Article

Feb 2023

CHAT GPT Friend or Foe?

Being a new, cutting-edge technology, cyber adversaries are likely to use or have already used ChatGPT to improve their scamming skills and impersonate your colleagues to exploit organisations.

CHAT GPT Friend or Foe?

We've all seen or used Chat GPT at one point. Some of us write tough e-mails, some to write our wedding vows (yes, some people have actually done this), Gen Z is using it to help with homework or tertiary studies.

Some however, are using it for more sinister purposes.

Being a new, cutting-edge technology, cyber adversaries are likely to use or have already used ChatGPT to improve their scamming skills and impersonate your colleagues to exploit organisations.

So, is ChatGPT our new best friend or will it end up being our foe?

Here's some info about what ChatGPT is & what it does.

"ChatGPT is a large language model developed by OpenAI. It is designed to process and generate natural language text, which allows it to carry on conversations with people in a variety of contexts.

At its core, ChatGPT is a type of artificial intelligence that uses deep learning techniques to understand language and generate text. Specifically, it is built on a deep neural network architecture called a transformer, which is particularly good at processing long sequences of text.

ChatGPT has been trained on a massive corpus of text data from the internet, which includes a wide range of written content in many different languages. This training data allows ChatGPT to understand the nuances of language and generate text that is both grammatically correct and contextually appropriate.

One of the key features of ChatGPT is its ability to carry on conversations with people in a way that feels natural and intuitive. Users can interact with ChatGPT using natural language text input, and the model will respond with text that is appropriate to the context of the conversation.

Overall, ChatGPT represents an exciting development in the field of artificial intelligence and natural language processing. It has many potential applications, including chatbots, virtual assistants, and customer service interfaces, to name just a few."

...And yes, ChatGPT wrote this.

One of the biggest dangers of ChatGPT is that it can be used to impersonate real people.

Because it is designed to generate text that is contextually appropriate, it can be very difficult to distinguish between responses generated by ChatGPT and those written by a human.

This can be exploited by attackers to impersonate employees, customers, or other individuals in order to gain access to sensitive information or carry out other nefarious activities.

Another danger of ChatGPT is that it can be used to launch social engineering attacks. Social engineering is a technique used by cybercriminals to manipulate people into divulging sensitive information or carrying out actions that are harmful to their organization. This comes in the form of phishing e-mails.

Many phishing scams can come from overseas and scammers' grammar, punctuation and spelling is usually a dead giveaway something's not right. However...

With the help of ChatGPT, attackers can create more convincing and sophisticated phishing emails, for example, or craft more convincing messages that can trick people into clicking on malicious links or downloading malware.

For chief cyber security executives, these dangers represent a significant threat to their organization's security posture.

An approach for organisations to minimise these risks are by implementing sophisticated phishing simulations, appropriate consulting with Cyber Security organisations, robust security measures. A quick win could also be simply implementing 2FA/ MFA for all members of the organisation.

Additionally, businesses should consider deploying advanced security technologies like behavioural analytics (essentially where a program monitors in the background people's behaviours and picks up when something isn't right; for example, you log in from Sydney every day but one day a login is tracked in New Zealand). This can help detect potential social engineering attacks or other malicious activity before it causes significant damage.

On the flip side.. There are many benefits to ChatGPT, here are some benefits to organisations that you might not have thought of...

- ChatGPT can be used to improve customer service in the tech industry by providing fast, personalized responses to customer inquiries and technical support issues.
- ChatGPT can be used to automate repetitive tasks and save time and resources for security analysts and IT professionals.
- ChatGPT can assist in the development of security policies and procedures by generating and analysing reports and data related to security incidents and vulnerabilities.
- ChatGPT can be used to create training materials for security professionals, such as simulated phishing attacks, to help improve their security awareness and response capabilities.
- ChatGPT can assist in the development and testing of security software and tools by generating test cases and data that can be used to evaluate their effectiveness and performance.

We've discerned that ChatGPT is neither friend nor foe. But simply is. Meaning, there are many pros and cons. If we look at any advancements in technology, there are always benefits. There are always downfalls.

If organisations stay educated, keep their employees in the loop and trained well & your security measures are consistently monitored, you reduce your risks of being subject to an attack by someone using this software.

P.S. ChatGPT helped us write some of this article... So, we think it's pretty cool.