Q3/2025

Gen Threat Report

This quarter, we uncovered major shifts across the landscape: scammers using AI website builders to clone trusted brands, ransomware that accidentally made file recovery possible and a sharp rise in SMS-based scams targeting people worldwide.

VibeScams

190k unique users protected from AI scam sites
~580 new scam sites per day

Ransomware

“Midnight” - new ransomware
New free decryptor from Gen

SMS scams

Smishing on the rise
$470M loss in text scam 2024

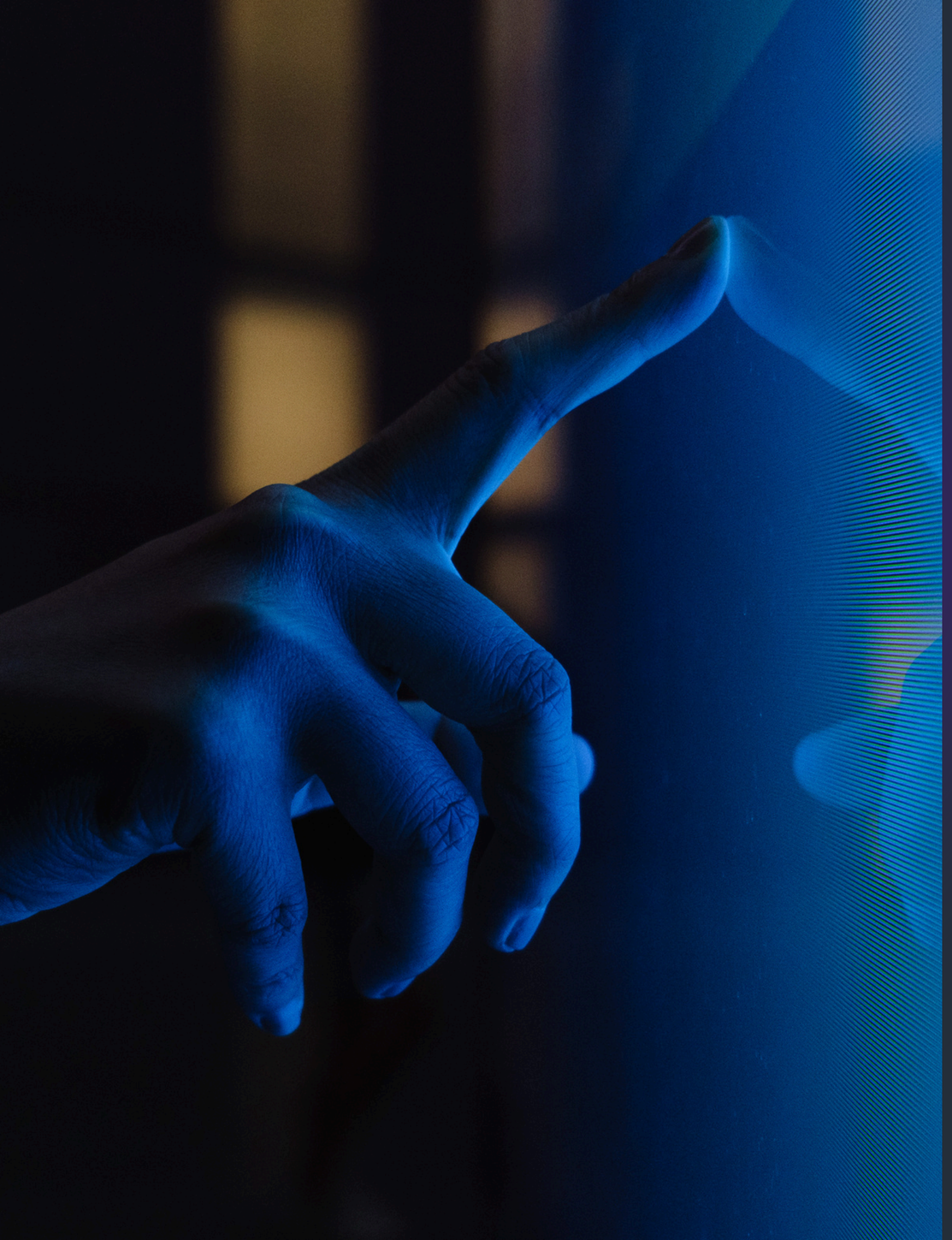


Table of Contents

The threat landscape

Next wave of digital deception

Cyber threats in Q3 2025 evolved faster, smarter, and became much more personal. Mobile scams and adware dominated, with HiddenAds-style fake apps sneaking into official stores and new “Scam-Yourself” flows tricking users into tapping into danger. On desktops, Remote Access Trojans like Wincir continued to spread, alongside waves of sextortion, gambling, and tech-support scams. Beyond devices, data breaches surged 82%, but with fewer total records exposed — a shift showing attackers are now trading scale for precision, focusing on high-value data like passwords and financial details.

AI officially became part of the threat landscape. Criminals are now steering AI assistants, hijacking extensions, and embedding AI inside malware to create more adaptive attacks. Emerging threats like PromptLock ransomware suggest a future where malware can generate commands in real time. State actors are following suit — using AI to craft fake IDs and spear-phishing lures — while AI-written pages and texts mimic brands so well that a few seconds of trust is all it takes. Meanwhile, Gen’s Media Shield telemetry on Windows AI PCs detected early-stage deepfake scams, showing how manipulated media is being used not to go viral, but to quietly deceive.

