23 NOVEMBRE 2026 • 15 MIN DI LETTURA • DANILO GIUDICE

Usi un codice via SMS? Perché non basta a proteggere le tue crypto

Una password riusata non viene indovinata: viene letta da un elenco. E il codice che ti arriva via SMS dipende da un numero che qualcuno può farsi spostare su un’altra SIM, come dicono i dati europei del 2026. Che cosa funziona davvero, in ordine e senza comprare nulla. Puntata 6 di Anatomia di una truffa, la rubrica di sicurezza di MoneyViz.



PERCHÉ TI RIGUARDA

- Una password riusata non viene *indovinata*: viene **letta da un elenco**. Basta che una sia finita nella violazione di un sito qualsiasi, e quella coppia mail-password viene provata in automatico su migliaia di servizi
- Il codice via SMS **è meglio di niente, ed è il più debole dei secondi fattori**: non dipende da te, ma da un numero che qualcuno può far spostare su un’altra SIM
- Non è teorico: i dati europei verificati alla fonte da **MoneyViz** dicono che nel primo semestre 2026 le sostituzioni di SIM non autorizzate sono passate **dal 2% al 10% delle segnalazioni di frode**, e servono proprio a **intercettare i codici**
- L’allarme ce l’hai in tasca: **il telefono che resta senza linea** senza motivo
- La difesa non chiede di comprare niente: **password lunghe e diverse una per sito**, e **i codici spostati dall’SMS a un’applicazione**. È la sesta 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. L'ordine conta: **si parte dalla casella di posta**, perché da lì si rimettono a posto tutte le altre.
>
> 1. **Metti in sicurezza prima la mail, poi il conto.** La casella di posta non è un account come gli altri: è quello da cui si reimpostano gli altri. Password nuova, lunga e usata solo lì, e secondo fattore attivo.
> 2. **Controlla quali tue password sono già in circolazione.** Esistono servizi gratuiti che lo verificano senza ricevere la password: dal tuo dispositivo escono solo i primi cinque caratteri della sua impronta, e il confronto finisce in locale. Se una risulta già vista, cambiala dove l'hai usata.
> 3. **Sposta i codici dall'SMS a un'applicazione di autenticazione.** Si fa dalle impostazioni di sicurezza del conto, costa zero e toglie di mezzo l'intero problema del numero di telefono. Dove è disponibile, una chiave fisica o una *passkey* è un gradino ancora sopra.
> 4. **Non ignorare l'SMS del tuo operatore.** Se ti avvisa di una sostituzione di SIM o di una portabilità che non hai chiesto, quello è l'unico momento utile: per le regole italiane devi poter fermare la procedura, e come farlo deve essere scritto in quel messaggio e sul sito dell'operatore.
>
> Se temi che sia già in corso, vai direttamente a che fare nei primi dieci minuti. E se non sai da dove cominciare, o vedi un movimento che non ti torna, **chiedi a noi**: è esattamente il tipo di domanda che l'assistenza di **MoneyViz** riceve tutti i giorni.

Immagina di guardare il telefono e di vedere, al posto delle tacche, la scritta «Nessun servizio». Capita: in ascensore, in treno, in una valle. Si riavvia e passa. **Tieni a mente quella barra vuota, perché ci torniamo alla fine.**

In questa sesta puntata di **Anatomia di una truffa**, la rubrica di sicurezza di **MoneyViz**, parliamo delle chiavi che si possono cambiare: la password e il codice di verifica. La puntata precedente riguardava l'unica cosa che non si cambia. Queste si cambiano in un minuto — ed è proprio per questo che nessuno le cambia.

Perché una password riusata è già in mano a qualcun altro?

Perché non viene indovinata: viene letta. Quando un sito qualunque — un forum, un negozio online, un servizio che hai usato una volta nel 2017 — subisce una violazione, le coppie di mail e password finiscono in elenchi che circolano. A quel punto nessuno sta provando a entrare nel *tuo* conto: un programma prova quelle stesse coppie su centinaia di servizi diversi, in automatico, e si ferma dove funzionano. Se la password del conto cripto è la stessa del forum, il lavoro è già finito.

È la ragione per cui «una password diversa per ogni sito» non è pignoleria: è l'unica cosa che impedisce a una violazione altrui di diventare un problema tuo. In Italia la Polizia Postale, nel report annuale 2025, scrive che le truffe passano soprattutto da campagne di phishing — anche nelle varianti telefonica e via SMS — il cui obiettivo è l'acquisizione di dati personali «nonché password e credenziali di accesso». Nello stesso anno il cybercrime economico-finanziario ha prodotto **27.085 procedimenti** e **oltre 269 milioni di euro** sottratti.

