

12 OTTOBRE 2026 • 14 MIN DI LETTURA • DANILO GIUDICE

Approval phishing: la firma che ti svuota il conto mesi dopo

Una firma data e dimenticata può restare valida per anni, e chi la possiede sceglie quando usarla. Che cosa autorizzi davvero, perché la firma che non costa niente è la più pericolosa e come si ripulisce il portafoglio in dieci minuti. Puntata 3 di Anatomia di una truffa, la rubrica di sicurezza di MoneyViz.



PERCHÉ TI RIGUARDA

- Una firma approvata e dimenticata può restare valida **per anni**: non scade da sola, e chi la possiede sceglie quando usarla
- La difesa non è l'attenzione, che prima o poi cede: è una **manutenzione a calendario**, due pulizie l'anno delle autorizzazioni concesse
- Nel 2025 questa famiglia di attacchi ha sottratto **83,85 milioni di dollari** a **106.106 persone**, quasi sempre partendo da una firma
- Dal 2025 esiste una delega di livello superiore che **i revocatori classici non vedono**: sapere che esiste è metà del lavoro
- È la terza puntata di **Anatomia di una truffa**, la rubrica di sicurezza di **MoneyViz**

Hai firmato una richiesta che il portafoglio ti ha presentato come una formalità, non è successo niente, e te ne sei dimenticato. Il rischio è che quella non fosse una conferma ma una **delega**: il permesso, senza scadenza e spesso senza limite di importo, di prelevare i tuoi token quando chi la possiede deciderà di usarla. La difesa esiste e richiede dieci minuti: apri un revocatore di autorizzazioni e guarda l'elenco di quelle che hai concesso negli anni. **Controllare è**

gratuito; togliere quelle che non ti servono più costa le normali commissioni di rete. Fallo oggi, non quando te ne accorgerai.

Questo è l'*approval phishing*, e si distingue da tutti gli altri attacchi della rubrica per una cosa sola: il momento in cui firmi e il momento in cui perdi i soldi possono essere separati da mesi. Nessun allarme suona in mezzo. A settembre 2025 una singola firma del tipo *Permit* ha portato via **6,5 milioni di dollari** — il furto da phishing più grande dell'anno secondo il rapporto annuale di Scam Sniffer. Tieni a mente la delega dimenticata: ci servirà ancora.

In **MoneyViz** ricostruiamo storici di operazioni su decine di piattaforme e portafogli, e questa è la categoria in cui la domanda del cliente arriva sempre nella stessa forma: “non ho fatto niente, come hanno fatto a prendermeli?”. La risposta, quasi sempre, è che qualcosa era stato fatto — molto tempo prima, in pochi secondi, e senza che sembrasse pericoloso.

Questa puntata smonta il meccanismo: che cosa autorizzi davvero quando firmi, perché la firma che non costa nulla è la più insidiosa, che cosa è cambiato nel 2025 con una nuova forma di delega, e come si ripulisce il portafoglio delle autorizzazioni vecchie senza essere tecnici.

Perché una firma può svuotarti il conto mesi dopo?

Perché una autorizzazione non è un pagamento: è una delega che resta aperta finché non la chiudi tu. Quando usi uno scambio decentralizzato per vendere un token, il programma che esegue lo scambio deve poter prelevare quel token dal tuo portafoglio. Non glielo consegna a mano: gli concedi il permesso di prenderlo. È un passaggio normale, necessario, e lo hai fatto decine di volte.

Il problema è che quel permesso, nello standard più diffuso, non ha una data di scadenza e molto spesso non ha nemmeno un tetto: autorizza una quantità praticamente illimitata. Resta valido mentre dormi, mentre cambi telefono, mentre ti dimentichi del progetto che lo aveva richiesto. Se il programma a cui l'hai concesso era malevolo in partenza, o se viene compromesso dopo, quella delega è già in mano a qualcun altro.

