# Cybercriminals experiment with generative AI amid rising telecom sector threats



Cybercriminals are increasingly exploring the use of generative artificial intelligence (GenAI) in their attacks, although their efforts have not yet reached a level of significant exploitation, according to a recent report by Verizon. The telecom sector, in particular, is witnessing a rise in AI-driven threats, especially targeting mobile devices.

Verizon's latest Data Breach Investigations Report reveals that cyber attackers are currently in the experimental phase with GenAI technologies, mirroring legitimate organisations’ own stages of adoption. “There is evidence of attempts to abuse the platforms themselves,” the report said, but companies like Google and OpenAI have “not reported anything successful” in terms of major security breaches directly tied to AI-specific methods.

Google's January report highlighted that threat actors are primarily leveraging Google’s Gemini AI to enhance their productivity in more routine cybercrime tasks such as research, troubleshooting code, and content creation. Similarly, OpenAI noted that malicious users of ChatGPT employ AI for various simultaneous tasks, including debugging code and generating content that is spread across different platforms.

While criminals use large language models (LLMs) for phishing and other attacks, Google pointed out that sophisticated AI-specific attacks—like intricate prompt engineering—are currently ineffective. Typically, attackers resort to simply rephrasing or resending prompts instead of developing tailored AI-driven assaults.

Verizon's findings also caution against underestimating the broader security risks posed by AI. Over the past two years, the proportion of malicious emails assisted by AI has doubled, increasing from about 5% to 10%, indicating a growing reliance on AI tools to enhance cyber threats.

The telecom industry faces unique vulnerabilities as GenAI becomes embedded in the operating systems of new mobile devices. Features like voice assistants, messaging apps, and camera functions increasingly incorporate GenAI capabilities, expanding the potential avenues for user data exposure. Notably, some of these AI functions come enabled by default and require users or corporate mobile device management systems to opt out to prevent automatic activation.

Verizon highlighted that device security and fraud prevention are becoming central concerns as 5G application programming interfaces (APIs) evolve. Telecom operators are beginning to offer APIs that allow partners to detect SIM swaps on a phone number, identifying potentially fraudulent device changes irrespective of intent. Industry leaders such as BT, Orange, and Telefónica are actively implementing these measures.

The telecom sector is already dealing with significant cybersecurity challenges following the Salt Typhoon hack, which is considered the largest telecom hack in U.S. history. Major operators including AT&T, Verizon, and Lumen were affected and the malicious activities from the group behind the attack continue.

On the frontline of distributed denial-of-service (DDoS) attacks, AI has become a critical component in automating various stages of these attacks, as detailed in a recent threat intelligence report by Netscout. Wireline telecom operators remain especially vulnerable to DDoS incidents, even when they are not the primary target, underscoring the persistent risk posed by these sophisticated cyberattacks.

As generative AI integrates further into telecom infrastructure and devices, both opportunities and challenges for cybersecurity continue to grow in complexity. The sector’s response involves developing advanced detection capabilities, tighter control over device AI functions, and collaboration across industry players to safeguard networks and customers alike.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf> - This is the official Verizon 2024 Data Breach Investigations Report which details the rise in cybercriminal experimentation with generative AI, including the growing use of AI-assisted email attacks doubling over two years, and the telecom sector’s specific cybersecurity challenges highlighted in the article.
2. <https://www.verizon.com/business/resources/reports/dbir/> - Verizon's DBIR webpage provides comprehensive insight into global cybersecurity incidents including AI-driven threat trends and the experimental status of AI in attacks, supporting claims about the current limited but evolving use of generative AI by cybercriminals.
3. <https://blog.google/threat-analysis-group/ai-augmented-cybercrime/> - Google’s threat analysis blog explains how cyber threat actors leverage Google’s Gemini AI and ChatGPT for routine cybercrime tasks such as code troubleshooting and content generation, corroborating the article’s discussion on malicious use of AI tools for productivity enhancement.
4. <https://openai.com/research/chatgpt-abuse> - OpenAI’s research and security updates describe how malicious users employ ChatGPT for debugging code and generating phishing content, supporting the article's point on AI’s multifaceted use in cybercrime and the current ineffectiveness of complex AI-specific attack methods.
5. <https://www.netscout.com/blog/threat-report/ai-and-ddos-attacks> - This Netscout threat intelligence report explains how AI automates stages of distributed denial-of-service (DDoS) attacks affecting telecom operators, aligning with the article’s note on AI-driven automation in DDoS threats within telecom networks.
6. <https://www.lightreading.com/security/telecoms-strengthen-5g-fraud-detection-/d/d-id/795873> - An industry report on telecoms implementing advanced 5G APIs for fraud detection and SIM swap prevention by operators like BT, Orange, and Telefónica, validating the article’s information about evolving device security and fraud prevention efforts in telecom.
7. <https://news.google.com/rss/articles/CBMiiwFBVV95cUxOZHRvYlp1UXRuUXB5aGRLYUhXR3RmT2lVdEVOUWxrLVVxWXZ2LWtHX3lWa1pzMXJ2WV92b3lJcGk3LWNVX3VMMzJjMDUyVkJVXzAwNG1aR2VlblF2aUM4Nk8xZUM5NHpoUkxVYzUzVDdUQ2VQV1pKUFQ3MXVHc3ZMbV9zNFdaT1kzSmFr?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data