QR Code Phishing Ledger: lettere truffa con codici QR colpiscono i possessori di crypto wallet



Il *QR code phishing* contro i possessori di hardware wallet Ledger rappresenta una delle convergenze più significative emerse nel panorama del *cybercrime* nel 2026: l'uso della posta tradizionale – il vettore di comunicazione più antico e apparentemente innocuo – per colpire i detentori di dispositivi crittografici, il target più tecnologicamente avanzato dell'ecosistema finanziario digitale.

A partire da febbraio 2026, possessori di dispositivi Ledger e Trezor hanno iniziato a ricevere lettere cartacee (*scam letters*) che riproducono fedelmente la comunicazione ufficiale dei due produttori, complete di loghi, ologrammi, intestazioni corporate e persino firme attribuite ai rispettivi dirigenti. Le lettere contengono un QR code e un messaggio urgente: completare un "Authentication Check" o un "Transaction Check" obbligatorio entro una data precisa, pena la perdita delle funzionalità del dispositivo.

Non si tratta di un fenomeno isolato o marginale. Questa campagna rappresenta un salto qualitativo nell'evoluzione del *quishing* – un attacco che aggira per design ogni filtro anti-spam, ogni sandbox, ogni sistema di rilevamento automatizzato, perché non transita attraverso alcun canale digitale. La domanda che pone ai professionisti della sicurezza è radicale: come si difende un perimetro che non esiste più?

Anatomia dell’attacco: dalla lettera alla seed phrase rubata

Il meccanismo operativo della campagna è tanto semplice quanto efficace, e merita un’analisi dettagliata perché rivela una sofisticazione psicologica notevole, anche in assenza di complessità tecnica.

La vittima riceve una lettera cartacea recapitata al proprio indirizzo di residenza. La lettera è stampata su carta intestata che replica fedelmente il branding ufficiale di Ledger o Trezor. Nel caso delle lettere a tema Trezor, il documento reca la firma del CEO Matěj Žák, sebbene in almeno un esemplare documentato il nome compaia erroneamente come “Ledger CEO” — un indizio di produzione massiva con controllo qualità approssimativo che, paradossalmente, molte vittime non notano. Le *scam letters* includono ologrammi apparentemente autentici e un QR code stampato in posizione prominente.

Il testo della comunicazione è costruito secondo i principi classici dell’ingegneria sociale. Un esemplare analizzato da BleepingComputer invitava l’utente a completare l’Authentication Check entro il 15 febbraio 2026, scansionando il QR code con il proprio dispositivo mobile e seguendo le istruzioni sul sito web indicato. Il messaggio presenta tre elementi chiave: un’azione apparentemente ragionevole (verifica di sicurezza), una deadline precisa (che genera urgenza) e una conseguenza negativa in caso di mancata azione (perdita di accesso). Una variante destinata agli utenti Ledger richiede di completare un “Transaction Check” con scadenza al 15 ottobre 2025 e include l’avvertimento di non condividere la seed phrase online — un dettaglio che costruisce falsa credibilità prima di reindirizzare la vittima esattamente verso quella trappola.

La scansione del QR code conduce a siti web che replicano con precisione le interfacce ufficiali di configurazione dei

dispositivi, ospitati su domini come “trezor.authentication-check.io” o “ledger.setuptransactioncheck.com”. Il percorso di navigazione è progettato per simulare un processo di verifica plausibile: una landing page che spiega la necessità dell’”Authentication Check”, un pulsante “Get Started”, una serie di avvertenze su possibili malfunzionamenti in caso di mancata verifica (errori nella firma delle transazioni, incompatibilità con futuri aggiornamenti firmware) e infine la pagina critica che richiede l’inserimento della recovery phrase da 12, 20 o 24 parole.

La recovery phrase – o seed phrase – è la rappresentazione testuale della chiave privata che controlla l’accesso a un wallet crittografico. Chi la possiede può ripristinare il wallet su qualsiasi dispositivo compatibile e trasferire tutti i fondi. L’inserimento della seed phrase su un sito controllato dagli attaccanti equivale alla consegna totale e irreversibile di tutti gli asset custoditi nel wallet. I fondi vengono tipicamente drenati nel giro di minuti.

La supply chain delle informazioni: da dove vengono gli indirizzi

Ogni campagna di *QR code phishing* mirato richiede dati di targeting. Nella fattispecie, gli attaccanti necessitano di un dato particolarmente sensibile: l’indirizzo fisico di residenza di persone che possiedono un hardware wallet crittografico. Questo dato non è banale da ottenere, e la sua disponibilità è direttamente riconducibile a una catena di data breach che coinvolge Ledger da quasi sei anni.

