ОБОБЩЕННАЯ ИНФОРМАЦИЯ
о способах совершения различных видов хищений, совершенных дистанционным способом на территории Сахалинской области за январь 2023 года

О схемах мошенников много пишется в СМИ. На телеканале «Солнце-ТВ» в эфире ежедневной новостной программы «ЧП 65» выходят информационные сюжеты об актуальных схемах мошенничества, которые были применены в отношении сахалинцев, а также социальные ролики обозначенной тематики. Сотрудники полиции раздают гражданам памятки о способах совершения преступлений, но население Сахалинской области, несмотря на проводимую работу, попадает под влияние аферистов, на их уловки.

Так, за январь 2023 года в УМВД России по Сахалинской области зарегистрировано 48 преступлений, по факту совершения хищений денежных средств, совершенных дистанционным способом, что свидетельствует о недостаточной просвещенности населения о способах совершения преступлений и чрезмерной доверчивости граждан.

Из 48 зарегистрированных преступлений - 12 совершены посредством сети «Интернет». На различных сайтах: «Sakh.com», «Юла», «Авито» и др. мошенники размещают объявления о продаже имущества (автомобилей, снегоходов, запасных частей), дешевых авиабилетов, об аренде жилья, оказании услуг, в приложениях для знакомств размещают ложные анкеты и далее обманным путем разными способами похищают денежные средства. Таким образом, у граждан было похищено 2 589 448 рублей.

Например, гражданин А. в сети интернет в приложении «Тиндер», познакомился с девушкой. В дальнейшем по инициативе девушки продолжили общение посредством приложения «Телеграмм». В ходе переписки неизвестная предложила встретиться, чтобы пообщаться лично, обозначив при этом, что хочет сходить на концерт «Stand up» комика Руслана Белого. После чего отправила ссылку на интернет сайт для покупки билетов на концерт. Гражданин А. перешел по ссылке, где ввел номер карты, срок действия и трехзначный код с оборотной стороны, а также имя и фамилию. После того, как были списаны денежные средства за покупку билетов, стали приходить уведомления о том, что с накопительного счета гражданина А. происходит списание денежных средств. Общий ущерб составил более 1 млн. рублей.

4 преступления совершены посредством аккаунтов, на которые поступили сообщения различного характера, с просьбой от знакомых одолжить денежные средства либо с предложением заработать. Граждане обманным путем перевели мошенникам денежные средства в размере 51 350 рублей.

Так, на профиль заявителя «Вконтакте» пришло сообщение от её знакомой: «Привет Ирина, хочешь получить 3500 рублей на карту в

честь дня рождения Сбербанка, у меня знакомая в Сбербанке, мне пришло, только надо сейчас. Вышли номер карты без первых двух цифр и код, который придет по СМС». Заявитель сообщила номер карты и код, после чего с карты потерпевшей произошло списание денежных средств.

Чтобы не стать жертвой мошенника и не попасть на вышеперечисленные уловки, необходимо:

-критически оценивать любую информацию, сообщения, объявления, размещенные в интернете.

-не заказывать имущество через непроверенные сайты, денежный расчет за продаваемую вещь производить непосредственно при ее передаче от продавца покупателю.

- не верить на слово внезапным обращениям от знакомых, друзей, родственников, так как неожиданная просьба о деньгах может поступить от мошенника, который взломал аккаунт.

- не открывать неизвестные ссылки, которые приходят по электронной почте, в мессенджерах, социальных сетях, особенно если предлагают что-то бесплатное или на весьма выгодных условиях.

Очень распространенный способ хищений, на который попадает большинство населения Сахалинской области, это поступающие на телефоны граждан звонки от мошенников, которые представляются сотрудниками различных кредитных организаций (банков), Пенсионного Фонда, сотрудниками правоохранительных органов, судебных приставов, родными людьми (дочь, сын и др.) Эти мошенники преследуют единственную цель - обманным путем получить как можно больше денежных средств. Они обладают психологическими навыками, умеют расположить к себе, играть на эмоциях, чувствах, запугивать. В ходе разговора с ними граждане сообщают данные своей карты и СМС-код, который приходит на номер телефона либо самостоятельно переводят свои денежные средства на номера карт, указанные мошенниками.

