‘Grim’ Criminal Abuse of ChatGPT is Coming, Europol Warns

Criminals are set to take advantage of artificial intelligence like ChatGPT to commit fraud and other cybercrimes,
Europe’s policing agency warned on Monday.

From phishing to disinformation and malware, the rapidly evolving abilities of chatbots will be used not only to better mankind, but to scam it too, Europol said in a new report.

Created by US startup OpenAI, ChatGPT appeared in November and was quickly seized upon by users amazed at its ability to answer difficult questions clearly, write sonnets or code, and even pass exams.

“The potential exploitation of these types of AI systems by criminals provides a grim outlook,” The Hague-based Europol said. Europol’s new “Innovation Lab” looked at the use of chatbots as a whole but focused on ChatGPT during a series of workshops as it is the highest-profile and most widely used, it said.

Criminals could use ChatGPT to “speed up the research process significantly” in areas they know nothing about, the agency found.
This could include drafting text to commit fraud or give information on “how to break into a home, to terrorism, cybercrime and child sex abuse,” it said.

The chatbot’s ability to impersonate speech styles made it particularly effective for phishing, in which users are

tempted to click on fake email links that then try to steal their data, it said.

ChatGPT's ability to quickly produce authentic sounding text makes it "ideal for propaganda and disinformation purposes, as it allows users to generate and spread messages reflecting a specific narrative with relatively little effort."

ChatGPT can also be used to write computer code, especially for non-technically minded criminals, Europol said.

"This type of automated code generation is particularly useful for those criminal actors with little or no knowledge of coding and development," it said.

An early study by US-Israeli cyber threat intel company Check Point Research (CPR) showed how the chatbot can be used to infiltrate online systems by creating phishing emails, Europol said.

While ChatGPT had safeguards including content moderation, which will not answer questions that have been classified harmful or biased, these could be circumvented with clever prompts, Europol said.

AI was still in its early stages and its abilities were "expected to further improve over time," it added.

"It is of utmost importance that awareness is raised on this matter, to ensure that any potential loopholes are discovered and closed as quickly as possible," Europol said.

Related: ChatGPT and the Growing Threat of Bring Your Own AI to the SOC

Related: ChatGPT Integrated Into Cybersecurity Products as Industry Tests Its Capabilities

Related: Malicious Prompt Engineering With ChatGPT

Related: Cyber Insights 2023 | Artificial Intelligence

‘Grim’ Criminal Abuse of ChatGPT is Coming, Europol Warns