La breach del 2020: il peccato originale

Nel giugno 2020, un attaccante ha sfruttato una chiave API mal configurata per accedere al database e-commerce e marketing di Ledger. L’incidente, inizialmente sottostimato, si è rivelato devastante: quando il contenuto integrale dei database rubati

è stato pubblicato su un forum nel dicembre 2020, è emerso che oltre un milione di indirizzi email erano stati esposti e, dato cruciale, circa 272.000 record contenenti nomi completi, numeri di telefono e indirizzi postali dei clienti. Come documentato da Have I Been Pwned, i dati sono stati inizialmente venduti e poi resi integralmente di pubblico dominio.

A questa breach si è aggiunto un secondo incidente legato a Shopify: dipendenti infedeli del partner e-commerce di Ledger hanno esfiltrato record di clienti in due episodi distinti, ad aprile e giugno 2020. Secondo le indagini forensi condotte da Ledger con Orange Cyberdefense, la breach Shopify ha coinvolto complessivamente circa 292.000 record, di cui circa 20.000 erano nuovi record non compresi nella breach precedente, contenenti email, nomi, indirizzi postali, prodotti ordinati e numeri di telefono. Il risultato complessivo è stato un database di centinaia di migliaia di individui identificabili come acquirenti di hardware wallet, con tanto di indirizzo di casa.

La breach Trezor del 2024

Nel gennaio 2024, Trezor ha reso noto che un accesso non autorizzato al portale di supporto gestito da un provider terzo aveva potenzialmente esposto i dati di contatto di circa 66.000 utenti – email e nomi/nickname – che avevano interagito con il supporto dal dicembre 2021. Sebbene in questo caso non risultino compromessi indirizzi postali, l'incidente ha fornito un ulteriore set di dati per la correlazione e il targeting.

La breach Global-e del gennaio 2026: l'ultima goccia

Il 5 gennaio 2026, come riportato da CoinDesk e confermato da The Register, Ledger ha informato i propri clienti di un nuovo

incidente di esposizione dati, riconducibile a Global-e, il processore di pagamenti utilizzato per gli ordini internazionali su Ledger.com. Un soggetto non autorizzato ha ottenuto accesso a un sistema cloud di Global-e contenente dati ordine di clienti di diversi brand, incluso Ledger. I dati esposti comprendono nomi, informazioni di contatto e dettagli degli ordini (prodotti acquistati e prezzi), sebbene non risultino compromesse informazioni di pagamento o credenziali.

Ledger ha specificato in una comunicazione a BleepingComputer che l'incidente non ha riguardato la piattaforma, l'hardware o il software Ledger, e che Global-e non ha accesso alle 24 parole della recovery phrase, ai saldi blockchain o ad alcun segreto relativo agli asset digitali. Tuttavia, il valore operativo di questa breach non risiede nell'accesso a chiavi crittografiche, bensì nella possibilità di costruire un profilo di targeting preciso: questa persona ha acquistato un dispositivo Ledger, risiede a questo indirizzo, e il suo ordine è datato.

La cronologia è significativa: la breach Global-e viene resa nota il 5 gennaio 2026, le prime *scam letters* con *QR code phishing* iniziano a circolare nelle settimane successive. Sebbene non sia possibile stabilire con certezza un collegamento causale diretto — gli attaccanti potrebbero utilizzare anche i dati del 2020, ampiamente disponibili — la coincidenza temporale suggerisce quantomeno che i dati freschi abbiano alimentato o ampliato la campagna.

Il pattern ricorrente: Ledger e il debito di fiducia sulla supply chain commerciale

L'analisi più rilevante per un professionista della sicurezza non riguarda la singola campagna di *crypto scams*, ma il

pattern strutturale che la rende possibile.

Ledger produce un dispositivo la cui ragion d'essere è la sicurezza: un hardware wallet che custodisce chiavi private in un elemento sicuro isolato, offline, inaccessibile da remoto. Il paradosso è che il dispositivo stesso non è mai stato compromesso. In nessuno degli incidenti documentati gli attaccanti hanno violato il secure element, estratto chiavi private o bypassato le protezioni crittografiche. Ciò che viene compromesso, sistematicamente e ripetutamente, è l'infrastruttura commerciale attorno al prodotto: il database e-commerce (2020), il partner logistico Shopify (2020), il processore di pagamenti Global-e (2026).

