Keeper Security Research Reveals AI is Driving a New Generation of Advanced Cyber Attacks

New data shows AI is making phishing and smishing attacks harder to detect, with 84% of IT leaders acknowledging the increased challenge

LONDON, UNITED KINGDOM, October 10, 2024 /EINPresswire.com/ -- The rise and continued advancement of Artificial Intelligence (AI) is transforming cybersecurity, introducing new complexities in threat detection and response. New research from Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, shows that while organisations are implementing AI-related policies, there is still a notable gap in overall preparedness.

Keeper's survey highlights that 84% of IT and security leaders find AI-powered tools have made phishing and smishing attacks – already a critical threat – even more difficult to detect. In response, 81% of organisations have implemented AI usage policies for employees. Confidence in these policies is also high, with 77% of leaders stating they are either extremely or very familiar with best practices for AI security.

Despite these efforts, the gap between policy and preparedness persists. Keeper's 2024 Top Data Threats report revealed that 51% of security leaders identify AI-powered attacks as the most serious threat facing their organisations, and 35% feel their organisations are least prepared to combat these attacks, compared to other types of cyber threats.

To tackle these emerging challenges, organisations are focusing on several key strategies:

Data Encryption: This is the most widely adopted measure, with 51% of IT leaders incorporating it into their security strategies. Encryption helps protect sensitive information from unauthorised access, which is crucial in defending against AI-driven attacks.

Employee Training and Awareness: Recognised as a high priority, 45% of organisations are focusing on enhancing their training programs to better prepare employees for the evolving threat landscape. Effective training can help employees recognise and respond to AI-powered

phishing and smishing attempts.

Advanced Threat Detection Systems: With 41% of organisations investing in these systems, there is a clear emphasis on improving the ability to detect and respond to sophisticated AI-driven threats. Advanced threat detection solutions can provide early warnings and mitigate potential damage from these attacks.

The emergence of AI-driven cyber attacks presents new challenges, but the fundamental cybersecurity practices – such as data encryption, employee training and advanced threat detection – remain essential. Organisations must ensure these foundational measures are consistently updated and adapted to meet emerging threats.

In addition to these fundamentals, adopting advanced security frameworks like zero trust and implementing Privileged Access Management (PAM) solutions like KeeperPAM can significantly improve resilience. Zero trust ensures that every user, device and application is continuously verified before accessing critical systems, minimising the risk of unauthorised access and limiting the blast radius if an attack does occur. PAM helps secure an organisation's most sensitive accounts by controlling, monitoring and auditing privileged access, which is especially important in defending against sophisticated AI-driven attacks targeting high-level credentials.

Organisations should also stay proactive by regularly reviewing security policies, conducting routine audits and fostering a culture of cybersecurity awareness. While organisations are making progress, cybersecurity is an ever-evolving field that requires ongoing vigilance. Combining fundamental practices with modern approaches like zero trust and PAM will help organisations stay ahead of evolving AI-powered threats.

For additional information about these insights and key statistics, please see Keeper's infographic.

###

About Keeper Security
Keeper Security is transforming cybersecurity for people and organisations globally. Keeper's intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Our zero-trust privileged access management platform deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance. Trusted by millions of individuals and thousands of organisations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging. Learn how our zero-trust and zero-knowledge solutions defend against cyber threats at KeeperSecurity.com.

Charley Nash
Eskenzi PR

email us here