

Shopping Natalizio a rischio: le scorciatoie degli acquisti online nel mirino dei truffatori

Norton avverte: acquirenti e truffatori usano gli stessi strumenti — intelligenza artificiale e social media — per spuntare la loro lista dei desideri.

Milano, 16 ottobre 2025 — L'intelligenza artificiale e i social media stanno alimentando la corsa agli acquisti natalizi di quest'anno — ma secondo una ricerca di Norton, le stesse scorciatoie preferite dai consumatori vengono sfruttate anche dai truffatori. Il **Norton Cyber Safety Insights Report: Holiday 2025** evidenzia come l'utilizzo di scorciatoie per risparmiare denaro, le decisioni prese con urgenza e una fiducia eccessiva online espongano milioni di persone a rischi.

Nonostante ciò, l'**88% degli acquirenti online italiani** afferma che dedicherà del tempo alla ricerca di codici sconto sul web e quasi la metà degli italiani (**43%**) dichiara di essere incline ad approfittare immediatamente di un'offerta natalizia non appena la vede, spesso senza verificarne la provenienza. Il **73%** afferma di lasciarsi influenzare dalle buone offerte durante la stagione natalizia 2025, in aumento rispetto al 60% dello scorso anno.

Aiutanti di Babbo Natale o paradisi per hacker? Come i social media e l'AI aumentano i rischi dello shopping

Gli acquirenti di oggi cercano sempre più velocità e semplicità: il **44%** degli italiani ha già effettuato acquisti natalizi tramite annunci pubblicitari sui social media, incluso un **64%** della Gen Z. Tuttavia, secondo questo report natalizio di Norton, le stesse piattaforme rappresentano spesso un terreno fertile per le truffe: l'**81%** delle vittime di truffe natalizie ha perso denaro, con una perdita media di **172,70 € a persona**.

Allo stesso tempo, l'intelligenza artificiale si sta affermando come nuovo assistente per lo shopping natalizio: oltre un terzo degli italiani (**35%**) prevede di utilizzare strumenti come ChatGPT per trovare idee regalo quest'anno — in aumento rispetto al 25% dello scorso anno — e il **49%** della Gen Z conferma l'intenzione di usare ChatGPT in questo periodo. Tuttavia, la fiducia nello shopping online resta bassa: il **55%** degli italiani ritiene che durante le festività natalizie ci siano più truffe rispetto al resto dell'anno.

“Dagli strumenti basati sull'AI ai clic sugli annunci social, le persone cercano la comodità,” ha dichiarato **Leyla Bilge, Direttrice dei Norton Scam Research Labs**. “Ma anche i truffatori fanno lo stesso: proprio come nascondere una chiave di scorta sotto lo zerbino è rischioso, sono le piccole abitudini sottovalutate a rendere le persone più vulnerabili”.

Più costoso del previsto: le offerte natalizie possono costare caro

Il periodo delle festività aumenta il senso di urgenza, e i cybercriminali lo sanno bene: il **99% degli acquirenti italiani** farà almeno in parte acquisti online. Tra tutti gli intervistati, il **43%** afferma che probabilmente acquisterebbe subito un prodotto se vedesse un'offerta imperdibile online e circa **tre italiani su quattro (72%)** temono che i propri dati personali possano essere compromessi.



Le giovani generazioni risultano particolarmente vulnerabili. Il **49% ha già fornito dati personali** per ottenere sconti, percentuale che sale al **66% tra la Gen Z**.

Queste azioni possono avere conseguenze gravi: **circa la metà (49%)** delle persone nel mirino è effettivamente caduta vittima di truffe.

“I truffatori prosperano sfruttando la pressione, la distrazione e le decisioni emotive, e il periodo delle festività offre tutto questo in abbondanza,” ha dichiarato **Leyla Bilge**. “Non aspettano che tu commetta un errore: contano sul fatto che tu sia occupato, stressato e di fretta. E nel momento in cui abbassi la guardia, loro sono pronti. Oggi, con la sofisticazione delle truffe, anche chi è attento può essere attaccato”.

Il **Norton Cyber Safety Insights Report: Holiday 2025** rivela una tendenza chiara: se da un lato la tecnologia sta migliorando l’esperienza di acquisto natalizia, dall’altro sta anche ampliando la superficie di attacco a disposizione dei truffatori.

Dagli strumenti basati sull’intelligenza artificiale all’influenza dei social media fino alla cultura delle “offerte lampo”, **la vigilanza è più importante che mai**.

Norton 360 con rilevamento delle truffe basato sull’IA, [Norton Secure VPN](#) e [Norton Mobile Security](#) aiutano i consumatori proteggendoli da siti e annunci falsi, rilevando tentativi di phishing e mantenendo al sicuro le informazioni personali e di pagamento durante la stagione natalizia.

Per consigli su come fare acquisti in modo più sicuro per te e i tuoi cari, visita [Norton.com](#) e leggi il report completo qui: <https://newsroom.gendigital.com/Norton-Cyber-Safety-Insights-Holiday-2025>

A proposito del Norton Cyber Safety Insights Report: Holiday 2025

Lo studio è stato condotto online in Italia da Dynata per conto di Gen tra il 31 luglio e l’11 agosto 2025 su un campione di 1.000 adulti di età pari o superiore a 18 anni. I dati sono stati ponderati, ove necessario, per età, genere e regione, per essere rappresentativi a livello nazionale

Gen Threat Labs

Gen Threat Labs è il team di ricerca sulla sicurezza informatica di Gen, responsabile dell’identificazione, analisi e monitoraggio delle minacce digitali emergenti e delle truffe a livello globale. Questo team di esperti fornisce le informazioni innovative che alimentano le tecnologie di sicurezza del portafoglio di marchi affidabili di Gen, tra cui Norton, Avast, LifeLock e altri.

A proposito di Norton

Norton è leader nella Cyber Safety ed è parte di Gen (NASDAQ: GEN), un’azienda globale dedicata a potenziare la digital freedom con una famiglia di marchi consumer affidabili. Norton protegge milioni di individui e famiglie con soluzioni pluripremiate per la protezione dei dispositivi, della privacy online e dell’identità. I prodotti e i servizi Norton sono certificati da organizzazioni di test indipendenti, tra cui AV-TEST, AV-Comparatives e SE Labs. Norton è membro fondatore della Coalition Against Stalkerware. Scopri di più su <https://us.norton.com>.