

Информация
об основных схемах преступлений с использованием информационно-
телекоммуникационных технологий, совершённых на территории
Магаданской области в феврале – апреле 2024 года

Несмотря на принимаемые меры по предупреждению преступлений, совершенных с использованием информационно-телекоммуникационных технологий, противоправные деяния данной категории регистрируются органами внутренних дел Магаданской области ежедневно.

Нередко жертвами преступных действий злоумышленников становятся работники государственных учреждений, государственные гражданские служащие и работники исполнительных органов Магаданской области, работники органов местного самоуправления муниципальных образований Магаданской области и подведомственных им муниципальных учреждений. Как показывает практика, чаще других среди потерпевших фигурируют работники сферы здравоохранения.

Анализ текущей оперативной обстановки в Магаданской области позволяет определить наиболее распространенные схемы совершения кибермошенничеств, применяемых к жителям региона:

1. По-прежнему самым распространенным способом хищения денежных средств в настоящее время является преступная схема, когда гражданам поступают **звонки от злоумышленников, которые обманным путём вводят в заблуждение потерпевших, представляясь сотрудниками банков и правоохранительных органов** (чаще всего сотрудниками ФСБ России), в результате чего получают доступ к их счетам и списанию денежных средств.

Справочно:

1) В дежурную часть ОМВД России по г. Магадану поступило заявление от работника одного из горнодобывающих предприятий Магаданской области, что неустановленное лицо 27 марта 2024 года

совершило звонок в мессенджере «WhatsApp» с абонентского номера мобильного оператора ПАО «Мегафон», представившись сотрудником безопасности Сбербанка, под предлогом пресечения мошеннических действий убедило потерпевшего при помощи «Сбербанк-онлайн» перевести на указанный ему банковский счёт денежные средства в сумме 148 000 руб. (личные накопления), чем причинило ему значительный материальный ущерб.

2) В дежурную часть ОМВД России по г. Магадану 23 февраля 2024 года поступило заявление от работницы одного из магазинов областного центра о том, что неустановленное лицо путём обмана, используя подменный номер, представившись сотрудником ФСБ России, под предлогом того, что неизвестные лица, пытаются оформить кредит на её имя, убедило последнюю взять кредит в банке «Газпромбанк» (Акционерное общество) на сумму 600 000 руб. и перевести данные денежные средства на банковский счёт, причинив своими действиями материальный ущерб в крупном размере.

3) В дежурную часть ОМВД России по г. Магадану 29 февраля 2024 года поступило заявление от работницы одного из горнодобывающих предприятий региона о том, что неустановленное лицо, представившись сотрудником ФСБ России, под предлогом предотвращения мошеннических действий похитило денежные средства в размере 995 000 руб. (оформлен в кредит в ПАО «ВТБ»). Потерпевшая совершила 2 операции зачисления денежных средств на банковский счёт через банкомат ПАО «ВТБ», расположенный по адресу: г. Магадан, 2-й км основной трассы, ТЦ «Моремолл».

4) В дежурную часть ОМВД России по г. Магадану 3 апреля 2024 года поступило заявление от работницы одного из медицинских учреждений, расположенных в областном центре, о том, что потерпевшей от неустановленного лица поступил телефонный звонок по мессенджеру «Whatsapp» якобы от сотрудника ФСБ России, который под предлогом предотвращения мошеннических действий, совершаемых с её счётом в

банке, убедил перевести денежные средства на «безопасный» счёт. Заявительница по указанию злоумышленников установила на свой мобильный телефон приложение Mir PAY, с помощью которого совершила 2 операции зачисления денежных средств на указанные преступником банковские счета в размере 298 000 руб. (личные накопления) через банкомат ПАО «Сбербанк», расположенный по адресу: г. Магадан, ул. Комсомольская площадь д.4 и в магазине «Спутник».

