Gen Q4 Threat Report Shows Scams Thriving Inside Ads, Feeds, and Video

20.1.2026 - | Avast Software

Fake ads led all consumer cyberthreats in 2025, with over 45 million fake shop attacks blocked in Q4 and deepfake scams surging on social media.

TEMPE, Ariz. and PRAGUE, Jan. 20, 2026 /PRNewswire/ -- Gen (NASDAQ: GEN), a global leader powering Digital Freedom with a family of trusted brands including Norton, Avast, LifeLock, MoneyLion and more, today released its Q4 2025 Gen Threat Report, looking at trends from October through December.

The report reveals how cybercrime in late 2025 increasingly relied on ordinary digital actions rather than sophisticated exploits. Across browsers, social feeds, messaging apps, and money tools, the most damaging attacks succeeded when people completed the final step themselves: clicking a link, scanning a QR code, approving a device pairing, or entering a verification code.

"Increasingly throughout 2025, scams did not announce themselves as threats. They blended into everyday digital routines," said Siggi Stefnisson, Cyber Safety CTO at Gen. "Attackers leaned on familiar platforms, trusted interfaces, and automated persuasion, then scaled those tactics across devices and channels."

Scams and Malvertising Dominate Shopping and Social Media

Scams showed up where people already spend their time online: in social feeds and videos. Fake online shops dominated during the holiday season with over 45 million blocked fake shop attacks in Q4, more than half of all fake shop attacks blocked in 2025 and a more than 62% increase from the same period in 2024. These fake shops also accounted for 65%[1] of all threats blocked on social media, and were heavily concentrated on Facebook and YouTube, where most risky shopping clicks began. Phishing spread more broadly across platforms, led by Facebook (77%), followed by YouTube (13%) and Reddit (4%). For consumers, scam delivery increasingly felt indistinguishable from ordinary ads, posts, and videos until the moment money, credentials, or remote access were requested.

Gen telemetry also showed that malvertising – fake advertisements – was the top cyberthreat to individuals in 2025, accounting for 41% of all attacks and serving as the first click leading to many scams across social media and the internet at large. This aligns with recent reporting citing internal Meta documents suggesting scam and banned-goods advertising may represent roughly 10% of annual ad revenue (about $16 billion).

Dangerous Deepfakes
Gen introduced on-device detection on Windows focused on the intersection of manipulated media and scam intent. Early telemetry from this launch showed that YouTube accounted for the largest share of blocked AI scam videos, followed by Facebook and X. Most blocked content was tied to financial, investment, and cryptocurrency lures, and was intercepted during playback, not downloads.

Identity and Financial Risk Broadened

Identity abuse continued to compound beyond traditional credit misuse. Gen telemetry shows the

number of breaches increased 176% quarter over quarter, with a significant upward trend throughout the year. Data also shows rising alerts tied to:

The rising risk ratios in these categories reinforce what external reports suggest: identity fraud is getting more layered, touching property records, deposits, credit instruments and scam-driven social engineering in parallel.

Threats Continue to Move Across Platforms

In Q4, Gen saw scams increasingly move back and forth between devices, using people to carry the attack across platforms. Some campaigns started on desktop with fake tutorial pages, then pushed victims to scan the screen with their phone, shifting the next steps onto mobile where permissions, sideloading, or verification were more likely. Others moved in the opposite direction. In GhostPairing attacks, first uncovered and named by Gen Threat Labs, victims entered a numeric code in WhatsApp on their phone, unknowingly linking an attacker-controlled browser as a trusted device and enabling rapid spread through contacts. Together, these patterns showed how modern scams crossed device boundaries to scale quickly and stay invisible.

As 2025 closed, Gen's Q4 data showed that the attack surface had become continuous across browsers, chats, social platforms, and money apps. The most damaging incidents began with small, familiar actions performed under time pressure or false reassurance.

To read the full Q4/2025 Gen Threat Report, visit https://www.gendigital.com/blog/insights/reports/threat-report-q4-2025

About Gen

Gen (NASDAQ: GEN) is a global company dedicated to powering Digital Freedom through its trusted consumer brands including Norton, Avast, LifeLock, MoneyLion and more. The Gen family of consumer brands is rooted in providing financial empowerment and cyber safety for the first digital generations. Today, Gen empowers people to live their digital lives safely, privately and confidently for generations to come. Gen brings award-winning products and services in cybersecurity, online privacy, identity protection and financial wellness to nearly 500 million users in more than 150 countries. Learn more at GenDigital.com.

About the Gen Threat Labs

Gen Threat Labs is the Cyber Safety research team within Gen, focused on uncovering and analyzing the latest digital threats and scams worldwide. Rooted in data, research, and technical expertise, the team identifies patterns and risks that shape the evolving cyber landscape. Their insights power the security technologies that protect people across Gen's portfolio of trusted brands, including Norton, Avast, LifeLock, and others.

Brittany Posey
Gen
Press@GenDigital.com

Courtney Rowles
Edelman for Gen
Courtney.Rowles@Edelman.com

SOURCE Gen Digital Inc.

https://newsroom.gendigital.com/2026-01-20-Gen-Q4-Threat-Report-Shows-Scams-Thriving-Inside-Ads,-Feeds,-and-Video