Comunicato stampa

Le dieci regole Visa

per smascherare potenziali frodi online

* *Visa ha lanciato il “Fraudolese”, vocabolario realizzato per incoraggiare i consumatori a imparare il linguaggio delle frodi*
* *Negli ultimi cinque anni, Visa ha speso più di 9 miliardi di dollari per potenziare la sicurezza informatica e ridurre le frodi[[1]](#footnote-1)*

*6 settembre 2022* – Lo shopping online offre un mondo di possibilità a portata di click, tuttavia è bene essere consapevoli di ciò che si può fare per mantenere la sicurezza durante i nostri acquisti. Una nuova analisi commissionata da Visa ha introdotto il "[Fraudolese](https://www.visa.co.uk/content/dam/VCOM/regional/ve/unitedkingdom/PDF/visa-fraudulese-report.pdf)", vocabolario delle frodi che svela le strategie comunicative dei truffatori da cui tenersi in guardia per navigare e fare acquisti online in tutta sicurezza.

**I nostri dieci migliori suggerimenti per smascherare potenziali frodi**

1. Controllare l'ortografia dei messaggi: le incongruenze nel linguaggio, come gli errori di grammatica, la disposizione delle parole o le differenze tra il nome del mittente e il link all'URL fornito, potrebbero indicare che si tratta di una frode. Se si riceve un messaggio inaspettato da un'azienda o da un individuo, è bene fare attenzione a questi errori.
2. Diffidare delle richieste urgenti: un linguaggio che incoraggia a intraprendere un'azione urgente è una tattica comunemente usata nelle comunicazioni fraudolente. Bisogna diffidare di espressioni come "invia (...) qui" o "clicca (...) qui sotto", o di scadenze senza una data precisa come "entro 48 ore" o "entro domani mattina". È bene prendersi sempre il tempo necessario per valutare se il messaggio è autentico. Se si ha il dubbio possa essere falso, è importante non cliccare su alcun link per evitare di compromettere i dati personali.
3. Attenzione alle richieste sospette: i truffatori spesso usano come esca un problema (ad esempio, chiedono di riorganizzare una consegna) o fanno un'offerta allettante (ad esempio, la vincita di un premio). In questo caso, è utile fare mente locale sui rapporti recenti con quell'organizzazione o persona e, qualora non si abbia evidenza del problema che viene chiesto di risolvere o dell'offerta a cui si chiede di reagire, è probabile si tratti di frode. Se non si è sicuri, meglio non cliccare su alcun link e non contattare in alcun modo il mittente.
4. Verificare che il mittente sia effettivamente chi dice di essere: i truffatori spesso si impegnano a fondo per convincere della loro credibilità, a volte utilizzando parole e frasi riscontrabili in comunicazioni autentiche. Può essere difficile distinguerle, quindi se non si è sicuri, meglio verificare, per esempio, contattando direttamente l'azienda per essere sicuri si tratti di una richiesta autentica.
5. Verificare il messaggio con una persona di fiducia: può sembrare ovvio, ma se non si è sicuri della legittimità di un messaggio, può essere utile discuterne con una persona di fiducia. Forse anche lei ha ricevuto un messaggio simile e potrebbe essere in grado di consigliare la migliore linea d'azione da seguire. Condividere la propria esperienza potrebbe inoltre evitare che altri ne siano vittima.
6. Trovare il sito web giusto: è importante controllare che i siti web scelti per gli acquisti online siano sicuri. Si consiglia, inoltre, di verificare che nella barra degli indirizzi sia presente l'icona del "lucchetto" e che l'indirizzo del sito web inizi con HTTPS (la "S" offre infatti maggiori garanzie di sicurezza). Infine, è bene assicurarsi che il nome della pagina web non contenga errori di ortografia o caratteri inusuali.
7. Controllare il sito web e le recensioni del venditore: è utile informarsi sul sito web, social media o azienda presso cui si sta per acquistare. Conviene anche dare un'occhiata alle recensioni per conoscere l’esperienza d’acquisto degli altri utenti.
8. Attenzione alle truffe di phishing: è bene fare attenzione alle e-mail o alle telefonate non richieste e sospette. Potrebbero tentare di rubare informazioni personali come il numero di conto, il nome utente e la password. In caso di dubbio, non si deve cliccare su nessun link o scaricare alcun file.
9. Usare i "token" e i servizi one-click per pagare in modo facile e sicuro: quando si aggiunge la carta al proprio smartphone, o la si collega all’app di alcuni esercenti, i dati vengono spesso sostituiti da un "token" digitale: ciò significa che i dati della carta non vengono memorizzati risultando quindi ancora più sicuri. In certi negozi è possibile invece ricorrere al pagamento one-click, il che significa che basta impostarlo e dimostrare di essere il titolare della carta per poter poi fare acquisti online senza dover inserire ogni volta i dati della carta.
10. Utilizzare un modo sicuro, rapido e semplice per identificarsi: la Strong Customer Authentication (SCA)[[2]](#footnote-2), requisito della seconda direttiva sui servizi di pagamento (PSD2), comporta l’esecuzione di ulteriori controlli da parte delle banche per l’identificazione dei consumatori quando effettuano un pagamento, per assicurarsi che provenga dal titolare e non da un truffatore. Qualora sia possibile, è bene impostare metodi come le impronte digitali o il riconoscimento facciale sugli smartphone e all'interno delle app bancarie.

