6 NOVEMBRE 2026 • 16 MIN DI LETTURA • DANILO GIUDICE

Hai fotografato la seed phrase? Perché le tue crypto sono a rischio

Una foto della frase di recupero nella galleria del telefono: è esistita una campagna che cercava esattamente quella, e fra le parole cercate c'era anche l'italiano. Perché la seed phrase è l'unica cosa che non puoi cambiare, e dove si conserva davvero. Puntata 5 di Anatomia di una truffa, la rubrica di sicurezza di MoneyViz.



PERCHÉ TI RIGUARDA

- La frase di recupero è **l'unica cosa che non puoi cambiare**: una password si sostituisce in un minuto, queste dodici o ventiquattro parole no — e chi le ha è te, per sempre
- Nel 2025 gli episodi su portafogli personali sono stati **158.000**, ma il valore medio sottratto a ciascuno è **sceso**: non serve essere ricchi per rientrarci, serve avere la frase in un posto raggiungibile
- Una campagna attiva dal 2024 cercava **la fotografia** della frase nella galleria del telefono, leggendola con lo stesso riconoscimento del testo che usi tu per copiare un numero da uno scontrino. Nell'elenco delle parole cercate **c'era anche l'italiano**
- Il pericolo era difficile da riconoscere: le app provenivano anche **da store ufficiali** e chiedevano permessi apparentemente ragionevoli. La lezione è semplice: **un'applicazione può essere utile e funzionare perfettamente, senza per questo meritare accesso a tutte le nostre fotografie**
- La difesa non richiede di comprare niente oggi: **la prima mossa è mettere quelle parole su carta**, e solo dopo togliere la fotografia — mai il contrario. È la quinta puntata di **Anatomia di una truffa**, la rubrica di sicurezza di **MoneyViz**

> **LA CHECKLIST, PRIMA DI TUTTO IL RESTO**
>
> Quattro mosse che puoi fare **oggi**, senza comprare niente. Vanno fatte in quest'ordine, e l'ordine è la parte importante: **non cancellare niente prima di avere un'altra copia.**
>
> 1. **Scrivila a mano su carta, adesso.** Trascrivi le parole dall'app del portafoglio o dalla foto, poi rileggile due volte confrontandole con l'originale. Se quella fotografia è la tua unica copia, cancellarla prima di averne un'altra è il modo più rapido di perdere il portafoglio da solo.
> 2. **Verifica la copia, poi mettila in due posti diversi.** Prova a ripristinare un portafoglio vuoto con quelle parole, una volta sola: una copia mai provata non è una copia, è una speranza. Poi due *luoghi*, non due fogli nello stesso cassetto.
> 3. **Solo adesso togli le copie digitali.** Galleria del telefono e del computer, cestino, copie sincronizzate, note, mail a te stesso, messaggi salvati: cerca una delle parole della tua frase dentro la posta e dentro l'app delle note. Se esce qualcosa, quella è una copia.
> 4. **Se quella foto è esistita, cancellarla non chiude il problema.** Non puoi sapere se qualcuno l'ha già letta, e la frase non si cambia: quel portafoglio va trattato come compromesso e i fondi vanno spostati su una frase nuova.
>
> Se l'hai già fotografata o inserita da qualche parte, vai direttamente a che fare nei primi dieci minuti. E se non sai da dove cominciare, o vedi un movimento che non ti torna e non capisci da dove arrivi, **chiedi a noi**: è esattamente il tipo di domanda che l'assistenza di **MoneyViz** riceve tutti i giorni.

Da qualche parte nella galleria del tuo telefono, fra le foto delle vacanze e le ricevute fotografate di fretta, potrebbe esserci l'immagine di un foglio scritto a mano con dodici parole. L'hai scattata il giorno in cui hai configurato il portafoglio, per prudenza: perdere quelle parole significa perdere tutto, e un foglio di carta si perde. **Tieni a mente quella fotografia, perché ci torniamo alla fine.**

Dal marzo 2024 è esistita una campagna che cercava esattamente quella. Non la tua password, non le credenziali del conto: la fotografia. In questa quinta puntata di **Anatomia di una truffa**, la rubrica di sicurezza di **MoneyViz**, vediamo che cos'è davvero la frase di recupero, perché è l'unica cosa che non puoi cambiare dopo, e dove si conserva qualcosa che non si può né cambiare né recuperare.

