

О правилах безопасности в цифровом пространстве

На сегодняшний день нейросети все чаще и чаще появляются в нашем информационном поле. Каждую секунду нейросети обогащаются, развиваются и становятся все полезнее. В то же время, такую на первый взгляд полезную технологию быстро освоили преступники. Мошенники научились использовать нейросети для совершенствования своих методов введения в заблуждение и обмана и дальнейшего выманивания у граждан благ. К примеру, с помощью нейросетей мошенники генерируют шаблоны для общения с потенциальными жертвами. Здесь работает принцип: чем больше общаешься с нейросетью, тем больше она развивается. Практически любое мошенничество можно привести к базовому сценарию из трех пунктов: жертву нужно заинтересовать, втереться в доверие и заставить совершить действие.

Как же мошенники привлекают внимание граждан? В первую очередь, нужен яркий информационный вброс, цепляющий взгляд, чтобы заставить человека задержаться у телефона, дочитать до конца сообщение. Дальше – заставить поверить в рассказанную историю, используя в том числе несуществующие фотографии.

Мошенники обычно используют нейросети не как основной инструмент, а как вспомогательное звено своей цепочки. Из популярных нейросетей сегодня можно выделить чат-боты с искусственным интеллектом и нейросети для генерации текста, искусственных фото и видео. В первом случае мошенники используют ChatGPT и другие чат-боты, чтобы сгенерировать грамотный текст для фишингового письма или рассылки. Также их применяют для имитации определенного стиля общения, например создают фальшивые страницы в соцсетях, или в других приложениях.

Что касается нейросетей для генерации фото и видео, то здесь у мошенников есть несколько схем, как воздействовать на жертву. Например, они создают фейковые интимные фото жертвы на основе ее реальных фото из соцсетей, а затем шантажируют и требуют выкуп. Или создают реалистичные картинки для фальшивых сборов на благотворительность.

Правила защиты от мошенников не зависят от того, какие схемы те применяют – с использованием нейросетей, или без. Они базовые, и требуют исполнения от каждого: не стоит распространять в интернете и переписках конфиденциальную информацию (от паспортных данных до банковских реквизитов), верить слишком приятным и заманчивым предложениям в Интернете, переводить по просьбе неизвестных лиц денежные средства и тем более вводить на сомнительных сайтах данные

своих банковских карт. Не стоит забывать и про технические средства защиты – антивирус способен защитить от большого количества угроз. Кроме того, рекомендуется устанавливать на устройствах разные и сложные пароли, в которых присутствуют цифры, заглавные буквы. Чтобы не стать жертвой мошенничества, не стоит отвечать на звонки с незнакомых номеров, не верить и сразу направлять денежные средства на тот конец телефона. Кроме того, если в разговоре вы почувствовали что-то неладное, лучше всего будет задать собеседнику случайный вопрос – это поможет понять, что вы общаетесь с живым человеком, а не с ботом.

Для защиты ваших данных и денежных средств рекомендуем придумать секретные слова и кодовые фразы, чтобы обеспечить безопасность ваших переписок и звонков. К примеру, если вам позвонит кто-то из близких со своего номера и будет говорить с вами своим голосом и просить перевести денежные средства, вы можете не понять, что с вами разговаривает нейросеть. И в таком случае спасают кодовые слова. Кодовые фразы и секретные слова помогут отличить вашего близкого от мошенника, использующего нейросеть.

Будьте бдительными, не передавайте личную информацию, если есть сомнения в подлинности звонка или сообщения. Это может помочь защитить вас и ваших близких от возможных атак со стороны кибермошенников.