



101010
100101
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010
101010

Muddying the Line between Human and Machine

ChatGPT's Longevity in our Evolving Digital Era

Written by Tenzin Kunga
Illustrated by Rishi Chiratanagandla

I sighed. Racked my brain. Here I was, faced with a device designed to converse with only me, while somehow containing most of the knowledge of the internet. It did not help that I was about six months late to the AI chatbot engagement game. To make matters worse, it now oddly felt like I had to impress it. At last, I decided on a question. Quickly my fingers flew across the keys: "When will you leave?"

ChatGPT has indeed snagged the attention of a few people since its release a few months ago. After launching in November of 2022, OpenAI's chatbot ChatGPT's impact on the digital sphere has proven to be nothing short of unfathomable.

Within two months of its launch, the website has garnered nearly 100 million users. In doing so, it has earned its title as one of the fastest-growing apps in history, breezily surpassing social media giants such as Tiktok and Instagram. Still, considering the accessible nature of the app — only having to create a username and password before the chatbot can seemingly answer anything you could think of in a digestible, conversational format — this particular piece of data should come as too much of a shock.

It is one of ChatGPT's strongest selling points: ask it anything under the sun, and it will do its best to condense it into a shorter, understandable — and occasionally inaccurate — substance. OpenAI's text-generating AI GPT-3 and GPT 3.5 are the trained language models behind ChatGPTs' ability to engage in such an advanced dialogue. Derivative of Transformer Architecture and Reinforcement Learning, all these sophisticated machine learning algorithms substantiate ChatGPT's ability to digest the extent of these complex language processing tasks. As such, ChatGPT's capacity to engage in a manner so humanistic is an irrevocable, technological feat. But at what cost?

As such, ChatGPT's capacity to engage in a manner so humanistic is an irrevocable, technological feat. But at what cost?

Well, none - for now. Being a free research preview, ChatGPT is currently offered to its users on a plan with no charge, in a constant rolling state of improvements and updates, and, as of the February 9 of 2023 upgrades. At \$20 a month, plan users can now enjoy access to ChatGPT, even throughout its peak internet traffic hours, and the option to choose between the standard ChatGPT structure or "Turbo" ChatGPT, where the responses are optimized for speed.

The chatbot has amassed quite the user base, but public reception continues to grow murky. If OpenAI CEO Sam Altman has anything to say about the productization of his near-omniscient brainchild, it is the importance of the general public's reconciliation with its mere existence. In an interview with Forbes, he points out, "Google does not put [Artificial Generated Intelligence] out for public use. Other research labs don't do it for other reasons; some fear it's unsafe. But I believe we need society to get a feel for this, to wrestle with it, to see the benefits, to understand the downsides."

As it happens, the downsides to this colossal access are increasing in nature. After all, as it usually goes with monumental mainstream technology, we can expect an impressive display of creativity and ethically questionable behavior to follow quickly in its footsteps.

A principal security researcher for CyberArk Labs created polymorphic malware with the help of ChatGPT. "[ChatGPT's] malware's advanced capabilities can easily evade security products and make mitigation cumbersome with minimaleffort or investment by the adversary." The vast array of techniques that can be created through ChatGPT's capabilities, such as persistence strategies, Anti-VM modules, and other malicious code, presents a wide range of opportunities for creating and proliferating this malware. IT cybersecurity experts across North America, Australia, and the United Kingdom reinforce this notion, stating in a Forbes Magazine article published in 2023 that they are "51 percent in agreement that a ChatGPT-powered cyberattack is likely to happen before the end of the year," while "71 percent said they thought nation-states are probably already employing the technology against other countries."

The vast array of techniques that can be created through ChatGPT's capabilities presents a wide range of opportunities for creating and proliferating this malware.

As it usually goes, overreliance on any objective force can take its range of debilitating turns. Experimentation and exploration are reasonable - necessary, even - but they call for moderation. Striking this balance in the realm of ChatGPT is still somewhat difficult to gauge amongst its users, considering its recency, but it is not far-fetched to predict the obstructive effects of not doing so.

Senator Barry Finegold of Massachusetts has propped an innovative bill that would necessitate corporations utilizing AI chatbots, such as ChatGPT, to undergo comprehensive risk assessments and implement robust security protocols. This would also obligate them to divulge details about their algorithmic processes to the government. As an added safeguard, the bill would additionally require the use of watermarks by these chatbots, thereby protecting against potential theft of intellectual property.

In any case, I was well aware that asking a robot the extent of its existence felt oddly combative. Still, I figured I needed to start our first "conversation" on a somewhat speculative note. The response was instant:

As an AI language model, I don't have a physical existence and I'm not capable of leaving or going anywhere. I will remain here to assist you with any questions or concerns you may have. So, I'm not leaving anytime soon!

Given the hefty technological strides AI algorithms have made in the past months, it was a reasonable but muddling response. Even now, constantly reaching the maximum capacity from the daily swarm of requests from its massive user base, the app shuts down rather frequently, flashing an apologetic request for you to "hang tight as we work on scaling our systems." At this point in time, it seems the most human trait about ChatGPT is the uncertainty of its point in evolution.

As I mulled this all over, the text of the chatbox title rolled out on the top left corner of the screen, answering my question in the meantime. "AI Assistant Stays Put." ●●●