82%
increase in data breaches

VibeScams

AI-generated phishing factories

- Scammers now use AI website builders to clone legitimate sites instantly.
- Platforms like Lovable, Webflow, and Elementor are being abused to mass-produce phishing pages.
- Over 140,000 AI-generated scam sites detected and blocked, ~580 new per day.
- Scams imitate brands like Coinbase, Microsoft, DHL and Amazon.
- Attackers need zero coding skills — just prompts.

Why it matters:

AI has made cybercrime faster, cheaper, and more convincing — anyone can now become a "web developer" of scams.

Top advice: verify URLs, use MFA, and rely on reputable AV tools to filter malicious domains.

190k
unique users protected from AI scam sites

~140k
AI-generated scam sites blocked since Jan 2025

Midnight ransomware: decrypted

When a cybercriminal's mistake becomes a victim's lifeline

- New ransomware "Midnight" discovered by Gen researchers, evolved from Babuk.
- **How does ransomware work?** Ransomware encrypts (scrambles) your files using a mathematical algorithm, so you can't open them unless you have the unique decryption key (which attackers demand payment for).
- Gen built and released a free decryptor to help users reclaim data.

What a decryptor does:

A decryptor uses knowledge of the ransomware's **encryption flaws, leaked keys**, or **reverse-engineered code** to unlock those files safely. It works like a master key built by cybersecurity researchers.

Why it matters:

A decryptor tool lets people get their files back **without paying hackers**. It breaks the ransom cycle and helps stop ransomware from being profitable.

