Tips for using ChatGPT to detect phishing links

Instructions on using ChatGPT and Malwarebytes to check for phishing links, emails, and messages.

Have you ever received a suspicious link, phone number, email, or text message and wondered if it's actually safe? With scams becoming increasingly sophisticated, distinguishing between genuine and fake is becoming more and more difficult.

The good news is you can now leverage ChatGPT to check suspicious content before clicking. A new integration between ChatGPT and Malwarebytes lets you check links, phone numbers, emails, and messages right within the chat. This tool uses Malwarebytes' security database—built over years with data on phishing, malware, and malicious domains—to help you quickly detect threats. Here's how to use this feature—it's incredibly simple.

How to use Malwarebytes in ChatGPT

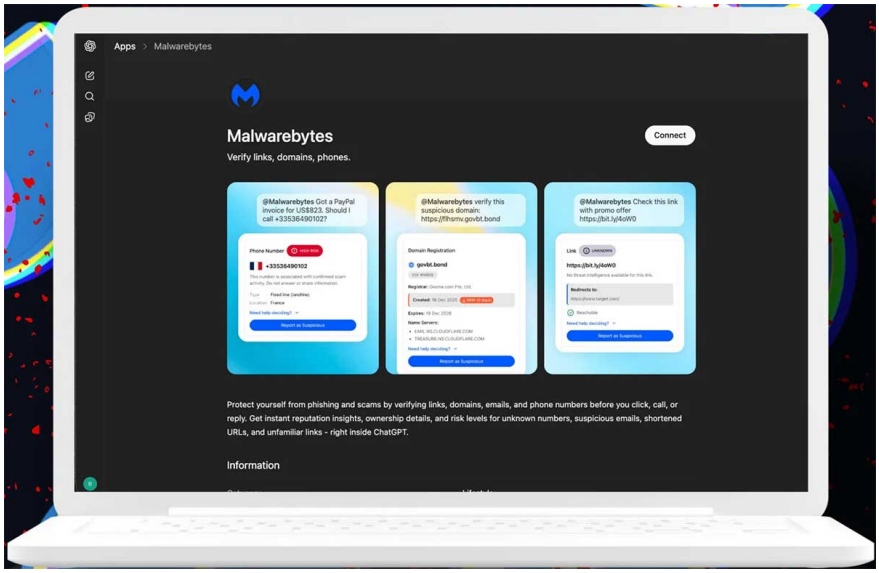
1. Connect Malwarebytes in ChatGPT

Before using it, you need to enable Malwarebytes integration in ChatGPT. The good news is that you only need ChatGPT; you don't need to create a Malwarebytes account or pay any fees.

The steps are as follows:

1. Open ChatGPT
2. Go to Settings
3. Select Apps
4. Find Malwarebytes
5. Connect to enable integration.

After the initial connection, Malwarebytes will always be available for subsequent conversations. This feature is currently being rolled out to ChatGPT Free, Plus, Team, and Enterprise users in supported regions.



2. Check messages or content that you suspect are scamming.

The simplest way is to ask ChatGPT to check any content you find suspicious.

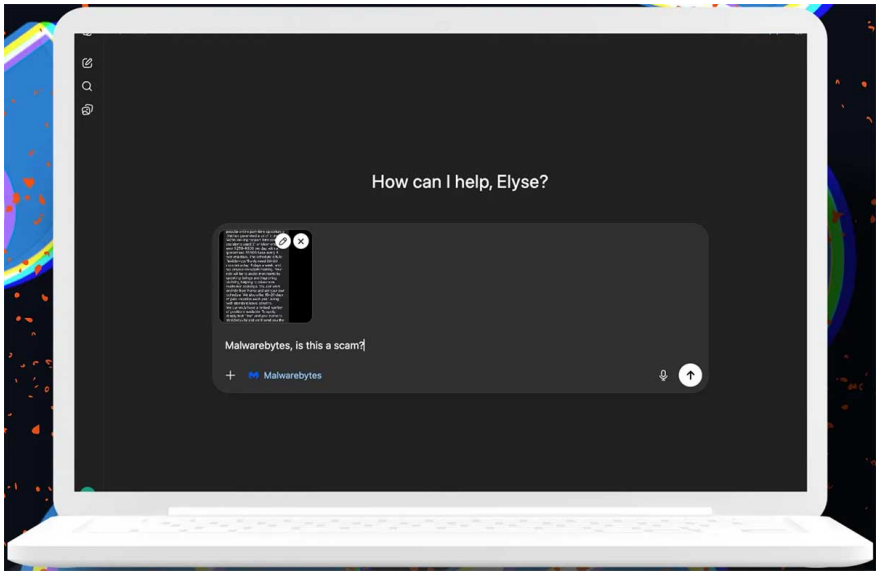
You can check the following information:

