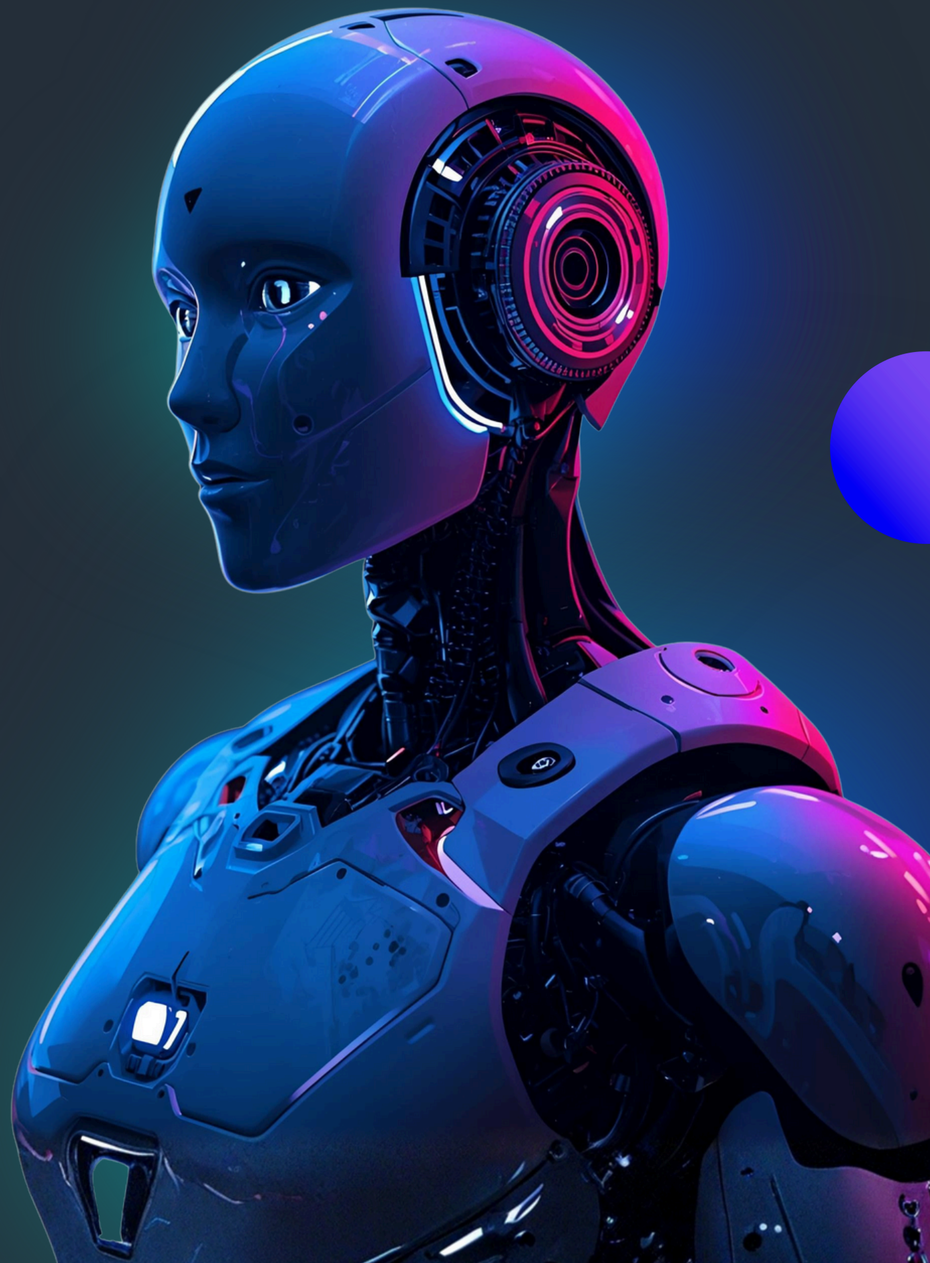
Q4/2025 KEY HIGHLIGHTS

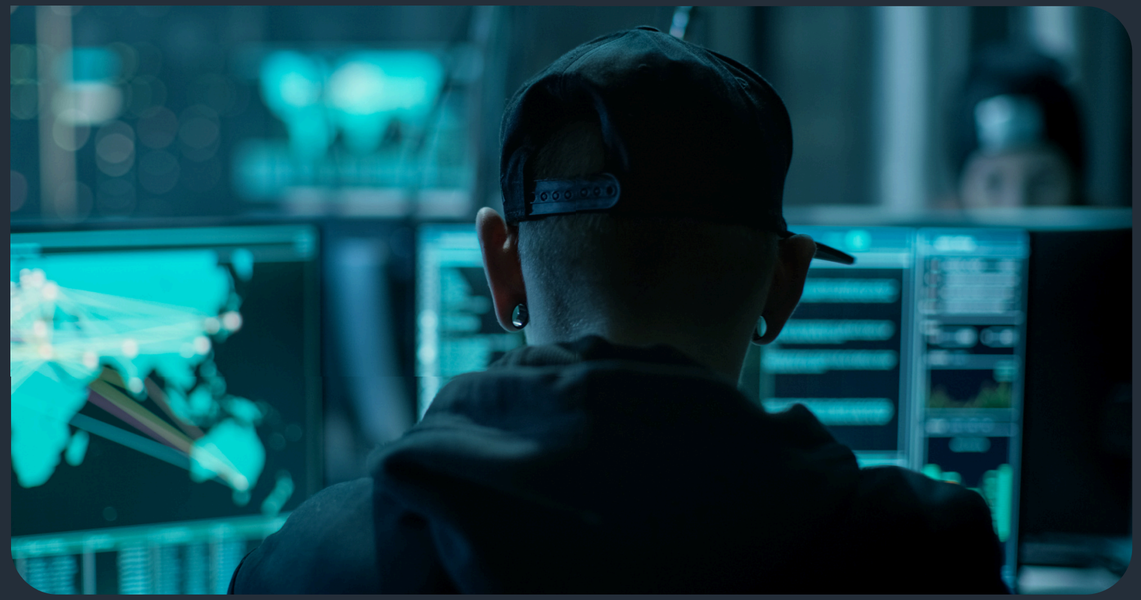
Gen Threat Report

How scams hid in plain sight



norton™ Avast™ LifeLock™ by norton MoneyLion®

Where the threats hit & what the data shows



In Q4, scams scaled by blending into trusted platforms, not by using new exploits.

What stood out this quarter

- 45M+ fake online shop attacks blocked in Q4
- +175% QoQ increase in data breach events
- +157% QoQ increase in breached records, peaking at 2M+ in December
- 41% of all attacks in 2025 began with malvertising
- 65% of social media threats were tied to fake shops

Attacks now start with “normal” actions

Scanning a QR code. Clicking a tutorial. Tapping a sponsored post. In Q4, some of the most damaging attacks didn’t rely on exploits; they relied on people completing a familiar step themselves.

How it showed up ↓

- Clicking ads and shopping links
- Scanning QR codes
- Approving device pairings
- Entering verification codes

Why it matters ↓

The attack didn’t look suspicious. The moment of compromise looked routine.

Fake shops and ads that turn browsing into scams

In Q4, scams increasingly arrived as ordinary ads, product listings and shopping links. Rather than redirecting users to obviously malicious sites, attackers embedded fraud directly into familiar browsing and buying flows, especially during the holiday shopping period.

45M+ fake online shop attacks blocked in Q4

What we saw

- A sharp Q4 surge in fake online shops, accounting for over half of all fake shop attacks blocked in 2025
- Scam activity concentrated on high-traffic platforms
- Ads and sponsored content increasingly served as the first click in scam chains

Tactics used

- Fake storefronts mimicking real brands and seasonal deals
- Malvertising embedded in social feeds, search results and video platforms
- Payment prompts designed to look like legitimate checkout flows

Why it matters

Malvertising accounted for 41% of all attacks in 2025, while fake shops drove 65% of social media threats, making scams increasingly indistinguishable from normal shopping until payment or credentials were requested.

AI moved from novelty to financial weapons

In Q4, AI made scams more personal, scalable and persistent, amplifying both initial fraud and downstream identity abuse.

What we saw

- AI-generated voices and videos used in investment, finance and crypto scams
- Breach exposure resurfacing later as account takeovers and new financial activity

Tactics used

- Deepfake and manipulated media paired with urgency and money requests