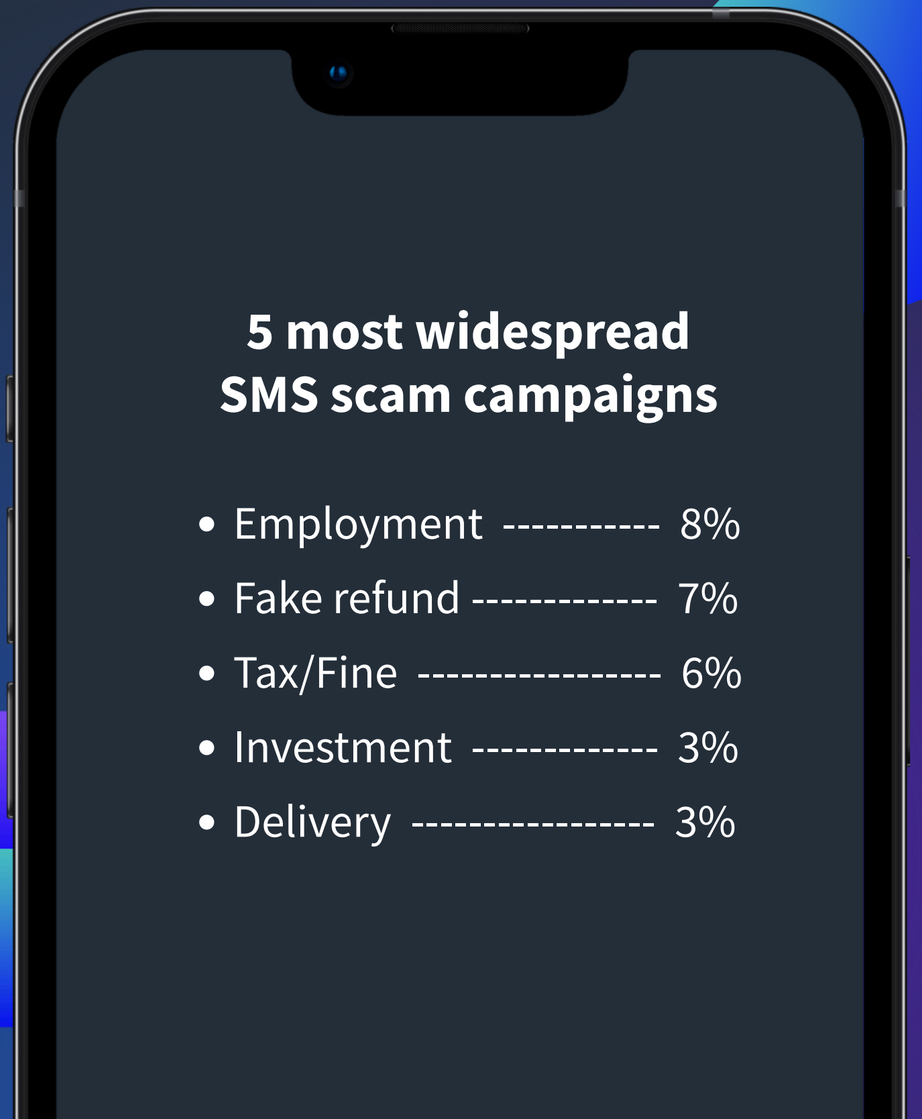
SMS threats: the tiny texts criminals love

Big scams in small places

- Surge in SMS-based phishing (“smishing”) across delivery, banking, and refund scams.
- Common hooks: fake package delivery, OTP theft, tax fines, job offers, crypto tips.
- Scammers exploit brand-style threads (e.g., “Your package couldn’t be delivered – reschedule now”).
- Why it’s rising: phones now store wallets, IDs, 2FA codes.
- Over 15 scam archetypes identified, from “Hi Mom” impersonations to fake WhatsApp support.

$470M

in loss that started with a text in 2024



Fast Facts. What to Watch.

3 Things to Know:

190,000
unique users protected from AI-generated scam sites since January 2025

500+
new malicious sites created daily using AI builders

1 in 4
scam texts were fake job offers, refund, tax, investment, or delivery scams.

Trends to watch in cybersecurity are rapidly reshaping the threat landscape. **Artificial intelligence is democratizing cybercrime**, making it easier and faster for bad actors to launch sophisticated attacks that are increasingly difficult to detect.

At the same time, **scams are blending across multiple platforms**, with SMS, web, and social media now overlapping to create more convincing and coordinated schemes. In response, **decryptors are emerging as a powerful line of defense**, with innovation from the Gen family of brands helping victims reclaim control and recover from attacks effectively.

Q3 Threats	Response from Gen
AI-Phishing (VibeScams) - 140k AI-built fakes blocked	Coordinated abuse reporting with builders; boosted in-product link protection
Top 5 smishing campaigns - 26% of all scam SMS	Upgraded mobile filters; AI-based message defense
Midnight Ransomware - Copy-paste strain with crypto flaw	Release free decryptor; shared global analysis
HiddenAds Adware Surge - +77% Q/Q Android	Blocked fake-app installs; strengthened detection models
Data & ID Fraud - + 82% breaches, 83% with passwords	Expanded BreachGuard + Credit Alerts for faster lock & response
Deepfake scams - AI-voice/video fraud rising	Rolled out media shield deepfake detection on Windows AI PCs

Read the full Gen Threat Report

GenDigital.com/Blog