campo, nessun “provo a vedere”. Se la pagina ha aperto una richiesta di firma, annullala.
2. **Se hai digitato 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, partendo da ciò che vale di più.
3. **Se hai firmato qualcosa,** sei nel territorio della terza puntata: prima sposti i fondi, poi revochi le autorizzazioni. In quest’ordine.
4. **Se hai inserito la password di un conto,** cambiala, chiudi tutte le sessioni attive, sostituisci il secondo fattore e metti in sicurezza la casella di posta collegata, che è la chiave di tutto il resto.
5. **Documenta tutto subito:** indirizzo del sito, data e ora, schermate, identificativi delle operazioni. Non ripulire niente. Serve per la denuncia, e la denuncia — come vedrai tra poco — ha anche un effetto fiscale concreto.

Dal punto di vista fiscale, quella perdita conta?

No, e questa è la parte che fa più male: **il furto non è una cessione, quindi non genera né plusvalenza né minusvalenza.** Quando le cripto escono dal tuo portafoglio verso un indirizzo di terzi non c’è corrispettivo e non c’è realizzo. Non nasce nulla da tassare, e non nasce nemmeno una perdita da portarsi dietro negli anni buoni. Attenzione però: non tassabile non vuol dire non dichiarabile. Il furto non cancella gli obblighi dichiarativi dell’anno in cui è avvenuto — le operazioni fatte prima restano da dichiarare, e la posizione va comunque ricostruita indirizzo per indirizzo.

Sul monitoraggio la denuncia non è una formalità: **con una denuncia formale il bene sottratto esce dal quadro RW,** perché non lo detieni più. Senza denuncia, formalmente, quel token risulta ancora tuo e va comunque dichiarato. È il classico cornuto e mazziato: i soldi non ci sono più, la perdita non è deducibile, e in assenza di denuncia resta anche l’obbligo di monitorare qualcosa che non possiedi più.

CHE COSA CAMBIA IN DICHIARAZIONE

Se invece hai venduto in perdita — nessun furto, solo una cessione a un prezzo più basso — la minusvalenza esiste e si può usare, ma dentro un recinto preciso: le cripto-attività sono una categoria a sé dal periodo d’imposta 2023, e **dal periodo d’imposta 2024** le minusvalenze su cripto-attività 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. Monitoraggio e tassazione viaggiano su due binari distinti: il possesso si dichiara nel quadro RW, plusvalenze e perdite riportabili stanno nel quadro RT, nella sezione dedicata alle cripto-attività. Nelle guide di **MoneyViz** trovi la compilazione passo per passo di entrambi.

C’è poi la parte che vediamo più spesso e che nessuno mette nel conto: i mesi dopo. Un portafoglio svuotato lascia uno storico da spiegare — uscite verso indirizzi sconosciuti, operazioni a metà su piattaforme diverse — e quello storico va ricostruito riga per riga prima di poter compilare qualsiasi cosa. Con **MoneyViz** ogni valore resta tracciabile

fino alla singola operazione che l'ha generata, ed è la differenza fra ricostruire una posizione e tirare a indovinare. Se è successo a te e non sai da che parte prendere quello storico, **chiedi a noi**: rimetterlo in fila è il lavoro che facciamo tutti i giorni.

Che cosa vediamo nella prossima puntata?

La frase di recupero. È comparsa tre volte in questa puntata come il danno peggiore, e merita una puntata sua: dove finisce quando la scrivi, perché una foto nel telefono è già una copia in cloud, e come si conserva qualcosa che non si può né cambiare né recuperare.

Torniamo alle due ore del 2018. Chi ci è passato non era distratto: aveva digitato l'indirizzo a mano, l'indirizzo era giusto, e il solo segnale rimasto era un avviso tecnico che quasi nessuno è attrezzato a interpretare. È questo che rende il phishing diverso dagli altri attacchi della rubrica: non punta sulla tua disattenzione, punta sul fatto che i tuoi controlli guardano tutti nello stesso punto.

Per questo la difesa che regge non è un occhio più allenato, è una porta sola. Comincia da lì: apri adesso i due o tre servizi che usi davvero e mettili nei segnalibri. Da domani entri solo da quelli, e la maggior parte di questa puntata smette di riguardarti.

