Разъясняет помощник прокурора Промышленного района Корешкова Яна Алексеевна.

«Новый вид мошенничества: дипфейк и как не стать его жертвой?»

Образцы голоса потенциальной жертвы для создания дипфейков злоумышленники могут добывать разными путями, мошенникам помогают публичные аудио- и видеозаписи в соцсетях, а также утечки биометрических данных. Кроме того, они могут просто позвонить человеку по телефону и записать его голос на диктофон.

Для того чтобы создать голосовой дипфейк, имитирующий речь конкретного человека, злоумышленникам нужны образцы его голоса. При наличии нескольких образцов голоса мошенники могут с помощью нейросети создать аудиозапись с необходимым им содержанием. Инструменты для этого существуют даже в открытом доступе.

Мошенники стали имитировать голоса знакомых, родных или коллег при помощи специальных программ. Злоумышленники звонят потенциальным жертвам под видом близких, чтобы получить необходимые сведения или заставить человека перевести деньги. Сегодня злоумышленники активно используют комбинированные схемы мошенничества, главным образом телефонного.

При этом всё чаще создаются так называемые адресные схемы, составленные по цифровому портрету человека. Мошенники могут собрать его на основании тех данных, которые сам пользователь разместил в сети, используя информацию о родственниках и друзьях, работе или досуге.

Рекомендации: осторожно подходить к размещению личной и финансовой информации в социальных сетях и других открытых ресурсах.

Никогда не пересылайте в мессенджерах и социальных сетях сведения из документов, не вводите свои данные на сомнительных сайтах.

Не нужно совершать какие-либо денежные операции по просьбе позвонившего незнакомца.

В случае любых сомнений рекомендуют связаться с человеком, от имени которого вам позвонили, и уточнить у него всю информацию.

Подделывать голос можно с помощью большого количества сервисов и программ, которые способны генерировать голос человека по записанному образцу. При этом «похожесть» синтезированного голоса зависит от качества и объема записанных образцов, в генерации голосовых дипфейков большую роль играет искусственный интеллект (ИИ). При помощи нейросетей преступники могут воспроизвести интонацию, ритм и особенности речи конкретного человека, чтобы создать убедительное аудиосообщение.

В первую очередь под угрозой обмана при помощи дипфейков находятся те, кто меньше всего подготовлен с точки зрения технологий. Это, конечно, люди старшего возраста. В то же время рискуют и родственники публичных людей, поскольку образцы голосов звезд легче найти в открытом доступе.

Для того чтобы создать голосовой дипфейк, имитирующий речь конкретного человека, злоумышленникам нужны образцы его голоса. При наличии нескольких образцов голоса мошенники могут с помощью нейросети создать аудиозапись с необходимым им содержанием. Инструменты для этого существуют даже в открытом доступе. Однако в режиме реального времени создавать подобную запись не получится.

В случае, если Вы стали жертвой мошенников и, заблуждаясь, участвовали в криминальной схеме, передав свои персональные данные организаторам преступлений, следует обращаться в правоохранительные органы.

Прокуратура Промышленного района г. Самары – 951-17-77

Отдел полиции по Промышленному району УМВД России по г. Самаре - 995-86-83, - 995-90-60