Информация о профилактике кибермошенничества

Дистанционные мошенники: схемы обмана и способы защиты

На сегодняшний день жизнь большинства из нас сложно представить без сотовых телефонов и сети интернет. Заказать еду, оплатить счета, купить одежду, найти человека и многое другое можно сделать, не выходя из дома, достаточно иметь мобильный телефон или компьютер с доступом в интернет. Но если для одних людей это отличная возможность сэкономить свое время и максимально облегчить себе жизнь, то для других более «предприимчивых» граждан открывается огромное поле для мошеннической деятельности.

Дистанционные мошенничества на сегодняшний день являются одним из самых распространенных и трудно раскрываемых преступлений не только на территории г. Красноярска, но и на всей территории России в целом.

Уровень преступности в сфере информационных технологий, несмотря на принимаемые органами прокуратуры и правоохранительными органами меры, остается стабильно высоким. За 10 месяцев 2024 года по Красноярскому краю всего зарегистрировано 1353 преступления (увеличение на 28,5 % по сравнению с прошлым годом), уровень преступности составляет 14,9 % по краю. С начала 2024 года жертвами интернет-преступников 11 748 жителей края, а причиненный ущерб составил более 3 млрд 144 млн руб.

РАСПРОСТРАНЕННЫЕ СПОСОБЫ МОШЕННИЧЕСТВА

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.

В ходе общения злоумышленники могут присылать фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок о неразглашении следственной тайны и т.д.

2. 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.

Еще одна разновидность преступной схемы – 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.

3. 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.

Вторая разновидность таких преступлений – звонок злоумышленника об истечении срока действия медицинского страхового полиса, а для его продления необходимо сообщить код из СМС доступа к аккаунту Госуслуг, в дальнейшем следует оформление заявок на кредиты в банках, получение персональных данных, таких как сведения о доходах, наличие банковских счетов и т.д.

4. 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.

5. 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.

6. 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 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.

7. Заработок на бирже, заманивание прибыльными инвестициями – получившая широкое распространение в последнее время схема, в результате использования которой причиняется наиболее крупный ущерб. 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 прибыль. Однако их дальнейший вывод невозможен.

8. 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.

9. 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).

10. Поступила заявка о смене абонентского номера, привязанного к банковскому счету, для отмены заявки сообщите код подтверждения, поступивший в смс-сообщении.

11. Произошла попытка взлома личного кабинета, установите программу (в таких случаях устанавливается программа удаленного доступа и происходит списание денежных средств).

12. Положена выплата (компенсация), сообщите код, поступивший в смс для подтверждения операции, или перечислите деньги за бумаги, доставку, страховку и т.д., заполните «бланк» (при заполнении «бланка» вводятся данные банковской карты и происходит списание денежных средств). Или - вам положены акции, заплатите налог, чтобы их получить.

13. Просят внести предоплату или оформить доставку при покупке (продаже) товара, после чего скидывается ссылка, в которой заполняются данные

банковской карты и происходит списание всех денежных средств либо посылка не доставляется или поступивший товар не соответствует заказу.

14. Произошла вирусная атака, сообщите данные банковской карты и коды, поступающие в смс-сообщениях.

Здесь представлены далеко не все используемые мошенниками схемы, их приемы постоянно меняются и становятся все более изощренными. Длительность общения с жертвой до совершения преступления может достигать нескольких месяцев.

Зачастую после произошедшего люди говорят, что в момент совершения преступления находились в прострации, в результате оказанного психологического и морального давления. От них требуют незамедлительно принять решение и не дают времени на раздумья или возможности связаться с родственниками, друзьями. Преступники действуют настойчиво, в ходе разговора очень грамотно поставлена речь, как правило звонят посредством приложения Ватсп, Вайбер, Телеграм.

Изначально в ходе разговора сложно определить мошенника, пока не начнут просить сообщить пароли и номера карт. Будьте бдительны, не дайте себя обмануть!

