Phishing Attacks and the Role ChatGPT May Play

Office of Information Technology
Division of Information Security
APRIL 2023

As many of you know, phishing attacks are a major threat to businesses and individuals alike. Phishing emails can look like legitimate emails from a trustworthy source, but they are actually designed to steal sensitive information or install malware. Unfortunately, these attacks are becoming more sophisticated every day.

One of the newest developments in the world of phishing is the use of artificial intelligence chatbots like ChatGPT. ChatGPT can be a useful tool, for example, organizations can use it to perform the following tasks:

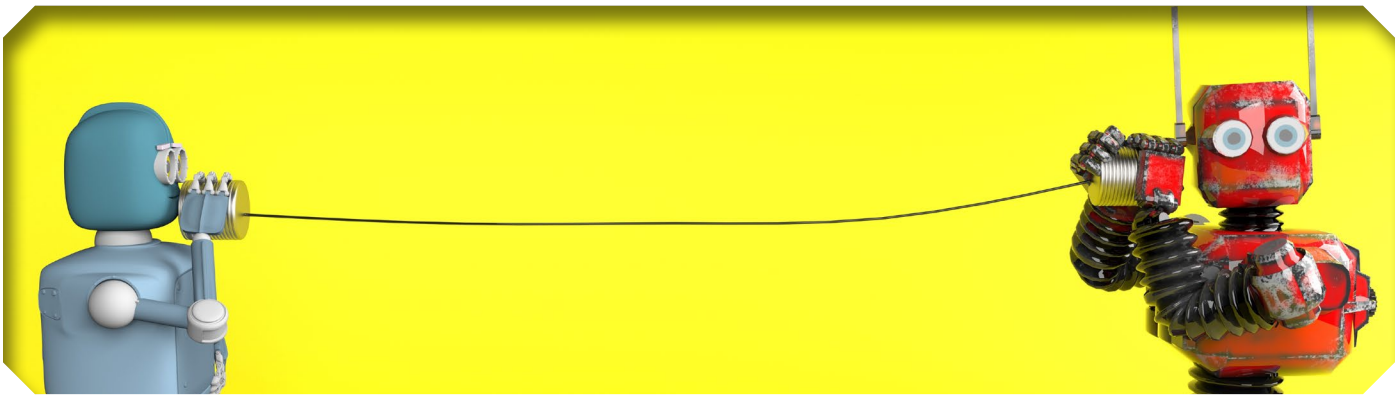
- **Language Translation.** Users can communicate in multiple languages without the need for human translators. This is especially useful for businesses that operate on a global scale and must communicate with partners or customers who speak a different language.
- **Content Creation.** Users can create content such as articles, essays, or reports based on a given topic or input prompt. This can be useful for businesses or individuals who need to quickly create large amounts of written content.
- **Customer Service.** Providing customer service via chatbots allows customers to ask questions and receive instant responses without requiring human intervention. This has the potential to improve customer satisfaction while also reducing the workload of customer service representatives.

Now let's take a look at the dangers of ChatGPT. It has become more evident that chatbots can generate realistic-sounding emails that are almost indistinguishable from those written by humans. This makes it easier than ever for attackers to craft phishing emails that can trick even the most vigilant users. Concerns about ChatGPT include the following potential risks:

- **Privacy.** Because ChatGPT is designed to learn from the input data it receives, it may collect and store sensitive information about users. Personal information such as names, addresses, and financial information may be included. If organizations do not properly safeguard this information, it may be hacked or stolen. Attackers can then use this data for illicit purposes, including additional targeted phishing campaigns.
- **Bias and Discrimination.** ChatGPT, like all artificial intelligence models, is only as unbiased as the data on which it is trained. If the data used to train ChatGPT is biased, the model may learn and perpetuate that bias, potentially resulting in increasing discrimination against specific groups of people.
- **Misinformation.** Although ChatGPT generates responses based on the input data it receives, it may not always be able to differentiate between correct and incorrect information. As a result, it may inadvertently spread misinformation or false information.
- **Misuse.** Bad actors may use ChatGPT for nefarious activities like producing fake news, and launching phishing or social engineering attacks.

While ChatGPT is not explicitly designed to create phishing emails, cybercriminals can use a combination of tactics, such as collecting information from previously stolen communications or other data breaches, and then use ChatGPT to generate more realistic and convincing phishing emails based on that information.

For example, attackers can use a company's stolen email communications to learn about their targets and interact in a way that is believable and makes the victim feel comfortable. They send phishing emails to company employees that often claim to come from a manager, business partner, or customer. The email lures a victim into clicking on a link or downloading an attachment that then installs malicious code onto the device as malware.



Regardless of how cybercriminals are crafting phishing emails, it is important to remain vigilant and take appropriate security measures to protect against phishing attacks. Here are a few tips to protect yourself from cybercriminals' using ChatGPT:

- Be cautious of unsolicited messages.
- Verify the identity of the person you're chatting with.
- Scrutinize text.
- Use two-factor authentication for your online accounts.
- Be cautious when downloading files or clicking on links.
- Use caution when talking to strangers online.

If you encounter a phishing incident outside of work, report it to the following organizations:

- Cybersecurity and Infrastructure Security Agency
- Federal Trade Commission
- FBI Internet Crime Complaint Center

If you suspect a phishing incident has occurred at work, report it to the IHS Cybersecurity Incident Response Team at Incident@ihs.gov.

ChatGPT is a new tool, and IHS does not permit its use on IHS-furnished equipment or for IHS business. To ensure compliance with regulations, please refrain from using ChatGPT as part of your IHS duties and when using your IHS devices.

Thank you for your attention to this important issue. The IHS Division of Information Security will continue to keep you updated on the latest developments in cybersecurity.

If you have any questions about this article, please contact Cybersecurity@ihs.gov.