# ANY.RUN Warns on AI Risks in Cyber Security: Key Threats and Solutions to AI Safety

DUBAI, DUBAI, UNITED ARAB EMIRATES, March 12, 2025 /EINPresswire.com/ -- ANY.RUN, a leading malware analysis and threat intelligence service provider, presents a research overview on the risks of AI's and LLMs' abuse and failures. Our analysts dwell on three major AI threats: phishing and malware generation, the misuse of AI for opinion shaping and unethical purposes, and unintended AI failures leading to harmful consequences.

□□□ □□□□□□□□□□ □□□□□□□□□□□ □□ □□□ □□□□□□□:

□. □□-□□□□□□□ □□□□□□□□ □□□ □□□□□□□ □□□□□□□□□□

· AI-generated phishing emails and deepfakes have become more sophisticated, making fraudulent activities harder to detect.

· Attackers use AI to automate the creation of malware, bypassing ethical safeguards through jailbreaking techniques.

□. □□ □□□□□□□□□ □□□□□□□□□□□□ □□□ □□□□□□□ □□□□□□□

· AI providers have the ability to subtly influence model outputs, raising concerns over transparency and bias.

· AI-generated misinformation poses risks to public discourse and electoral integrity.

□. □□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□ □□□□□□□□ □□□ □□□□□

· Researchers and AI companies are developing countermeasures and adaptive AI defenses, cybersecurity companies learn to work with the new types of threats while employing AI tools in their own products.

For the detailed insights on the threats and the proposed solutions, see the research in ANY.RUN's blog.

□□□□□ □□□.□□□

ANY.RUN is a provider of interactive malware analysis and threat intelligence solutions, allowing cybersecurity professionals to analyze threats in real time, detect malicious activity, and respond proactively.

ANY.RUN actively researches AI-related threats while leveraging AI-driven solutions to enhance cybersecurity. Within the ANY.RUN Interactive Sandbox, AI-generated summaries help users understand potential risks. The platform's AI capabilities also facilitate automated interactivity, such as handling CAPTCHAs and executing specific actions within virtual environments.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
LinkedIn