Users should remove ChatGPT fake applications immediately if they do not want to 'lose money'

Many hackers have prepared to attack users through completely free ChatGPT fake applications on both the App Store and Google Play Store.

Many people use ChatGPT for a variety of legitimate uses, including answering questions, creating content, explaining complex concepts, and writing code. However, the limitations of the free version of the chatbot, such as slow responses, may annoy you.

Malicious actors often exploit these limitations by encouraging users to download a supposedly premium version of ChatGPT for free. Fake chatbots may contain malware that can be used for cyber attacks, such as data theft.

Below is a list of domains and malicious applications impersonating ChatGPT that you need to know.

Fake ChatGPT domains and applications

1. chat-gpt-pc.online

Security researchers at Cyble Research and Intelligence Labs (CRIL) discovered cybercriminals using the domain name "chat-gpt-pc.online" to lure unsuspecting users into downloading a supposed desktop client. is ChatGPT Windows. However, this client contains malware that steals RedLine information.

Cybercriminals used a Facebook page impersonating OpenAI, complete with official ChatGPT logos, to redirect unsuspecting users to the malicious website.

2. openai-pc-pro.online

Experts at CRIL also discovered an unknown type of malware being distributed through the domain name 'openai-pc-pro.online', a malicious domain masquerading as the official ChatGPT website.

This domain is promoted by 'Chat GPT AI', a popular ChatGPT-themed Facebook page that regularly posts about ChatGPT and OpenAI's Jukebox. The posts often contain links to malicious domains, including openai-pc-pro.online.

Suspicious domain directs users to a fake OpenAI website that resembles the official one. The website has a 'DOWNLOAD FOR WINDOWS' button, which when clicked downloads an executable file containing data-stealing malware.

3. chat-gpt-pc.online

ChatGPT AI, the fake ChatGPT Facebook page, also had posts that included links to 'chat-gpt-pc.online', another domain that redirects users to a malicious ChatGPT-themed website.

4. chatgpt-go.online

The domain 'chatgpt-go.online' leads users to a website that is a clone of the official ChatGPT website. However, the copied website swapped the 'TRY CHATGPT' button link with malicious links containing Lumma Stealer. This domain also hosts various types of malicious files, including clipper and Aurora stealer malware.

5. pay.chatgptftw.com

Cybercriminals also use ChatGPT themed payment sites to commit financial fraud. For example, on the domain 'pay.chatgptftw.com', Cyble came across a page designed to steal credit card information. This website serves as the official payment site for ChatGPT Plus.

6. ChatGPT1

Cy's report highlights another malware application that uses the ChatGPT logo. The malicious app 'ChatGPT1' is an SMS payment fraud application downloaded as chatGPT1.apk. It operates discreetly, subscribing users to premium services without their consent.

7. AI Photo

'AI Photo' is another app that uses the ChatGPT icon but with malicious intent. This application was found to contain SpyNote malware, capable of stealing device files, contact lists, call logs and text messages.

8. Trojan-PSW.Win64.Fobo

Kaspersky researchers have discovered that cybercriminals are using a fake ChatGPT client for Windows to spread information-stealing Trojans. The Trojan, named Trojan-PSW.Win64.Fobo, if installed on a user's

computer, can steal account information stored in various browsers, including Chrome, Edge, Firefox and Brave.

The Trojan targets Facebook, TikTok, and Google accounts, stealing login credentials and financial information, like ad spend and current balance. To achieve this, the perpetrators create social media groups that resemble official OpenAI accounts or enthusiast communities, where they post download links for the ChatGPT desktop client with malicious intent.

If you click the link, you will be redirected to a website that prompts you to download ChatGPT for Windows. Clicking the button will download an archive containing the executable file.

When extracting the archive and running the file, you may or may not receive an installation error message. In both cases, the Trojan is installed.