ЧТО ДЕЛАТЬ

Проверьте номер, с которого пришло сообщение, сверить его с реальным телефонным номером абонента. Для проверки подлинности адресата необходимо позвонить ему с использованием других средств связи и уточнить отправлял ли он данное сообщение.

Представители правоохранительных органов, а также представители банков никогда не будут звонить по Ватсап, Телеграм, Вайбере. Иные учреждения и коммерческие организации также не звонят с использованием мессенджеров.

Следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка России, не осуществляют работу с физическими лицами.

Если нет сомнений, что это злоумышленник, то необходимо заблокировать этого абонента и удалить сообщение. Ни в коем случае не вступайте в переписку и не переходите по ссылкам, содержащимся в сообщении!

В случае, если вы прошли по ссылке, незамедлительно измените пароль своего аккаунта в Телеграм, проверьте устройства, подключенные к вашему аккаунту. Удалите любые незнакомые устройства. Обратитесь в службу поддержки Телеграм и сообщите о произошедшем. Убедитесь, что включена двухфакторная аутентификация для дополнительной защиты вашего аккаунта. Будьте осторожны с любыми другими подозрительными ссылками и сообщениями.

Никогда не сообщайте по телефону код из СМС, а также свои персональные данные (паспорта, ИНН, СНИЛС, номера банковских карт, и т.п.).

Если вы сообщили код из СМС для подтверждения транзакции (банковского перевода) необходимо незамедлительно обратиться на горячую линию банка и сообщить о данном факте. Также обратиться к сотовому оператору с просьбой заблокировать номер телефона.

В случае взлома учетной записи Госуслуг необходимо заблокировать учетную запись. Сделать это можно либо через мобильное приложение Госуслуги, либо через техподдержку МФЦ, либо лично обратиться в МФЦ.

Не сохраняйте для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

Проверяйте из других источников предоставленную вам информацию. Будьте бдительными и не поддавайтесь на манипуляции мошенников!

ИСТОРИИ ИЗ ЖИЗНИ

***

Пенсионерке пообещали 3 000 рублей за то, что она переболела ковидом, но в итоге обманули более чем на 300 000 рублей.

Потерпевшей позвонила женщина с доброжелательным голосом, которая знала все ее данные, ФИО, место жительства, предыдущие ее места работы. Она представилась сотрудником пенсионного фонда и сообщила радостную новость, что ей якобы положены выплаты: 19 тысяч рублей за выслугу лет в советское время и еще тысячи рублей в качестве меры поддержки переболевшим ковидом.

Пенсионерка обрадовалась и принялась со спокойной душой диктовать собеседнице все цифры и пароли, которые ей тут же начали приходить на сотовый телефон. Спустя 15 минут у женщины пропали с карты деньги в размере 340 тысяч рублей, а доброжелательная сотрудница отключилась и пропала.

***

Недавно очередной жертвой мошенников стал 37-летний житель нашего края, которому мошенники предоставили фото, видео и документы, подтверждающие хищение его денежных средств.

В один из дней молодому человеку поступил звонок от сотрудника полиции г. Москвы с таким сообщением – Ваш личный счет взломан! Необходимо все деньги перевести на безопасные счета. Далее последовали звонки от службы безопасности банка, руководителя департамента по борьбе с мошенничеством, сотрудников полиции.

Далее скинули фото о возбуждении уголовного дела в отношении взломщика счета, даже позвонили по видеозвонку от лица руководства органов полиции и убедили установить себе на телефон приложение RuDesktop (удаленный доступ к системе из любой точки мира).

Разрешив доступ к своему телефону, мужчине оставалось лишь наблюдать как робот-помощник оформляет на его имя заявки на кредиты в различных банках.

Далее, получая одобрение в разных банках, они объяснили потерпевшему о необходимости снятия всех кредитных денег в банке и их последующем зачислении на безопасные счета.

Исчерпав кредитный потенциал и начиная получать отказы в банках, преступники оставили жертву в покое. А молодой человек, поняв, что это все обман, обратился в полицию. Помимо заявления, он принес 6 кредитных договоров на сумму более 6 миллионов рублей.