Таким способом совершено 19 преступлений, из них в 11 случаях мошенники представлялись сотрудниками той или иной кредитной организации (банка), в том числе службы безопасности, в 3 случаях - сотрудниками Пенсионного Фонда, в 3 случаях - следователями Следственного комитета, в 1 случае мошенница представилась дочерью, в другом - сотрудником судебных приставов. Граждане обманным путем перевели мошенникам денежные средства в размере 9 612 974 рубля.

Так, гражданке М. позвонил неизвестный, представился сотрудником следственного комитета г. Москва и сообщил, что произошла утечка персональных данных, и на имя заявительницы открыты заявки на кредиты в общей сумме 3 150 000 рублей. Для безопасного выведения денежных средств из заявок на кредиты, которые были оформлены на неё, необходимо зайти в «Сбербанк онлайн», до конца оформить кредитные заявки и перевести денежные средства на безопасный счет. Неизвестный продиктовал заявительнице пошаговую инструкцию оформления кредитов. Получив через банкомат наличные, заявительница перевела денежные средств на продиктованные неизвестным счета.

В другом случае, на телефон гражданина М. поступил звонок через мессенджер WhatsApp от неизвестной женщины, которая представилась сотрудником ВТБ банка и сообщила данные заявителя и что в его личном

кабинете проводятся мошеннические действия через другой телефон. Звонившая девушка сказала, что необходимо скачать программу поддержки ВТБ «AveSun», через Play Market. Скачав приложение и зайдя в данную программу, гражданин М. ввел данные, которые продиктовала девушка. После высветилось «AveSun» дублирование экрана, так же был виден код доступа, который постоянно менялся. Далее гражданину М. стали приходить смс-сообщения о списании денежных средств, также пришло сообщение о том, что поступила заявка на кредит, которая была оформлена на сумму 998 767 рублей. Всего с его счета было похищено более 2 млн. рублей, с учетом взятого кредита.

На телефон гражданки С. поступил звонок. Звонившая представилась сотрудником «Пенсионного фонда РФ» и сообщила, что гражданке С. положена выплата за выслугу лет в размере 39 000 рублей. В ходе телефонного разговора гражданка С. сообщила мошеннице номер карты и код, поступивший в смс, после чего с банковского счета гражданки С. произошло списание денежных средств в размере 40 000 рублей.

На домашний телефон гражданки А. поступил звонок от неизвестного лица, которое сообщило, что ее дочь попала в ДТП и требовало 1 000 000 рублей, для того что бы сделать операцию. Гражданка А. продиктовала номер своего сотового телефона, после чего ей на сотовый телефон поступил звонок и в трубку женский голос говорил «Мама, мама, помоги я попала в ДТП и у меня сломано два ребра». Когда заявительница собирала деньги, пришла ее дочь и сообщила, что в ДТП не попадала, это звонят мошенники.

Другой пример, матери гражданки А. позвонил неизвестный, представился судебным приставом, который сказал, что у ее дочери имеется задолженность. После чего мать сообщила об этом дочери, которая перезвонила на номер телефона, поступивший на телефон ее матери. Гражданке А. ответил мужчина и представился судебным приставом, который сообщил, что примерно два года назад она брала микро займ в размере 5000 рублей, а все что свыше, - это набежавшие проценты которые необходимо погасить, иначе к ней домой приедут пристава и будут изымать ее имущество в счет погашения задолженности. После чего, судебный пристав дал ей номер юридического отдела банка «Русский Стандарт», для решения вопроса об уплате долга. Гражданка А. позвонила на номер юридического отдела банка и в ходе телефонного диалога, женщина пояснила, что действительно у нее имеется долг на сумму 14500 рублей, а их банк непосредственно связан с микро кредитной организацией и они осуществляют ее финансирование. Далее посредством мессенджера «Whats App» с юридического отдела банка «Русский Стандарт» ей были отправлены реквизиты для оплаты долга в сумме 14500 рублей, а также инструкция для оплаты. После чего гражданка А. осуществила перевод денежных средств в сумме 14500 рублей. Однако документы о погашении микро займа она не получила и денежные средства ей не вернули.

Также от действий мошенников пострадало четыре водителя такси, из них трое, в ходе телефонного разговора, самостоятельно продиктовали номера банковских карт и смс-код, который поступил им на телефон. В одном случае мошенник попросил водителя пополнить баланс нескольких абонентов, заверив, что переведет ему обратно 39 000 рублей. Поверив мошеннику,

водитель посредством банкомата перевел денежные средства на баланс продиктованных злоумышленником абонентских номеров. В результате преступных действий мошенников у таксистов похищены денежные средства на общую суму более 170 тыс. рублей.

