BIZCOMMUNITY

ChatGPT will boost today's cybercrime

ChatGPT is a new artificial intelligence (AI) that understands natural human language, providing comprehensive and concise responses. It can answer questions that sound like human responses, it can write essays that feel like a person was the author (much to the concern of teachers and professional writers), and it can also create computer code, sparking worry that ChatGPT could be used as a cybercrime tool. That may happen. But the real risk lies in how this software and its peers could amplify impersonation and other existing cybercrime attacks that already work very well.

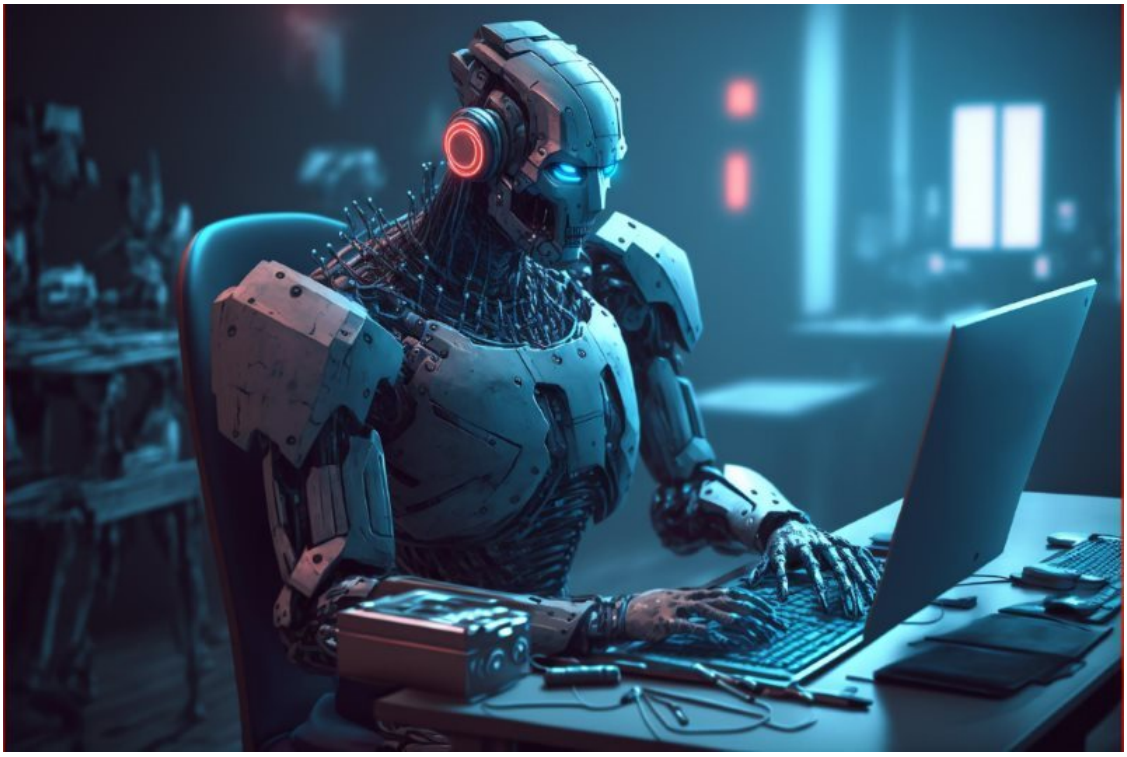

Image supplied

Gerhard Swart, CTO at cybersecurity company, Performanta, says

"I can see how ChatGPT will make it easier to access cybercrime tools and learn how to use them, but that is a side concern, at least for now. The bigger problem is how it will be used for scams. ChatGPT and similar AIs won't create new cybercrime threats, they will make current threats worse."

The generative AI revolution

ChatGPT is part of a new trend called generative AI. While it conjures written paragraphs, image generators such as DALL-E and Stable Diffusion create spectacular art in minutes. Several companies, including Google, have AI systems that generate realistic videos. Last year, a startup showcased a fake voice interview between podcast star Joe Rogan and the late Apple CEO, Steve Jobs—created by an AI.

OpenAI, the company behind ChatGPT, also created an AI called Codex that writes computer code. It wasn't long before criminals and security experts tested the combination of Codex and ChatGPT to create hacker scripts. Darkweb forums, where online criminals meet, started posting examples of AI-generated attack code. This trend is a concern in the long run.

“ChatGPT won't make a newcomer good at cybercrime coding. They still need a lot of experience to combine different codes. But an AI could generate code at a pace and scale that would help experienced criminals do more, faster. And it could help inexperienced people get better access to the many crime tools available online and learn how to use them. I don't think the concerns about cybercrime are overhyped. They're just not that simple, for now,” says Swart.

The real cybersecurity threat

Yet generative AI still poses a very real cybersecurity risk. Cybercrime often uses social engineering, a set of proven techniques that scam people into sharing access details or valuable information.

"Social engineering is the oldest trick in the book," says Swart. "It's when someone pretends to be somebody or something else. The Trojans thought they got a big wooden horse as a gift, not an invading army. That has never changed. Cybercriminals do this all the time, using methods like phishing and man-in-the-middle attacks."

Phishing is when someone fakes correspondence to fool a user, such as pretending to be a bank and getting their victim to log in on a fake banking page. Man-in-the-middle attacks intercept and replace correspondence, for example, an invoice with altered banking details. Social engineering can use phone calls, instant messaging and other communication channels designed to fool someone into thinking they are dealing with a trustworthy party.

From that perspective, generative AI could become a significant cybercrime enabler. Criminals can generate emails that mimic the language and style of executives. They can create correspondence in different languages, and they might even start to clone people's voices and faces. There is no evidence that these latter activities have happened, but it's no longer science fiction.

Microsoft launches new AI search engine 'more powerful than ChatGPT'

8 Feb 2023

Fortunately, the cybersecurity world knows these tricks. Modern security can deal with phishing and impersonation attacks. It can detect and prevent the type of tricks that generative AI generates. But to create that advantage, people and companies need to take security more seriously.

“Most attacks happen not because we can't secure systems properly but because we don't bother to do so," says Swart. "Companies leave security as an afterthought, or just throw money at the problem. They don't collaborate with staff to create security awareness and they don't involve their security people in business conversations. They don't create what I call a cyber-safe environment."

This change means that any organisation that hasn't yet sorted its cybersecurity has an even bigger target on its back. In the future, generative AI may radically change cybercrime, but it may also already be amplifying what online criminals can do.