5 things not to be shared with AI chatbots

There are inherent risks associated with using AI chatbots, such as privacy concerns and potential cyberattacks. It is important to exercise caution when interacting with chatbots.

The popularity of AI chatbots has increased. While their capabilities are impressive, it's important to admit that chatbots aren't perfect. There are inherent risks associated with using AI chatbots, such as privacy concerns and potential cyberattacks. It is important to exercise caution when interacting with chatbots.

Let's explore the potential dangers of sharing information with AI chatbots and see what types of information should not be disclosed to them. To ensure your privacy and security, it is essential to pay attention to the following 5 things when interacting with AI chatbots.

1. Financial details

Can cybercriminals use AI chatbots like ChatGPT to hack your bank account? With the widespread use of AI chatbots, many users have turned to these language models for personal financial advice and management. While they can enhance financial literacy, it's important to be aware of the potential dangers of sharing financial information with AI chatbots.

When using a chatbot as a financial advisor, you run the risk of disclosing your financial information to potential cybercriminals who could exploit that information to withdraw funds from your account. Although companies claim to anonymize conversation data, third parties and some employees may still have access to that data. This raises concerns about profiling, where your financial details could be used for malicious purposes like a ransomware campaign or sold to marketing agents.

To protect your financial information from AI chatbots, you must be mindful of what you share with these Generative AI models. Your interactions should be limited to gathering general information and asking broad questions. If you need personalized financial advice, there may be better options than relying solely on AI bots. They can provide inaccurate or misleading information, potentially putting your hard-earned money at risk. Instead, consider seeking advice from a financial advisor who can provide consistent and reliable guidance.

2. Your personal and intimate thoughts

Many users are turning to AI chatbots to seek therapy, unaware of the potential consequences for their mental health. Understanding the dangers of disclosing personal and confidential information to these chatbots is essential.

Firstly, chatbots lack practical knowledge and can only give general answers to questions related to mental health. This means that the medications or treatments they recommend may not be suitable for your specific needs and could be harmful to your health.

Furthermore, sharing personal thoughts with AI chatbots raises privacy concerns. Your privacy can be compromised as secrets and intimate thoughts can leak online. Malicious individuals can exploit this information to track you or sell your data on the dark web. Therefore, it is extremely important to protect the privacy of personal thoughts when interacting with AI chatbots.

It is important to approach AI chatbots as a general information and support tool rather than as an alternative to professional therapy. If you need mental health advice or treatment, you should always consult a qualified health professional. They can provide personalized and trusted guidance while prioritizing your privacy and well-being.

3. Confidential information about your workplace

Another mistake users must avoid when interacting with AI chatbots is sharing confidential work-related information. Even well-known tech giants like Apple, Samsung, JPMorgan and Google, the creators of Bard, have restricted their employees from using AI chatbots in the workplace.

A report by Bloomberg highlighted a case where a Samsung employee used ChatGPT for programming and accidentally uploaded sensitive code to the Generative AI platform. This incident resulted in the unauthorized disclosure of confidential information about Samsung, prompting the company to enforce a ban on the use of AI chatbots. As a developer looking for AI assistance to solve programming problems, here's why you shouldn't trust AI chatbots like ChatGPT with confidential information. It is essential to exercise caution when sharing sensitive code or work-related details.

Likewise, many employees rely on AI chatbots to summarize meeting minutes or automate repetitive tasks, posing the risk of accidentally exposing sensitive data. Therefore, it is extremely important to maintain the privacy of confidential work information and limit its sharing with AI chatbots.

Users can protect sensitive information and their organization from unintended data leaks or breaches by being mindful of the risks associated with sharing work-related data.

4. Password

It's important to emphasize that sharing your passwords online, even with language models, is an absolute no-no. These models store your data on public servers, and revealing your password to them jeopardizes your privacy. In the event of a server breach, hackers can access and exploit your passwords for financial harm.

A serious data breach related to ChatGPT occurred in May 2022, raising serious concerns about the security of the chatbot platform. Furthermore, ChatGPT has been banned in Italy due to the General Data Protection Regulation (GDPR) of the European Union. Italian regulators argue that the AI ??chatbot does not comply with privacy laws, highlighting the risks of data breaches on the platform. Therefore, it becomes paramount to protect your login information from AI chatbots.

By limiting sharing your passwords with these chatbot models, you can proactively protect your personal information and reduce your chances of falling victim to cyber threats. Remember, protecting your login information is an essential step to maintaining your privacy and security online.

5. Housing details and other personal data

It is important not to share personally identifiable information (PII) with AI chatbots. PII includes sensitive data that can be used to identify or locate you, including your location, social security number, date of birth, and health information. A top priority is to ensure the privacy of personal and residential details when interacting with AI chatbots.

To maintain the privacy of your personal data when interacting with AI chatbots, here are some key practices to follow:

1. Familiarize yourself with the chatbot's privacy policies to understand the risks involved.
2. Avoid asking questions that may inadvertently reveal your identity or personal information.
3. Be cautious and do not share your medical information with AI bots.
4. Be mindful of potential vulnerabilities in your data when using AI chatbots on social platforms like SnapChat.