# Gen Half-Year Threat Report: Attackers are Moving Closer to the Systems People Trust

2026-07-15

*New research finds cybercriminals are increasingly exploiting trusted digital experiences rather than relying on obvious malware or technical exploits*

TEMPE, Ariz. and PRAGUE, July 15, 2026 /PRNewswire/ -- Gen (NASDAQ: GEN) today published its H1 2026 Threat Report to help people understand what cyber threats are emerging and what risks are shaping digital life today. A common thread runs through the report: attackers are moving closer to the trusted parts of digital life. Not only are they sending malicious links or dropping malware, they're also abusing context, sessions, workflows, brands, update systems, advertising platforms and delegated authority.

**Trust Has Become the New Attack Surface**
The Threat Report's central finding is a shift in how attacks work. The most effective threats in the first half of 2026 did not rely on technical exploits or obvious deception, they succeeded because they were hard to distinguish from normal digital life. Scams arrived through hotel booking platforms, referencing a real reservation. WhatsApp accounts were compromised not through stolen passwords but by tricking people into approving an attacker's browser as a linked device. Fraud flowed through real, verified financial accounts whose owners were recruited on social media with promises of quick cash. And AI agents, running with permissions the user had already granted, were stopped before executing a reverse shell.

"The most effective attacks in the first half of 2026 didn't look like attacks," said Vita Santrucek, Chief Technology & Development Officer at Gen. "They arrived through booking platforms, family message threads, software update channels and AI agent workflows – all places people already trust. As attackers blend into everyday digital experiences, protection has to move closer to the moments where confidence is earned, exploited or broken."

Across scams, identity breaches, and privacy violations, the pattern is the same: the attack moved inside trusted systems before the danger became visible.

**Threat Report Highlights**
Gen telemetry and research findings show the following trends across key threat areas over the last six months:

- 114.2 million e-shop scam attacks blocked, up 109% – highlighting the growing risk of fake online stores targeting shoppers
- A 387% increase in government impersonation scams – showing criminals are increasingly exploiting trust in public institutions to steal money and information
- A more than 454% increase in family impersonation scams, while separate "GhostPairing" activity showed how WhatsApp's linked-device feature can be abused to gain persistent access to an account and allow people to impersonate loved ones

- 20.3 million tech support scam attacks blocked – reflecting continued attempts to trick people into giving scammers remote access to their devices or financial information
- More than 304 million scam-ad impressions identified across the EU and UK in less than one month, underscoring how easily fraudulent ads can reach people
- Roughly 1.9 billion tracking attempts blocked during H1 2026 – demonstrating the scale of online tracking that can erode consumer privacy
- Norton and LifeLock breach notification alerts with attributed leak sources increased 628.1% up to 3.3 million, with more than 10 million breach notifications sent in total – proving more people's personal information is being exposed in data breaches
- Bank account activity alerts increased 734% – reflecting both expanding monitoring coverage and a sharp rise in flagged financial activity
- 1 million web skimming attacks blocked, up 212% – showing how attackers continued to target checkout flows where users already expect to enter payment details
- More than 15.7 million breached records containing email addresses identified, giving cybercriminals more opportunities to target consumers with phishing, scams, and account takeover attempts

The report also identifies agentic AI as an emerging security frontier. As AI systems gain the ability to browse, install software, access files, connect to services and take action on behalf of users, attackers are increasingly targeting the permissions and trust these systems rely on. Early telemetry from Sage, Gen's agentic security platform behind features like Norton and Avast's AI Agent Protection, found the most common high-risk AI agent behaviors involved:

Trying to run dangerous system commands
Attempting to open a remote command channel, which could let an attacker control the system
Downloading and running code from the internet
Reading credential files without authorization
Creating persistent remote access, such as adding a trusted SSH key
Working to override the agent's instructions
The full Gen H1 2026 Threat Report is available at https://www.gendigital.com/blog/insights/reports/threat-report-h1-2026

**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.

Media Contact:
Brittany Posey
press@gendigital.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/gen-half-year-threat-report-attackers-are-moving-closer-to-the-systems-people-trust-302826372.html

SOURCE Gen Digital Inc.