1. Link
2. E-mail
3. Phone number
4. SMS messages
5. Unknown domain

Simply open a new conversation and enter a command like this:

" **Malwarebytes, is this a scam** ?"

Then paste the suspicious content or upload a screenshot. Malwarebytes will analyze it and provide you with information about the sender, the risk level, signs of phishing, and suggested appropriate action.



During testing, a suspicious recruitment message was flagged as a scam by Malwarebytes. Although the phone number and email address lacked clear data, the system advised against responding and recommended verifying the information through official channels.

3. Check the link before clicking.

Another useful feature is checking the safety of the link.

You just need to:

1. Copy suspicious link
2. Do not click the link.
3. Ask ChatGPT something like:
   "Malwarebytes, is this website safe?"

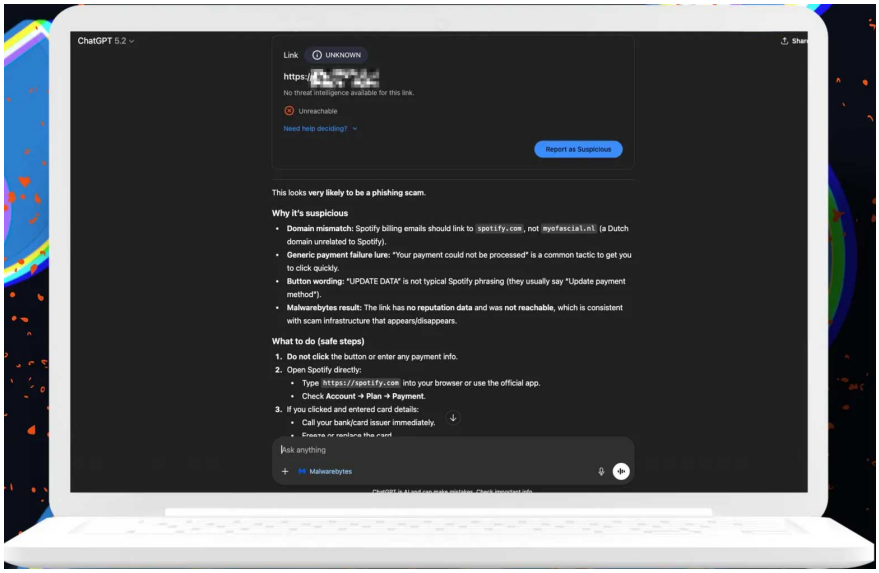
Then paste the link into the conversation.

Malwarebytes will check for dangerous signs such as:

1. Phishing
2. Malware
3. Fake domain
4. Fake login page

In one test, a fake Spotify email requesting a payment update was flagged as phishing. Malwarebytes detected a mismatched domain and an invalid URL.

Conversely, when checking the official Spotify link, Malwarebytes confirmed the domain was valid and HTTPS secure. However, the system still recommended accessing the site directly instead of clicking on the link in the email.



4. Report fraudulent content.

One interesting aspect of this feature is that you can contribute to the security system.

After receiving the analysis results, you can click "Report as suspicious" to report any suspicious content.

You can report:

1. Message
2. E-mail
3. Phone number
4. Link
5. Other suspicious content

After submission, Malwarebytes will update its database to improve its phishing detection capabilities in the future.

AI is becoming an effective tool for combating fraud.

With Malwarebytes integration, ChatGPT is not just a chatbot but also a useful security tool. You can quickly check suspicious content without installing additional software.

In the context of increasingly sophisticated scams, this is a simple yet incredibly useful tool to protect your data and accounts.

You finished reading the article "**Tips for using ChatGPT to detect phishing links**" 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.

© 2019 TipsMake.com