Отделение МВД России «Камбарское» информирует:

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости и чувства в своих корыстных интересах.

Основные известные схемы дистанционных хищений:

1. Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками правоохранительных органов за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанёс тяжкие телесные повреждения). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас деньги необходимо привезти в определенное место, передать какому-либо человеку, либо перевести на счет (абонентский номер телефона).

Так в дежурную часть отделения МВД России «Камбарское» с сообщением о хищении денежных средств обратилась 76-летняя местная жительница.

Сотрудниками полиции установлено, что в дневное время на её стационарный телефон позвонила молодая девушка, голос которой показался потерпевшей похожим на голос её внучки. «Внучка» сообщил, что стала виновницей ДТП, в результате которого пострадал другой участник дорожного движения. После этого женщине перезвонил мужчина, представившийся сотрудником полиции, и подтвердил сказанное девушкой ранее, пояснил, что для освобождения её от уголовной ответственности необходимо срочно передать денежные средства потерпевшей стороне для компенсации. Введенная в заблуждение пенсионерка передала 125 000 рублей подъехавшему к её дому курьеру, а спустя некоторое время выяснила, что её внучка не совершал ДТП.

В ходе оперативно-розыскных мероприятий сотрудниками уголовного розыска установлена личность «курьера». Им оказался 23-летний неработающий ранее судимый житель г. Сарапула. Как пояснил подозреваемый, в конце июля посредством одного из мессенджеров с ним связался неизвестный с предложением заработка в курьерской службе на территории Удмуртской Республики. Похищенные у потерпевших денежные средства он перечислял неустановленным лицам, часть денег оставлял себе.

В настоящее время оперативниками проводятся мероприятия, направленные на установление лиц, причастных к совершению преступлений.

2. «На вас пытаются взять кредит»

Наконец, еще один популярный метод — звонок из «Центробанка»/службы безопасности госуслуг/правоохранительных органов. Чаще звонить пытаются через мессенджеры, чтобы вместо номера определялся аккаунт, на аватаре которого — российский герб и название организации (хотя с физическими лицами Центральный банк не работает вообще. Впрочем, иногда мошенники звонят с аккаунта, подписанного «МВД России»). По телефону говорят, что кто-то пытается получить на вас кредит, и, чтобы не платить по чужим долгам, эти кредитные деньги нужно срочно забрать в отделении банка или перевести на «безопасный счет».

Почти 700 тысяч рублей похищено у жителя Удмуртии под предлогом защиты от незаконной транзакции

Установлено, что в дневное время потерпевшему позвонил неизвестный мужчина, представился сотрудником банка и сообщил о том, что неизвестные пытаются оформить кредит на его имя. Для предотвращения незаконной транзакции звонивший убедил ижевчанина перевести имеющиеся на банковской карте денежные средства на безопасный счет.

3. Программы удаленного доступа

Злоумышленники звонят клиентам, представляются «специалистами технической поддержки» и предлагают установить на смартфон «официальное» приложение банка для проверки устройства и поиска уязвимостей.

Отличие от других схем состоит в том, что злоумышленники начали самостоятельно разрабатывать подобные программы. После установки такого приложения они получают удаленный доступ к смартфону и пытаются вывести деньги из онлайн-банка.

На первом этапе мошенники под видом специалистов из технической поддержки банка связываются с клиентом. Звонки совершаются по любому каналу связи, но преимущественно — в мессенджерах. Для убедительности используется логотип банка или подпись «Тех. поддержка». Клиенту сообщают, что в личном кабинете его банковского приложения заметили новые подключенные устройства или мошеннические операции. Далее ему предлагают скачать якобы «сертифицированное приложение» банка для проверки телефона на уязвимости, присылают ссылку на фишинговый сайт с подробной инструкцией, которая объясняет, как установить приложение.

После установки пользователю предлагают запустить новую программу, сообщить «оператору» идентификационный номер (который является кодом доступа) и открыть свой мобильный банк. Таким образом, мошенники получают удаленный доступ к устройству, обладают полной конфиденциальной информацией и данными онлайн-банка, после чего начинают попытки похищения средств. Приложение, которое просят установить мошенники, является программой удаленного управления для телефонов на Android.

