

19 gennaio 2026

I criminali delle criptovalute hanno rubato 700 milioni di dollari alle persone

di [Redazione](#)

C'è qualcosa di particolarmente angosciante nel subire il furto delle proprie criptovalute. Tutte le transazioni vengono registrate su un registro digitale, noto come blockchain, quindi anche se qualcuno prende i tuoi soldi e li deposita nel proprio portafoglio crittografico, questi rimangono visibili online.

"Puoi vedere i tuoi soldi lì sulla blockchain pubblica, ma non c'è nulla che tu possa fare per recuperarli", afferma Helen, che ha perso circa 315.000 dollari a causa dei ladri.

Lo paragona al guardare un ladro che ammuccia i tuoi beni più preziosi dall'altra parte di un baratro invalicabile.

Per sette anni Helen e suo marito Richard (nome di fantasia), entrambi residenti nel Regno Unito, avevano acquistato e accumulato criptovalute chiamate Cardano.

Apprezzavano l'idea di investire in un asset digitale che aveva il potenziale per aumentare drasticamente il suo valore, a differenza dei fondi risparmiati in modi più convenzionali.

Sapevano che era più rischioso, ma erano attenti a proteggere le loro chiavi digitali.

Ma in qualche modo gli hacker sono riusciti a entrare nel loro account di archiviazione cloud, dove conservavano informazioni sui loro portafogli crittografici e su come accedervi.

Nel febbraio 2024, dopo un piccolo trasferimento di prova, i criminali hanno inviato tutte le monete della coppia ai propri portafogli digitali, con un attacco rapido e silenzioso.

La coppia ha poi assistito per mesi allo spostamento del loro denaro da un portafoglio all'altro, senza poter fare nulla. (La contraddizione intrinseca delle criptovalute è che tutte le transazioni sono pubblicamente tracciabili, ma gli utenti possono rendersi pubblicamente non rintracciabili se lo desiderano.)

Helen e Richard non sono ricchi. Lei è un'assistente personale, lui un compositore, e riponevano grandi speranze nei loro investimenti in Cardano.

"Compravamo queste monete da così tanto tempo... Abbiamo usato ogni spicciolo che riuscivamo a trovare per comprarne altre", racconta Richard. "A parte la morte dei miei genitori, questo furto è la cosa peggiore che mi sia mai capitata."

Da allora, Helen è in missione per recuperare i loro soldi. Ha ottenuto rapporti dettagliati da diverse forze di polizia e dagli sviluppatori di Cardano. Ora, anche se ha l'indirizzo del portafoglio dei criminali, non c'è nulla che si possa fare per smascherarli.

Il loro piano è quello di risparmiare abbastanza soldi per ingaggiare investigatori privati e cercare di rintracciare gli hacker.

"Ti lascia con un senso di impotenza", dice, "ma continuerò a provarci".

Un'esplosione di crimini basati sulle criptovalute

Un sondaggio condotto per la Financial Conduct Authority (FCA) nell'agosto 2024 ha rilevato che circa il 12% degli adulti britannici possedeva criptovalute, ovvero circa sette milioni di persone.

A livello globale, si stima che 560 milioni di persone detengano criptovalute. Ma con l'aumento

del numero di possessori, sono aumentati anche i furti. La pandemia ha portato a un'impennata del valore delle criptovalute e, con essa, a un'esplosione di attacchi al settore.

E il 2025 è stato un altro anno eccezionale per i criminali informatici che sfruttano le criptovalute, con furti totali per oltre 3,4 miliardi di dollari, secondo gli investigatori della società di analisi blockchain Chainalysis. La cifra annuale è rimasta invariata dal 2020.

La maggior parte del denaro viene rubata tramite massicci attacchi informatici alle aziende crypto. Ad esempio, gli hacker nordcoreani hanno rubato 1,5 miliardi di dollari dall'exchange di criptovalute Bybit nel febbraio 2025.

Le perdite in questo caso e nella stragrande maggioranza degli altri sono coperte dalle ricche aziende crypto, con scarso impatto sui singoli individui. Tuttavia, il 2025 ha visto anche un aumento del numero di attacchi ai singoli investitori in criptovalute.

Secondo una ricerca di Chainalysis, questi attacchi individuali sono aumentati da 40.000 nel 2022 a 80.000 l'anno scorso.