Questo schema solleva una questione strategica che trascende il caso specifico: il modello di self-custody promette di eliminare i *trusted third party* dalla custodia degli asset digitali, ma non può eliminare i *trusted third party* dal processo di acquisto e distribuzione del dispositivo fisico che rende possibile la self-custody stessa.

Ogni acquisto online genera una traccia di dati personali — nome, indirizzo, email, dati ordine — che transita attraverso una catena di fornitori terzi (piattaforme e-commerce, processori di pagamento, provider logistici, servizi di localizzazione valutaria). Ciascuno di questi anelli rappresenta una superficie d'attacco. E nel caso specifico dei clienti di hardware wallet, quei dati identificano con certezza una persona come detentore di criptovalute — un'informazione che ha valore sia per i phisher digitali sia per i criminali nel mondo fisico.

La psicologia della lettera: perché il cartaceo funziona

La domanda che ogni CISO dovrebbe porsi è: perché una lettera cartacea è più efficace di un'email di phishing?

La risposta risiede in un’asimmetria cognitiva che vent’anni di *cybersecurity awareness* non hanno affrontato. L’intera infrastruttura di formazione anti-phishing è costruita attorno ai canali digitali: non cliccare su link sospetti, verificare l’indirizzo del mittente, diffidare delle email con senso di urgenza. Secondo Keepnet Labs, il 12% di tutti gli attacchi phishing nel 2025 conteneva un QR code, e i dirigenti C-level risultano 40 volte più esposti al *quishing* rispetto ai dipendenti ordinari. Ma queste statistiche si riferiscono al *quishing* digitale. La variante fisica opera in un territorio cognitivo sostanzialmente non presidiato.

Una lettera cartacea attiva almeno tre bias cognitivi che l’email non può replicare con la stessa intensità. Il primo è l’autorità percepita del medium fisico: nella percezione comune, la posta cartacea è associata a comunicazioni ufficiali, istituzionali, importanti – banche, enti pubblici, studi legali. Il secondo è l’assenza di sospetto contestuale: abbiamo interiorizzato che le minacce informatiche arrivano attraverso schermi, non attraverso la cassetta delle lettere. Il terzo è l’investimento percepito: una lettera stampata su carta intestata con ologrammo comunica un impegno di risorse che un’email di massa non trasmette, generando una credibilità implicita.

A questi si aggiunge un fattore tecnico determinante: il *QR code phishing* fisico bypassa per design l’intero stack di sicurezza digitale. Non transita attraverso gateway email che possono intercettare link malevoli. Non viene analizzato da sandbox o filtri anti-phishing. Il QR code non è ispezionabile prima della scansione (a meno di non utilizzare scanner con funzione di anteprima dell’URL, ancora poco diffusi). Il passaggio dal mondo fisico a quello digitale avviene nel momento in cui la vittima punta la fotocamera del proprio smartphone personale – un dispositivo che tipicamente non è protetto con la stessa profondità di un endpoint aziendale.

Dal phishing fisico al wrench attack: la catena che arriva al corpo

Il *QR code phishing* contro i possessori di wallet Ledger non può essere analizzato come fenomeno isolato. Si inscrive in un trend più ampio e più grave: la convergenza tra *cybercrime* e crimine fisico.

Il caso più emblematico è quello di David Balland, cofondatore di Ledger, rapito insieme alla compagna nel gennaio 2025 dalla propria abitazione a Méreau, nel centro della Francia. Come riportato da Fortune, CoinDesk e France 24, i rapitori hanno tenuto i coniugi separati in due località diverse, hanno contattato un altro cofondatore di Ledger chiedendo un riscatto in criptovalute e hanno amputato un dito a Balland per forzare il pagamento. L'unità d'élite GIGN della Gendarmerie nazionale è intervenuta liberando Balland mercoledì notte, mentre la compagna è stata ritrovata giovedì legata in un veicolo nella zona di Essonne. Dieci persone, di età compresa tra i 20 e i 40 anni, sono state arrestate, come confermato dalla procura di Parigi.

Il caso Balland non è isolato. Nel novembre 2024, Dean Skurka, CEO della più grande crypto company canadese WonderFi, è stato sequestrato a Toronto da criminali che chiedevano un riscatto di un milione di dollari canadesi. L'escalation è documentata e sistematica: i dati digitali rubati nelle breach — indirizzi, abitudini di acquisto, patrimoni stimabili — forniscono l'intelligence necessaria per identificare e localizzare fisicamente i target.

