26 ottobre 2023 9:54

ITALIA: Truffe online. Temute dal 79% degli italiani

Mentre le frodi permeano l'economia digitale, una nuova ricerca di SAS e 3GEM evidenzia un panorama di utenti disposti ad accettare metodi di autenticazione più severi in cambio di maggiori tutele per i propri dati sensibili

Oltre il 60% è stato vittima di una truffa almeno una volta, il 33% crede che il numero di frodi sia sensibilmente salito nel 2022 e il 79% teme di diventare una vittima in futuro, mentre una schiacciante maggioranza del 90% ritiene che istituzioni e aziende dovrebbero impegnarsi maggiormente nel proteggere i consumatori. A rispondere sono gli intervistati italiani della ricerca condotta da SAS, azienda leader negli analytics, in collaborazione con 3Gem su un campione di 13,500 rispondenti globali. I risultati raccolti evidenziano un clima di allerta dove 9 persone su 10, nel nostro Paese, si dichiarano considerevolmente più preoccupate e consapevoli, nonché disposte a rivolgersi a nuovi fornitori nel caso in cui dovessero offrire una migliore forma di protezione e vigilanza.

La vulnerabilità della digitalizzazione

La pandemia ha rivoluzionato i pagamenti digitali, che a loro volta hanno ridefinito radicalmente le aspettative dei consumatori, per cui opzioni di pagamento flessibili e in tempo reale nell'intero percorso digitale sono oggi esigenze basilari. Per i truffatori, tuttavia, l'improvviso aumento delle transazioni digitali e delle modalità di pagamento ha offerto innumerevoli nuove opportunità di frode attraverso schemi che, se inizialmente sfruttavano elementi tipici della pandemia e il social engineering, oggi si sono evoluti in frodi continue e disparate, con truffe sentimentali, false opportunità di lavoro e investimenti fasulli quali tattiche maggiormente ricorrenti.
La maggior parte degli attacchi, vari e numerosi, viene eseguita online, ma alcuni utilizzano metodi più comuni quali telefonate, e-mail e persino visite a domicilio. In Italia, in particolare, il contatto su cellulare e attraverso la mail risulta la modalità maggiormente impiegata, riportata dal 66% e 72% degli intervistati rispettivamente, che denunciano il sostanziale perseguimento di un obiettivo principale: l'ottenimento di dati bancari o personali sensibili.
La digital economy e la "global scam economy", sembrano pertanto destinate a convivere ed evolversi in parallelo.

La sicurezza giustifica maggiori controlli?

Il 71% dei rispondenti italiani alla ricerca di SAS ha dichiarato di essere disposto a tollerare ritardi o giustificare controlli aggiuntivi in nome di una maggiore protezione contro tentativi di furto di identità o di natura economica. Sebbene il 41%, infatti, affermi che i controlli di sicurezza abbiano portato ad una customer experience generalmente negativa e che ci sia molto da fare per rendere più agevoli i processi di autenticazione e riconoscimento, i consumatori sembrano anche disposti a pagare il prezzo richiesto per una maggiore sicurezza. Il 63% preferisce già ricorrere a un metodo di autenticazione piuttosto che a una password durante le transazioni, ed il 74% cambierebbe il provider dei propri servizi se questo offrisse un sistema anti-frode migliore, dimostrandosi favorevole anche nel caso in cui si vedesse costretto ad utilizzare sistemi di rilevazione biometrici (81,9%) nell'ambito di una transazione, o condividere maggiori dati personali (64%) con il proprio provider e utilizzare metodi di pagamento P2P (78,7%).
Ciò indica come un impegno attivo nella prevenzione di scam possa dimostrarsi per le aziende un vantaggio competitivo fondamentale, e come l'atteggiamento generale dell'utenza non sia quello di un abbandono delle nuove tecnologie per paura di subire frodi, quanto l'aspettativa che tali tecnologie, e quindi le singole persone che ne usufruiscono, vengano protette adeguatamente.
"La fiducia dei consumatori nell'ecosistema globale dei pagamenti digitali, in continua espansione, è un imperativo, che si basa sull'uso efficace da parte delle aziende di tecnologie avanzate di autenticazione dei clienti e antifrode, tra cui l'intelligenza artificiale, il machine learning e la biometria, per rilevare e prevenire le frodi attraverso i diversi canali", dichiara Stu Bradley, Senior Vice President Fraud & Security Intelligence di SAS.

L'anti-frode integrata nel digitale getta le basi per il futuro – Le otto strategie degli esperti

In un clima di tale insicurezza e timore, è possibile combattere, o perlomeno evitare, le numerose frodi? Ecco otto raccomandazioni per combattere le frodi nell'era digitale secondo SAS e Javelin1:

1. Implementare controlli di autenticazione forte dei clienti a livello aziendale su tutti i punti di accesso digitali.
2. Abilitare l'autenticazione a più fattori (MFA) e gli avvisi account-based.
3. Creare strategie anti-frode inclusive dal punto di vista digitale.
4. Incorporare il protocollo 3DS per ridurre le frodi nell'e-commerce.
5. Sfruttare lo standard ISO 20022 per la prevenzione delle frodi e la lotta al riciclaggio di denaro.
6. Educare i titolari di conto corrente a riconoscere e segnalare le tattiche di truffa.
7. Consolidare le pratiche di monitoraggio dell'AML e del know-your-customer (KYC) in un'unica piattaforma.
8. Sviluppare un protocollo di valutazione delle minacce multicanale.

Il rilevamento delle frodi basato sull'intelligenza artificiale può aiutare le organizzazioni a individuare più frodi, in anticipo e molto più rapidamente, migliorando sia l'efficienza che l'accuratezza delle loro strategie di rilevamento e prevenzione delle frodi in tempo reale. A differenza delle regole, che sono facili da testare e aggirare per i truffatori, l'applicazione del machine learning può aiutare le aziende a identificare meglio le anomalie in tempo reale e a restare un passo avanti a minacce in rapida evoluzione.
....
"La rapida ascesa degli strumenti di intelligenza artificiale generativa non farà altro che rendere più facile per i truffatori e le associazioni criminali organizzate superare i metodi tradizionali di rilevamento delle frodi", ha dichiarato Bradley. "L'impiego di capacità di rilevamento delle frodi stratificate che utilizzano le stesse tecnologie di analisi avanzate può aiutare le organizzazioni a battere i criminali al loro stesso gioco. Chi è all'altezza delle aspettative dei propri clienti può trasformare la prevenzione delle frodi in un fattore di fidelizzazione e, in ultima analisi, in un vantaggio competitivo che lo aiuti ad automatizzare e a far crescere il proprio business, riducendo al contempo le perdite dovute alle frodi".

(Data Manager Online del 23/10/2023)