**L’impegno di Visa per contribuire a creare fiducia e proteggere dalle frodi online**

Negli ultimi cinque anni, Visa ha speso più di 9 miliardi di dollari per potenziare la sicurezza informatica e ridurre le frodi. Grazie a ciò, nonostante i trend in crescita dei pagamenti digitali, Visa ha continuato a registrare un tasso di frode globale basso (0,1%).[[3]](#footnote-3) In particolare, l'attenzione di Visa si concentra su due aspetti: proteggere la rete Visa da potenziali minacce e fornire a clienti e partner una difesa proattiva.

I centri dati globali Visa monitorano la rete per garantire che i sistemi continuino a funzionare e aiutino a elaborare le transazioni in tutto il mondo, mentre i centri cyber fusion Visa monitorano 24 ore su 24, 7 giorni su 7, le potenziali minacce alla rete. Circa 1000 specialisti di cybersecurity nel mondo lavorano a tempo pieno per proteggere la rete Visa da malware, attacchi zero-day e minacce interne, lavorando insieme a modelli di machine learning per prevedere e risolvere potenziali punti di vulnerabilità della rete e bloccare i rischi prima che si verifichino.

Per quanto riguarda i clienti, la sicurezza Visa scansiona e controlla i sistemi dei clienti alla ricerca di attività sospette e vulnerabilità. I soli test di vulnerabilità hanno fatto risparmiare ai clienti circa 31 milioni di dollari in frodi evitate nell'anno fiscale 2021, così come Visa Account Intelligence[[4]](#footnote-4) ha contribuito a prevenire circa 2,2 miliardi di dollari di tentativi di frode con l'intelligenza artificiale e il machine learning.[[5]](#footnote-5)

L'intelligenza artificiale\* è un potente strumento di prevenzione delle frodi. Grazie all'investimento di 500 milioni di dollari nell'intelligenza artificiale e nell'infrastruttura dati, Visa è in grado di attivare oltre 60 diverse funzionalità di AI che possono automatizzare gran parte del lavoro di rilevamento delle frodi, un'attività che richiede molto tempo e che molti clienti oggi svolgono manualmente. Visa Advanced Authorization, per esempio, ha contribuito a prevenire frodi per 26 miliardi di dollari nel 2021.[[6]](#footnote-6)

*\*La tecnologia all'avanguardia di Visa utilizza l'intelligenza artificiale (IA) e sofisticati algoritmi per aiutare le banche a identificare e prevenire le frodi prima che accadano. La rete Visa valuta 500 caratteristiche uniche per ogni singola transazione in tempo reale, analizzando i dati di oltre 3,5 miliardi di conti di carte per individuare attività insolite. La tecnologia IA di Visa aiuta a prevenire ogni anno a livello globale circa 25 miliardi di dollari di frodi[[7]](#footnote-7), che si verificano in meno dello 0,1% delle transazioni Visa[[8]](#footnote-8) – fra i tassi più bassi di tutte le modalità di pagamento.*

**Visa\*\***

Visa Inc. (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 ogni anno. 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/>, oltre che il [blog Visa Italia](https://www.visaitalia.com/visa-everywhere/blog.html), e seguici su Twitter [@Visa\_IT](https://twitter.com/Visa_IT).

*\*\*Le raccomandazioni di Visa contenute nel presente documento sono fornite a scopo puramente informativo e non devono essere considerate come consigli di marketing, legali, normativi o di altro tipo. Ogni raccomandazione deve essere valutata autonomamente alla luce delle vostre specifiche esigenze e delle leggi e regolamenti applicabili. Visa non è responsabile dell'utilizzo da parte vostra delle raccomandazioni o di altre informazioni, compresi errori di qualsiasi tipo, contenute nel presente documento.*

**Contatti ufficio stampa Visa**

Enrica Banti, Senior Manager Corporate Communication, Visa Italy [bantie@visa.com](mailto: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

1. <https://www.visa.co.uk/visa-everywhere/blog/bdp/2022/05/26/visa-continues-to-1653576045810.html> [↑](#footnote-ref-1)
2. <https://www.visaitalia.com/collabora-con-noi/tecnologia-di-pagamento/strong-customer-authentication.html> [↑](#footnote-ref-2)
3. <https://www.visa.co.uk/visa-everywhere/blog/bdp/2022/05/26/visa-continues-to-1653576045810.html> [↑](#footnote-ref-3)
4. <https://www.visa.co.uk/visa-everywhere/blog/bdp/2022/05/26/visa-continues-to-1653576045810.html> [↑](#footnote-ref-4)
5. <https://www.visa.co.uk/visa-everywhere/blog/bdp/2022/05/26/visa-continues-to-1653576045810.html> [↑](#footnote-ref-5)
6. <https://www.visa.co.uk/visa-everywhere/blog/bdp/2022/05/26/visa-continues-to-1653576045810.html> [↑](#footnote-ref-6)
7. VisaNet Data [↑](#footnote-ref-7)
8. VisaNet Data [↑](#footnote-ref-8)