Мошенники используют звонки через мессенджеры, поскольку они бесплатны, их можно автоматизировать для массированных атак, а также

есть возможность скрыть номер телефона и показывать название организации или логотип.

Более 450.000 рублей похищено у жительницы Ижевска с помощью программы удаленного доступа

Потерпевшей позвонил неизвестный, представился сотрудником безопасности банка, в ходе разговора убедил, что в кредитной организации зафиксированы попытки хищения сбережений женщины.

Поверив звонившему, потерпевшая с целью сохранения своих денежных средств стала действовать по его указаниям. Она установил программу удаленного доступа, с помощью которой злоумышленник получил доступ к мобильному приложению банка, оформил кредит на сумму более 450.000 рублей, после чего похитил денежные средства. Потерпевшая обратилась в полицию.

4. Продажа имущества на интернет-сайтах.

При звонке на телефон, размещенный на Интернет-сайтах объявлений (Авито, ФарПост, Дром и др.) правонарушитель просит пополнить счет его телефона, либо сообщить данные и номер карты потерпевшего для перевода денежных средств в качестве задатка за товар. После сообщения данных карты происходит списание денежных средств.

В Удмуртии сотрудниками полиции задержан подозреваемый в 50 фактах мошенничества с использованием сайта бесплатных объявлений

Сотрудниками Межрайонного отдела №5 Управления уголовного розыска МВД по Удмуртской Республике в результате оперативно-розыскных мероприятий задержан 24-летний безработный житель Ижевска, подозреваемый в мошенничестве.

Сотрудниками полиции установлено, что задержанный на одном из сайтов бесплатных объявлений размещал сообщения о продаже обуви по заниженным ценам. Гражданам, желавшим приобрести данный товар, молодой человек сообщал о возможной доставке курьерской службой, но предупреждал, что стоимость с данной услугой будет выше. После чего предлагал оплатить напрямую на указанные им банковские карты с существенной разницей в цене. Потерпевшие соглашались на оплату переводом. После получения денег, подозреваемый товар не высылал и некоторое время убеждал потерпевших о проблемах с загрузкой на складе, после чего и вовсе переставал выходить на связь.

В настоящее время установлено 50 фактов противоправной деятельности задержанного, общий ущерб составил более 300.000 рублей.

5. Фишинговая ссылка – гиперссылка, которая маскирует адрес вредоносного ресурса. После нажатия на нее пользователь переходит на мошеннический сайт. Если вовремя не остановить процесс и успеть ввести в предложенную форму логин и пароль, номер карты, пин-код, серию и номер паспорта или конфиденциальные служебные данные, их используют в преступных целях. (напр. МВидео).

Запланировав свой отпуск, ижевчанка решила самостоятельно выбрать и забронировать номер в одном из санаториев на территории Крыма.

Набрав в одной из поисковых систем в сети Интернет понравившийся санаторий, она перешла по одной из предложенных ссылок. На главной странице этого сайта было указано, что это официальный сайт санатория.

Она выбрала нужное время, оформила заказ и произвела оплату в размере более 63 000 рублей.

Затем ижевчанка решила позвонить по указанному на сайте номеру, чтобы подтвердить оплату. Но на звонок автоинформатор сообщил, что «сейчас этот номер свободен, подключить этот номер вы можете в течение одного дня…». После этого она решила проверить информацию о выбранном ей санатории и обнаружила в сети Интернет сведения о том, что в настоящее время этот санаторий не функционирует, а сайт является мошенническим.

6. Взлом аккаунта друга.

Люди могут даже не подозревать, что им пишет посторонний человек под видом родственника, друга, с просьбой перевода денег в связи с произошедшим горем. Таким образом, войдя в доверие, мошенники пытаются украсть ваши деньги.

Денежные средства похищены со счета жителя Воткинска после переписки его дочери с подругой в социальной сети

В межмуниципальный отдел МВД России «Воткинский» с заявлением о хищении денежных средств обратился рабочий одного из предприятий города. Он пояснил, что в вечернее время его несовершеннолетняя дочь в социальной сети получила сообщение со страницы подруги о том, что ее телефон сломался, а ей должна прийти важная информация. По просьбе «подруги» дочь заявителя написала номер своего телефона, а также два пришедших в смс пароля.