5) В дежурную часть ОМВД России по г. Магадану 14 марта 2024 года поступило заявление от жительницы областного центра, работающей в одном из финансовых учреждений региона, о том, что неустановленное лицо в период с 12 по 13 марта т.г. осуществило телефонный звонок с мессенджера «Whatsapp» (Тинькофф Мобайл, Омская область), представилось сотрудником ФСБ России. Далее по указанию «сотрудника» заявитель оформила кредит в ПАО «Сбербанк» в сумме 450 000 руб. и указанные денежные средства перевела на неустановленный счёт, якобы для того, чтобы погасить кредит, который на неё взяли мошенники.

2. Ещё одним распространённым способом мошенничества является преступная схема, когда взламывается **учётная запись в мессенджерах и контактам потерпевшего якобы от его имени направляются различные сообщения с конечной просьбой занять в долг денежные средства.**

Справочно:

1) В дежурную часть ОМВД России по г. Магадану 15 марта 2024 года поступило заявление от жителя областного центра том, что неустановленное лицо, используя в мессенджере «WhatsApp» учётную запись потерпевшего от его имени под предлогом займа денежных средств попросило знакомого, работающего в финансовом учреждении в областном центре, осуществить перевод денежных средств в сумме 7 000 руб. на счёт банковской карты АО «Тинькофф Банк».

Знакомый потерпевшего, догадавшись об обмане, с предложением о переводе денежных средств на указанную выше банковскую карту не согласился и деньги не перевёл.

Необходимо отметить, что последнее время вышеуказанная преступная схема усложнилась, она сочетается с первым вышеуказанным способом: как правило, сначала через мессенджер «Телеграм» поступает сообщение от «руководителя», который предупреждает о предстоящем звонке сотрудников ФСБ России или Центробанка РФ и о том, что необходимо следовать их инструкциям. Далее поступает звонок от мошенников – «сотрудников безопасности».

Справочно:

2) В марте текущего года сотрудниками безопасности регионального филиала банка ВТБ (ПАО) пресечены множественные попытки выдачи потерпевшим кредитов для последующего перевода их злоумышленникам по стандартной схеме: через взломанный аккаунт руководителей организаций (среди потенциальных жертв фигурировали в том числе работники системы здравоохранения) в мессенджере «Телеграм» от якобы их имени подчинённым сотрудникам приходило сообщение с просьбой занять денежные средства, для чего предлагалось взять автокредит в ВТБ-банке. Введённые в заблуждение граждане, не проверив необходимость заёма денег в ходе телефонного звонка либо личной встречи с руководителем, подавали заявку на оформление кредита в указанном финансово-кредитном учреждении и были готовы перевести денежные средства преступникам. Только благодаря бдительности сотрудников банка удалось предотвратить хищения денежных средств и убедить граждан о том, что они имеют дело с фейковыми аккаунтами.

3) В дежурную часть Отд МВД России по Ольскому району поступило заявление от жительницы пос. Ола, работающей в одном из медицинских учреждений, о том, что неустановленное лицо 14 марта 2024 года, используя мессенджер «Телеграм», с фейкового аккаунта руководителя того

же медучреждения направило сообщение потерпевшей о том, что через некоторое время к ней обратятся сотрудники ФСБ России и Центрального банка РФ и ей необходимо следовать их инструкциям. В дальнейшем после поступившего телефонного звонка, путём обмана, под предлогом предотвращения мошеннических действий по расчётному счёту заявителя, неустановленное лицо похитило денежные средства в сумме 104 000 руб. (личные накопления), причинив своими действиями значительный материальный ущерб. Для связи злоумышленник использовал абонентские номера ООО «МегаФон» и мессенджер «WhatsApp» (при этом телефонный номер, с которого совершался звонок, отображался в виде имени пользователя аккаунта и **являлся официальным номером ФСБ РФ**).