Un numero onesto anche quando è scomodo: nel rapporto Verizon 2026 le password rubate hanno *perso* il primo posto fra le vie d'ingresso, superate dalle vulnerabilità del software (31% dei casi). Restano la seconda porta. E sui dispositivi mobili il tasso di clic è **superiore del 40%**: il messaggio che inganna funziona meglio sul telefono.

Che cosa è cambiato nelle regole su come si fa una password?

Che la lunghezza ha battuto la complessità, ufficialmente. Le linee guida del NIST, l'istituto di standard statunitense che di fatto detta le regole anche fuori dagli Stati Uniti, nella versione aggiornata chiedono **almeno 15 caratteri** per una password usata da sola, ammettono il minimo di otto solo quando c'è un secondo fattore, impongono di accettarne **almeno 64** e dicono una cosa che suona ancora controintuitiva: **non imporre regole di composizione**. Maiuscola, numero e simbolo obbligatori non producono password robuste, producono «Password2026!».

Lo stesso documento chiede a chi gestisce un servizio di confrontare le password scelte con **un elenco di password già comparse nelle violazioni**: il problema non è la fantasia, è la ripetizione.

> **QUATTRO PAROLE CHE NON C'ENTRANO NIENTE**
>
> Il modo pratico di avere una password lunga e ricordabile è una fila di parole senza legame fra loro: *tram-basilico-ferro-quaranta* è più facile da ricordare e più difficile da ritrovare in un elenco di «Giulia1985!». Le parole vanno scelte male, cioè senza senso: un verso di una canzone o i nomi dei figli in fila stanno negli elenchi come tutto il resto. Serve per i pochi accessi che devi ricordare a memoria — la posta, il computer, il gestore delle altre password. Per le decine di account restanti il gestore le genera lui, diverse una per sito.

Perché il codice via SMS è il punto debole?

Perché non protegge te, protegge un numero di telefono — e quel numero può cambiare SIM senza che tu partecipi. Partiamo da una cosa giusta, però: **un conto con il codice via SMS è molto più difficile da svuotare di un conto con la sola password.** Se oggi hai solo quello, non toglierlo. Il punto è che esiste un gradino sopra, gratis.

Che l'SMS sia il piano più fragile non è un'opinione. Il NIST classifica l'uso della rete telefonica per i codici di verifica come **autenticatore «limitato»**, e nella sua tabella delle minacce mette, fra gli esempi, esattamente questo: un codice inviato via SMS che arriva a chi *ha convinto l'operatore telefonico a dirottare il numero della vittima*. Nello stesso documento raccomanda a chi offre un servizio di considerare come indicatori di rischio il cambio di dispositivo, **la sostituzione della SIM** e il trasferimento del numero.

Che succede quando quel consiglio non viene seguito lo sappiamo per esperienza altrui. Fra marzo e il 20 maggio 2021 **almeno 6.000 clienti** di una grande piattaforma di scambio cripto si sono visti svuotare il conto: non era stata violata l'azienda, era stato sfruttato un difetto nella **procedura di recupero via SMS**. Lo si sa con precisione perché la lettera di notifica inviata ai clienti è depositata presso il Procuratore generale della California: un documento, non una ricostruzione.