LA DELEGA BANCARIA CHE NESSUNO REVOCA

Il paragone più vicino è la delega su un conto corrente. Firmi una volta perché serve a una persona per una commissione precisa, e poi quella delega resta depositata in banca: non si annulla quando la commissione finisce, si annulla quando vai tu a chiuderla. Con una differenza che rende il caso crypto più serio: in banca la delega ha un nome e un volto, qui ha l'indirizzo di un programma che non conosci e che nessuno ti ha presentato.

LA DELEGA DIMENTICATA

Fra la firma e il prelievo possono passare mesi

1

FIRMI

Martedì, trenta secondi.
Una finestra che sembra
una formalità.

2

SILENZIO

Non succede niente.
Nessun avviso, nessun
movimento, nessuna spia.

3

IL PRELIEVO

Un giorno qualunque,
mesi dopo. La delega
era ancora valida.

Nessun altro attacco ha questa distanza fra la causa e l'effetto: è il motivo per cui chi la subisce è convinto di non aver fatto niente.

MoneyViz · Anatomia di una truffa

Fra la causa e l'effetto possono passare mesi: è il motivo per cui chi lo subisce è convinto di non aver fatto niente. Elaborazione MoneyViz.

Che cosa stai autorizzando davvero, quando firmi?

Tre cose molto diverse, e il portafoglio te le mostra in modo quasi identico. È questa somiglianza — la stessa leva vista nella prima puntata — a rendere l'attacco efficace: la finestra che ti chiede di firmare una vendita legittima e quella che ti chiede di consegnare il controllo dei tuoi token si assomigliano moltissimo.

CHE COSA FIRMI	CHE COSA CONCEDE	TI COSTA COMMISSIONI?	LO VEDI NEL REVOCATORE?
Una transazione normale vendita, invio, scambio	Sposta una quantità precisa, una volta sola	Sì	Non serve: si esaurisce subito
Un'autorizzazione approve	Il permesso di prelevare quel token, spesso senza limite e senza scadenza	Sì	Sì
Una firma fuori catena <i>Permit, Permit2</i>	Lo stesso permesso, ma concesso con una firma che non appare subito sulla blockchain	No — ed è il motivo per cui abbassi la guardia	Solo dopo che viene usata
Una delega dell'indirizzo possibile dal 2025	Affida il comportamento dell'intero indirizzo a un programma, non di un singolo token	Sì, ma può pagarle un altro	No: i revocatori classici non la leggono

Le tre firme che ti possono chiedere, e che cosa concede ciascuna

Le prime due righe sono la vita normale di chiunque usi la DeFi. Le ultime due sono il terreno dove l'attacco si è spostato, e meritano una spiegazione ciascuna.

Perché la firma che non costa niente è la più pericolosa?

Perché il cervello usa il costo come segnale di importanza, e quella firma non ne ha. Una transazione normale ti chiede di pagare una commissione: è un piccolo attrito che ti fa rileggere. Una firma di tipo *Permit* non costa nulla, non compare subito sulla blockchain e nella finestra del portafoglio sembra uno di quei messaggi innocui che si firmano per entrare in un sito.

Non lo è. Concede esattamente lo stesso potere di un'autorizzazione, con un vantaggio in più per chi la raccoglie: può tenercela in tasca e presentarla quando vuole. È la delega dimenticata della nostra storia, in forma pura — tu non vedi nulla sulla blockchain, perché finché non viene usata lì non c'è scritto niente.

Nel rapporto annuale 2025 di Scam Sniffer le firme *Permit* risultano il tipo più sfruttato in assoluto, e il singolo caso più costoso dell'anno — i **6,5 milioni di dollari** di settembre — passa esattamente da lì. Nello stesso anno le perdite complessive da svuotamento del portafoglio sono però **scese a 83,85 milioni di dollari**, contro i 494 milioni del 2024: una buona notizia che riguarda comunque 106.106 persone.

PERCHÉ PERMIT ESISTE, SE È COSÌ RISCHIOSO

Non è stato inventato per rubare. Serve a risparmiare un passaggio: senza *Permit* ogni volta che usi un token nuovo devi fare due operazioni e pagare due commissioni. Con *Permit* ne fai una. La comodità è reale, il problema è che sposta una decisione importante dentro una finestra che sembra irrilevante. *Permit2*, la versione introdotta da Uniswap, aggiunge una cosa che la prima non aveva: una **scadenza**. È un miglioramento vero, ma vale solo dove è implementato.

