Какие сейчас новые виды мошенничества?

Самые актуальные новые схемы мошенничества связаны с **использованием искусственного интеллекта (дипфейки)**, **лжесотрудниками поликлиник или ЖКХ** в мессенджерах и **демонстрацией экрана смартфона**. Аферисты создают реалистичные видео и аудио сгенерированные образы руководителей или родственников, а также убеждают жертв включать показ экрана, чтобы украсть доступы к банковским приложениям.
Искусственный интеллект и дипфейки:

- **Видеозвонки от «родных»:** мошенники подделывают лицо и голос близких людей, которые якобы попали в беду, с просьбой срочно перевести деньги.
- **Сообщения от «директора»:** подчиненным приходят аудио- или видеосообщения от имени руководства компании с требованием провести финансовую операцию.

Обман через мессенджеры и демонстрацию экрана:

- **Лжемедики и коммунальщики:**

  злоумышленники пишут от имени поликлиник или жилищной инспекции, предлагают «сверить данные» или пугают штрафами за счетчики.

- **Показ экрана:** под предлогом замены счетчиков или настройки связи просят включить демонстрацию экрана в мессенджере, чтобы увидеть СМС-коды или данные для входа в банк.

Какие фразы выдают мошенников?

Мошенников выдают фразы о срочной угрозе деньгам и призывы перевести средства на «безопасный счет», такие как «Ваши деньги в опасности», «На ваше имя оформляют кредит» или «Сообщите код из СМС»

Распознать мошенника по переписке можно по резкому требованию денег или личных данных, угрозам, давлению, обещаниям легкого заработка, а также по подозрительным ссылкам, нехарактерному поведению знакомого и откровенному выманиванию личных фото.

Обратите внимание на 5 главных сигналов опасности:

1. **Разговоры о деньгах и паролях.** Вас просят оплатить «комиссию», оформить «возврат», перевести деньги на «безопасный счет» или продиктовать код из СМС. Настоящие банки и службы поддержки никогда не запрашивают пароли или данные карт.
2. **Искусственный дефицит времени.** Мошенники давят и торопят («акция закончится через 5 минут», «переведите сейчас, иначе заблокируют»), чтобы вы не успели перепроверить информацию.
3. **Необычный стиль общения от знакомого.** Если друг или родственник пишет с просьбой срочно занять денег, это может быть взлом. Задайте ему контрольный вопрос, ответ на который знаете только вы вдвоем, либо позвоните ему лично, чтобы подтвердить просьбу.
4. **Несуществующие выплаты и подозрительные ссылки.** Вам сообщают о неожиданном выигрыше или компенсации. Для ее получения просят перейти по ссылке (ведет на фишинговый сайт) или скачать приложение/файл, которые могут оказаться вредоносными.
5. **Слишком стремительное развитие событий и избегание встреч.** В чатах знакомств мошенники могут быстро признаваться в любви, а затем просить финансовой помощи (например, для покупки билета к вам или лечения несуществующего больного родственника), при этом всегда находя отговорки для личной встречи или видеозвонка.

Для проверки полученной информации всегда используйте официальные контакты поддержки или перепроверяйте факты через независимые источники. Если вы подозреваете, что аккаунт собеседника взломан, свяжитесь с ним по другому каналу связи.