3 chatbot privacy risks you should know

Millions of people are now using AI chatbots worldwide, but there are some important risks and privacy concerns to keep in mind if you want to try one of these tools.

Chatbots have been around for many years, but the rise of major language models, such as ChatGPT and Google Bard, has given the chatbot industry a new lease of life.

Millions of people are now using AI chatbots worldwide, but there are some important risks and privacy concerns to keep in mind if you want to try one of these tools.

1. Collect data

Most people don't use chatbots just to say hello. Modern chatbots are designed to handle and respond to complex questions and requests, with users often including a lot of information in their prompts. Even if you're just asking a simple question, you don't really want it to go beyond the conversation.

According to OpenAI support, you can delete ChatGPT chat logs whenever you want, and those logs will then be permanently deleted from OpenAI's systems after 30 days. However, the company will retain and review certain chat logs if they are determined to be harmful or inappropriate content.

Another popular AI chatbot, Claude, also keeps track of your previous conversations. Anthropic's support center states that Claude tracks *"your prompts and outputs in the product to provide you with a consistent product experience over time under your control"*. You can delete your conversations with Claude so that it forgets what you were saying, but this does not mean that Anthropic will immediately delete your logs from its system.

Of course, this leads to the question: Is your data kept? Do ChatGPT or other chatbots use your data?

But the concerns don't stop here.

2. Data theft

Like any online tool or platform, chatbots are vulnerable to cybercriminals. Even if a chatbot has done all it can to protect its users and data, there is always the possibility that a skilled hacker will find a way to penetrate its internal systems.

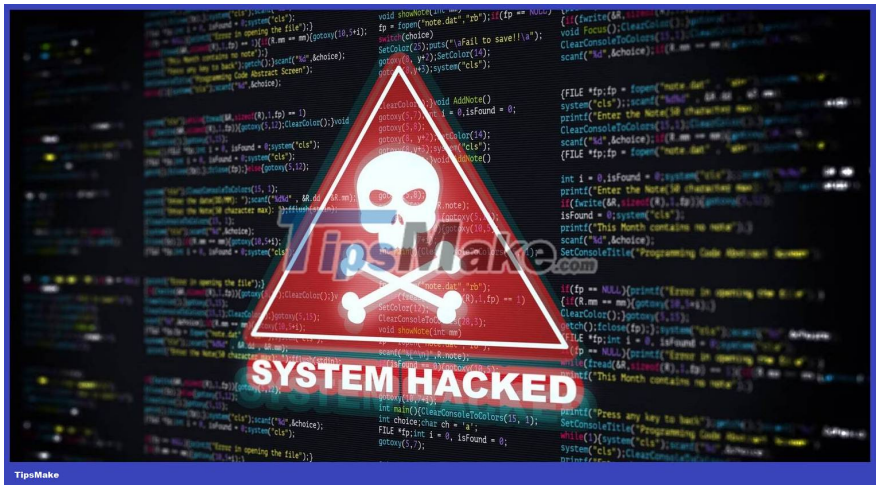
If a certain chatbot service is storing your sensitive information, such as payment details for a paid subscription, contact data or similar information, this information could be stolen and exploit if a cyber attack occurs.

This is especially true if you are using a less secure chatbot whose developer has not invested in adequate security protection. Not only can a company's internal systems be hacked, but your own account is also at risk of being compromised without a login warning or authentication layer.

Now that AI chatbots are so popular, cybercriminals have naturally flocked to use this industry for fraud. Fake ChatGPT websites and plugins have become a major problem since OpenAI's chatbots became popular in late 2022, causing people to fall into scams and provide personal information under the guise of being legitimate. and reliable.

In March 2023, MUO reported on a fake ChatGPT Chrome extension that steals Facebook login credentials. The plugin can exploit Facebook's backdoor to hack premium accounts and steal users' cookies. This is just one example of many fake ChatGPT services designed to scam unsuspecting victims.

3. Malware infection



If you are using a shady chatbot without realizing it, you may find the chatbot providing you with links to malicious websites. Maybe the chatbot alerted you to a great giveaway or provided a source for one of its answers. If the service operator has hidden intentions, the overall purpose of the platform may be to spread malware and phishing through malicious links.

Additionally, hackers could compromise a legitimate chatbot service and use it to spread malware. If this chatbot was truly human, thousands or even millions of users would be exposed to this malware. Fake ChatGPT apps have even appeared on the Apple App Store, so it's best to be careful.

In general, you should never click on any link a chatbot provides before running it through a link checking website. This may seem annoying, but it's best to make sure that the website you're being directed to doesn't have a malicious design.

Additionally, you should never install any chatbot plugins and extensions without first verifying their legitimacy. Do a little research around the app to see if it has good reviews, and look up the app developer to see if you can find anything shady.