После этого школьница получила сообщение, что ее номер привязан к номеру ее отца, и если его не отвязать, то со счета будут списываться деньги. В последующем девушка, следуя получаемым указаниям, дождалась, когда уснул отец, взяла его телефон и совершила ряд операций в мобильном приложении.

Утром заявитель обнаружил, что с его банковского счета списано 18 000 рублей и оформлен запрос на кредит на сумму 93 000 рублей. Также выяснилось, что аккаунт подруги его дочери взломан.

7. Игра на бирже

Мошенники в красках рассказывают своим жертвам, что уже завтра они смогут преувеличить свой доход в два раза, а через неделю – в десять. Устоять перед таким соблазном сложно.

Как это работает? Мошенническая схема проста. В поисках быстрого и легкого заработка человек попадает на сайт-двойник известных инвестиционных компаний, созданный аферистами. Мошенники предлагают ему услуги лжефинансового аналитика. Ничего не смысля в бирже,

гражданин соглашается. После этого ему даже переводят часть средств, чтобы убедить, что игра на бирже – то просто и прибыльно. Аферисты могут предоставить даже фиктивные графики роста дохода гражданина. Поверив в себя, человек решает сыграть по-крупному, берет кредит или занимает деньги у друзей. Как правило, длится это несколько месяцев. А когда потерпевший просит вывести свои деньги, связь с мошенниками обрывается.

Около 1,5 миллиона рублей похищено мошенниками у пенсионерки из Сарапула

Сотрудниками полиции установлено, что потерпевшая в начале июня в сети Интернет нашла информацию о возможности получения дополнительного заработка путем совершения различных финансовых сделок (покупка, продажа, различных акций, инвестиции). Она позвонила по указанному в рекламе номеру телефона для уточнения подробностей. В последующем потерпевшая общалась с неизвестными, представлявшимися сотрудниками брокерской компании, по указанию которых она переводила денежные средства для «пополнения депозита её инвесторского счета».

Кроме того, женщине неоднократно звонили лица, представлявшиеся сотрудниками правоохранительных органов и банков. И также требовали перевести сбережения на продиктованные счета под предлогом «разморозки банковского счета», «защиты от незаконной транзакции», «оказания услуг нотариуса для возврата денежных средств».

В результате за полтора месяца женщина перевела на указанные ей счета почти 1 500 000 рублей. При этом она оформила несколько кредитов в разных банках и брала в долг у знакомых.

В ходе дальнейшего общения «правоохранители» сообщили потерпевшей, что в г. Москва на её имя пытались оформить кредит, но «злоумышленника» задержали. Далее ей стали угрожать, что вышлют за ней группу задержания. После чего пенсионерка поняла, что общается с мошенниками и обратилась в полицию.

8. Интим-услуги

Мошенники создают специализированные сайты и агрегаторы эскорт-услуг. Они загружают фотографии девушек из Интернета, берут предоплату и исчезают.

Или же на звонок клиента отвечает диспетчер, пообещав, что девушка отправится на указанный клиентом адрес сразу перечисления денежных средств. Однако после перевода денег перезванивают и просят перевести сумму еще раз, так как возникли некие «технические неполадки на сайте». Переведя необходимую сумму клиент снова звонит по указанному на сайте телефону, где нарывается уже на откровенное вымогательство вкупе с угрозами и шантажом.

После посещения сайта интимных услуг у ижевчанина похищены денежные средства

26-летний заявитель пояснил, что решил воспользоваться сайтом по предоставлению интимных услуг и позвонил на указанный на нем номер телефона. Неизвестный, представившийся менеджером, сообщил, что необходимо оплатить услугу. Мужчина выполнил эти требования и перевел на указанный счет 7 700 рублей,

после чего «менеджер» перезвонил потерпевшему и потребовал дополнительную плату, на что получил отказ. В последующем мужчине стали звонить неизвестные, требовать деньги и высказывать угрозы.