Fake ChatGPT application on App Store and Google Play Store

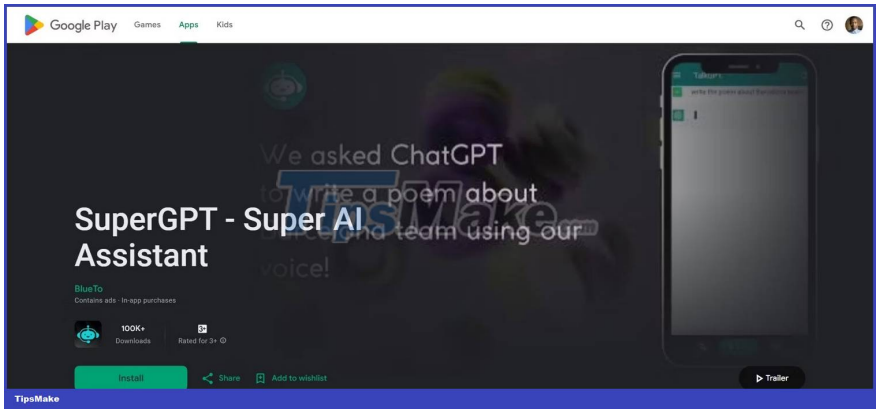
ChatGPT, super AI is extremely hot in Vietnam and around the world, attracting the attention of many users. Therefore, in recent times, this Chatbot has been used by many bad guys as a new form of fraud. Many hackers have prepared to attack users through completely free ChatGPT fake applications on both the App Store and Google Play Store.

When users download and install these fake applications, hackers can steal data or demand a monthly usage fee.

Many users, because they have not researched carefully, do not have accurate information, and do not know much about technology, can download these fake applications.

?On Android:

1. Meterpreter pretends to be a 'SuperGPT' app: SuperGPT is an AI assistant app built on ChatGPT. However, researchers from Unit 42 discovered a malicious APK sample masquerading as this app. This fake 'SuperGPT' is a Meterpreter Trojan, a RAT that allows remote access to Android devices.



1. AI Chat Companion
2. ChatGPT 3: ChatGPT AI
3. Talk GPT – Talk to ChatGPT
4. ChatGPT AI Writing Assistant
5. Open Chat – AI Chatbot App

On iOS:

1. Open Chat – AI Chatbot
2. Wisdom AI – Your AI Assistant
3. Chat AI: Personal AI Assistant
4. Alfred – Chat with GPT 3
5. TalkGPT – Talk to ChatGPT
6. Write For Me GPT AI Assistant
7. Genie – GPT AI Assistant

According to Top10VPN's assessment, the user's location information after being stolen by the above fake applications will be shared with ByteDance, Amazon, Appodeal and InMobi."

ChatGPT is currently still in the research stage. The tool is available for free, can only be accessed through OpenAI's website, and has no mobile app.

Recently, OpenAI launched a $20/month subscription package with ChatGPT Plus version that provides faster and more stable service with the opportunity to try out new features.

What should I do if I discover a fake ChatGPT website?

If you see any signs or websites that at first glance seem suspicious, report them immediately (for example, to CISA in the US and NCSC in the UK - both national computer crime agencies). Don't use your personal information, don't even log in, and don't use credit cards or other financial information. Also, avoid downloading attachments or clicking on website links.

Alternatively, post about the site with its URL on a public forum (somewhere like Reddit or X) and explain why you think the site is suspicious. It will prevent other users from falling victim and may encourage security researchers to investigate it.

What to do if you have fallen victim to the fake ChatGPT website

If you have fallen victim to the ChatGPT scam website, there are several steps you can take to repair the damage.

1. If you just visited a phishing site and haven't done anything else, you're probably safe. All you have to do is leave the site and never visit again.
2. If you bought a product or signed up for a service on a fake website and realized it too late, immediately contact your credit card company or bank for a refund and ask them Monitor your account for suspicious activity.

Websites without SSL certificates are mainly used to steal your personal information and then sell it to scammers. Therefore, if you have used your credit card on a shady website, ask your bank or company to freeze it. If you registered on the scam site using your primary email ID or phone number, watch out for future scam emails or phone calls and change any passwords you use.

Notify the authorities of any breach of personal (and important) information you mistakenly share on the website, including social security number, name, address, etc. This will help you avoid legal consequences if scammers misuse your information.

If you've downloaded an attachment disguised as an important document or file, scan your device for malware and make sure it's not infected. If you have any apps installed, uninstall them as soon as possible.

If you've clicked on a link or pop-up on a website, check your browser for signs of an attack. If it looks like your browser has been hacked, completely uninstall it and then reinstall it.

You finished reading the article "**Users should remove ChatGPT fake applications immediately if they do not want to 'lose money**'" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
