Truffe digitali ai merchant: Come le API di Trust Score stanno stroncando le truffe online sul nascere

Non più solo reazione, ma prevenzione predittiva. Mentre il cybercrime si evolve, le aziende adottano sistemi di screening silenzioso.

MILANO, ITALY, December 17, 2025 /EINPresswire.com/ -- Si parla sempre di clienti truffati online ma nel mercato dell'e-commerce secondo gli ultimi report sulla sicurezza informatica, le frodi ai siti web basate su furto d'identità e account falsi sono aumentate a doppia cifra nel 2025.

> I truffatori creano profili mescolando dati reali e falsi. Se il numero di telefono è una linea VoIP anonima o risulta "leaked" nel dark web, la probabilità che la carta sia rubata sfiora il 90%."
>
> *Alan Andrews (Risk manager)*

Il fenomeno è noto tecnicamente come "Card Not Present (CNP) Fraud" ed è l'incubo di ogni merchant. Quando un truffatore usa una carta rubata su un sito, il danno non ricade sulla banca o sul proprietario della carta (che vengono rimborsati), ma quasi interamente sul titolare del sito web.

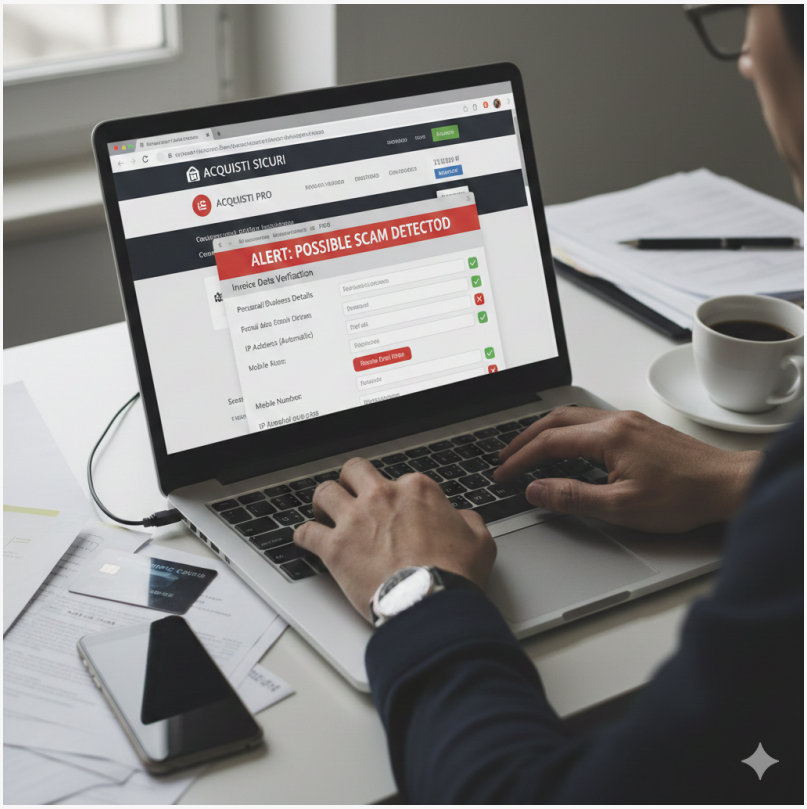
Uno dei dati più impressionanti riguarda il costo reale di ogni euro rubato.
Secondo il True Cost of Fraud Study 2024-2025, per ogni euro di transazione fraudolenta persa, un merchant spende in media 4,61 €.

Questo moltiplicatore include:
- La perdita della merce (costo del bene spedito).
- Le spese di spedizione e logistica.
- Le commissioni di Chargeback: Le banche applicano penali che variano dai 15 ai 50 euro per ogni transazione contestata.
- Spese amministrative: Il tempo del personale impiegato per gestire la disputa.

Statistiche Chiave sulle Frodi Merchant (2024-2025)
Perdite Globali E-commerce: 44,3 miliardi di $ nel 2024 (proiezione 107 mld entro il 2029).
Incidenza sui Ricavil merchant europei perdono in media il 2,8% del fatturato annuo in frodi.
Identity Theft (Furto d'identità)Colpisce il 36% dei merchant ogni anno.

Friendly Fraud (Truffa "amica")Rappresenta il 45-55% di tutte le contestazioni (utenti reali che fingono di non aver ricevuto il pacco).
Efficacia delle Difese Solo il 16% dei merchant europei effettua controlli preventivi (screening) prima del checkout.