Perché la frase di recupero è l'unica cosa che non puoi cambiare?

Perché non è una credenziale che apre il portafoglio: è il portafoglio. Quelle dodici o ventiquattro parole non sono una chiave conservata da qualche parte in un archivio, sono il numero da cui tutte le tue chiavi vengono calcolate. Da quella sequenza si ricostruiscono gli indirizzi, i saldi e la facoltà di firmare: su qualunque dispositivo, in qualunque momento, senza bisogno del tuo telefono e senza che tu te ne accorga.

È la differenza che rende questa puntata diversa dalle precedenti. Una password rubata si cambia e il danno si ferma. Un'autorizzazione firmata si revoca, come nella terza puntata; un sito clone lo smetti di visitare, come nella quarta. **La frase di recupero no:** non esiste un pulsante per generarne una nuova sullo stesso portafoglio, e l'unica risposta possibile è creare un portafoglio diverso e spostare tutto, prima che lo faccia qualcun altro.

> **FRASE DI RECUPERO, SEED PHRASE, MNEMONICO: PERCHÉ TRE NOMI**
>
> Sono la stessa cosa. In inglese si chiama *seed phrase*, dove *seed* — seme — dice bene il funzionamento: non è una copia delle chiavi, è il seme da cui ricrescono tutte. Il termine tecnico è *mnemonic*, in italiano **mnemonico**, e viene dallo standard che ha reso queste parole uno strumento comune a portafogli diversi: per questo la stessa sequenza funziona anche su un'app che non è quella con cui l'hai creata. Tienilo a mente, perché proprio la parola «mnemonico» torna fra poco, e non in un contesto rassicurante.

Con una conseguenza che quasi nessuno mette nel conto: **chi ottiene quelle parole non deve usarle subito**. Può aspettare che il portafoglio si riempia, o solo il momento in cui nessuno sta guardando. È il motivo per cui tante persone raccontano di essere state svuotate «dal nulla», senza aver fatto niente di strano quel giorno: il giorno sbagliato era stato molto tempo prima.

Che cosa è successo quando un programma ha imparato a leggere le fotografie?

È successo che la galleria del telefono è diventata un archivio consultabile, e qualcuno l'ha consultato. Nel febbraio 2025 i ricercatori di Kaspersky hanno pubblicato l'analisi di una campagna, battezzata SparkCat, attiva almeno dal marzo 2024. Il meccanismo è disarmante: dentro alcune app comuni — consegna cibo, messaggistica — era stato inserito un componente che, ottenuto l'accesso alle immagini, le passava a un riconoscimento del testo. Lo stesso che usi tu quando copi un IBAN da una fotografia.

Il componente non prendeva tutte le foto. Chiedeva a un server un elenco di parole chiave e mandava indietro **solo le immagini in cui quelle parole comparivano**. L'elenco ottenuto dai ricercatori era in nove lingue, e una era l'**italiano**: la parola cercata era **«Mnemonico»**. Non è un dettaglio folkloristico — significa che fra i bersagli previsti c'erano persone che scrivono la propria frase di recupero in italiano, e che qualcuno aveva ritenuto valesse la pena cercarle.



I cinque passaggi fra la fotografia e il server. Nessuno richiede una tua disattenzione: l’unico gesto evitabile è il primo. Fonte: ricostruzione MoneyViz sull’analisi Kaspersky, febbraio 2025.