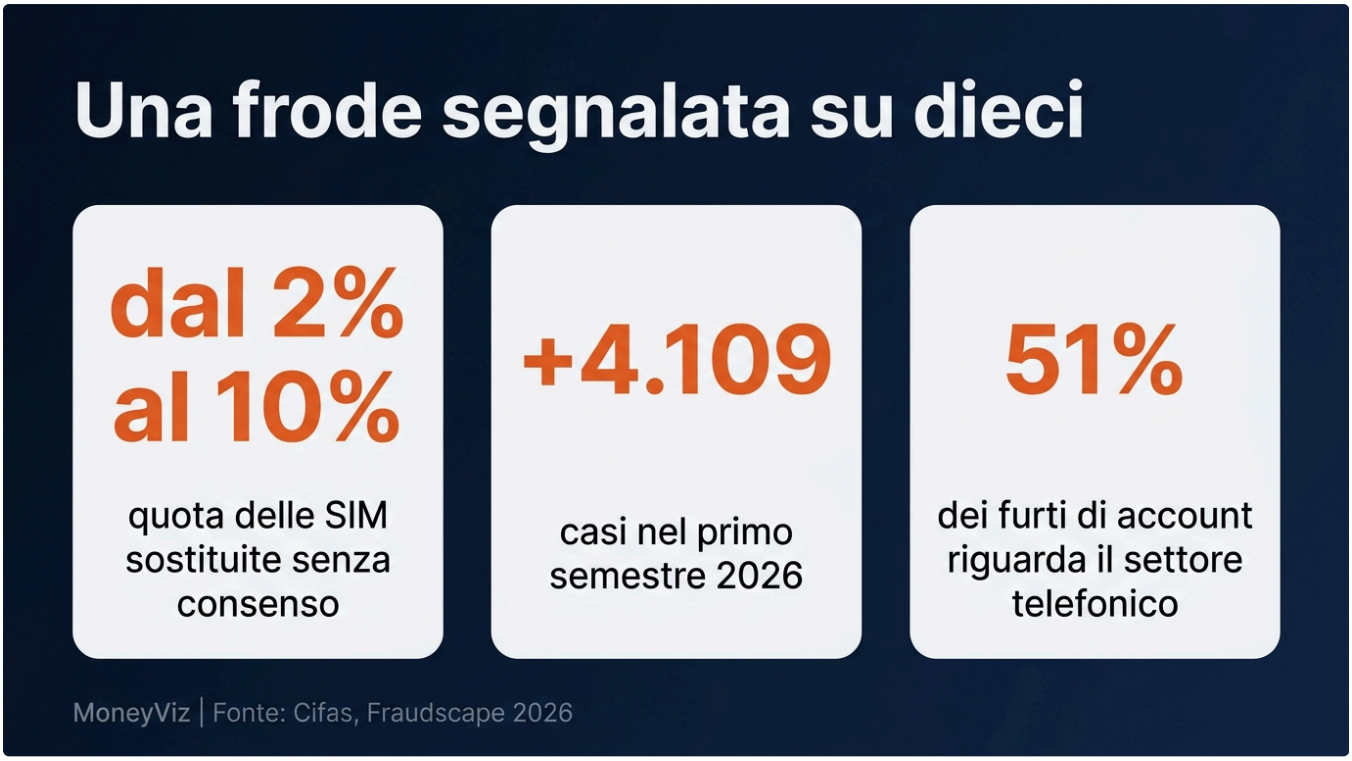


I cinque passaggi con cui un numero cambia SIM. L'unico in cui puoi intervenire è il terzo, e dura pochi minuti. Fonte: ricostruzione MoneyViz sulle procedure fissate dalla delibera AGCOM 86/21/CIR.

Quanto è diffuso lo scambio di SIM?

Abbastanza da essere diventato una voce a sé nelle statistiche europee sulle frodi. I dati migliori li pubblica Cifas, il servizio antifrode britannico che gestisce il registro nazionale delle segnalazioni. La serie, anno per anno, dice questo: **+1.055% nel 2024**, con quasi 3.000 casi; **+38% nel 2025**, in un anno da 444.993 segnalazioni totali; **+402% nel primo semestre 2026**, cioè 4.109 casi in più rispetto allo stesso periodo dell'anno prima.

Quelle percentuali vanno lette con prudenza: nascono da basi piccole, e un +1.055% fa più rumore di quanto pesi. La misura onesta è un'altra e dice la stessa cosa più sobriamente: le sostituzioni di SIM non autorizzate sono passate **dal 2% al 10% di tutte le segnalazioni di frode** del registro. Una su dieci. Cifas scrive anche *a che cosa servono*: a **intercettare i codici di autenticazione**, aggirare le misure di sicurezza e arrivare ad altri account. Non sono il fine, sono il mezzo.



La quota, non la percentuale di crescita: è il numero che resta vero anche quando la base è piccola. Fonte: Cifas, Fraudscape 2026 e aggiornamento semestrale.

Che la responsabilità non sia tutta del cliente lo ha stabilito anche un arbitrato: nel marzo 2025 è diventato pubblico un lodo da 33 milioni di dollari contro un grande operatore americano, pagato per le proprie mancanze di sicurezza in uno scambio di SIM finito in un furto di cripto. Dagli atti esce la cosa che conta per te: quando la sostituzione avviene, **il telefono della vittima viene staccato dalla rete** e chiamate e messaggi vanno all'apparecchio di chi ha fatto la richiesta.

