Comunicato stampa

Pensi di saper riconoscere una frode?

Il nuovo studio Visa rivela che anche i consumatori più esperti

si lasciano ingannare dal linguaggio delle truffe

*‘Vincere,’ ‘regalo gratuito,’ ‘offerta esclusiva‘ ‘approfittane subito’ sono tra le principali trappole linguistiche citate all’interno del report Visa ‘Fraudulese: il linguaggio delle frodi’*

*Milano, 20 dicembre 2022*— Non è una vostra impressione: le truffe digitali sono in agguato ovunque nella nostra vita quotidiana. E con l'avvicinarsi delle festività natalizie, i truffatori contano sul fatto che abbassiate la guardia e abbocchiate all'amo. Sia sul posto di lavoro che in viaggio, siamo tempestati di chiamate, messaggi ed e-mail con offerte di “regali gratuiti” e inviti ad “approfittarne subito” e fornire informazioni personali prima che un servizio essenziale venga interrotto. E questa raffica di messaggi in "*fraudulese*" sta sortendo i suoi effetti.

Un nuovo studio pubblicato da Visa, in partnership con Wakefield Research, (NYSE: V), “*[Fraudulese: The Language of Fraud](https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/visa-fraudulese-report.pdf)*,” rivela, che sul fronte dell’identificazione delle frodi, ormai i cybercriminali riescono a trovare punti di vulnerabilità anche nei consumatori più esperti di tecnologia. E sebbene quasi la metà della popolazione sia sicura di saper riconoscere una truffa, il 73% non è in grado di individuare i segnali di pericolo presenti nelle comunicazioni digitali.

Da una notifica di servizio falsa da parte della vostra compagnia di energia elettrica, a un'e-mail che vi avvisa di aver vinto dei prodotti presso il vostro negozio preferito, fino agli annunci di lavoro che vi fanno credere di essere stati assunti da un'azienda prestigiosa, le truffe toccano quasi tutti gli aspetti della nostra vita digitale. Solo nell'ultimo anno, Visa ha bloccato 7,2 miliardi di dollari di tentativi di pagamento fraudolenti in 122 milioni di transazioni, prima che impattassero sui clienti.

“*Comprendere il linguaggio delle frodi è essenziale in un mondo sempre più digitale. I truffatori hanno raggiunto nuovi livelli di sofisticazione sia nel linguaggio che nella tipologia: nessuno è immune*,” ha dichiarato Paul Fabara, Chief Risk Officer, Visa. “*L'educazione al linguaggio delle frodi è parte integrante del nostro impegno a protezione dei consumatori e mettere in evidenza i punti in comune nel linguaggio delle frodi aiuta a prevenire la criminalità a livello globale*.”

All'inizio di quest'anno, nell’ambito delle iniziative per aiutare i consumatori a riconoscere il linguaggio dei truffatori digitali, Visa ha commissionato [un'analisi linguistica](https://www.visa.co.uk/content/dam/VCOM/regional/ve/unitedkingdom/PDF/visa-fraudulese-report.pdf), la prima nel suo genere, ad alcuni ricercatori nel Regno Unito, che ha rivelato come questo linguaggio venga utilizzato dai truffatori nei messaggi brevi. Lo studio ha svelato che le soluzioni che invitano i consumatori a rispondere a un problema o a un’offerta sono il messaggio fraudolento più comune, presente nell'87% degli SMS che contengono frodi, mentre le enunciazioni di problemi che causano una reazione da parte del destinatario sono al secondo posto.

“*Segnalando le strategie comunicative, le parole e le frasi utilizzate dai truffatori, confidiamo che le persone possano riconoscere più facilmente il linguaggio delle frodi, contribuendo così a proteggerle*,” ha dichiarato il Dr. Marton Petyko, dell'Aston Institute for Forensic Linguistics, che ha condotto la ricerca nel Regno Unito.

**Esaminare il linguaggio delle frodi: il divario tra consapevolezza e azione**

Cadere vittima di una frode informatica è costoso. Nel 2021, l'Internet Crime Complaint Center dell'FBI ha registrato un numero record di denunce, con perdite potenziali superiori a 6,9 miliardi di dollari, rispetto ai 4,1 miliardi del 2020.

Secondo il nuovo studio Visa, che ha intervistato 6.000 adulti in 18 mercati in tutto il mondo, inclusa l’Italia, i truffatori sembrano approfittare del gap tra la conoscenza del linguaggio delle frodi da parte dei consumatori e il loro comportamento effettivo. Ecco i risultati principali emersi.

* **Riteniamo che gli altri siano più esposti di noi alle frodi.** Sebbene i consumatori si sentano sicuri della propria capacità di prevenire le frodi, la stragrande maggioranza (90%) è preoccupata che amici o familiari possano cadere in potenziali truffe come e-mail o messaggi di testo in cui si chiede di verificare i dati del proprio conto corrente, si richiedono informazioni sui conti bancari scoperti e si comunica la vincita di una carta regalo o di un prodotto da un sito di shopping online.

I messaggi di clickbait più persuasivi approfittano dell’entusiasmo dei consumatori, e pubblicizzano in modo fraudolento "vincite", "offerte esclusive" o "omaggi", come rivelato dallo studio.

