How AI can be a powerful cybersecurity tool for preventing digital frauds

By **Aaratrika Talukdar** On **Nov 6, 2024**

0 76

Share

In an exclusive interview, **Vishal Salvi, CEO, Quick Heal,** an industry veteran with over two decades of experience in cybersecurity, sheds light on the fast-evolving cybersecurity space in India and emerging threats citizens and businesses face today. At a time when digital and financial frauds are growing day in and day out, Salvi talks about the key trends that shape the world of cybersecurity today, how AI is shaping cybersecurity prospects, and the development of AntiFraud.AI – "Made in India" fraud prevention solution.

What is your general impression of the overall cybersecurity landscape in India? What are some of the key trends?

The cybersecurity landscape in India is evolving rapidly, and we've seen a number of significant trends. Advanced malware, particularly ransomware, has become a dominant threat, impacting the digital ecosystem indiscriminately. It no longer matters if an organisation is specifically targeted; anyone can become a victim. We're also observing an increase in cyber crime across industries, especially in sectors like banking. Other common attack vectors include espionage, advanced persistent threats (APTs), denial of service attacks, and the theft of sensitive data. There is no clear perimeter to any environment, securing access to the data, remote systems, and user credentials has turned into an important defense against such threats. Organisations invest in more robust systems, such as AI and machine learning, to counter the evolution of threats.

How do you see the role of AI in the cybersecurity space – from a defensive perspective as well as an offensive one?

AI is a powerful tool in the cybersecurity industry. As far as the industry is concerned, we have been using machine learning for many years to automate security controls and processes, which has allowed us to better protect organisations. Now, with advancements in AI, we can enhance our security solutions even further. At Quick Heal and Seqrite (our enterprise security platform), we've integrated several AI models to better detect and respond to threats, especially ransomware. On the defensive side, AI enables us to quickly analyse and mitigate risks. While companies like ours don't engage in offensive cybersecurity measures, state and government bodies may use AI to identify vulnerabilities and protect critical infrastructure. The battle between attackers and defenders will continue to play out with AI on both sides. It is going to be a cat-and-mouse game that will run as AI continues to develop on both sides.

AntiFraud.AI is India's first 'Made in India' fraud prevention solution. First of all, congratulations on that. Please share with us the journey behind the creation, and what motivated Quick Heal to focus on this area?

The rise in fraud, especially digital and financial frauds, has been significant. Citizens are losing their hard-earned money to these scams. Quick Heal has always been at the forefront of providing B2C antivirus solutions, but as fraud

increased, we realised we needed to leverage our deep research and knowledge to develop a solution tailored to combating fraud. Anti-Fraud.AI is an amalgamation of technology, behavioural science, and expertise. Our goal is to provide a holistic platform that addresses the full spectrum of threats, from monitoring the dark web to implementing behavioural safeguards. We've packed it with features that help customers protect themselves proactively while also providing step-by-step guidance if they've been defrauded.

In the world of digital and financial frauds that evolve so rapidly, what are some of the notable differences in features that AntiFraud.AI possesses vis-à-vis other fraud prevention tools that already exist in the marketplace?

Anti-Fraud.AI is unique in many ways. One of the standout features is the risk score it provides after installation, which evaluates the security status of a user's phone. It scans for rogue apps, checks if your email has been part of any data breaches, and monitors various risks, like weak Wi-Fi networks. Based on the score, users can take steps to lower their risk, which is a more tangible form of gratification and security for consumers. Another key aspect is that it provides real-time monitoring of apps. The application provides safety for monetary transactions by scanning for threats such as a weak Wi-Fi connection and a jailbroken device. Our application is like a kind of watchman over the activity of your cell phone; it prevents fraudulent links or applications from influencing your gadget.

This granularity in monitoring combined with real-time remediation makes Anti-Fraud .AI unique from others in the market.

The application is for all ages. How does AntiFraud.AI ensure a convenient user experience among the demographics crossing such diverse age groups, particularly in case of the elderly and non-techie users?

We have designed AntiFraud.AI so as to be intuitive as well as simple for people from all walks of life. The UI of the application is modern, aesthetically pleasing; however what is most important is it's easy to navigate. Once the application has been set up, it runs automatically in the background and protects the user transparently-there are frequent warnings, though the choice

to proceed or stop is always at the discretion of the user. However, for highly malicious threats like fraudulent links sent via WhatsApp or SMS, we take it a notch further to block them to keep the user safe, especially if the user is not very tech-savvy.

What does AntiFraud.AI's underlying technology do for AI and machine learning to detect and prevent emerging sophisticated fraud techniques?

AI and machine learning form a very integral part of AntiFraud.AI, approximately 95% of our backend operations are automated using AI, allowing the solution to evolve and combat sophisticated fraud techniques. In this manner, we monitor and notice emerging patterns that indicate new threats. And through this analysis, it enables us to give relevant real-time decisions geared towards safeguarding our users against emerging threats. This, in turn, assists us to curb more imminent attacks, which include ransomware attacks, phishing attacks, among others. An example is how we continue to fine-tune our AI models so we can identify rogue apps or insecure environments before users make their financial transactions. The app also uses AI to monitor real-time activity on the device-for example, unauthorised microphone or camera use-and delivers alerts with detailed reports.

AI plays a very crucial role in real-time detection of rogue applications, phishing attempts, and other frauds. So our solution will be proactive and adaptive towards any form of new cybercrime. We want to be one step ahead of the fraudsters who are increasingly leveraging AI to develop more complex attacks.

What is the future of consumer protection in India with solutions like AntiFraud.AI, and what role does Quick Heal see for itself in this landscape?

We see a great shift in the cybersecurity landscape, where consumers begin demanding more protection for themselves. Solutions such as AntiFraud.AI will be instrumental for users to take up the fight against digital and financial fraud. Quick Heal will continue developing its technology further, embrace AI and machine learning capabilities, and collaborate with other stakeholders in order to provide a safer digital space. Our focus will continue to lie in more

holistic, user-friendly solutions that not only identify threats but go one step ahead of time by showing the user how to protect themselves as well.