Ижевчанин понял, что общается с мошенниками, и обратился в полицию.

9. Розыгрыш призов (это могут быть телефон, ноутбук, автомобиль, онлайн-курсы и др.).

На телефон абонента сотовой связи приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл автомобиль. Для уточнения всех деталей потенциальной жертве предлагается посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из указанных телефонных номеров. Во время разговора по телефону мошенники сообщают о том, что для выполнения необходимых формальностей (уплаты госпошлины, оформления необходимых документов, оплаты за комиссию перевода) счастливому обладателю новенького автомобиля необходимо перечислить на счет указанную ими сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки поступления денег на счет и получения «кода регистрации». Как только жертва завершает указанные манипуляции, счет обнуляется, а мошенники исчезают в неизвестном направлении.

48-летняя жительница Воткинска в сети интернет получила сообщение от неизвестного пользователя с предложением принять участие в розыгрыше денежного приза: в указанной строке ввела данные своей банковской карты, после чего с ее счета было списано 8000 рублей.

Приведенный перечень мошеннических схем не ограничивается данными примерами. Преступники находят все новые и новые схемы и способы для достижения своих преступных замыслов.

Всегда убеждайтесь в достоверности информации, полученной в ходе телефонного разговора и интернет переписки с неизвестными. Мошенники могут представляться сотрудниками правоохранительных органов, представителями операторов сотовой связи и банковских учреждений, знакомыми и даже Вашими родственниками. Обязательно свяжитесь с теми, от чьего имени действуют незнакомцы, и убедитесь в правдивости информации.

Ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и карт, тем более пароли от них.

По возможности проверяйте информацию, получаемую в интернете, особенно если вас просят произвести какие-либо действия, связанные с передачей денежных средств.

Ни при каких обстоятельствах не разглашайте персональные данные о себе и об имеющихся в наличии банковских картах. Тем более, если не уверены, что общаетесь с представителем банка. Если же получили СМС-сообщение о возникших проблемах с картой, ни в коем случае не перезванивайте на предлагаемые номера. Обращайтесь по официальным номерам банков, если у вас возникли вопросы. Или непосредственно в отделения банков.

Будьте внимательны! В случаях продажи/покупки товаров через торговые площадки никому, ни при каких обстоятельствах, не сообщайте сведения об имеющихся банковских картах, номерах счетов. Если возникла необходимость в получении предоплаты, лучше договориться о личной встрече. Также необходимо обратить внимание, если продавец не желает встречаться лично, придумывая различные отговорки.

Наверняка он нечист на руку и задумал лишить вас денег.

10. Взлом сервиса Госуслуги.

Портал предоставляет множество государственных услуг. С его помощью можно записаться к врачу, зарегистрировать автомобиль, получить различные выписки. Зайдя в личный кабинет портала можно узнать номера телефонов, адреса проживания, ИНН, СНИЛС, ОМС, сведения об имуществе.

При взломе портала Госуслуги главная добыча мошенников – это большой объем ваших данных.

Схема мошенников заключается в том, что на мобильный телефон гражданину звонит якобы представитель сотового оператора, у которого обслуживается номер телефона. Мошенники говорят, что номер телефона старый, либо обслуживается более 10 лет в следствии чего его необходимо «пролонгировать», либо переоформить договор, иначе абонентский номер телефона будет передан другому абоненту. «Пролонгировать» абонентский номер, или перезаключить договор мошенники предлагают через портал «Гос услуги». Для этого на абонентский номер телефона приходит СМС с кодом, который мошенники просят продиктовать. Если гражданин выполняет все указания звоняего, то у мошенников сразу появляется доступ к личному кабинету «Госуслуг». Отсюда сразу различные негативные последствия, самые нежелательные из которых – микрозаймы и кредиты на имя граждан.

В таких случаях необходимо незамедлительно связаться с техподдержкой «Госуслуг», а так же банками, чтобы заблокировать свои счета и вернуть украденный аккаунт сервиса «Госуслуги», после чего обратится в правоохранительные органы.

Отделение МВД России «Камбарское»