In questo contesto, il *QR code phishing* fisico via posta rappresenta il livello iniziale di una scala di rischio che può arrivare fino alla violenza fisica. La lettera con QR code è l'equivalente di un probe: testa la reattività della

vittima, raccoglie la seed phrase se va a buon fine, e in ogni caso conferma che a quell'indirizzo risiede effettivamente un possessore di crypto wallet. Come ha osservato DL News, il confine tra rischio online e rischio nel mondo reale è più sottile di quanto la maggior parte delle persone voglia ammettere.

Il quishing nel 2025-2026: un trend in esplosione

Le *scam letters* con QR code ai possessori di wallet sono un sottoinsieme di un fenomeno molto più ampio: l'esplosione del *quishing* (QR code phishing) a livello globale.

I dati raccolti da Keepnet Labs tratteggiano un quadro allarmante: gli attacchi phishing basati su QR code sono aumentati di cinque volte nel 2025. Le email di *quishing* sono passate da circa 47.000 nel mese di agosto a oltre 249.000 a novembre 2025. Il 68% degli attacchi *quishing* ha preso di mira specificamente utenti mobile. Secondo Abnormal Security, gli attacchi basati su QR code sono cresciuti del 400% tra il 2023 e il 2025, con energia, sanità e manifattura tra i settori più colpiti.

La ragione di questa esplosione è strutturale: i QR code rappresentano un punto cieco per le difese tradizionali. Un QR code in un'email è un'immagine, non un link testuale, e molti sistemi di filtraggio non lo decodificano. Nel contesto fisico – cartelli, parchimetri, volantini, lettere – non esiste alcun livello di protezione automatizzato. L'utente è completamente solo nella decisione di scansionare o meno.

Tra le autorità che hanno già riconosciuto la gravità del fenomeno, lo United States Postal Inspection Service (USPIS) ha pubblicato advisory specifici sul *quishing* postale, mentre la Federal Trade Commission (FTC) ha emesso alert dedicati ai QR code contenuti in pacchi non richiesti. Nel Regno Unito,

tra aprile 2024 e aprile 2025, Action Fraud ha registrato 784 segnalazioni di *quishing* con perdite prossime a 3,5 milioni di sterline, un dato citato anche nell'analisi annuale di CloudSEK sulle tendenze phishing 2026.

Contromisure: cosa può fare concretamente un'organizzazione

Il *QR code phishing* fisico pone sfide di difesa non convenzionali. Le contromisure tradizionali – filtri email, sandbox, DNS sinkholing – sono strutturalmente irrilevanti. La risposta deve operare su tre livelli: consapevolezza, procedura e architettura.

Consapevolezza: estendere la formazione al mondo fisico

I programmi di *security awareness* devono essere aggiornati per includere esplicitamente il phishing fisico come vettore di attacco. Il messaggio chiave è semplice ma ancora poco diffuso: nessun produttore di hardware wallet chiederà mai di inserire la seed phrase su un sito web, tramite QR code, o in qualsiasi contesto diverso dal dispositivo fisico stesso. Come ribadisce Ledger nella propria pagina dedicata alle campagne di phishing: non esiste mai un motivo legittimo per digitare la propria recovery phrase su un computer. Questa regola è assoluta e non ammette eccezioni, indipendentemente dal canale di comunicazione.

Procedura: verificare sempre attraverso canali ufficiali

Qualsiasi comunicazione che richieda azioni urgenti relative a dispositivi di sicurezza – sia essa digitale o cartacea – deve essere verificata attraverso i canali ufficiali del produttore, navigando manualmente verso il sito web noto (non

attraverso link o QR code forniti nella comunicazione). Per gli utenti Ledger, la pagina di stato delle campagne phishing e il supporto ufficiale sulla truffa postale elencano le varianti note, inclusa espressamente la variante postale. Per gli utenti Trezor, il blog ufficiale e i canali di supporto verificati sono gli unici punti di riferimento attendibili.

Architettura: minimizzare l'esposizione dei dati personali

Per chi deve ancora acquistare un hardware wallet, la contromisura più efficace è la minimizzazione dei dati personali ceduti durante l'acquisto. Questo include l'utilizzo di indirizzi di consegna alternativi (ufficio postale, punto di ritiro, indirizzo aziendale), email dedicate non collegate all'identità principale e, dove possibile, metodi di pagamento che non richiedano la divulgazione di dati anagrafici completi.

