BIZCOMMUNITY

Should companies invest in ChatGPT?

Microsoft is reportedly investing $10bn in OpenAI, the owner of the somewhat controversial large language model chatbot ChatGPT. It uses a deep learning technique to generate text and conversations often indistinguishable from those created by actual humans.

Source: Unsplash

ChatGPT has dazzled amateurs and industry experts ever since its launch at the end of November last year. Given a prompt, ChatGPT can answer complex questions, provide suggestions and even debug programming code all while sounding extremely human.

“It’s very hard to believe the text was created by a machine learning algorithm,” says Stephen Osler, co-founder and business development director at Nclose.

Prompted with the question of how it works, ChatGPT explained it uses “a large dataset of text” so that it has “knowledge about a wide range of topics and can respond to a wide variety of questions and prompts”.

#BizTrends2023: Will AI make content writing a process of the past?
Justin Beswick 13 Jan 2023

On the surface this might sound like an amazing invention that can be used to explain complex concepts in simple terms, brainstorm creative ideas or even automate certain actions like customer support, writing memos or keeping minutes of meetings. But it also poses a serious threat to cyber security, warns Osler.

“Because ChatGPT can be used to write code, malicious actors have already started using it to build malware, sites on the dark web and other tools for enacting cyber-attacks.” Someone with no prior knowledge of coding can theoretically use ChatGPT to produce dangerous malware. OpenAI, the developer of ChatGPT, gave assurances that it has put restrictions in place to restrict the use of the bot to create malware, but on various online forums users are boasting about still being able to find workarounds.

“There isn’t much the average internet user can do to stop these actors from creating malicious software using ChatGPT. It just means that everyone should be extra vigilant of possible malware attacks,” says Osler.

Risk in phishing emails

The risk is especially prevalent in phishing emails, a method often used by criminals to serve malware embedded within links or attachments. Usually, poor spelling and incoherent grammar are the most telling traits of a scam email.

“Everyone knows to be on the lookout for dodgy wording in an email and then to never click on links or open attachments in such emails, but ChatGPT brings with it a new threat: perfectly written, human-sounding emails that can be very, very convincing.”

This means a bad actor can ask ChatGPT to write a perfectly harmless-looking email that can either contain a link that downloads a malicious file or convince the reader to supply compromising information like login information.

“Cybercriminals have gotten very good at convincing the untrained eye that they are trustworthy. With the advent of ChatGPT it will become even harder to spot the fakes from the real deal,” says Osler.

“Internet users should always double, no triple check if the recipient of an email is indeed the correct one. Always make sure you are receiving from and sending an email to the correct recipients.

“Legitimate email address is something that an AI language bot like ChatGPT cannot fake. At least not yet.”