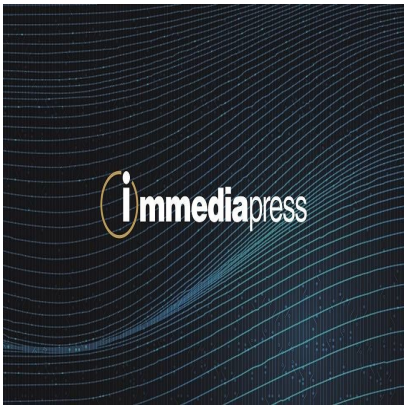

Kaspersky: evoluzione dello shopping digitale e nuove sfide per la privacy nel retail ed e-commerce nel 2026

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky ha pubblicato il Security Bulletin 2025, dedicato alla sicurezza informatica nel settore retail ed e-commerce. Il report analizza incidenti reali e le principali tendenze delle minacce che colpiscono gli utenti nella vita quotidiana, affrontando anche alcune sfide di sicurezza nel contesto B2B.

Cybersecurity nel settore retail e e-commerce nel 2025: i dati

Uno sguardo alla sicurezza informatica nel 2025 per retail ed e-commerce: tendenze e incidenti

Uno stealer con un debole per la consegna di pizza a domicilio. Fare shopping e ordinare cibo tramite app mobile Ã¨ ormai un comportamento abituale. Tuttavia, il 2025 ha dimostrato che anche scaricare unâ??app apparentemente legittima da uno store ufficiale non garantisce automaticamente la sicurezza, nÃ© assicura che i dati degli utenti e le credenziali finanziarie non vengano compromessi.

I rilevamenti di ransomware nel settore B2B sono aumentati a causa di un unico attore dominante. Il numero di utenti nel settore retail ed e-commerce che ha riscontrato rilevamenti di ransomware Ã¨ aumentato del 152% nel 2025 rispetto al 2023 (periodo novembre 2024 â?? ottobre 2025 rispetto a novembre 2022 â?? ottobre 2023). La crescita piÃ¹ significativa si Ã¨ verificata nel periodo 2024-2025 ed Ã¨ in gran parte attribuibile alla rapida diffusione della famiglia Trojan-Ransom.Win32.Dcryptor, diventata particolarmente diffusa nel settore retail ed e-commerce in alcuni dei mercati analizzati. Questo malware Ã¨ una variante di ransomware trojanizzata che sfrutta lâ??utilitÃ legittima

DiskCryptor per crittografare le partizioni del disco sui sistemi delle vittime.

Il phishing continua a giocare un ruolo centrale nel retail online. Nonostante sia una tecnica di attacco consolidata, il phishing rimane estremamente diffuso nel contesto degli acquisti online. Da novembre 2024 a ottobre 2025, i prodotti Kaspersky hanno bloccato 6.651.955 tentativi di accesso a link di phishing rivolti agli utenti di negozi online, sistemi di pagamento e corrieri. Di questi tentativi, il 50,58% era diretto agli acquirenti online, il 27,3% imitava sistemi di pagamento e il 22,12% prendeva di mira gli utenti dei corrieri.

Le stagioni dei saldi continuano a favorire gli hacker. I picchi stagionali degli acquisti online offrono agli hacker opportunitÃ prevedibili per intensificare gli attacchi mirati. I periodi di maggiore attivitÃ promozionale riducono la vigilanza degli utenti e consentono ai familiari scenari di phishing e spam di confondersi con il traffico di marketing legittimo, aumentando lâ??efficacia complessiva degli attacchi.

Previsioni: cosa potrebbe riservare il 2026 alla sicurezza informatica nel settore del retail e dellâ??e-commerce.

I chatbot diventeranno uno strumento frequente per la ricerca di prodotti online.

A differenza della ricerca tradizionale, le interfacce conversazionali incoraggiano gli utenti a condividere richieste piÃ¹ dettagliate e in linguaggio naturale, rivelando preferenze, vincoli e informazioni contestuali. Questo cambiamento amplia la superficie di attacco alla privacy, poichÃ© le piattaforme accumulano profili utente sempre piÃ¹ ricchi attraverso le interazioni in chat. Di conseguenza, i log dei chatbot possono diventare sensibili quanto i dati transazionali, aumentando i rischi di raccolta eccessiva, uso improprio o esposizione delle informazioni personali.

