Using Your IQ To Fight Cybercriminals With AI

cyber security artificial intelligence

Summary: A recent experiment found cybercriminals would be significantly more successful in their phishing efforts if they were to add AI to those efforts. What this could mean for community banks and their cybersecurity.

Measuring intelligence in humans can be a tricky thing. After all, some people you know might be book smart, some are street smart and some are just wicked smart. The intelligence quotient (IQ) is a score that comes from various standardized tests designed to assess overall intelligence in humans. The IQ median raw score when developed was 100 and scores move based on standard deviations around that number. In short, about 67% of people score from 85 to 115, while 2.5% score above 130 and 2.5% score below 70.

As you ponder where you might score and where that genius friend or colleague of yours might land, we shift our discussion to the intelligence of machines or what is generally known as artificial intelligence (AI) or machine learning (ML).

AI and ML are all the rage right now and the biggest banks are actively embracing these technologies for everything from customer service assistance to compliance. Many banks have been especially successfully at employing AI in their efforts to identify suspicious activities and transactions for BSA/AML.

However, a recent experiment found cybercriminals would be significantly more successful in their phishing efforts, if they were to start using AI. This experiment was conducted by scientists at security company, Cyxtera, to determine how AI could potentially be used to help cybercriminals perfect their phishing attacks.

According to "DeepPhish: Simulating Malicious AI," a paper documenting the results of the experiment, bank systems that currently utilize AI to identify and fend off cybercrime are successful 99% of the time. But, when scientists applied AI to cybercriminals' side of the equation, things changed.

By using AI to generate synthetic phishing URLs, scientists were able to successfully circumvent security systems designed to flag false URLs 21% and 36% of the time vs. previous success rates of less than 1% and 5%, respectively.

Needless to say, ignoring such findings could mean millions of dollars of losses for banks. According to the latest "Cost of Cyber Crime Study" produced by Accenture and the Ponemon Institute, security breaches within the financial services industry cost attacked organizations an average of $18mm annually.

Though the efforts of cybercriminals aided by AI and ML will make IT efforts to secure sensitive information notably harder, there are lessons to be learned from these findings. The most important lesson is the fact that AI has the capacity to learn and evolve. That means anti-fraud security programs, incorporating AI and ML, should be consistently updated and re-trained using the latest data available. In the case of this experiment, scientists accomplished this by teaching existing anti-fraud systems to interpret URL creation strategies, which allowed these anti-fraud programs to identify existing patterns and recognize any new patterns created by potential fraudsters using AI.

Given that AI and ML are now pretty available to everyone, it is only a matter of time until cybercriminals begin using these tools to enhance their endeavors to compromise financial information. We hope we have helped you stay on top of this rapid technology.

CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your bank minimize its credit exposure, increase operational efficiency and deliver faster fraud notification. Learn more about our check imaging for Canadian cash letters.