4) В дежурную часть ОМВД России по г. Магадану 11 марта 2024 года поступило заявление от работника одного из муниципальных учреждений в пос. Сокол о том, что, злоумышленник в мессенджере «Телеграм», используя поддельный аккаунт руководителя данного учреждения, от его имени сообщило, что с заявителем будут общаться сотрудники Центрального банка РФ и ФСБ. В ходе поступивших в дальнейшем телефонных звонков от якобы сотрудников органов безопасности, заявителю было сообщено об угрозе безопасности его банковских счетов. Злоумышленники убедили потерпевшего перевести денежные средства в размере 4 000 000 руб. (личные накопления), а также 2 900 000 руб. (кредитные средства) на «безопасные» счета.

5) В дежурную часть Отд МВД России по Сусуманскому району 2 марта 2024 года поступило заявление от работника одной из частных предприятий по продаже техники в регионе о том, что неустановленное лицо, используя аккаунт директора данной организации в мессенджере «Телеграм», заверило заявителя, что последнему поступит телефонный звонок от сотрудника органов безопасности. После чего неустановленное лицо, представившись сотрудником ФСБ России, под предлогом предотвращения мошеннических действий, похитило денежные средства

потерпевшего в сумме 286 000 руб. (личные накопления), а также совершило покушение на хищение денежных средств в сумме 2 000 000 руб., пыталось оформить кредит в ПАО «АТБ». Заявитель совершил 2 операции зачисления денежных средств на банковский счёт, открытый в АО «РосБанк» через банкомат ПАО «Сбербанк» в г. Сусумане. Злоумышленник использовал абонентский номер ООО «Мобильные коммуникационные системы» (ЛНР) и Yota (Республика Башкортостан).

3. Актуальным остаётся мошеннический способ «покупка-продажа» имущества (предоставление услуг) через сайты объявлений.

Преступник, выступая в роли продавца, размещает на таких сайтах информацию о продаже какого-либо товара, сдаче в аренду недвижимости или же оказании тех или иных услуг, за которые в последующем получает предоплату, сам же товар (услуга) не предоставляется, тем самым похищаются денежные средства.

Справочно:

1) В дежурную часть Отд МВД России по Тенькинскому району 1 апреля 2024 года поступило заявление от жителя пос. Усть-Омчуг, работающего в одной из частных организаций, что неустановленное лицо на сайте «gc-sale.ru» разместило объявление о продаже каминной вытяжки. После перевода денежных средств на банковский счёт АО «Альфа-банк» товар покупателю не поступил. Ущерб составил 14 600 руб. Злоумышленник использовал абонентские номера: Ростелеком (г. Москва) и Мегафон (Кировская область).

2) В дежурную часть Отд МВД России по Тенькинскому району 2 марта 2024 года от работника одной из частных транспортных компаний региона поступило заявление о том, что неустановленное лицо путём обмана, под предлогом продажи автомобильных покрышек, объявление о продаже которых было размещено на торговой интернет-площадке «Яндекс-маркет», похитило денежные средства в сумме 47 560 руб.,

которые были переведены через систему быстрых платежей в АО «Альфа-банк». Неустановленное лицо использовало абонентские номера ПАО «МТС» (г. Санкт-Петербург и Ленинградская область).

3) В дежурную часть ОМВД России по г. Магадану 1 марта 2024 года поступило заявление от жителя областного центра о том, что неустановленное лицо на сайте «Форпост» разместило объявление о продаже автомобильного турбокомпрессора «Hitachi». Заявителем денежные средства в сумме 15 300 руб. были переведены на банковский счёт АО «Тинькофф Банк», однако товар покупателю не поступил.

4. Другой распространённой преступной схемой является ситуация, когда граждане хотят получить пассивный доход и в этих целях соглашаются на предложения мошенников поучаствовать **в заработках на фейковых биржах, якобы осуществляющих брокерскую и инвестиционную деятельность.**

Жертвами преступников чаще всего становятся люди, далекие от биржевой торговли, преимущественно жители административных центров отдалённых регионов России и относительно небольших населённых пунктов.