Si stima che il 20% del valore totale delle criptovalute rubate sia dovuto a hacking, truffe o coercizioni ai danni di individui, per un valore stimato di 713 milioni di dollari.

Ma l'azienda aggiunge che il numero potrebbe essere molto più alto, poiché non tutte le vittime scelgono di denunciare pubblicamente i furti. Quando ciò accade, si rischia di rimanere soli.

Molti furti o truffe nella finanza tradizionale sono coperti da banche o società di carte di credito.

Nel Regno Unito è possibile presentare un reclamo al Financial Ombudsman Service e ottenere un risarcimento tramite il Financial Services Compensation Scheme.

"Le criptovalute rimangono in gran parte non regolamentate nel Regno Unito e ad alto rischio", afferma la FCA. "Se qualcosa va storto, è improbabile che tu sia protetto, quindi dovresti essere pronto a perdere tutti i tuoi soldi".

Un duro promemoria di ciò si ha cercando online "account Binance hackerato": Binance è il più grande exchange di criptovalute al mondo, con 1,4 milioni di utenti segnalati nel Regno Unito, ma la pagina del suo sito web che offre consigli alle vittime di furto è bloccata nel Regno Unito.

L'azienda non accetta nuovi clienti nel Regno Unito dal 2023, perché non è autorizzata a operare dalla FCA. Eppure, ai criminali non importa dove si trovino le vittime, e le persone vengono prese di mira indiscriminatamente in tutto il mondo.

Chainalysis ha descritto questi attacchi contro singoli individui come "la frontiera poco documentata dei crimini basati sulle criptovalute".

Secondo loro, il volume dei crimini è dovuto al numero di persone che sono entrate nel mondo delle criptovalute come investitori, dato che il valore delle monete è aumentato, e sostengono che il miglioramento delle pratiche di sicurezza nei principali servizi avrebbe potuto spingere "gli aggressori verso individui percepiti come bersagli più facili".

Poi c'è il fatto che più criptovalute si possiedono e più si rende pubblica la situazione, più è probabile che si venga presi di mira: i piccoli detentori (o hodler, come li chiama la comunità) hanno molte meno probabilità di essere colpiti.

Furti con scasso, rapine e "aggressioni con chiavi inglesi"

Per quanto riguarda i ladri, potrebbero essere ovunque.

A ottobre, i ricercatori di blockchain di Elliptic, una società di analisi crittografica, hanno lanciato l'allarme: gli hacker nordcoreani, finanziati dallo Stato, stanno prendendo sempre più di mira i ricchi possessori di criptovalute. Ci sono anche molti giovani truffatori e hacker provenienti da altri Paesi.

A dicembre negli Stati Uniti, il ventiduenne Evan Tangeman si è dichiarato colpevole di far parte di un gruppo di ladri di criptovalute che si autodefinisce Social Engineering Enterprise, accusati di aver rubato più di 260 milioni di dollari (194 milioni di sterline) tra ottobre 2023 e maggio 2025. Gli inquirenti sostengono di aver preso di mira i ricchi in criptovalute utilizzando database

hackerati, ingannando le vittime facendole credere che fossero exchange di criptovalute e convincendole a trasferire monete.

Si dice che i membri della banda, tutti giovani uomini per lo più residenti negli Stati Uniti, abbiano speso il denaro rubato in jet privati, auto costose e borse di lusso che poi regalavano nei locali notturni.

In alcuni casi, affermano i pubblici ministeri, la banda ha organizzato irruzioni nelle abitazioni per rubare hardware contenente le chiavi per accedere a criptovalute nascoste.

Furti con scasso e rapine sono diventati così comuni che nella comunità delle criptovalute è stato coniato un termine per definirli: "attacchi con chiavi inglesi", così chiamati perché è noto che i criminali minacciano le vittime con delle chiavi inglesi.

Lo scorso aprile, alcuni criminali informatici in Spagna hanno cercato di costringere un uomo e una donna a separarsi dalla loro criptovaluta.

La polizia spagnola ha dichiarato che l'uomo è stato colpito a una gamba e che lui e il suo compagno sono stati tenuti prigionieri per diverse ore, mentre i criminali cercavano di accedere ai loro portafogli di criptovalute. Alla fine la donna è stata rilasciata, ma il suo compagno è rimasto disperso, il cui corpo è stato successivamente ritrovato in un bosco.

In relazione al caso, in Spagna sono state arrestate cinque persone, mentre in Danimarca sono state incriminate altre quattro.