Che cosa è cambiato nel 2025, e perché revocare non basta più?

È comparsa una delega che non riguarda un singolo token, ma l'indirizzo intero. Fino a ieri potevi concedere il permesso di prelevare un token alla volta. Da quest'anno puoi anche affidare il comportamento del tuo indirizzo a un programma: una funzione utile e richiesta, che serve a pagare le commissioni in un token diverso, a raggruppare più operazioni in una, a far firmare qualcun altro al posto tuo. Si attiva soltanto se la autorizzi tu, con una firma: esattamente come tutto il resto di questa puntata.

La conseguenza pratica è una sola, ed è quella che conta: **i revocatori di autorizzazioni non la mostrano**. Loro elencano i permessi concessi sui singoli token, mentre questa delega sta un piano sopra. Puoi quindi aprire il revocatore, trovarlo pulito e avere comunque un indirizzo che non si comporta più come il tuo.

CHE COS'È EIP-7702?

È il nome tecnico di questa delega, arrivata su Ethereum nel 2025 con l'aggiornamento *Pectra*. Non è una falla: è una funzione pensata per rendere i portafogli più comodi, e nessuno può attivarla al posto tuo. Nei primi mesi, però, la ricerca di Wintermute ha trovato che oltre il **97 per cento** di queste deleghe puntava a copie dello stesso identico programma, ribattezzato ironicamente *CrimeEnjoyor*: poche righe che svuotano in automatico qualsiasi somma arrivi su un indirizzo già compromesso. Quella campagna, aggiungeva Wintermute, non stava nemmeno guadagnando granché — circa 2,88 ether spesi per autorizzare quasi 79.000 indirizzi, e pochissimo incassato. Il dato che conta non è il bottino: è il meccanismo.

IL PUNTO DA PORTARSI VIA

Se usi un revocatore e lo trovi pulito, hai verificato una cosa sola: che non ci sono autorizzazioni sui token. Non hai verificato se l'indirizzo è stato delegato. Per quello serve guardare l'indirizzo su un esploratore di blockchain e controllare se risulta associato a del codice: un indirizzo personale, normalmente, non ne ha.

Da dove arriva la richiesta di firma?

Da un posto che sembra quello giusto, perché l'intero attacco sta nel contesto, non nella firma. La firma in sé è identica a una legittima: è dove ti viene chiesta che cambia tutto. I canali ricorrenti sono pochi e si ripetono da anni.

- **Un annuncio pubblicitario sul motore di ricerca.** Cerchi il nome del protocollo che usi, clicchi il primo risultato e finisci su una copia. Il dominio è sbagliato di una lettera, o ha un trattino in più.
- **Un token che compare da solo nel portafoglio.** Non l'hai comprato, c'è scritto che vale qualcosa, e l'unico posto dove si può vendere è un sito indicato nel nome del token stesso. Vendere richiede una firma. Quella firma è l'attacco.
- **Un avviso urgente su un canale ufficiale che è stato violato.** Account social di progetti veri, bucati per qualche ora, che annunciano una migrazione obbligatoria o un rimborso da riscattare.
- **Un messaggio privato da chi finge di assisterti,** esattamente il meccanismo della seconda puntata: il finto supporto non ti chiede la frase di recupero, ti chiede di firmare per “sbloccare” qualcosa.

- **Un'estensione del browser installata mesi prima**, aggiornata in silenzio con codice che riscrive le richieste di firma prima che tu le legga.

Nota la cosa importante: in nessuno di questi casi ti viene chiesta la frase di recupero. È il motivo per cui le vittime, interrogate, dicono in buona fede di non aver dato niente a nessuno. Non hanno dato le chiavi, hanno dato un permesso — e il risultato pratico è lo stesso.

Come ti difendi, in concreto?