* **È legittimo?** Più di 4 intervistati su 5 (81%) verificano i dettagli sbagliati per stabilire l'autenticità di una comunicazione, concentrandosi su informazioni che i truffatori possono facilmente falsificare, come il nome o il logo dell'azienda (46%). Gli individui possono proteggersi meglio dai truffatori controllando i dettagli più difficili da falsificare, come i numeri di conto o i dettagli delle loro interazioni con l'azienda.
* **Trascurare i segnali di pericolo.** Solo il 60% delle persone ha dichiarato di verificare se una comunicazione è inviata da un indirizzo e-mail valido. Meno della metà (47%) si assicura che le parole siano scritte correttamente.
* **Gli utenti di criptovalute si muovono con cautela.** Gli utenti di criptovalute sono più propensi a identificare gli elementi di una potenziale frode rispetto a chi non possiede cripto. Ad esempio, sono più predisposti a controllare le informazioni sul proprio conto (49% contro 37%) per confermare la validità delle comunicazioni digitali.

**Qualche momento in più per decifrare il linguaggio delle frodi**

I consumatori possono proteggersi meglio prendendosi qualche momento in più prima di cliccare, anche per capire il modo in cui i truffatori utilizzano il linguaggio. Tra le misure [più semplici ed efficaci](https://usa.visa.com/visa-everywhere/blog/bdp/2020/03/23/fraudsters-are-getting-1585004301034.html): tenere per sé le informazioni personali, non cliccare sui link prima di aver verificato che vi portino dove dicono, attivare gli avvisi di acquisto che forniscono una notifica quasi in tempo reale via SMS o e-mail degli acquisti effettuati sul conto, chiamare il numero indicato sui siti web delle aziende o sul retro delle carte di credito e di debito se non siete sicuri che una comunicazione sia valida, non limitarsi a chiamare l’eventuale numero fornito dal truffatore nel testo o nell'e-mail.

**Proteggere è una priorità assoluta di Visa**

In un mondo sempre più digitale in cui la criminalità informatica continua a proliferare, Visa prosegue nella propria mission a protezione dei consumatori e per ridurre le frodi. Negli ultimi cinque anni, l'azienda ha investito più di 10 miliardi di dollari in tecnologia, anche per limitare le frodi e aumentare la sicurezza della rete. Più di mille specialisti si occupano di proteggere la rete di Visa da malware, attacchi zero-day e minacce interne 24x7x365. Negli ultimi 12 mesi, il monitoraggio in tempo reale di Visa ha bloccato in modo efficace oltre 7,2 miliardi di dollari di pagamenti fraudolenti, impedendo a molti di trovarsi a contatto con una potenziale transazione fraudolenta. Per saperne di più, visitate il sito visa.com/security.

**Visa**

Visa (NYSE: V) è tra i leader mondiali nei pagamenti digitali e facilita transazioni tra consumatori, esercenti, istituzioni finanziarie e governi in più di 200 Paesi e territori. La nostra missione è quella di connettere il mondo attraverso la rete di pagamenti più innovativa, conveniente, affidabile e sicura, che consenta a privati, aziende ed economie di prosperare. Crediamo infatti che le economie capaci di includere tutti ovunque possano far crescere tutti ovunque e riteniamo l'accessibilità fondamentale nella movimentazione del denaro del futuro. Per maggiori informazioni, visita [https://www.visaitalia.com/](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.visaitalia.com%2F&data=05%7C01%7CPartner%40salonedeipagamenti.com%7C515dd00d03654693135808dac33bb4b4%7Cb4fa40cc86e445c38c3bda5bd30219f6%7C0%7C0%7C638036958470196950%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=GYuwBwIjLo9yt%2B6IjkDlxTnCdK3FGHJtvPHDvaf2DuA%3D&reserved=0), oltre che il [blog Visa Italia](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.visaitalia.com%2Fvisa-everywhere%2Fblog.html&data=05%7C01%7CPartner%40salonedeipagamenti.com%7C515dd00d03654693135808dac33bb4b4%7Cb4fa40cc86e445c38c3bda5bd30219f6%7C0%7C0%7C638036958470351735%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=zn7JfW5N%2BVhdL1MTqlVP0l3Ewj4gPjal%2FTZsEPMux7M%3D&reserved=0), e seguici su Twitter [@Visa\_IT](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FVisa_IT&data=05%7C01%7CPartner%40salonedeipagamenti.com%7C515dd00d03654693135808dac33bb4b4%7Cb4fa40cc86e445c38c3bda5bd30219f6%7C0%7C0%7C638036958470351735%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=i1f4Pfzfo%2FTMxv3vWGDpyb1p4iyUOSHqL2WaeCcNH60%3D&reserved=0).

**Contatti ufficio stampa Visa**

Enrica Banti, Senior Manager Corporate Communication, Visa Italy bantie@visa.com

Alessandro Zambetti, DAG Communication a.zambetti@dagcom.com +39 338 9241387

Matteo Rasset, DAG Communication mrasset@dagcom.com +39 333 8032644

Barbara D’Incecco, DAG Communication bdincecco@dagcom.com +39 02 89054168