# НОВЫЕ СПОСОБЫ МОШЕННИЧЕСТВА В 2026г.

Мошенники активно используют нейросети для подделки голосов, дипфейки, а также различные схемы с мессенджарами «Госуслуги»/ «МАХ».

Основные схемы:

- Имитация голоса и лица (дипфейк): используя нейросети создаётся голосовое/видео сообщение например от «родственников» с просьбой срочно перевести деньги на неизвестный вам счет или перейти по ссылке, которая является вирусом или позволяет мошенникам получить доступ к вашим данным;
- «Фото с друзьями прошлого»: рассылается сообщение с подписью «нашла наши фото, вспоминаю прошлое, посмотри и ты» со ссылкой, ведущей на фишинговый сайт, через который осуществляется кража данных;
- Обман через «Госуслуги» и демонстрацию экрана: поступает звонок от «сотрудника» Госуслуг о взломе аккаунта и с просьбой включить удаленную демонстрацию экрана для «срочной помощи/смены пароля», фактически для получения кодов доступа;
- Мошенничество с маркетплейсами при возврате денежных средств: взлом аккаунта и оформление возврата, продавец связывается в постороннем мессенджере и предлагает перевести деньги за товар на прямую, для «завершения» сделки с последующей просьбой озвучить код или данные госуслуг и прочего.

Как защититься?

- Никогда не устанавливайте приложения по просьбе звонящих и не переходите по сомнительным ссылкам;
- Не сообщайте коды из SMS и CVC-коды карт. Помните сотрудники банка и госорганов не запрашивают эту информацию;
- При «страшных» звонка кладите трубку. Чуть позже перезванивайте по официальным номерам, указанным на официальных сайтах госорганизаций;
- Для проверки голосовых/видео сообщений - звоните человеку напрямую или свяжитесь лично.

2026г. Прокуратура г.Братска