Con tre abitudini, nessuna delle quali richiede competenze tecniche. Non si tratta di riconoscere un sito falso ogni volta: a quel gioco, prima o poi, perdi.

1. **Separa i portafogli.** Uno “di lavoro” con pochi fondi, che usi per interagire con i protocolli e che può permettersi un errore. Uno “di deposito” che non firma mai niente e non si collega mai a nessun sito. Questa singola mossa spegne l'intera categoria di attacco sui fondi che contano.
2. **Fai pulizia due volte l'anno.** Dieci minuti a giugno e dieci a dicembre su un revocatore di autorizzazioni. È una manutenzione, come cambiare le password: se la fai a calendario non devi ricordarti di farla.
3. **Arriva ai siti dai tuoi segnalibri**, mai da una ricerca e mai da un link ricevuto. I risultati sponsorizzati sono comprabili, i tuoi segnalibri no.

CHE COSA GUARDARE NELLA FINESTRA DI FIRMA, PRIMA DI PREMERE

Tre dettagli, in ordine di importanza. **Il tipo di richiesta:** se il portafoglio scrive *approval*, *permit* o “autorizzazione”, non stai concludendo un'operazione, ne stai aprendo una. **L'importo:** se compare un numero enorme o la parola “illimitato”, e tu volevi scambiare cento euro, i due numeri non coincidono. **Il destinatario:** un indirizzo che non hai mai visto, su un sito che ti ha raggiunto da un link, è il momento di chiudere la finestra. In caso di dubbio: annullare non costa niente, e l'operazione legittima si può rifare fra cinque minuti.

PRIMA DI FIRMARE

I tre campi da leggere nella finestra del portafoglio

Richiesta di firma

TIPO DI RICHIESTA

Autorizzazione (approve)

Non stai concludendo:

stai aprendo un permesso che resta valido.

IMPORTO

Illimitato

Volevi scambiare cento euro:

i due numeri non coincidono.

DESTINATARIO

0x9c41...b7e2 (sconosciuto)

Non l'hai mai visto:

il sito è arrivato da un link.

Annullare non costa niente: l'operazione legittima si rifà fra cinque minuti.

MoneyViz · Anatomia di una truffa

Tre campi, nell'ordine in cui conviene leggerli. Se anche uno solo non torna, la finestra si chiude. Elaborazione MoneyViz.

Come si revocano le autorizzazioni, passo per passo?

Si usa un **revocatore**, si collega il portafoglio in sola lettura e si cancellano le deleghe una per una. Gli strumenti più usati sono [Revoke.cash](#) e [il controllore di autorizzazioni di Etherscan](#); molti portafogli hanno la stessa funzione

incorporata, ed è la strada preferibile quando c'è.

1. **Apri lo strumento dal tuo segnalibro**, o digitando l'indirizzo a mano. Non cercarlo su un motore di ricerca: le copie dei revocatori esistono, ed è una trappola particolarmente cattiva perché colpisce chi sta facendo la cosa giusta.
2. **Incolla il tuo indirizzo pubblico prima di collegare il portafoglio**. L'elenco si vede in sola lettura: a questo punto non hai firmato niente e non rischi nulla.
3. **Leggi la lista con due criteri**: le autorizzazioni senza tetto di importo, e quelle verso progetti che non usi da più di qualche mese. Sono le due categorie da togliere per prime.
4. **Revoca**. Ogni revoca è una transazione vera e paga una commissione, quindi conviene farne diverse nella stessa sessione quando la rete è scarica. È il solo costo dell'operazione.
5. **Ripeti su ogni rete** dove hai operato. Le autorizzazioni non sono condivise: quelle di una rete non compaiono nell'elenco di un'altra, ed è l'errore più comune di chi fa pulizia una volta e si considera a posto.
6. **Controlla a parte le deleghe dell'indirizzo**. Apri il tuo indirizzo su un esploratore di blockchain e verifica che non risulti associato a del codice. Se lo è e non l'hai fatto tu consapevolmente, sposta subito i fondi su un portafoglio nuovo: in questo caso revocare le autorizzazioni non basta.