In Francia si sono verificati diversi casi simili, tra cui uno in cui un tentativo di rapimento è stato ripreso in video.

Un altro caso, avvenuto all'inizio del 2025, ha visto David Balland, co-fondatore di Ledger, un'azienda di sicurezza per criptovalute, rapito insieme alla moglie dalla loro casa nella Francia centrale.

Giorni dopo la polizia li ha salvati, ma durante il tentativo di estorsione a Balland venne loro amputato un dito.

Poi, il mese scorso, la polizia del Regno Unito ha arrestato sei persone dopo che uomini mascherati avevano fermato un'auto che viaggiava tra Oxford e Londra e costrinsero uno degli occupanti a trasferire criptovaluta per un valore di 1,5 milioni di sterline.

Phil Ariss, direttore delle relazioni con il settore pubblico del Regno Unito presso la società di intelligence blockchain TRM Labs, ha affermato in precedenza che i gruppi criminali già abituati a ricorrere alla violenza per raggiungere i propri obiettivi erano molto propensi a migrare verso le criptovalute.

"Finché esiste una via praticabile per riciclare o liquidare i beni rubati, per il trasgressore fa poca differenza se l'obiettivo è un orologio di valore elevato o un portafoglio crittografico.

"Le criptovalute sono ormai saldamente nella corrente principale e, di conseguenza, la nostra tradizionale comprensione della minaccia fisica e della rapina deve evolversi di conseguenza." È difficile stabilire con esattezza quanto siano diffusi gli "attacchi con chiavi inglesi", poiché sono pochi quelli denunciati pubblicamente. Ma sembra che questi tipi di furti rappresentino solo una piccola parte del crescente problema dei furti di criptovalute personali.

Molti criminali si affidano a tecniche di hacking o truffa collaudate e affidabili, che stanno diventando sempre più semplici grazie all'abbondanza di dati rubati durante massicci attacchi informatici alle aziende.

"I milionari di Bitcoin stanno diventando così frequenti"

"I dati sono un problema comune, dato che i milionari di Bitcoin stanno diventando sempre più numerosi e ci sono database rubati che arricchiscono costantemente la lista dei bersagli", afferma Matthew Jones, fondatore di Haven, un'azienda di sicurezza crittografica.

Un esempio calzante è la violazione dei dati avvenuta presso Kering, la società madre di marchi di lusso tra cui Gucci e Balenciaga, secondo un hacker intervistato dalla BBC.

Oltre a milioni di nomi e recapiti dei clienti, i database mostrano anche quanti soldi le persone hanno speso nei negozi.

L'hacker con cui ha parlato la BBC afferma di aver acquistato i fogli di calcolo per 300.000 dollari per prendere di mira i più grandi spendaccioni.

Sostiene di aver utilizzato le informazioni insieme ai dettagli di un altro database rubato per truffare diversi utenti di Coinbase e sottrarre loro almeno 1,5 milioni di dollari (1,1 milioni di sterline) in criptovalute.

Il criminale ha confermato di essere in possesso dei dati rubati e ha dimostrato alla BBC di possedere 700.000 dollari in Bitcoin, che secondo lui provenivano da una sola vittima.

"Compro database hackerati e li incrocio con altri per verificare la presenza di persone ricche e per trovare numeri di telefono ed e-mail aggiornati. Sto ancora scorrendo la lista e ho triplicato i miei soldi molto velocemente", ha affermato.

L'hacker non ha voluto fornire alcun dettaglio su di sé, se non il fatto di essere uno studente di un'università statunitense.

Quando gli è stato chiesto se si considerasse un hacker o un truffatore, ha risposto: "Nessuno dei due, mi interessa solo fare soldi".

Kering non ha risposto alla richiesta di commento in merito, ma in precedenza aveva dichiarato alla BBC che i suoi sistemi IT erano stati protetti dopo la violazione dei dati e aveva sottolineato che durante l'attacco non erano stati rubati numeri di conto bancario, informazioni di carte di credito o numeri di identificazione rilasciati dal governo.

(Joe Tidy su BBC del 19/01/2026)

CHI PAGA ADUC

l'associazione non **percepisce ed è contraria ai finanziamenti pubblici** (anche il 5 per mille)

La sua forza economica sono iscrizioni e contributi donati da chi la ritiene utile

[DONA ORA](#)