La Legge e la Responsabilità: Chi Paga?
In Italia e in Europa, la normativa di riferimento è la PSD2 (SCA - Strong Customer Authentication).



openapi trust

Se il sito non richiede la SCA (il classico 3D Secure con codice sul cellulare), la responsabilità finanziaria del furto ricade al 100% sul sito web.
Il paradosso del merchant, anche se il sito vince la disputa, il solo fatto di avere un Chargeback Rate superiore all'1% può portare i circuiti (Visa/Mastercard) a inserire l'azienda in programmi di monitoraggio,

Il problema principale dei flussi di vendita tradizionali è la verifica post acquisto: controllare il cliente solo quando il danno è potenzialmente già fatto.

Ma la vera notizia non è l'attacco, quanto la difesa: una nuova generazione di strumenti di verifica preventiva sta cambiando radicalmente le regole del gioco, permettendo alle aziende di "pesare" l'affidabilità di un utente prima ancora che questi prema il tasto "Acquista".

Abbiamo analizzato e provato i servizi TRUST di OpenAPI.com, è possibile implementare una "verifica preventiva" a costo quasi nullo.

Il cuore di questa rivoluzione sono le API (Application Programming Interface). Questi connettori digitali permettono ai sistemi aziendali di interrogare istantaneamente database globali, ottenendo una "scheda di affidabilità" ricchissima di dettagli.

Tipicamente in fase di acquisto i dati che vengono richiesti sono i dati personali o aziendali per la fattura, l' email, indirizzi IP (automatico) e il numeri di cellulare. Tutti questi dati possono essere verificati prima del pagamento.

Per ognuno di questi dati esistono specifiche APi per fare dei controlli puntuali dalla verifica dei dati aziendali (utili oltre a vedere i dati di bilancio e quindi eventuali linee di credito anche per l'emissione della fattura) al controllo della email (se è credibile o meno, se è stata creata da poco, se ha una storia di frodi etc.) o degli IP.

In questo articolo abbiamo approfondito solo la verifica del Cellulare come "Impronta Digitale" del Rischio. Lasciamo a voi lettori eventualmente darci indicazioni se volete che valutiamo e descriviamo altri servizi.

La prima cosa che abbiamo notat è che non si tratta di un semplice controllo sintattico, ma di un'operazione di HLR Lookup (Home Location Register) che scava nelle profondità della rete telco.

Quando un utente inserisce il proprio numero in un form, il sistema invia una richiesta POST /mobile-advanced. In pochi secondi, l'azienda riceve una risposta che include oltre 25 parametri critici. Non è solo questione di sapere se il numero esiste, ma di valutarne la "storia"

Abbiamo fatto delle prove per i lettori e sono emersi questi punti interessanti:

- Il Fraud Score: Un punteggio che, se supera la soglia di 85-90, segnala un rischio alto o altissimo di attività malevola.
- Lo Stato della Linea: Il numero è attivo o appartiene a una sim disconnessa? Il telefono è spento? Un dato fondamentale per prevenire tentativi di account takeover.
- L'Effetto "Leaked": L'API segnala se quel numero è stato recentemente esposto in violazioni di dati (data breach) di colossi come Google o Amazon. Un numero "leaked" è una bandiera rossa: potrebbe essere in mano a un malintenzionato che ha acquistato database nel dark web.
- Analisi della Portabilità e Carrier: Conoscere l'operatore attuale e originario (MNC/MCC) e sapere se la linea è una VoIP (spesso usata per l'anonimato) permette di profilare istantaneamente il rischio.

L'adozione di questi sistemi permette di creare processi di vendita "intelligenti". Se il sistema rileva un Fraud Score elevato o una discrepanza tra prefisso geografico e posizione reale, l'azienda può:

- Bloccare l'operazione sul nascere, risparmiando sui costi di gestione delle frodi (chargeback).
- Richiedere controlli supplementari, come l'invio di un documento d'identità (KYC).
- Correggere errori: Identificare banali errori di battitura del cliente, migliorando l'esperienza utente e la qualità del database marketing.

Compliance e Futuro: Il Sistema Integrato
L'uso di queste tecnologie si sposa con il GDPR, basandosi sul "legittimo interesse" del titolare a prevenire frodi e garantire la sicurezza dei propri sistemi. Ma il vero salto di qualità avviene quando questi dati vengono incrociati. Il canale TRUST di OpenAPI non si ferma al cellulare:

integra Business Information, verifiche su Sanction List (liste antiriciclaggio), KYC (Know Your Customer) e KYB (Know Your Business).

In un mondo dove il crimine è automatizzato, la risposta non può essere manuale. L'integrazione di questi servizi "Start" o "Advanced" rappresenta oggi il discrimine tra un'azienda vulnerabile e una realtà pronta a scalare il mercato globale in totale sicurezza.

Luca Scuriatti
Openapi Spa
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
