The New Face of Cybercrime and How to Fight Back with AI

A recent increase in phishing attacks, driven by profit-seeking criminal hackers, has been linked to the utilization of OpenAI tools. However, a new report from Microsoft reveals that state-sponsored hacking groups are also capitalizing on these AI capabilities. Microsoft's findings indicate that attackers currently hold the advantage in AI utilization, with cybersecurity defenses struggling to effectively counter these advancements. Notable state-sponsored hacking groups from China, Russia, North Korea, and Iran have been identified as active users of OpenAI tools and other large language models (LLMs).

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.