Чтобы не стать жертвой мошенника и не попасть на вышеизложенные уловки, необходимо:

- не поддаваться эмоциям и как можно быстрее прекратить общение, ведь сотрудник кредитной организации никогда заочно не попросит дооформить кредит и перевести Ваши денежные средства на безопасный счет. Также не будет просить перейти по отправленным Вам ссылкам.
- ни в коем случае не сообщать личные данные карты и не вводить их на незнакомых сайтах, не указывать коды безопасности из смс- сообщений.
- быть бдительным, не верить на слово, проверять любую информацию, поступившую от лиц, представляющихся сотрудниками различных организаций, государственных учреждений (Пенсионного фонда, судебных приставов и др.) путем самостоятельного обращения к официальным источникам органов государственной власти, организаций и учреждений.

Не нужно бояться прерывать общение с данными лицами. Они будут убеждать Вас в обратном. Например: «если вы выключите телефон, то произойдет снятие денежных средств».

Запомните! Если Вы не сообщали данные карты или смс-код, который поступил Вам на телефон, не переходили по подозрительной ссылке, которая пришла на Ваш номер телефона, Ваши денежные средства останутся в сохранности.

Ещё одним весьма распространённым способом хищения денежных средств в крупных размерах является обман граждан о возможности заработать денежные средства от вложений в инвестиции, покупки акций, торговли на бирже (газом, валютой, криптовалютой). Таким способом совершено 9 преступлений. Граждане обманным путем перевели мошенникам денежные средства в размере более 7 млн. рублей.

Так, гражданину М. поступил звонок от неустановленного лица с предложением дополнительного заработка в виде торговли на бирже, на что заявитель ответил согласием. Затем ему сказали установить два приложения «Бинанс» и «БТЦ Кэш», по которым в последующем он производил сделки по покупке и продаже криптовалюты. Гражданин М. приобретал криптовалюту и переводил деньги на банковские карты по номерам телефонов, которые ему указывал неизвестный, представившийся независимым трейдером «Газпром инвестиции», связь с которым заявитель поддерживал через «Скайп». За две недели потерпевший перевел денежные средства на указанные ему номера в общей сумме более 1 млн. рублей.

В другом случае, гражданин С. в сети «Интернет» увидел диалоговое окно, в котором имелась информация об инвестициях и ввел свои установочные данные. 07.12.2022 гражданину С. в мессенджере Телеграмм пришло сообщение якобы от старшего финансового эксперта компании «Интерактив Софтвэр». В ходе дальнейшего диалога гражданин С. перевел денежные средства для инвестиции в ценные бумаги в особо крупном размере.

Другой пример, гражданка Е. в сети интернет в приложении «Вотсап» в группе увидела объявление о заработке по распространению продукции компании «ОпПате» Гражданка Е. вошла в приложение, после чего с ней

связался неизвестный, предложил заработать денежные средства путем покупки акции с целью их дальнейшей продажи по более выгодной цене. Таким образом, гражданка Е. осуществила перевод денежных средств неизвестным лицам на общую сумму более 3 млн. рублей.

Чтобы обезопасить себя и не стать жертвой мошенников нужно всегда проявлять бдительность при совершении денежных операций с помощью банковских карт. Не поддаваться желанию легко заработать большие деньги либо получить выгодные проценты, проверять информацию о брокерах и трейдерах из официальных источников.

Имеются случаи и осторожного поведения граждан, которые не поддались на ухищрения мошенников.

Так, в вечернее время, на телефон гражданки Л. позвонил неизвестный, который представился сотрудником службы безопасности Сбербанка России и спросил: «Не теряла ли она свою банковскую карту, так как зафиксирована несанкционированная операция по счету». Гражданка Л. проверила сумку и сказала, что карта на месте. Далее звонивший назвал данные гражданина, который якобы пытался снять денежные средства со счета гражданки Л. и в целях пресечения попытки снятия денежных средств он переведет ее на сотрудника банка, который скажет, что ей делать дальше. На что гражданка Л. сказала, что ей необходимо проверить данную информацию и перезвонить в Сбербанк. Мошенник очень настойчиво и убедительно говорил, что в случае прерывания с ним разговора произойдет списание денежных средств. Гражданка Л., несмотря на свои переживания и опасения, прервала с ним разговор. Зашла в приложение «Сбербанк онлайн» и убедилась, что все денежные средства были на месте. Преступная схема мошенника не реализовалась.