Newest AI Scams to Look Out For

Discover the good and bad purposes for AI.

Artificial Intelligence (AI) and Machine Learning (ML) have become hot topics of everyday conversations. Advancements in these technologies have brought a plethora of new capabilities for both good and bad purposes. These capabilities are making their way into all aspects of our daily lives, both private and professional. In this article, we'll explore some evolving technologies that may be used in both your personal and professional lives.

How AI Helps with Phishing

One of the scariest capabilities is the ability to use AI to enhance attack vectors and assist in creating new ones. You may remember when you could identify a phishing message by poor grammar and spelling. Those days are going away as AI generators can now assist in creating more precise and error-free messages.

Another example of this advancement is AI-generated or augmented Malware. These technologies have already been used by security companies to bypass current-generation defensive software in testing laboratories. We expect that these technologies will make it into the wild over time. This will make the threat landscape increasingly tumultuous as AI and ML technologies advance.

KARL EPPS
EnCE, CEH, CCFE, CHFI, CCPA

Karl can assist with digital device and email forensics as well as internet/cloud forensics, hacking events and data recovery/ preservation.

Karl Epps is an EnCase Certified Examiner (EnCE); Certified Ethical Hacker (CEH); Certified Computer Forensic Examiner (CCFE); Certified Hacking Forensic Investigator (CHFI) and a Cellebrite Certified Physical Analyst (CCPA).

Contact Karl at: 602.463.5544 or karl@epps4n6.com

EPPS DIGITAL FORENSICS LLC
ANALYSIS | PRESERVATION/RECOVERY | LITIGATION

AI Software to Know About

For over 50 years, malicious actors and security professionals have been battling for dominance between exploitation and protection. AI is a new frontier in this battle. One way to protect your systems immediately is to adopt better security platforms. There are now AI-enhanced antivirus/malware software suites, such as SentinelOne. These platforms can monitor your computer network in more "aware" ways. For example, they can monitor for unusual network activity, such as a computer sending/receiving data in the background. These platforms can instantly lock down a system suspected of compromise, greatly reducing the duration and severity of a breach. In many cases, breaches will exist for minutes instead of months.

Conversely, AI tools such as ChatGPT are being used to help write malicious code, which exponentially expands the ability for threat actors to create new types of attacks. AI preforms the translation between "plain English" and programing languages; thus the necessary skill set is reduced to possessing bad intentions, empowering a new set of bad actors to create malicious code.

Watch Out for Deep Fakes

Another rapidly advancing attack vector is Deep Fake technology. While arguments over the use of AI in movies to replace or even resurrect actors is a contentious topic, fraudsters are using it for theft. In one case, a closed-door deal involved internal C-Level employees at Arup, a British Engineering giant. These meetings were virtual and involved co-workers familiar with the Arup financial officer responsible for distributing funds for a top-secret transaction. The faces and voices of the CFO and other staff appeared legitimate, but everyone in the meeting was fake except for the target of the fraud scheme, the financial officer, who distributed approximately $25 million before catching on.

Social media influencers are also becoming victims of fraudsters using their own content to create deep fakes. Recently there was a case where a CEO called his office and asked the store manager to transfer him $10,000 in Bitcoin. The business was all cash, and the request did not trigger concern. The voice on the phone sounded like the CEO's voice to a seasoned employee, and the fraud wasn't discovered until after the bitcoin had been transferred and became unrecoverable.

A peer recently watched a presentation at a financial conference. The presenter said he would show a short video of himself presenting. After the video finished, he asked if the audience would like to see the presentation in Spanish. The presenter then explained that he spent about 1.5 hours training an AI tool about his topic, and the AI program created the presentation and presented it as him. When questioned, the audience had no idea that the video or presenter was AI-generated and that the presenter didn't know Spanish!

We are encouraged by the fact that AI-powered deep fake detection are also progressing. For example, TrendMicro will soon have "Trend Vision One™" Deep Fake detection technology available. I am also personally involved in testing new AI technologies in digital forensics and educating people on AI pitfalls and protection.

In closing, AI adds powerful capabilities to our digital forensics tools, which is constantly advancing. This allows for our tools to learn about the nuances of specific cases. AI behavioral monitoring will increasingly assist in digital investigations, allowing us to "teach" our software the facts of cases. This will contribute to more expeditious and accurate case analysis. ■