DIECI MINUTI, DUE VOLTE L'ANNO

La sequenza della pulizia, nell'ordine giusto

- 1 Apri il revocatore dal tuo segnalibro**
Mai da una ricerca: le copie dei revocatori esistono.
- 2 Incolla l'indirizzo pubblico, senza collegare il portafoglio**
L'elenco si legge in sola lettura: non hai firmato niente.
- 3 Togli per prime le autorizzazioni senza tetto di importo**
Poi quelle verso progetti che non usi da mesi.
- 4 Ripeti su ogni rete dove hai operato**
Le autorizzazioni non sono condivise fra una rete e l'altra.
- 5 Controlla a parte se l'indirizzo risulta delegato a del codice**
I revocatori classici non lo mostrano: si vede sull'esploratore.

Ogni revoca è una transazione vera e paga una commissione: conviene farne diverse nella stessa sessione, quando la rete è scarica.

MoneyViz · Anatomia di una truffa

La manutenzione completa, in ordine. Il quinto passo è quello che i revocatori da soli non coprono. Elaborazione MoneyViz.

Che fare se hai appena firmato qualcosa di cui non sei sicuro?

Conta l'ordine delle azioni, non la velocità con cui le fai. La reazione istintiva — mettersi a revocare — è spesso quella sbagliata: se la delega è già in mano a qualcuno, la revoca è una transazione che resta in attesa e può essere superata da una con commissione più alta.

1. **Sposta prima i fondi** su un portafoglio nuovo, partendo da quello che vale più. L'autorizzazione vale su un token specifico: ciò che non è più lì, non può essere prelevato.
2. **Poi revoca** quello che resta, con calma.
3. **Non toccare nulla** di quello che è successo: non “ripulire” la cronologia, non cancellare messaggi, non chiudere l'account da cui è arrivato il link. Servono dopo.
4. **Annota tutto subito:** data e ora, il sito, l'indirizzo del programma autorizzato, il codice identificativo della transazione, il tuo indirizzo. Uno screenshot per ciascuno. È il materiale della denuncia, e la denuncia — come vedrai tra poco — ha anche un effetto fiscale concreto.
5. **Non rivolgerti a chi ti scrive per primo.** Appena il fatto diventa visibile sulla blockchain arrivano i profili che promettono di recuperare i fondi a pagamento: è la seconda truffa, costruita sulla prima, e la [prima puntata di questa rubrica](#) la racconta per esteso.

Dal punto di vista fiscale, quella perdita conta?

No, e è la parte che fa più male: il furto non è una cessione, quindi non genera né plusvalenza né minusvalenza. Quando i token 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.

La conseguenza pratica riguarda il monitoraggio, e qui 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: dal periodo d'imposta 2024 le minusvalenze su crypto-attività riducono soltanto plusvalenze da cessione di altre crypto-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 crypto-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 da una firma lascia uno storico da spiegare — uscite verso indirizzi sconosciuti, token che non ci sono più, 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 transazione che l'ha generata, ed è la differenza fra ricostruire una posizione e tirare a indovinare.

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 quasi tutte le firme di cui abbiamo parlato vengono chieste esattamente lì.

Torniamo alla delega dimenticata. Non è un'immagine: è la cosa che rende questo attacco diverso da tutti gli altri della rubrica. Negli altri casi il danno arriva mentre stai sbagliando, e almeno hai la possibilità di accorgertene. Qui arriva mesi dopo, quando hai smesso di pensarci: fra la firma e il prelievo non c'è nessun segnale che colleghi le due cose.

Per questo la difesa non è l'attenzione, che prima o poi cede: è la manutenzione. Dieci minuti, due volte l'anno, sull'elenco delle autorizzazioni, più il controllo a parte sulle deleghe dell'indirizzo. Inizia dal controllo delle autorizzazioni: puoi consultarle senza firmare nulla, e da lì decidi con calma che cosa vale la pena chiudere.

