How cyber scammers are trying to make AI tools pay

September 12 2023

Credit: CC0 Public Domain

Proponents of artificial intelligence say its potential is limitless. But cyber scammers could also use it to their advantage.

Analysts explained to AFP how the technology could increase the risk from online crime.

Phishers of emails

Chatbots are the best-known of all AI tools thanks to the rampant success of ChatGPT and many that have come afterwards, not least Google's Bard.

Phishing is the most ubiquitous form of cyber scam, and involves criminals posing as a company or an individual sending batches of emails that include links to counterfeit websites or malware.

The two worlds are already starting to collide, with cybercriminals trading tips in online forums on the best ways to get chatbots to generate phishing emails.

The big players block users from generating these kinds of emails, so developers have designed programs aimed at creating phishing messages—FraudGPT and WormGPT among them.

The effectiveness of these tools has yet to be tested, with Gerome Billois of consulting firm Wavestone telling AFP: "We're only at the very beginning."

Experts say the major skill of chatbots for phishing gangs is to generate fairly clean prose.

One of the telltale signs of a phishing email has long been dodgy spelling and scattergun punctuation.

"AI accelerates the pace of attacks," said Billois.

The FBI said it received 300,497 complaints about phishing scams last year, with losses suffered worth $52 million.

Attack of the clones

Earlier this year, US mother Jennifer DeStefano explained how she received a call from her daughter begging for help, before being told by a kidnapper to pay $1 million ransom.

"I never doubted for one second it was her," she told local media.

Only the voice was an AI-generated imitation and DeStefano quickly uncovered the ruse.

But it points to the risk of a future where deepfake impersonations of loved ones or colleagues appear on phone or video calls—a development that could be a gold mine for scammers.

With a recording of just few seconds of a person's voice, online tools can produce an imitation capable of tricking employees or friends.

Jerome Saiz, founder of the French OPFOR Intelligence consultancy, said "a whole industry of small-time crooks" already adept at extorting credit card details through text messages was likely to start using such tools.

He told AFP such scammers were often young and skilled with technical tools.

A programming guide

One of the much-vaunted talents of chatbots such as ChatGPT has been

their ability to generate passable computer code.

Scammers could employ those skills to create malware capable of locking a victim's computer or gaining access to files or accounts.

There are claims online that the new breed of bespoke chatbots are able to perform this kind of operation but solid evidence is hard to come by.

Chatbots can certainly identify flaws in existing code and even generate malicious code but they cannot execute it directly.

Saiz said he could see AI helping scammers who have little talent to become more skilled—a kind of coding tutor.

"But someone starting from scratch is not going to get ChatGPT to code malware for them," he said.

Saiz, who generally gets called when something major has gone wrong, said he had not seen any evidence that any of his cases over the past year had involved AI.

Shawn Surber of US cybersecurity firm Tanium is equally cautious.

"Much of the concern over how generative AI will affect risks for businesses is based on fear of the unknown rather than specific threats," he said.