- AI-assisted impersonation of trusted figures and institutions
- Reuse of breached data to enable identity-based fraud over time

The takeaway

Breached records rose +157% QoQ, peaking at 2M records in December. As AI lowers the cost of persuasion, a single breach can now compound into months of financial and personal risk.

GhostPairing: How attackers quietly hijack WhatsApp accounts

GhostPairing abuses WhatsApp's device-linking feature through social engineering. Attackers send messages that appear to come from someone you know (like "Hey, I just found your photo!"), leading to a fake pairing page. When users enter their phone number and code, they unknowingly link an attacker-controlled device to their account.

What we saw

- Messaging accounts became live surveillance and impersonation tools
- Attacks spread rapidly through trusted contacts and group chats
- Compromise persisted without malware, password theft, or SIM swaps

Tactics used

- Fake pages prompting users to "verify" or "continue" via device pairing
- Abuse of legitimate numeric code–based linking flows
- Account mirroring that enabled real-time message access and propagation

Why it matters

GhostPairing turns trusted account features into takeover tools, enabling persistent access and impersonation without exploiting security systems.

Fast Facts. What to Watch.

Routine actions now trigger attacks

Risk was up nearly 18% QoQ

Extortion is shifting to data theft

Only ~23% of ransomware victims paid

Breaches drive ongoing identity abuse

176% increase in breaches QoQ

Phones are now prime surveillance targets

Mobile spyware detections peaked in November

Scam delivery is concentrating

Nearly 96% of social-origin scams came from Facebook and YouTube (based on desktop detections)

Identity fraud is moving beyond credit

Alerts tied to property records (+252%) and bank accounts (+112%) surged

Gen’s Q4 Threat Response

Fake online shops: Detected and blocked large-scale fake shop and malvertising campaigns

Deepfakes & AI-enabled financial scams: Flagged scam intent where manipulated media and financial lures intersect

Data breaches at growing scale: Monitored accelerated breach activity and surfaced exposure signals that reappear later as account takeover, fraud and identity misuse

Identity abuse beyond credit misuse: Expanded identity alerts to include property records and more

GhostPairing & account takeover: Identified and blocked cross-device social engineering flows

Read the full Q4/2025 Gen Threat Report

GenDigital.com/Blog

Instagram.com/GenDigital

LinkedIn.com/company/GenDigitalInc