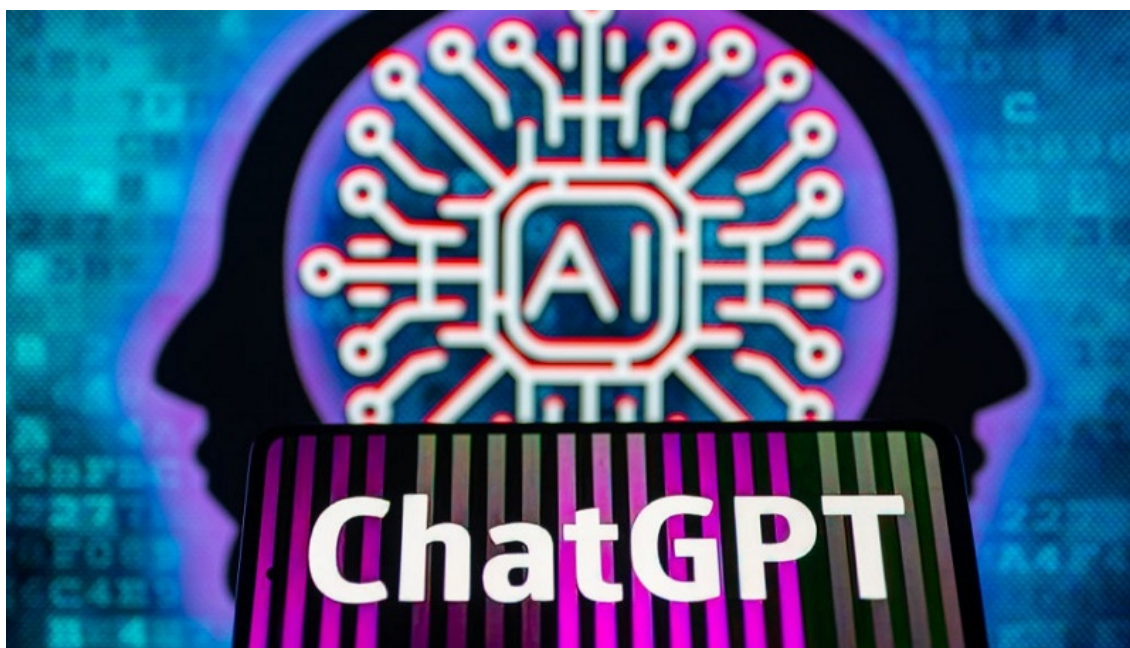


ChatGPT tiềm ẩn nhiều nguy cơ về an ninh mạng

21:06 21/03/2023

Sức nóng của ChatGPT tạo cơ hội cho nhiều đối tượng tạo các ứng dụng giả mạo với logo hay tên gọi gần giống ChatGPT để kiếm tiền của người dùng.



Ảnh minh họa. (Ảnh: internet)

Một số ứng dụng trên nền tảng Android yêu cầu người dùng cấp quyền truy cập sau đó đánh cắp thông tin và dữ liệu người dùng. Google Play đã rà soát và gỡ bỏ các ứng dụng giả mạo nhưng vẫn còn tồn tại khá nhiều ứng dụng như thế.

Một số website có tên miền gần giống với website chính thức, khi truy cập người dùng sẽ được kết nối với trang thông tin yêu cầu điền các thông tin thẻ ứng dụng để mua bản cao cấp từ đó đánh cắp thẻ của người dùng.

Lợi dụng khả năng viết code của GPT, nhiều mã lệnh phục vụ mục đích xấu được tạo ra, các đoạn code đó được công khai chia sẻ trên nhiều diễn đàn hacker. Các biện pháp đã được đưa ra để ngăn chặn ứng dụng này đưa câu trả lời cho các hành động nguy hiểm nhưng hiệu quả chưa cao.

Lợi dụng ChatGPT, nhiều tin tặc cũng thực hiện hành vi lừa đảo qua tin nhắn hoặc email với cơ chế tinh vi, vượt mặt các công nghệ phát hiện email spam.

Để tránh mối nguy hiểm mà ChatGPT có thể tạo ra, các chuyên gia Bkav khuyến cáo:

ChatGPT hiện chỉ cung cấp duy nhất qua trang web tại địa chỉ:

<https://chat.openai.com>. Microsoft và OpenAI cũng đã đưa AI được cải tiến dựa trên ChatGPT vào công cụ Bing. Các trang web, ứng dụng khác đều là giả mạo, không nên sử dụng.

Người dùng cũng cần cẩn trọng với các email có đính kèm đường dẫn, file thực thi. Có thể kiểm tra đường dẫn trước khi mở bằng cách sử dụng các công cụ <https://sitecheck.sucuri.net/> hay <https://check.spamhaus.org/> để kiểm tra đường dẫn và <https://www.virustotal.com/>.

Bên cạnh đó, người dùng cũng cần sử dụng các giải pháp, phần mềm an ninh mạng trên máy tính cũng như điện thoại để bảo vệ chúng khỏi các mối nguy hại.

Hà Trần (t/h)