

ПРОКУРАТУРА ТРОСНЯНСКОГО РАЙОНА РАЗЪЯСНЯЕТ

**Основные виды дистанционного мошенничества**

****Потерпевшими от дистанционного мошенничества являются граждане абсолютно всех категорий, включая как социально-незащищенные слои населения (инвалиды, пенсионеры, несовершеннолетние), так и люди, занимающие руководящие посты в организациях, имеющие несколько высших образований.

В современных условиях выделено несколько основных способов совершения мошенничества дистанционным способом.

**1. СМС от работодателя.**

Потерпевшему поступает СМС сообщение или сообщение в мессенджере от работодателя, о том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации и следует с ним пообщаться, а также направляет ссылку в мессенджере Телеграм, по которой нужно пройти.

После этого звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета, либо финансирование терроризма, либо ВС Украины и т.п. В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

**2. Злоумышленники «продают» вашу квартиру или автомобиль.**

Звонившие представляются представителями службы безопасности коммерческого банка, Госуслуг, Центрального банка России, либо правоохранительного органа.

Сообщают о том, что ваши персональные данные с личного кабинета утекли и теперь преступники могут от вашего имени продать квартиру либо автомобиль, используя электронно-цифровую подпись.

В целях защиты вас убеждают срочно их продать - перевести вырученные деньги на («защищенный канал», «безопасный счет», («резервную ячейку»).

**3. Перевод денег на «безопасный счет», якобы для их сохранности.**

Звонившие представляются либо представителями службы безопасности коммерческого банка, Центрального банка России, либо правоохранительного органа и сообщают, что мошенники с использованием ваших персональных данных оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета вам необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения вам сообщают о необходимости оформления кредитов и их перевода.

**4. Звонок злоумышленника под видом мобильных операторов,** которые сообщают, что срок действия вашей сим-карты истек либо истекает договор обслуживания, а для его продления необходимо сообщить код, который поступит в СМС, либо пройти по ссылке, в противном случае сим-карта будет заблокирована.

**5. Сдача налоговых деклараций и справок о доходах.**

Звонившие представляются сотрудниками Госуслуг, управления по делам Президента России, сообщают, что в рамках декларационной кампании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах.

Со слов злоумышленников для подтверждения следует назвать паспортные данные и код из СМС. Результат - списание денег с ваших счетов, оформление на ваше имя кредита.

**6. Взлом либо копирование аккаунта пользователя в мессенджерах** Ватсап, Вайбер, Телеграм, социальных сетей Вконтакте и дальнейшее направление сгенерированных искусственным интеллектом (нейросетью) голосовых либо видео сообщений от имени вашего знакомого, родных, коллег и т.д. (у которых ранее взломали аккаунт), которые полностью копируют их голос и видеоизображение, используя при этом ранее отправленные видео и аудио сообщения вашего знакомого.

А дальше все по типичной схеме - у вас просят одолжить взаймы, присылают фото банковской карты для перевода денежных средств.

**7. Хищение денежных средств через систему быстрых платежей (СБП).**

Например, покупатель на сайте оставляет заявку на приобретение товара, ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или по QR-коду затем злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду Покупатель подтверждает платеж и денежные средства поступают на счет мошенника.

**8. Заработок на бирже.** Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпром-инвестиции, РБК-инвестиции, Тинькофф-инвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков.

Под их руководством создается якобы личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и даже прибыль. Однако их дальнейший вывод невозможен.

**9. Рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика.**

В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы. Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика.

**10. Схема «ваш родственник попал в ДТП»**, наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего, либо представителем правоохранительного органа и сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства (взятку).



**Берегите себя и своих близких!**