БАРАБИНСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА

ПАМЯТКА

МОШЕННИЧЕСТВО С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Клонирование голоса

"Благодаря имеющимся технологиям хакерам достаточно всего лишь 20-секундного фрагмента с разговором, взятым из социальной сети, для создания клона голоса любого человека. Идентичность поражает настолько, что даже мать не сможет отличить голос своего ребенка от робота", — предупреждают эксперты.

Преступники получают аудиообразцы голосов различными способами, например, записывая звук во время телефонных разговоров, используя видеозаписи в социальных сетях или записывая звук в общественных местах, например, в кафе.

После обработки через специальные программы вам может поступить звонок, и вы услышите речь и голос своего товарища или родственника, но на самом деле это мошенники.

Схема обмана та же: гражданин звонит и просит перевести деньги. Преступники заставляют жертв думать, что они разговаривают с родственником, которому вдруг понадобились деньги, например, на возмещение ущерба в результате ДТП. Необходимо сразу перезвонить своим родным и знакомым, от которых и была получена просьба. Еще лучше придумать кодовое слово, для своих, чтобы можно было понять: звонят родные, а не мошенники.

Так, в январе 2020 года управляющему одного из банков в Дубае позвонил директор. Он предупредил, что в почте того ждет запрос на перевод 35 миллионов долларов, подчеркнув, что оплату важного корпоративного приобретения следует одобрить как можно скорее. Что и сделал исполнительный сотрудник.

Прежде он не раз общался с директором и сразу узнал его голос в трубке. Но менеджер ошибался: распоряжение отдал вовсе не его директор, при этом внушительная сумма стала быстро растворяться в глобальных банковских сетях.

Имитация образа

Подделать можно не только голос, но и образ. Преступникам удается наложить ненастоящие изображение или видео на реальные. Технология называется "дипфейк" (от англ. deepfake — "подделка").

За рубежом злоумышленники опробовали дипфейки при устройстве на удаленную работу в сфере IT для получения доступа к базам данных. Однако созданные видеоклоны выдают свою искусственность темпом речи, асинхронностью и неестественными эмоциями.

Новые технологии используются не только передовыми IT-компаниями, но и вовсю группами мошенников. Не за горами момент, когда обманы со звонками от силовых ведомств и сотрудников банка будут полностью осуществляться программными алгоритмами на базе нейросетей.

Как распознать дипфейк:

Неестественная мимика — движения губ не попадают в такт с произносимыми словами, одно и то же выражение глаз, не видно смены эмоций.

Низкое разрешение, пикселизация или нечеткость изображения, особенно в областях с активной мимикой — брови, уголки рта.

Звук опережает картинку или не успевает за движениями персонажа.

В случае совершения в отношении Вас мошеннических действий, необходимо незамедлительно обратиться в правоохранительные органы.