Справочно:

1) В дежурную часть Отд МВД России по Сусуманскому району 15 марта 2024 года с заявлением обратился работник одной из энергетических компаний о том, что неустановленное лицо, путём обмана посредством мессенджера «Skype» под предлогом получения пассивного дохода от инвестиций в ПАО «Газпром» завладело денежными средствами его банковского счёта, оформленного в ПАО «Сбербанк», в общей сумме 420 000 руб. (личные накопления). Денежные средства автоматически списывались с банковского счёта, после того как потерпевший сообщал злоумышленнику коды из поступающих СМС-сообщений.

2) В дежурную часть ОМВД России по г. Магадану 18 марта 2024 года поступило заявление от работницы частного предприятия в областном центре о том, что неустановленное лицо путём обмана при помощи интернет-сайта «Blaq TUX» и мессенджера «Skype» под предлогом получения пассивного дохода под большие проценты от инвестиций в ценные бумаги, перевела 954 061 руб. (личные накопления) несколькими переводами онлайн с со счёта ПАО Сбербанк на указанные преступником различные счета.

3) В дежурную часть Отд МВД России по Ягоднинскому району 27 февраля 2024 года поступило заявление от неработающей жительницы пос. Ягодное о том, что неустановленное лицо, используя группу «Лена Биток» в мессенджере «Телеграм», под видом оказания услуг биржевого брокера, заключило с заявителем договор доверительного управления денежными средствами в сумме 79 479 руб., которые в последующем похитило. Потерпевшая денежные средства перевела четырьмя операциями на различные счета ПАО «Сбербанк».

И это далеко не полный перечень способов совершения преступных деяний с использованием ИТТ, зарегистрированных в Магаданской области.

Обращает на себя внимание тот факт, что во всех перечисленных случаях мошенничеств потерпевшие знали о подобных преступлениях из средств массовой информации, квитанций ЖКХ, профилактических бесед сотрудников полиции либо руководителей организаций, однако пренебрегли элементарными правилами безопасности и пошли на поводу у мошенников.

Поэтому, чтобы не стать жертвой злоумышленников, необходимо соблюдать следующие правила безопасного поведения:

1. Не следует отвечать на звонки или СМС-сообщения с неизвестных номеров с просьбой положить на счёт деньги.

2. Ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и карт, пароли от них и тем более не перечисляйте принадлежащие вам денежные средства по указанию лиц, представляющихся

сотрудниками банков (службы безопасности банков) и правоохранительных органов (полиция, ФСБ, Росфинмониторинг и т.д.), на безопасные счета! **Понятия «БЕЗОПАСНЫЙ СЧЁТ» НЕ СУЩЕСТВУЕТ!** Немедленно прервите разговор.

3. Не берите кредиты якобы для того, чтобы опередить злоумышленников. Такого способа защиты ваших средств не существует.

4. В случае поступления сообщения от руководителя (или знакомого) с просьбой занять денег или с информацией о том, что вам скоро позвонят из органов безопасности или Центробанка РФ и следует действовать по их инструкции, **перезвоните своему руководителю (знакомому) и уточните ситуацию.**

5. Не устанавливайте на свой смартфон никаких программ по указанию неизвестных. В то же время в качестве помощи в борьбе с мошенниками целесообразно установить на личные мобильные устройства бесплатные услуги сотовых операторов по блокировке спам-звонков и идентификации звонящих (МегаФон – «Помощник Ева», МТС – «Защитник», Билайн – «Виртуальный помощник», Теле2 – «Антиспам для звонков» и другие).

6. Не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом.

В случае возникновения указанных ситуаций обратитесь в ближайшее отделение вашего банка по известному вам телефону или уточните в очном формате все возникающие вопросы у оператора либо представителя службы безопасности банка.

При совершении в отношении вас противоправных действий незамедлительно обращайтесь в ближайшее подразделение органов внутренних дел. Также о фактах краж и мошенничеств можно сообщить

в дежурную часть органа внутренних дел или по номеру 102, а также по телефону доверия УМВД России по Магаданской области 69-66-55.
