SENSCY™

Your Trusted Guide to Sensible Cyber

CYBER Brief

ChatGPT and Phishing

In today's SensCy Cyber Brief, your SensCy team is investigating the potential use of the new Artificial Intelligence (AI) ChatGPT. In this brief, we will introduce the tool and review how ChatGPT will challenge traditional phishing indicators. Finally we will review other indicators you and and your employees need to be aware and how you can protect yourself.

What is ChatGPT?

ChatGPT is an artificial intelligence Chatbot launched in November of 2022 by the AI company OpenAI. The tool is built on top of three language models, allowing users to have a human-like conversation with the chatbot. The AI is trained to follow instructions and provide detailed answers. Some obvious areas where ChatGPT can be used are emails, articles, and coding languages.

How can hackers use ChatGPT in phishing attacks?

Traditionally Phishing can be detected by odd salutations like "Regards," "Hello," or "Hi." Grammatical errors are also widespread in phishing emails and are good indicators that you should not click the links in the emails. This is a result of many threat actors not being native speakers of English.

SensCy believes that with an AI platform like ChatGPT, we will see a sharp rise in phishing attacks in the next few months. Chatbots can produce large amounts of content instantaneously with zero grammatical errors and targeted at their chosen organization. Hackers can ask the Chatbot to create phishing emails targeting a specific industry, with directions like "make the email look urgent" or "write an email with high likelihood of recipients clicking on the link."

What can your company do to combat phishing?

There are other things to look for to identify phishing. Hackers will continue to incorporate a sense of urgency when building phishing emails. In this case, it is better to be safe and confirm directly with a vendor or a colleague if they are actually making the request. You should always click on the sender's name to reveal and verify it is the correct email address. Training your employees with regular controlled phishing campaigns and continued awareness training is still your first line of defense.

There are tools in the market that can detect anomalies in emails, from the content itself to the behavior of files that might be included in those emails.If you are interested in learning more about those tools, you can contact your SensCy Cyber Advocate.

SENSCY™

is The Trusted Guide to Sensible Cybersecurity for SMOs.

SensCy Inc.

info@senscy.com
734.276.9891
455 East Eisenhower
Suite 300
Ann Arbor, MI 48108

www.senscy.com

Issued: March 7, 2023