Le cifre aiutano a capire la scala. Le app infette presenti su Google Play erano state **scaricate oltre 242.000 volte**. E per la prima volta un programma costruito attorno al riconoscimento ottico del testo è stato trovato anche **nell’App Store di Apple**: è la frase che smonta la convinzione più diffusa fra chi usa iPhone, cioè che la revisione del negozio sia una garanzia. Apple ha rimosso le app il 6 febbraio 2025, Google il giorno dopo. Il 2 aprile 2026, a un anno di distanza, è stata trovata una nuova versione di nuovo in entrambi i negozi — due app nell’App Store e una su Google Play. Con una differenza che allarga il bersaglio: la variante per iPhone non cerca più parole in una lingua o nell’altra, cerca le frasi scritte **in inglese**, cioè quelle che un portafoglio genera per impostazione predefinita quasi ovunque.

Va detto con onestà, perché nella puntata precedente avevamo consigliato di scaricare solo dagli store ufficiali e quel consiglio resta valido: scaricare dallo store **riduce** il rischio, non lo azzera. La differenza è che qui il negozio non era il punto debole, lo era la fotografia. Se quella foto non fosse esistita, l’app infetta avrebbe trovato una galleria senza niente da leggere.

Perché il permesso che gli hai dato sembrava ragionevole?

Perché arrivava in un momento in cui concedere l'accesso alle foto ha perfettamente senso: quando apri la chat di assistenza. Non era l'unico momento — in alcune app il permesso scattava all'avvio della funzione principale — ma quello ricorrente era l'assistenza, dove è normale allegare una schermata per spiegare un problema. Se lo negavi, in certe configurazioni la richiesta tornava. Kaspersky lo dice con una formula che vale la pena rileggere: i permessi richiesti *sembrano ragionevoli*, ed è proprio questo che li rende facili da ignorare.

Chi segue questa rubrica riconoscerà la forma. Nella seconda puntata qualcuno fingeva di essere l'assistenza e ti chiedeva la frase. Qui l'assistenza è vera, l'app funziona davvero e non ti viene chiesto niente di sensibile: solo le foto, nel solo momento della giornata in cui quella richiesta non è sospetta. La leva è la stessa, ma stavolta non c'è nessuno da smascherare.

Una fotografia resta davvero nel telefono?

No, e questa è la parte che quasi tutti sottovalutano: una foto nasce già in più copie. I telefoni sincronizzano la galleria in automatico, perché è esattamente quello che vogliamo quando rompiamo lo schermo. Nel giro di pochi minuti l'immagine del foglio esiste sul telefono, sul servizio in rete collegato all'account e spesso sul computer di casa che ha la stessa libreria. Tre posti, nessuno dei quali hai scelto. Con tre conseguenze:

- **Cancellare dal rullino non basta.** Resta nel cestino per settimane, e resta nelle copie già sincronizzate altrove.
- **L'album nascosto non è una cassaforte.** È un'etichetta che cambia dove l'immagine compare quando sfogli: il file resta un file, e un programma che legge i file non sfoglia niente.
- **La sicurezza della foto coincide con quella dell'account**, non con quella del telefono. Chi entra nell'account entra nella libreria, senza toccare il dispositivo che hai in tasca.

Vale identico per le note, per le mail che ci mandiamo da soli e per i messaggi salvati: nascono già duplicati, perché la duplicazione è la funzione che paghiamo. Per qualunque altra cosa è un vantaggio. Per queste dodici parole è il problema.

Quante persone come te, davvero?

Più che mai, e con cifre individuali più piccole che mai. Nel rapporto annuale pubblicato a dicembre 2025, Chainalysis conta **158.000 episodi** su portafogli personali nel 2025 e almeno **80.000 persone colpite**. Eppure il valore complessivamente sottratto ai privati *scende*: 713 milioni di dollari, contro il miliardo e mezzo del 2024.



L'unico numero che scende è quello che conta di meno per te: il totale. Fonte: Chainalysis, Crypto Crime Report 2026 (dicembre 2025).

Letti insieme dicono una cosa sola: **più bersagli, cifre più piccole ciascuno**. Per un privato il significato pratico è chiaro e scomodo: non serve avere molto per rientrare nell'elenco, perché nessuno ti ha scelto. Un programma che legge fotografie non sa quanto vali: raccoglie, e poi si guarda cosa è arrivato.