In Italia che protezioni hai già, e che cosa tocca a te?

Ne hai più di quante immagini, ma funzionano solo se rispondi a un messaggio. Dal 2021 la delibera AGCOM 86/21/CIR ha cambiato le procedure di sostituzione della SIM e di passaggio a un altro operatore proprio per contrastare queste truffe. L'Autorità stessa spiega il motivo senza giri di parole: una SIM sostituita da un terzo non autorizzato permette anche un «furto per via telematica presso gli istituti bancari».

In pratica, oggi, in Italia:

1. **La validazione non è più facoltativa.** Prima era lasciata all'operatore, ora è un obbligo: per SIM rubata, smarrita o guasta **l'operatore deve sempre inviarti un SMS o chiamarti**.
2. **La finestra è corta.** Dopo l'SMS l'attesa minima prevista è di **cinque minuti**; se il canale è un codice temporaneo, l'attesa è la durata del codice.
3. **Devi poter dire no, in modo semplice.** Le regole impongono una procedura immediata per fermare una sostituzione indesiderata: rispondere negativamente al messaggio, mandare un SMS a un numero prestabilito *uguale per tutti gli operatori*, chiamare l'assistenza o usare l'area riservata. Le modalità esatte devono essere scritte in quel messaggio e restare facili da trovare sul sito dell'operatore.

4. **Per il cambio operatore, senza la tua conferma il processo si blocca.** Quando la richiesta entra nei sistemi sei chiamato a confermarla: in mancanza, l'iter non prosegue.

Da qui la conseguenza pratica, che vale più di qualunque impostazione: **quell'SMS non è spam**. È l'unico avviso che riceverai, arriva mentre la cosa sta succedendo, e ignorarlo è l'errore costoso.

E se il secondo fattore è un'applicazione, la storia finisce?

Non del tutto, ed è giusto dirlo invece di vendere una sicurezza che non esiste. Spostare i codici su un'applicazione elimina il problema del numero di telefono, che è il più grosso. Resta un altro modo di aggirare il secondo fattore, che non ruba il codice: ruba la *sessione*.

Nel luglio 2022 Microsoft ha documentato una campagna che ha tentato di colpire **oltre 10.000 organizzazioni**. Il meccanismo: una pagina di accesso identica all'originale, che fa da ponte verso il sito vero in tempo reale. Digiti la password e la pagina la gira al sito; il sito chiede il codice, lo digiti, gira anche quello. Entri davvero, tutto funziona. Solo che chi ha costruito il ponte si tiene il **biglietto di sessione**, la prova che sei già dentro, e con quello entra senza password né codici. Microsoft lo precisa: *non è un difetto dell'autenticazione a due fattori*, è un furto di quello che viene dopo.

È qui che le chiavi fisiche e le *passkey* smettono di essere un lusso da appassionati: sono legate al dominio del sito vero, quindi su una pagina clone il tuo dispositivo si rifiuta di rispondere.

CHE COSA USI	DA CHE COSA TI DIFENDE	DOVE CEDE
Solo la password	Da niente, se quella password è in un elenco	Alla prima prova automatica di una coppia mail-password riusata
Codice via SMS	Dalla password rubata e usata da sola: già un salto enorme	Quando il numero cambia SIM, o quando il codice viene chiesto da una finta assistenza
Applicazione di autenticazione	Anche dallo scambio di SIM: il codice nasce sul tuo dispositivo, senza passare dalla rete telefonica	Davanti a una pagina clone in tempo reale, che fa digitare il codice e si tiene la sessione
Chiave fisica o *passkey*	Anche dalla pagina clone: la risposta è legata al dominio del sito vero	Resta la custodia dell'oggetto e del dispositivo, e il recupero dell'accesso se li perdi: serve una seconda chiave

I secondi fattori, dal più debole al più robusto

Che cosa non ti salva, anche se sembra prudente?

Quasi tutte le abitudini che abbiamo imparato quindici anni fa, e che oggi sopravvivono per inerzia.

- **Il punto esclamativo in fondo, e il cambio ogni tre mesi.** «Password» con la maiuscola, un 1 e un punto esclamativo è la prima variante che un programma prova dopo «password»; e il cambio periodico obbligatorio

produce solo password numerate in fila. Si cambia quando c’è un motivo: una violazione, un accesso che non riconosci.

