moneycontrol

The dark side of technology: AI-driven cyberattacks call for upgraded security measures

Recent high-profile data breach reports involving Star Health exemplify this alarming trend, highlighting the urgent need for upgraded cybersecurity measures

PTI

OCTOBER 06, 2024 / 13:50 IST

In a conversation with PTI, Sneha Katkar, Head of Strategy and Product Custodian for the cybersecurity firm Quick Heal's antivirus lineup, pointed out that the landscape of cybercrime has undergone significant evolution.

In a world increasingly reliant on technology, cybercriminals are misusing artificial intelligence (AI) to execute sophisticated attacks, posing significant threats to individuals and organisations alike, according to an expert.

Recent high-profile data breach reports involving Star Health exemplify this alarming trend, highlighting the urgent need for upgraded cybersecurity measures.

In a conversation with PTI, Sneha Katkar, Head of Strategy and Product Custodian for the cybersecurity firm Quick Heal's antivirus lineup, pointed out that the landscape of cybercrime has undergone significant evolution.

"Cyber criminals today are not operating manually; they are using AI to automate attacks. They are using artificial intelligence to actually conduct these attacks. It's so sophisticated in nature that the best of the best fall prey to it," she noted.

This automation allows them to bypass traditional security measures, making it challenging for even the most robust systems to defend against such threats, she said.

Katkar said the recent breaches at Star Health are stark reminders of the vulnerabilities present in digital infrastructures.

In July 2024, an account on the dark web claimed to have accessed and stolen the data of 375 million Airtel customers and put it up for sale. However, Bharti Airtel dismissed any data breach and termed it a "desperate" attempt to tarnish the brand's image.

In September 2024, insurer firm Star Health experienced a significant breach that exposed the sensitive health information of its clients on Telegram chatbots.

No matter what kind of security you have in place, even if it's about a global major, Katkar said, a cybercriminal can design attacks that would penetrate through the security products that an organisation has. She further said that when such breaches occur, companies are liable to go back to their consumers and notify them that such a breach has happened.

"Essentially, what I'm trying to say is because fraudsters are getting technologically savvy, super smart, consumers also need to have technology to essentially beat this. Because awareness is always going to be one step behind," she stressed.

While awareness is crucial, it often lags behind fraudsters' evolving tactics. As soon as consumers become aware of one type of scam, fraudsters innovate newer methods, she elaborated.

This constant cat-and-mouse game necessitates a dual approach: leveraging technology alongside consumer education to stay ahead of cybercriminals.

According to the Indian Cybercrime Coordination Centre, the approximate amount that Indians lost to fraudsters between January and April 2024 stood at Rs 1,750 crore.

Cybercrimes have resulted in significant financial losses for individuals and organisations, with incidents like phishing, ransomware, and online fraud becoming increasingly prevalent.

With the notably quick adoption of artificial intelligence (AI), concerns have been raised about its potential to enhance cyberattacks, including creating more convincing phishing emails, automating malicious activities, and developing new forms of malware.

Moreover, in today's digital landscape, the threat of financial fraud is just one of many concerns; personal data and identity theft are equally pressing issues that are unfortunately on the rise.

In recent news, YouTube channels of India's apex court, and social media content creator Ranveer Allahbadia (Beer Biceps) were hacked.

Katkar highlighted another case where a CEO fell victim to a digital arrest scam, losing 7 crores due to a well-crafted deception that included fake legal documentation.

"The complexity of these scams means that even savvy individuals can be caught off guard," she noted.

"The interplay between technology and awareness is vital in combating these emerging frauds," she said.