Una precisazione, perché questa rubrica preferisce i numeri onesti a quelli comodi. La quota dei portafogli personali sul totale rubato nell'anno passa dal 44% del 2024 al 20% del 2025, ma quel calo è un effetto ottico: nel 2025 un singolo episodio su una grande piattaforma vale un miliardo e mezzo di dollari e gonfia il denominatore. Senza quell'episodio la quota sarebbe stata del 37%. Il fenomeno che riguarda te non si è ridotto: è stato coperto da uno più grande.

Dove si conserva qualcosa che non si può né cambiare né recuperare?

Fuori dalla rete, in più di un posto, e in una forma che sopravviva a te che te ne dimentichi. La scelta non è fra sicuro e insicuro, ma fra due rischi diversi. Quello digitale è remoto, automatico e ripetibile su centomila persone

insieme. Quello fisico — il foglio che brucia, l'allagamento, il trasloco — per colpirti richiede che qualcuno venga da te, di persona. Mettere la frase su carta non elimina il pericolo: lo sposta su un terreno dove i numeri sono dalla tua parte.

In pratica, in ordine di quanto costano:

1. **Carta, scritta a mano, in due o tre posti diversi.** Non due copie nello stesso cassetto: due *luoghi*. Costa zero ed è già meglio di qualunque soluzione digitale.
2. **Una piastra di metallo** su cui incidere o comporre le parole. Serve contro le due cose che distruggono la carta, cioè l'acqua e il fuoco, e costa qualche decina di euro. Ha senso quando l'importo giustifica il pensiero.
3. **Un dispositivo dedicato** per la custodia, dove la frase nasce offline e non viene mai digitata su un computer. È la scelta sensata quando le cifre diventano importanti, e sposta il problema dalla frase al dispositivo.

Qualunque strada scegli, resta un passaggio che quasi nessuno fa e che vale più della scelta stessa: **decidi chi la trova se tu non ci sei**. Un nascondiglio che non conosce nessuno funziona benissimo finché funzioni tu. L'altro, la prova di ripristino, è il secondo punto della checklist in testa: la fiducia non restituisce i fondi se hai sbagliato a trascrivere la settima parola.

> **LA PAROLA CHE NON STA SUL FOGLIO**
>
> Molti portafogli permettono di aggiungere alla frase una *passphrase*: una parola o una sequenza in più, decisa da te, senza la quale le dodici parole aprono un portafoglio diverso e vuoto. Il vantaggio è evidente — chi trova il foglio non trova i fondi — ma il prezzo lo è altrettanto: se la dimentichi, hai perso tutto, e stavolta senza nessuno da incolpare. Ha senso solo se quella parola ha una sua custodia, separata e altrettanto seria. Non è un trucco per rendere innocua una frase conservata male.

Che cosa non ti salva, anche se sembra prudente?

Quasi tutte le soluzioni intermedie, cioè quelle che tengono insieme la comodità del digitale e l'illusione della protezione. Sono i gesti più comuni fra le persone attente, ed è esattamente per questo che meritano un elenco esplicito.

IL GESTO PRUDENTE	PERCHÉ SEMBRA SICURO	DOVE CEDE
La foto in un album nascosto	Non compare quando sfogli la galleria	È un'etichetta, non una serratura: il file resta leggibile come gli altri
Le parole divise in due posti	Nessuna metà basta da sola	Metà frase riduce di molto il lavoro di chi la trova, e se perdi un pezzo hai perso tutto
Il gestore di password	È cifrato e ci tieni già tutto il resto	È raggiungibile dalla rete, e una sola password apre l'intero archivio
Una mail inviata a te stesso	La ritrovi sempre, da qualunque dispositivo	Resta per anni su un server che non è tuo, e in due caselle invece che in una
Impararla a memoria	Non c'è niente da rubare	Dodici parole in ordine esatto non reggono gli anni, e la memoria non si lascia in eredità

Le soluzioni intermedie e il punto esatto in cui cedono

Il filo comune è uno solo: **ogni volta che la frase diventa un file, eredita tutto quello che succede ai file**. Si copia da sola, si sincronizza, finisce nei backup, sopravvive alla cancellazione e si può cercare. Nessuna di queste proprietà è un difetto del tuo telefono: sono le funzioni per cui lo hai comprato.

