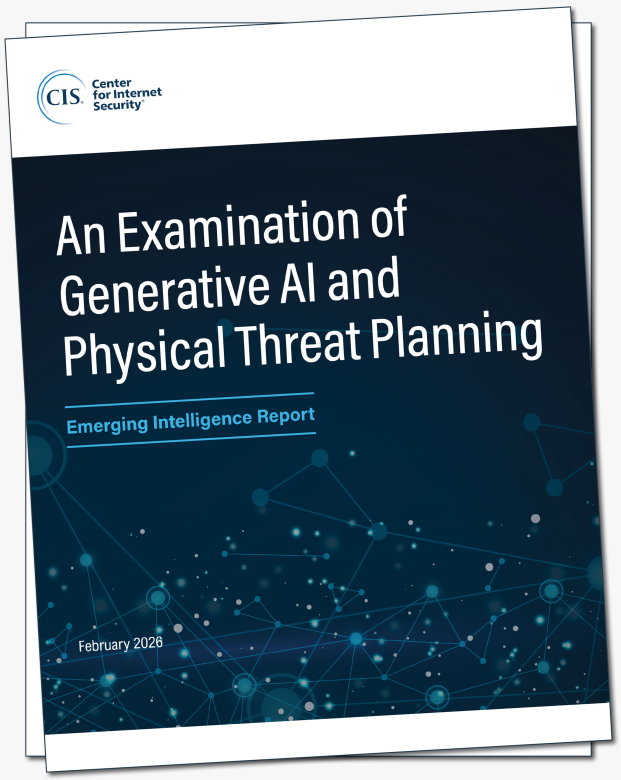
CIS Report Warns: AI Tools Can Aid Criminals in Planning Physical Attacks

EAST GREENBUSH, NY, UNITED STATES, March 12, 2026 /EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS®) has released a new report revealing that widely available generative artificial intelligence (GenAI) tools can make it easier for malicious actors to plan real world physical threats. The study, An Examination of Generative AI and Physical Threat Planning, shows how individuals, using only cleverly worded prompts, can bypass built in safety features in popular AI systems to obtain information that could support dangerous activities, such as targeting critical infrastructure or law enforcement.



An Examination of Generative AI and Physical Threat Planning

Researchers tested “jailbreak” techniques on three well known GenAI platforms, discovering that each system provided detailed responses when prompted on topics like constructing explosive devices, exploiting border vulnerabilities, or identifying weaknesses in essential services. While much of the information is technically available through open sources, the report highlights that AI systems make retrieving it faster, easier, and more precise, changing the risk landscape in ways that public safety officials need to know.

Key Findings from the Report:

• AI jailbreaks work across multiple platforms. All three models tested by CIS responded with detailed guidance on sensitive physical threat topics when prompted through bypass

techniques.

- Threat planning can be made easier for non experts. AI tools organized, summarized, and clarified information that previously required hours of specialized research.
- The threat environment is shifting quickly. CIS analysts assess it is “highly likely” that criminals will increasingly use GenAI to support malicious activities.
- Traditional safeguards are not keeping pace. The report concludes that current safety filters are unlikely to significantly improve without reducing functionality for legitimate users.

> “Our findings show GenAI is lowering the barrier of entry further than ever for people looking to plan real-world harm. It is essential that public safety officials update their threat assessments.”
>
> *TJ Sayers, Senior Director of Threat Intelligence at CIS*

“Our findings show that generative AI is lowering the barrier of entry further than ever for people looking to plan real-world harm,” said TJ Sayers, Senior Director of Threat Intelligence at CIS. “This technology is not creating entirely new information, but it’s making dangerous information far more accessible and quickly actionable. It's essential that law enforcement, public safety officials, and critical infrastructure operators update their threat assessments accordingly.”

For additional report details or media inquiries, please contact media@cisecurity.org.
###

About CIS:
The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities. To learn more, visit cisecurity.org or follow us on X: @CISecurity.

Kelly Wyland
Center for Internet Security
518-256-6978
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube

X