Per i possessori attuali i cui dati sono già potenzialmente esposti, le azioni prioritarie includono: monitoraggio attivo dell'attività del proprio wallet, valutazione della migrazione a un wallet con nuova seed phrase non correlata alle informazioni compromesse, adozione di configurazioni multi-signature che distribuiscano il rischio e implementazione di setup air-gapped che eliminino la connettività di rete dal processo di firma delle transazioni.

Per le organizzazioni: non sottovalutare il phishing fisico come vettore

Per i CISO e i responsabili della sicurezza aziendale, questa campagna di *crypto scams* ha implicazioni che vanno oltre il mondo crypto. Se il *QR code phishing* fisico funziona per i wallet crittografici, quanto tempo prima che venga adottato sistematicamente per il CEO fraud, l'ingegneria sociale aziendale o gli attacchi alle infrastrutture critiche? I

settori dove la corrispondenza cartacea è la norma – bancario, assicurativo, sanitario, legale, fiscale – sono naturalmente esposti. Le policy di sicurezza devono prevedere procedure di verifica anche per le comunicazioni ricevute su canale fisico, specialmente quando richiedono azioni digitali come la scansione di QR code.

La questione strutturale: i dati personali come arma persistente

Il *QR code phishing* contro i clienti Ledger illumina una verità scomoda che l'industria della cybersecurity non ha ancora pienamente metabolizzato: i dati personali rubati in una breach non perdono valore con il tempo. Anzi, il loro valore come strumento di targeting può aumentare man mano che vengono correlati, arricchiti e combinati con dati provenienti da breach successive.

I 272.000 indirizzi rubati nel 2020 sono stati utilizzati per campagne di phishing via email nel 2020-2021, per l'invio di dispositivi Ledger contraffatti nel 2021, e ora per *scam letters* con QR code nel 2025-2026. I dati della breach Global-e del 2026 non fanno che aggiornare e arricchire un database di targeting già esistente. Ogni nuova breach nella supply chain commerciale di Ledger non è un incidente isolato: è un aggiornamento dell'infrastruttura di intelligence a disposizione degli attaccanti.

Questo ha implicazioni profonde per il framework normativo. Il GDPR impone la minimizzazione dei dati e la limitazione della conservazione, ma non può impedire che dati già esfiltrati continuino a circolare e a essere sfruttati per anni. La Direttiva NIS2 richiede la gestione del rischio supply chain, ma la catena di fornitori e-commerce di un produttore di hardware raramente rientra nel perimetro delle valutazioni di sicurezza tradizionali.

Prospettive: il QR code phishing fisico è qui per restare

L’evoluzione del *quishing* fisico nel 2025-2026 suggerisce che non si tratta di un episodio estemporaneo ma di un nuovo vettore stabile nel repertorio del *cybercrime*. Le ragioni sono tre.

La prima è economica: il costo di produzione e spedizione di lettere cartacee è sceso drasticamente, e il ritorno potenziale per lettera (l’intero contenuto di un crypto wallet) giustifica ampiamente l’investimento. La seconda è tattica: il *QR code phishing* fisico aggira le difese digitali per design, e l’infrastruttura di consapevolezza e prevenzione è ancora inadeguata. La terza è strategica: le breach passate e presenti hanno creato un bacino permanente di dati di targeting che non può essere bonificato.

Come osservato da Secrets of Privacy, il pattern che rende possibile questa campagna — un settore dove la corrispondenza fisica è consueta, dove esiste urgenza reale, e dove una breach ha già messo gli indirizzi di casa nel dominio pubblico — descrive la maggior parte della vita moderna. I criminali hanno dimostrato il modello sui possessori di crypto perché il ritorno giustificava l’investimento. La fase successiva sarà la scalabilità: volumi più alti, valori unitari più bassi, settori più ampi.

Il *QR code phishing* fisico contro i clienti Ledger non è solo una notizia di cybersecurity. È un segnale che la separazione tra mondo digitale e mondo fisico — sulla quale è costruita gran parte della nostra architettura di sicurezza — si sta dissolvendo. E chi non aggiorna le proprie difese per riflettere questa realtà rischia di trovarsi esposto su un fronte che non sapeva nemmeno di dover presidiare.

Condividi sui Social Network:

https://www.ictsecuritymagazine.com/senza-categoria/qr-code-phishing/