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 mesi dopo** — questa puntata
4. [Phishing: siti, applicazioni ed estensioni clone](#) — in arrivo
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

- [Scam Sniffer](#) — rapporto annuale 2025 sul phishing crypto: 83,85 milioni di dollari sottratti e 106.106 vittime
- [Scam Sniffer](#) — rapporto annuale 2024, il termine di confronto da 494 milioni di dollari
- [CoinDesk](#) — la ricerca Wintermute sulle deleghe EIP-7702 e il codice ribattezzato CrimeEnjoyor
- [EIP-7702](#) — il testo della specifica che introduce la delega di un indirizzo a del codice
- [EIP-2612](#) — la specifica delle firme di tipo Permit
- [Ethereum.org](#) — che cosa ha introdotto l'aggiornamento Pectra
- [Revoke.cash](#) — che cosa sono le autorizzazioni sui token e come si revocano
- [Etherscan](#) — controllore delle autorizzazioni sui token

- [MetaMask](#) — come revocare le autorizzazioni concesse a un contratto
 - [Uniswap](#) — Permit2, la versione delle autorizzazioni con scadenza
 - [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

Che cos'è l'approval phishing?

È l'attacco in cui non ti viene rubata una password, ma viene fatta firmare un'autorizzazione: il permesso di prelevare un tuo token. Nello standard più diffuso quel permesso non ha scadenza e spesso non ha nemmeno un tetto di importo, quindi chi lo possiede può usarlo mesi dopo. È il motivo per cui le vittime sono convinte, in buona fede, di non aver fatto niente: la firma e il prelievo sono separati nel tempo.

Come faccio a vedere quali autorizzazioni ho concesso?

Con un revocatore di autorizzazioni come [Revoke.cash](#) o il controllore di [Etherscan](#), oppure con la funzione equivalente integrata nel tuo portafoglio, che è la strada preferibile. Incolla il tuo indirizzo pubblico senza collegare il portafoglio: l'elenco si legge in sola lettura, senza firmare niente. Apri lo strumento dai tuoi segnalibri e non da una ricerca, perché esistono copie false anche dei revocatori. Ripeti il controllo su ogni rete dove hai operato: le autorizzazioni non sono condivise fra una rete e l'altra.

Revocare le autorizzazioni costa qualcosa?

Leggere l'elenco è gratuito. Ogni revoca invece è una transazione vera e paga la commissione di rete, quindi conviene farne diverse nella stessa sessione quando la rete è scarica. È l'unico costo dell'operazione, e va confrontato con quello che la delega lasciata aperta può portare via.

Perché una firma che non costa commissioni è più pericolosa?

Perché è proprio l'assenza di costo a farti abbassare la guardia. Una firma di tipo Permit non paga commissioni e non compare subito sulla blockchain, quindi nella finestra del portafoglio sembra uno di quei messaggi innocui che si firmano per entrare in un sito. Concede invece lo stesso potere di un'autorizzazione, con il vantaggio, per chi la raccoglie, di poterla presentare quando vuole. Nel 2025 è stato il tipo di firma più sfruttato in assoluto.

Che cos'è la delega EIP-7702 e perché il revocatore non la mostra?

Dal 2025 un indirizzo normale può delegare il proprio comportamento a un programma: serve a pagare le commissioni in un altro token o a raggruppare più operazioni, e si attiva solo se la autorizzi tu. I revocatori classici non la elencano perché cercano autorizzazioni sui singoli token, mentre questa sta un piano sopra e riguarda l'indirizzo intero. Per verificarla apri il tuo indirizzo su un esploratore di blockchain e controlla se risulta associato a del codice: un indirizzo personale, normalmente, non ne ha.

Mi hanno svuotato il portafoglio dopo una firma: 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. Cambia però il monitoraggio: con una denuncia formale il bene sottratto esce dal quadro RW, perché non lo detieni più, mentre senza denuncia formalmente risulta ancora tuo e va dichiarato. Diverso il caso della vendita in perdita, che genera una minusvalenza compensabile solo con plusvalenze da cripto-attività e riportabile nei quattro anni successivi.

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