- **La domanda di sicurezza.** Il cognome di tua madre e la città di nascita non sono segreti. Dove è obbligatoria, trattala come una seconda password: una risposta senza senso.
- **Tenere nel gestore di password anche la frase di recupero del portafoglio.** Qui serve un dato, non un’opinione: nel marzo 2025 un atto federale statunitense ha ricostruito il furto di 283 milioni di XRP — circa 150 milioni di dollari al momento del colpo — scrivendo che la dinamica era *coerente con le violazioni di un gestore di password online* e con i furti subiti da altre vittime nella stessa situazione; l’azienda coinvolta dichiara di non avere prove conclusive del collegamento. Il gestore resta la scelta giusta **per le password**, che si cambiano; non per la frase di recupero, che non si cambia ed è il tema della puntata precedente.

Che fare nei primi dieci minuti, se sta succedendo adesso?

Il segnale di partenza è il telefono che perde la linea senza una ragione. Se ti accorgi che il numero è muto e intorno a te gli altri telefoni funzionano, muoviti in questo ordine.

1. **Chiama il tuo operatore da un altro telefono** e chiedi se risulta una sostituzione di SIM o una portabilità in corso. Se c’è e non l’hai chiesta tu, chiedi il blocco immediato: è la procedura che le regole AGCOM impongono di mettere a disposizione.
2. **Dall’altro dispositivo, cambia la password della casella di posta**, non del conto: la mail è la chiave da cui si reimposta tutto il resto.
3. **Poi il conto: password nuova e sessioni attive chiuse.** Chiudere le sessioni è il passaggio che quasi tutti dimenticano, ed è l’unico che annulla un accesso già ottenuto.
4. **Togli l’SMS dal secondo fattore** e mettici un’applicazione: finché il numero è in mano a qualcun altro, ogni codice via SMS arriva a lui.
5. **Documenta e denuncia.** Data e ora, schermate, indirizzi di destinazione, identificativi delle operazioni. La denuncia si presenta alla Polizia Postale, anche dal portale del Commissariato di P.S. online, che nel 2025 ha gestito oltre 94.000 segnalazioni. Non ripulire niente prima di aver copiato tutto: 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 — il meccanismo raccontato nella seconda puntata di questa rubrica.

Dal punto di vista fiscale, quella perdita conta?

No, e il meccanismo è lo stesso della puntata scorsa: il furto non è una cessione, quindi non genera né plusvalenza né minusvalenza. Quando le cripto escono dal tuo conto 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 usare 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, e le operazioni fatte prima restano da dichiarare.

Sul monitoraggio, invece, 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, quelle cripto risultano ancora tue e vanno dichiarate. Qui il vecchio detto ci sta tutto: **cornuti e mazziati**. Il conto è stato svuotato grazie a un codice di sei cifre che il tuo operatore ha consegnato a un telefono che non è il tuo; in dichiarazione quella perdita non vale un euro; e se non denunci sei anche l'unico a dover tenere il conto di ciò che non hai 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 un lavoro che nessuno considera finché non gli capita: ricostruire che cosa possedevi e quando, perché un conto svuotato in pochi minuti lascia uno storico spezzato a metà. Con **MoneyViz** ogni valore resta tracciabile fino alla singola operazione che l'ha generata: se è successo a te, **chiedi a noi**.

Che cosa vediamo nella prossima puntata?

L'address poisoning. Questa puntata ha riguardato le chiavi d'accesso; la prossima riguarda un trucco che non ha bisogno di nessuna chiave, perché sfrutta un gesto che facciamo tutti: copiare un indirizzo dalla cronologia delle operazioni invece di controllarlo. Un indirizzo somigliante al tuo, piazzato nella tua cronologia con una micro-transazione, e un pagamento che parte verso il posto sbagliato.

Torniamo alla barra senza tacche. Quasi sempre non sarà niente: un ascensore, una galleria, un'antenna in manutenzione. Ma ora sai che in rari casi quella barra vuota non è un disservizio, è **il momento esatto in cui il tuo numero ha cominciato a rispondere a qualcun altro** — e sai anche che in Italia, poco prima, un SMS ti aveva chiesto il permesso.