â??La ricerca stessa sta cambiando, compreso il modo in cui le persone cercano i prodotti online. Nel 2025 si Ã¨ assistito a un graduale passaggio dalle semplici ricerche per parole chiave a modalitÃ piÃ¹ conversazionali e visive. PoichÃ© questi modelli si basano su input piÃ¹ ampi da parte degli utenti, unâ??attenta gestione dei dati coinvolti rimarrÃ fondamentale per mantenere la fiducia degli utentiâ?• ,ha commentato Anna Larkina, Web Data and Privacy Analysis Expert di Kaspersky.

Le modifiche a imposte e norme commerciali potrebbero essere sfruttate per frodi online.

Cambiamenti nelle imposte, nei dazi doganali e nelle normative sul commercio transfrontaliero potrebbero essere utilizzati come esca in campagne di phishing e negozi online fraudolenti, promuovendo offerte irrealisticamente economiche o promettendo lâ??esonero dal pagamento delle tasse. Con lâ??evoluzione continua delle normative, la vigilanza degli utenti potrebbe diminuire, aumentando lâ??efficacia di questi schemi, in particolare nei confronti dei piccoli e medi rivenditori.

Gli assistenti allâ??acquisto basati sullâ??IA opereranno sempre piÃ¹ al di fuori delle piattaforme retail.

Lâ??integrazione in browser, app mobili e servizi di terze parti sposterÃ la raccolta dei dati al di fuori del perimetro diretto dei rivenditori, creando nuovi rischi per la privacy. Per funzionare efficacemente, questi agenti richiedono un accesso continuo al comportamento degli utenti, incluse attivitÃ di navigazione, intenzioni di ricerca, contesto geografico e interazioni con i prodotti su piÃ¹ siti. CiÃ² consente lâ??aggregazione di profili comportamentali dettagliati, aumentando i rischi di raccolta eccessiva, utilizzo opaco dei dati ed esposizione involontaria delle informazioni.

La ricerca di prodotti basata sulle immagini potrebbe rappresentare una nuova sfida per la privacy.

Se in passato le preoccupazioni erano limitate alle immagini condivise volontariamente nelle recensioni, in futuro il caricamento di foto diventerÃ una parte abituale dellâ??esperienza di acquisto. Le immagini possono contenere volti, ambienti domestici o dettagli sensibili â?? come nomi, numeri di telefono o indirizzi visibili su etichette di spedizione â?? rendendo fondamentali il trattamento sicuro, la minimizzazione dei dati e politiche di conservazione limitate.

Il report completo di KSB sul retail e lâ??e-commerce Ã¨ disponibile al link.

Per proteggersi, gli esperti di Kaspersky raccomandano di:

Per le aziende retail ed e-commerce Kaspersky consiglia di:

Proteggere lâ??infrastruttura aziendale da unâ??ampia gamma di minacce, tra cui phishing e ransomware. Utilizzare le soluzioni della linea di prodotti Kaspersky Next che forniscono protezione in tempo reale, visibilitÃ delle minacce, capacitÃ di indagine e risposta avanzata. Se unâ??azienda non

dispone di personale specializzato in sicurezza informatica, puÃ² adottare servizi di sicurezza gestiti come Kaspersky Managed Detection and Response (MDR) e/o Incident Response che coprono lâ??intero ciclo di gestione degli incidenti, dallâ??identificazione delle minacce alla protezione continua e alla risoluzione.

[1] Da novembre 2024 a ottobre 2025

[2] Da novembre 2024 a ottobre 2025

[3] Dati KSN, Da novembre 2024 a ottobre 2025

[4] Da novembre 2024 a ottobre 2025 vs Novembre 2022 â?? ottobre 2023

[5] Da novembre 2024 a ottobre 2025

[6] Da novembre 2024 a ottobre 2025

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Gennaio 12, 2026
Autore
redazione