Che fare nei primi dieci minuti, se l'hai già esposta?

Parti dal presupposto peggiore e muoviti nell'ordine, perché qui l'ordine conta più della velocità.

1. **Considera quel portafoglio perso, anche se adesso è intatto.** Un saldo ancora al suo posto non prova niente: come abbiamo visto, chi ha la frase può aspettare mesi. Non è una ragione per rimandare, è la ragione per muoversi ora.
2. **Crea un portafoglio nuovo su un dispositivo pulito**, e genera lì una frase nuova che non passerà mai da uno schermo fotografabile. Se il sospetto riguarda il telefono, usa un altro dispositivo: non quello.
3. **Sposta prima ciò che vale di più.** Non in ordine alfabetico e non partendo dalle posizioni facili: in ordine di valore. Se una parte è vincolata o in attesa, spostala appena si libera, e nel frattempo tratta il resto come già perso.
4. **Togli la fotografia da ogni copia**, non solo dal telefono: rullino, cestino, libreria sincronizzata, computer di casa, backup. E cambia la password dell'account collegato alla libreria, perché da lì si entra nella galleria senza toccare il dispositivo.
5. **Documenta e denuncia.** Data e ora, app coinvolte, indirizzi di destinazione, schermate, identificativi delle operazioni. Non ripulire niente prima di aver copiato tutto: serve per la denuncia, e la denuncia — come vedi qui sotto — ha anche un effetto fiscale concreto.

Una cosa che invece **non** devi fare: non cercare servizi che promettono di recuperare fondi sottratti. Non esistono, e chi ha appena perso dei soldi è il bersaglio più facile per il secondo giro — che è poi il meccanismo raccontato nella seconda puntata di questa rubrica.

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. Il risultato è il cornuto e mazziato in forma pura: il portafoglio è vuoto, in dichiarazione quella perdita non vale niente, e senza denuncia devi continuare a monitorare un bene che non hai più. La denuncia fa cadere almeno quest'ultimo pezzo.

> **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 una complicazione che qui pesa più che nelle altre puntate. Quando viene compromessa la frase non si svuota un indirizzo: si svuotano **tutti** quelli nati da quella frase, spesso su catene diverse e in momenti diversi. Ricostruire che cosa possedevi, dove e fino a quando diventa un lavoro di settimane proprio quando hai meno voglia di farlo. Con **MoneyViz** ogni valore resta tracciabile fino alla singola operazione che l'ha generata. 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?

Le password deboli e il secondo fattore aggirato. Questa puntata ha riguardato la chiave che non si può cambiare; la prossima riguarda quelle che si cambiano, e che proprio per questo vengono trascurate: come si arriva a un conto partendo da una password riusata, perché il codice via SMS non è la protezione che credi, e che cosa succede quando qualcuno convince il tuo operatore telefonico a spostare il tuo numero.

Torniamo alla fotografia. Non l'hai scattata per distrazione: l'hai scattata perché avevi capito benissimo che quelle parole erano importanti e che la carta si perde. Hai fatto una copia di sicurezza, cioè la cosa giusta, nell'unico posto che il telefono ti offriva. Il problema non è stata la tua leggerezza, è stato che quel posto si sincronizza da solo, è raggiungibile da un account e può essere letto da un programma che cerca la parola «mnemonico» in nove lingue, italiano compreso.