LE PUNTATE DI ANATOMIA DI UNA TRUFFA

1. Come difenderti dagli attacchi crypto
2. [Il finto supporto](#)
3. [Approval phishing: la firma che ti svuota il conto](#)
4. **Phishing: siti, applicazioni ed estensioni clone** — questa puntata
5. La frase di recupero esposta — in arrivo
6. Password deboli e secondo fattore aggirato — in arrivo
7. Address poisoning — 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

- [Trezor](#) — una copia di app che supera la revisione e finisce nell'App Store
- [CertiK](#) — Hack3d, rapporto sul primo semestre 2026: episodi di phishing in calo del 52,3%, perdite in calo solo dell'11%
- [CertiK](#) — Hack3d 2025: il phishing è il vettore con più episodi dell'anno, 248 per 722,9 milioni di dollari
- [CertiK](#) — Hack3d 2024: 1,05 miliardi di dollari su 296 episodi, dal quinto al primo posto in un anno
- [CertiK](#) — come il dirottamento del DNS viene usato per clonare i siti

- [BleepingComputer](#) — la cronaca del dirottamento di MyEtherWallet del 24 aprile 2018
 - [ESET WeLiveSecurity](#) — la ricostruzione tecnica: rotte BGP annunciate verso lo spazio di indirizzi di Amazon Route 53
 - [Trend Micro \(gennaio 2022\)](#) — 249 applicazioni che imitavano portafogli diffusi, oltre 4,3 milioni di dollari sottratti
 - [MetaMask](#) — che cosa l'assistenza non chiede mai, e come si riconoscono i canali ufficiali
 - [Polizia Postale](#) — portale del Commissariato di PS per la denuncia online
 - [MoneyViz](#) — quadro RW crypto 2026: guida completa alla compilazione
 - [MoneyViz](#) — quadro RT crypto 2026: come si compila
-

Domande frequenti

Come faccio a capire se un sito crypto è una copia?

Guardandolo, spesso non puoi: le copie di oggi sono identiche all'originale. Il 24 aprile 2018 chi apriva MyEtherWallet leggeva nella barra il nome corretto, perché a essere stata deviata era la strada per arrivarci, non il dominio. Per questo la difesa non è riconoscere il falso ma non passare dal punto in cui te lo mostrano: salva i siti che contano nei segnalibri e aprili solo da lì, mai da una ricerca e mai da un link ricevuto.

Il lucchetto e l'HTTPS garantiscono che il sito sia autentico?

No, e questo equivoco è fra i più diffusi. Il lucchetto dice che il traffico fra te e quel server è cifrato, cioè che nessuno lo legge lungo la strada. Non dice nulla su chi sia quel server: un certificato valido si ottiene gratis in pochi minuti, anche per un dominio registrato il giorno prima. Il lucchetto protegge il viaggio, non la destinazione.

Perché le estensioni del browser sono considerate il punto cieco?

Perché lavorano sulla pagina già aperta, dopo ogni controllo che potresti fare: dominio, certificato e lucchetto riguardano il viaggio, l'estensione agisce a viaggio finito e può riscrivere quello che vedi, per esempio sostituendo un indirizzo di destinazione nel momento in cui lo incolli. Il rischio maggiore è il cambio di proprietario: un'estensione onesta viene ceduta e l'aggiornamento successivo arriva in automatico, senza che tu abbia fatto nulla.

Come riconosco un'applicazione di portafoglio falsa?

Dalla provenienza, non dall'aspetto. Le copie non vivono sugli store ufficiali, dove c'è una revisione: arrivano da pagine di download raggiunte da un messaggio, da una mail che annuncia un aggiornamento necessario o da una telefonata di una finta assistenza. Scarica solo dallo store e controlla il nome di chi pubblica, non solo quello dell'app. Attenzione al tempo: molte copie funzionano normalmente, prendono la frase di recupero durante la configurazione e restano ferme per settimane.

Ho inserito la frase di recupero su un sito: che cosa faccio adesso?

Quel portafoglio è compromesso in modo definitivo, anche se adesso sembra intatto: la frase di recupero non si cambia. Crea un portafoglio nuovo su un dispositivo pulito e sposta subito quello che resta, partendo da ciò che vale di più. Poi documenta tutto — indirizzo del sito, data e ora, schermate — e presenta denuncia: serve anche ai fini fiscali.

Se mi hanno rubato le cripto con il phishing, la perdita conta per il fisco?

Il furto non è una cessione: non c'è corrispettivo e non c'è realizzo, quindi non genera né plusvalenza né minusvalenza deducibile. Non tassabile però non vuol dire non dichiarabile: gli obblighi dichiarativi dell'anno restano. Sul monitoraggio cambia la denuncia: con una denuncia formale il bene sottratto esce dal quadro RW, perché non lo detieni più, mentre senza denuncia risulta ancora tuo e va dichiarato.

Articolo pubblicato su moneyviz.it — Another Block In The Wallet. Le immagini sono in pubblico dominio, i crediti sono indicati nell'articolo.