Всегда ли нужно доверять чат-ботам?

То, что не так давно казалось фантастикой, сегодня является реальностью и развивается с такой скоростью, что уследить за появлением новых форм просто нереально. Речь, конечно же, об искусственном интеллекте (ИИ), который уже давно занимает прочную позицию в нашей жизни, хотя об этом многие потребители даже не догадываются. Одной из разновидностей ИИ являются чат-боты(от англ. chatbot), которые, по своей сути, должны помогать нам, потребителям, в решении определённых задач, тем самым сокращая время на их решение по сравнению с тем, что если бы мы сами занимались этим. Простыми словами, это виртуальный помощник с искусственным интеллектом для разных целей. Чат-бот — специальная программа, которая общается с пользователем по заданному сценарию. Чат-бот умеет отвечать на вопросы и задавать их пользователю, искать информацию и выполнять простые задачи. С чат-ботами можно общаться в текстовой или голосовой форме. По запросу пользователя он может заказать еду, вызвать такси, заказать билет на мероприятие, найти какую-либо информацию или товар в поисковике, проложить маршрут, ответить на вопрос и много других функций. Многие популярные мессенджеры используют чат-ботов, к ним относятся Telegram, WhatsApp, Viber и некоторые социальные сети, например, ВКонтакте. Банковские приложения стали активно использовать в работе чат-ботов, тем самым экономя свои ресурсы и помогая клиентам самостоятельно решать задачи онлайн.

Ритм жизни в 21 веке заставляет современного человека ускоряться, решать множество задач, используя при этом минимальное количество своего времени и без роботизированных помощников не обойтись. Чат-боты, в отличие от человека, могут работать 24/7 без отдыха, перерывов на обеды, праздников и выходных, обрабатывать тысячи запросов за короткий период времени и выдавать необходимые результаты. Таким образом, без помощи ИИ нам уже не обойтись и вовлечение в различные сферы нашей жизни ИИ со временем будет только увеличиваться.

Но всегда ли нужно доверять чат-ботам?

К сожалению, такая сфера деятельности, как мошенничество, развивается тоже очень быстро. Нажива лёгких денег преобладает над совестью и разумом и мошенники уже начали использовать ИИ в своих корыстных целях.

Недавно в СМИ появилась информация о новом способе обмана российских граждан при помощи чат-ботов, составляющих идеальные тексты. Это особенно актуально потому, что главным недостатком фишинговых текстов всегда был язык — не каждый мошенник пишет складно и грамотно.

Качественные тексты объявлений повышают вероятность того, что пользователь поверит автору и посетит сайт. Поэтому лучше не переходить по любым сомнительным ссылкам в мессенджерах — например, в сообщениях от банков и служб доставки. Особенно если в них говорится о больших скидках или щедрых бонусах.

Кроме того, с помощью чат-ботов хакеры научились распространять вирусы-шифровальщики и плагины для браузера, способные похищать пароли и данные банковских карт. Поэтому в целях безопасности лучше не сохранять такие данные в памяти браузеров.

Мошенники научились взламыватьчат-боты различных компаний, а послесоздают и организуют рассылку-опрос, с помощью которой собирают личную информацию: ФИО

пользователей, номера телефонов, геолокацию и т.д. Хакеры могут создавать и собственные чат-боты и использовать их в работе своих фишинговых (мошеннических) сайтах. Наличие чат-бота придает фишинговому сайту большую правдоподобность, — люди доверяют чат-ботам и не подозревают, что свои данные передают мошенникам.

Так, в 2023 году в России разоблачили мошенническую схему, связанную с социальными выплатами. Мошенники оставляли в общественных местах QR-коды с объявлением о бесплатной консультации по гарантированным выплатам, код в свою очередь вел на чат-бот в одном из мессенджеров. При общении с чат-ботом людей убеждали, что они имеют право на соцвыплату, после чего жертвы вводили свои финансовые данные, которые и похищали мошенники.

Как защититься от подобных действий? Способов много и все они не новы:

- не выкладывать в социальные сети слишком много информации о себе;
- не загружать в интернет личные фото или ограничивать их просмотр:
- использовать псевдоним и стоковые фото для аватарок;
- не переходить по ссылкам, присланным через мессенжеры или СМС;
- не скачивать и не устанавливать на мобильное устройство или компьютер различные программы, обновления и игры из непроверенных источников – таким образом можно вместе с нужным приложением скачать вирус, с помощью которого мошенники могут не только похитить данные потребителя, но и, завладев нужной информацией, онлайн оформить кредиты, совершить сделки с недвижимостью, похитить деньги с банковской карты и пр.;
- не брать трубку и не перезванивать на незнакомые номера, тем более, если звонок поступил через Ватсапп или Вайбер.

Способы защиты можно перечислять бесконечно, но главным способом защиты от мошенников является бдительность и осторожность самого потребителя.

Информация подготовлена с использованием сети интернет и ИС КонсультантПлюс.

специалистом
консультационного пункта для потребителей
филиала ФБУЗ «Центр гигиены и эпидемиологии в Иркутской области»
в Тайшетском и Чунском районах.