Per questo la difesa non chiede di diventare più diffidenti, e nemmeno di spendere. Chiede due gesti, in quest'ordine: **scrivi quelle parole su un foglio e verifica che siano giuste**, e **solo allora togli la fotografia da tutte le copie**. Non il contrario: se quella foto è l'unica copia che hai, cancellarla per prima ti fa perdere il portafoglio senza bisogno di nessun altro. E se è rimasta nella galleria per mesi, toglierla chiude il rischio da qui in avanti, non quello già corso: in quel caso la frase va considerata vista e il portafoglio va rifatto da zero. Fatto questo, 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
> 5. **La frase di recupero esposta** — questa puntata
> 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

- Kaspersky Securelist — l'analisi della campagna SparkCat: lettura del testo nelle immagini della galleria, oltre 242.000 download su Google Play, primo caso nell'App Store
- Kaspersky (2 aprile 2026) — una nuova versione dello stesso componente, due app nell'App Store e una su Google Play; la variante iOS cerca le frasi in inglese
- Chainalysis — Crypto Crime Report 2026: 158.000 episodi su portafogli personali nel 2025, almeno 80.000 persone colpite, 713 milioni di dollari
- The Register — la cronaca della rimozione delle app dai due negozi, il 6 e il 7 febbraio 2025
- MetaMask — che cosa l'assistenza non chiede mai, e perché la frase di recupero non si digita su richiesta altrui
- Trezor — che cosa fare e che cosa non fare con la frase di recupero: mai una fotografia, mai una mail, mai un gestore di password; copie in luoghi distinti, metallo contro acqua e fuoco, e l'accesso previsto nel lascito
- BIP-39 — lo standard che definisce le parole mnemoniche e il modo in cui da esse si ricavano le chiavi
- 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 la frase di recupero e perché non si può cambiare?

Non è una credenziale che apre il portafoglio: è il portafoglio. Quelle dodici o ventiquattro parole sono il seme da cui vengono calcolate tutte le tue chiavi, quindi chi le possiede può ricostruire indirizzi, saldi e facoltà di firmare su qualunque dispositivo, senza il tuo telefono. Non esiste un pulsante per generarne una nuova sullo stesso portafoglio: l’unica risposta possibile è crearne uno diverso e spostare tutto.

È sicuro fotografare la frase di recupero se poi cancello la foto?

No, perché una foto nasce già in più copie. La galleria si sincronizza in automatico, quindi nel giro di pochi minuti quell’immagine esiste sul telefono, sul servizio in rete collegato all’account e spesso sul computer di casa. Cancellarla dal rullino non tocca il cestino né le copie già sincronizzate, e l’album nascosto è un’etichetta, non una serratura: il file resta leggibile come gli altri. E se quella foto c’è già stata, cancellarla chiude il rischio da qui in avanti, non quello già corso: non puoi sapere chi l’ha letta, e quelle parole non si cambiano.

Posso tenere la frase di recupero nel gestore di password?

È sconsigliato, ed è una delle indicazioni esplicite dei produttori di portafogli. Il gestore è cifrato, ma è raggiungibile dalla rete e una sola password apre l’intero archivio: concentri in un punto solo le credenziali e la chiave che non puoi cambiare. Per la frase di recupero la regola è un’altra: fuori dalla rete, su carta o metallo, in due o tre luoghi diversi.

Un programma può davvero leggere il testo dentro una fotografia?

Sì, ed è successo. Nel febbraio 2025 Kaspersky ha documentato una campagna attiva almeno dal marzo 2024 in cui un componente inserito in app presenti su Google Play e App Store passava le immagini della galleria a un riconoscimento del testo e inviava solo quelle contenenti certe parole chiave. L’elenco era in nove lingue e comprendeva l’italiano, con la parola «Mnemonico». Le app infette su Google Play erano state scaricate oltre 242.000 volte.

Ho fotografato la frase di recupero: che cosa faccio adesso?

Tratta quel portafoglio come perso, anche se il saldo è ancora al suo posto: chi ha la frase può aspettare mesi prima di usarla. Crea un portafoglio nuovo su un dispositivo pulito, sposta prima ciò che vale di più, poi togli la fotografia da ogni copia — rullino, cestino, libreria sincronizzata, computer, backup — e cambia la password dell’account collegato alla libreria. Infine documenta tutto e presenta denuncia.

Se mi hanno svuotato il portafoglio, 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.