Comunicato stampa

Black Friday, i consigli di Visa per proteggersi dalle frodi

**Milano, 16 novembre 2023** – Il Black Friday rappresenta un’occasione da non perdere per i consumatori per assicurarsi l’offerta migliore nei negozi, ma soprattutto sul web. E per i criminali informatici per moltiplicare i loro tentativi di truffa sfruttando l’onda degli sconti. Secondo il report ***Holiday Edition Threats* di Visa**, tra i leader globali nei pagamenti digitali, con l’arrivo del Black Friday si preannuncia un intensificarsi delle attività cybercriminali sia sulle transazioni con carta in modalità fisica o tramite e-commerce. Il nuovo rapporto identifica le tattiche di frode più diffuse previste tra novembre 2023 e gennaio 2024 e avverte che gli attori delle minacce cercheranno di sfruttare il più possibile il maggiore interesse e l'urgenza dei consumatori nel trovare offerte uniche.

Le minacce salienti emerse dall’Holiday Edition Threats Report:

* **Web skimming**: con l'aumento degli acquisti online, per i truffatori c'è una maggiore opportunità di sottrarre dati degli account dagli store ecommerce dell’esercente e di monetizzarli.
* **Phishing e social engineering**: il progresso dell'intelligenza artificiale (AI) nell'ultimo anno offre ai truffatori la possibilità di realizzare campagne di phishing altamente personalizzate, rendendo più difficile per i consumatori individuare i messaggi fraudolenti.
* **Skimming presso bancomat e POS**: con l'aumento del traffico pedonale presso esercenti e sportelli bancomat, i truffatori prenderanno prevedibilmente di mira i terminali ATM e POS con attacchi di skimming.
* **Bypass e provisioning dell’OTP**: Visa ha [identificato](https://usa.visa.com/content/dam/VCOM/regional/na/us/support-legal/documents/visa-pfd-biannual-threats-report.pdf) nuovi schemi per aggirare il codice di accesso unico (one-time-passcode - OTP) e ottenere l'accesso ai conti dei titolari di carta inviando alle vittime modelli OTP che sembrano associati all'acquisto desiderato.
* **Furto fisico**: i truffatori potrebbero tentare di rubare fisicamente carte di pagamento e/o telefoni ai consumatori ignari nei negozi affollati, nei centri commerciali o nei parcheggi.

“*Il Black Friday rappresenta un’occasione per i truffatori, i quali approfittano dell'aumento delle attività e della maggiore distrazione dei consumatori alla ricerca dell’offerta più conveniente*”, ha dichiarato Andrea Zamboni, Digital Solutions Director, Southern Europe di Visa. "*In Visa ci preoccupiamo di garantire sicurezza e affidabilità, con l’impegno di un monitoraggio delle minacce 24 ore su 24, 7 giorni su 7, anche durante i periodi più intensi dell'anno. Il team di esperti di Visa lavorerà anche quest'anno 24 ore su 24 per identificare e prevenire le frodi sulla rete, in modo che i consumatori possano effettuare i loro acquisti con tranquillità*".

**Black Friday: i consigli di Visa**

Con l’imminente arrivo del Black Friday, Visa consiglia ai consumatori che si stanno preparando allo shopping, le migliori procedure per un acquisto sicuro:

* **Acquistare da negozi affidabili**: è importante rivolgersi a negozi fidati e conosciuti. Se si pensa di acquistare da un negozio che non si conosce, è consigliabile fare delle ricerche per verificarne la reputazione e l'autenticità.
* **Proteggere le informazioni personali**: nel caso di acquisti online, assicurarsi che il sito web utilizzi una tecnologia sicura. Al checkout, l'indirizzo del sito web deve iniziare con https://. La "s" sta per “secure” e significa che i dati sono criptati e inviati tramite una connessione sicura.
* **Evitare il Wi-Fi pubblico per fare acquisti**: le reti Wi-Fi pubbliche sono spesso non protette, il che rende più facile per gli hacker rubare le informazioni. Si consiglia di utilizzare sempre una connessione Internet sicura e privata quando si fanno acquisti.
* **Attenzione alle offerte troppo belle per essere vere**: i truffatori spesso attirano le vittime con offerte incredibili, relative a prezzi particolarmente vantaggiosi su articoli difficili da acquistare per esempio. Se un'offerta sembra troppo bella per essere vera, è bene non fidarsi, perché sarà nella maggior parte dei casi non veritiera.
* **Utilizzare metodi di pagamento sicuri**: Le carte di pagamento offrono spesso una migliore protezione contro le frodi rispetto ad altri metodi. È preferibile evitare i trasferimenti diretti di denaro, i bonifici bancari e le applicazioni mobile peer-to-peer, perchè tra i bersagli preferiti dei truffatori.
* **Controllare e-mail e messaggi**: le truffe di phishing sono piuttosto frequenti durante questi periodi. Si raccomanda di non cliccare mai sui link presenti nelle e-mail o nei messaggi non richiesti. Prima di fornire informazioni personali, è opportuno verificare sempre l’autenticità del mittente tramite il servizio clienti o l'applicazione mobile.
* **Aggiornare dispositivi e software**: gli aggiornamenti regolari spesso includono patch di sicurezza che proteggono da nuove minacce. È bene assicurarsi che i propri dispositivi e software siano aggiornati.
* **Impostare password specifiche e sicure e utilizzare la tecnologia di autenticazione a due fattori:** ogni account online dovrebbe avere una password specifica e dovrebbe essere abilitato all'autenticazione a due fattori (2FA) in modo da rendere più difficile l'accesso ai truffatori.
* **Controllare gli estratti conto della banca e della carta di credito**: conviene controllare regolarmente gli estratti conto per individuare eventuali transazioni non autorizzate, oltre che attivare gli avvisi di transazione. Se si nota un’attività sospetta, va segnalata immediatamente.
* **Proteggere le informazioni personali:** non fornire mai informazioni personali se non sono necessarie. È bene diffidare dalle richieste di questo tipo, anche se il messaggio sembra provenire da un amico o da un famigliare.

Per Visa, sicurezza e affidabilità sono una priorità: negli ultimi cinque anni, la società ha investito più di 10 miliardi di dollari in tecnologia, anche per ridurre le frodi e aumentare la sicurezza della rete. Più di mille specialisti dedicati proteggono la rete di Visa da malware, attacchi zero-day e minacce interne 24x7x365. Nei primi sei mesi del 2023, Visa ha contribuito a bloccare in modo proattivo 30 miliardi di dollari di frodi, evitando a molte persone di imbattersi in una potenziale transazione fraudolenta.

\*\*\*\*\*\*

**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).