Per questo la difesa non chiede di diventare diffidenti, e nemmeno di spendere. Chiede due gesti, in quest'ordine: **una password lunga e diversa sulla casella di posta**, e **il secondo fattore spostato dall'SMS a un'applicazione**. Il resto — la chiave fisica, la lista degli indirizzi di prelievo autorizzati, la chiave di scorta — è rifinitura. Fatti quei due, 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
6. **Password deboli e secondo fattore aggirato** — questa puntata
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

- NIST SP 800-63B — le linee guida sull'autenticazione: almeno 15 caratteri per una password usata da sola, nessuna regola di composizione, confronto con gli elenchi di password violate, e l'uso della rete telefonica per i codici classificato come «limitato»
- Lettera di notifica ai clienti depositata presso il Procuratore generale della California — almeno 6.000 conti svuotati fra marzo e il 20 maggio 2021 sfruttando la procedura di recupero via SMS
- Cifas, Fraudscape 2026 e aggiornamento semestrale — sostituzioni di SIM non autorizzate dal 2% al 10% delle segnalazioni, +4.109 casi nel primo semestre 2026, telecomunicazioni al 51% delle prese di controllo
- Cifas — il +1.055% del 2024 e i quasi 3.000 casi segnalati al registro nazionale delle frodi
- AGCOM, delibera 86/21/CIR — controlli e notifiche obbligatorie nella sostituzione della SIM e nel passaggio ad altro operatore
- Polizia Postale, Report annuale 2025 — 27.085 procedimenti per cybercrime economico-finanziario, oltre 269 milioni di euro sottratti, phishing e sue varianti come modalità principale
- Microsoft — la campagna che ha tentato di colpire oltre 10.000 organizzazioni rubando il biglietto di sessione invece del codice
- Il lodo arbitrale da 33 milioni di dollari del marzo 2025 contro un operatore telefonico per le mancanze di sicurezza in uno scambio di SIM
- Verizon, rapporto 2026 sulle violazioni di dati — il 31% parte da una vulnerabilità del software, e sui dispositivi mobili il tasso di clic è superiore del 40%
- Have I Been Pwned — il controllo gratuito delle password già comparse nelle violazioni, con il metodo che non trasmette la password
- MoneyViz — quadro RW crypto 2026: guida completa alla compilazione
- MoneyViz — quadro RT crypto 2026: come si compila

Domande frequenti

Che cos’è lo scambio di SIM e come fanno a prendersi il mio numero?

È la sostituzione della tua SIM chiesta all’operatore da qualcun altro, che si presenta come te con i tuoi dati personali. Se la richiesta passa, il tuo numero smette di funzionare sul tuo telefono e chiamate e messaggi, compresi i codici di verifica, arrivano sulla scheda di chi ha fatto la richiesta. In Italia le regole AGCOM impongono all’operatore di avvisarti e di darti un modo semplice per fermare la procedura: quell’avviso è l’unico momento in cui puoi intervenire.

Il codice via SMS è meglio di niente?

Sì, ed è importante dirlo: un conto con la sola password è molto più esposto di un conto con un codice via SMS. Resta però il più debole dei secondi fattori, perché non dipende da te ma da un numero che può essere spostato su un’altra SIM. Lo standard NIST americano lo classifica come autenticatore «limitato» proprio per questo. Se puoi scegliere, un’applicazione di autenticazione costa zero ed è su un altro piano.

Quanto deve essere lunga una password, e serve metterci i simboli?

Conta più la lunghezza della complessità. Le linee guida NIST aggiornate chiedono almeno 15 caratteri per una password usata da sola, ammettono il minimo di 8 solo quando c’è un secondo fattore, impongono di accettarne almeno 64 e dicono esplicitamente di non imporre regole di composizione: maiuscole, numeri e simboli obbligatori producono password prevedibili e difficili da ricordare. Quattro o cinque parole senza legame fra loro valgono più di «Password2026!».

Posso tenere le password in un gestore di password?

Sì, per le password è la scelta sensata: è il modo pratico per averne una diversa su ogni sito senza ricordarle. Vale però una distinzione che questa rubrica ha già fatto: le password si cambiano, la frase di recupero del portafoglio no. Per quella la regola resta un’altra, fuori dalla rete e su carta o metallo, come nella puntata precedente.

Come faccio a sapere se una mia password è già finita in una violazione?

Esistono servizi gratuiti che confrontano la password con gli elenchi già circolanti senza riceverla: il controllo avviene per k-anonimità, cioè dal tuo dispositivo escono solo i primi cinque caratteri dell’impronta della password e il confronto finale avviene in locale. Le stesse linee guida NIST chiedono a chi gestisce un servizio di fare questo controllo. Se una password risulta già vista, va cambiata dove l’hai usata, partendo dalla casella di posta.

Se mi svuotano il conto, 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.