AI Powered GPTs Now In The Hands of Cybercriminals

February 29, 2024 - In the realm of cybersecurity, a troubling trend is emerging. The misuse of artificial intelligence (AI) in search engines to fuel cybercrime and fraud. Recent revelations highlight the emergence of AI-driven chatbots on the dark-web. These bots, leveraging the same AI technology as mainstream models such as OpenAI's ChatGPT, are empowering cybercriminals to orchestrate more sophisticated and devastating attacks.

They can craft meticulously tailored phishing emails or fabricate convincing deepfake content and they are reshaping the threat landscape for consumers and businesses alike. A recent incident in Hong Kong, resulted in a $25.5 million fraud. Criminals used AI-generated deepfake voice technology impersonate the companyâ€™s CFO. The result of that call was that a company employee then ordered the transfer of funds.

The implications of AI-enabled cybercrime extend far beyond monetary losses. With the proliferation of AI-driven phishing attacks, consumers face heightened susceptibility to scams that are increasingly sophisticated and challenging to discern. For businesses, especially those in the public eye, the threat of targeted spear-phishing attacks looms large, carrying the potential for substantial financial losses and irreparable damage to reputation.

Compounding the issue is the accessibility of AI-enabled hacking services on the dark web, where virtually anyone with ill intent can procure tools powered by advanced AI models. There are a variety of open-source models available, as well as copied proprietary models that have been hacked to remove all of their safety protocols. Cybercriminals now have at their disposal a formidable arsenal to execute their malicious schemes with unprecedented efficiency and scale.

Consumers and businesses alike need to be especially careful now when they are solicited for funds, even when those solicitations come from people that they know. Take the time to double-check any request for money. We are now at a point that everyone needs to assume that the person on the other end of the phone or who sent you that unsolicited email may not be who you think it is.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS