Информация

об основных схемах преступлений с использованием информационно-телекоммуникационных технологий, совершённых на территории Магаданской области за 9 месяцев 2024 года

По итогам 9 месяцев 2024 года на территории Магаданской области отмечено некоторое снижение (-5,0%) числа **преступлений, совершенных с использованием информационно-телекоммуникационных технологий** (633; 9 месяцев 2023 г. – 666).

Из указанного массива противоправных деяний 60% составляют **мошенничества** (-23,2%; 271; 9 месяцев 2023 г. – 353) и **кражи** (-15,7%; 107; 9 месяцев 2023 г. – 127).

Тем не менее, несмотря некоторое снижение массива вышеуказанных преступлений, **причинённый ущерб** от них вырос, составив **159 млн 259 тыс.** рублей (9 месяцев 2023 г. – 152 млн 396 тыс. рублей).

Противоправные деяния данной категории регистрируются ежедневно. При этом отмечается, что 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. Согласно информации УМВД России по Магаданской области, чаще других среди потерпевших фигурируют работники сферы здравоохранения и образования.

Кроме того, несмотря на значительный объём проведённой адресной работы по правовому просвещению и информированию, часто преступления совершаются в отношении студентов и учащихся образовательных учреждений, а также пенсионеров.

Среди потерпевших нередко бывают работники энергетических, горнодобывающих и транспортных компаний региона.

Анализ текущей оперативной обстановки в Магаданской области свидетельствует, что наиболее распространенные схемы совершения кибермошенничеств, применяемых к жителям Магаданской области, за последнее время существенно не изменились:

1. По-прежнему самым распространенным способом хищения денежных средств является преступная схема, когда гражданам поступают **звонки от злоумышленников, которые обманным путём вводят в заблуждение потерпевших, представляясь сотрудниками банков, правоохранительных органов**, **операторов сотовой связи** и т.д., в результате чего получают доступ к их счетам и списанию денежных средств.

Справочно:

1) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года от пенсионерки поступило заявление о том, что неустановленное лицо, представившись сотрудником АО «Энергосбыт», под предлогом дистанционной записи в очередь на замену счетчика электроэнергии и настройки личного кабинета на сайте компании «Энергосбыт», уговорили заявительницу активировать функцию демонстрации экрана на мобильном телефоне и зайти в приложение «ВТБ-Банк». В результате чего с банковского счета заявителя были похищены денежные средства в сумме 990 000 рублей.

2) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление от работника одного из медицинских учреждений областного центра о том, что неустановленное лицо, представившись сотрудником Росфинмониторинга, под предлогом пресечения действий мошенников, получило доступ похитило к банковскому счёту потерпевшей и завладело денежными средствами заявительницы в сумме 1 600 000 рублей.

3) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление пенсионерки о том, что неустановленное лицо, представившись сотрудником Центрального банка России, а также сотрудником правоохранительных органов, под предлогом пресечения

действий мошенников похитило денежные средства заявителя в сумме 3 631 600 рублей.

Рассматривая вышеуказанный способ мошенничества, необходимо обратить внимание на тот факт, что злоумышленники не только похищают денежные средства граждан, но во многих случаях **получают доступ к личному кабинету жертв в Федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)»** (далее – «Госуслуги»).

В дальнейшем завладение персональными данными с портала «Госуслуги» позволяет преступникам, используя краденный профиль:

- оформлять на чужое имя кредиты и микрозаймы;

- получить чужой налоговый вычет;

- оформлять на другого человека сим-карты сотовых операторов.

Кроме того, персональные данные (паспортные данные, сведения о собственности, кредитная история и прочая информация) могут быть проданы в так называемом даркнете и в дальнейшем использоваться в различных преступных схемах.

Ниже приведены лишь несколько типичных примеров уловок, которые используют преступники для неправомерного доступа к персональным данным:

*1) В дежурную часть Отд МВД России по Омсукчанскому району поступило заявление от работника одной частной организации, проживающей в пос. Усть-Омчуг, о том, что неустановленное лицо путём обмана **под предлогом продления услуг мобильной связи, представившись сотрудником ПАО «МТС»**, убедило заявителя продиктовать код из СМС - сообщения, в результате чего получило доступ к персональным данным на портале «Госуслуги». В ходе проверки установлено, что неправомерный доступ к личному кабинету на портале «Госуслуги» осуществлялся с помощью IP-адреса, входящего в диапазон адресов государств Эстония и США.*

2) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года от пенсионерки поступило заявление о том, что неустановленное лицо, ***представившись сотрудником АО «Энергосбыт», под предлогом дистанционной записи в очередь на замену счётчика электроэнергии****, убедило назвать пришедший СМС-код, после чего осуществило неправомерный доступ к компьютерной информации, а именно завладело аккаунтом на портале «Госуслуги», принадлежащим заявителю.*

3) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года от работника одного из учреждений социального обслуживания поступило заявление о том, что неустановленное лицо, ***представившись сотрудником поликлиники, под предлогом дистанционной записи в очередь на замену полиса обязательного медицинского страхования*** *с бумажного на пластиковый убедило заявителя назвать код из СМС-сообщения, после чего осуществило неправомерный доступ к компьютерной информации, а именно завладело аккаунтом на портале «Госуслуги» и заблокировало к нему доступ последней;*

4) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года от жительницы областного центра поступило заявление о том, что неустановленное лицо, ***представившись сотрудником Пенсионного фонда РФ, под предлогом записи на приём с целью уточнения трудового стажа****, убедило назвать пришедший СМС-код, после чего осуществило неправомерный доступ к компьютерной информации, а именно завладело аккаунтом на портале «Госуслуги», принадлежащим заявителю.*

2. Другим 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 Отд МВД России по Тенькинскому району в августе т.г. поступило заявление от работника одного из горнодобывающих

предприятий региона о том, что ему по мессенджеру «Ватсап» поступило сообщение от знакомого коллеги по работе с просьбой занять денежные средства в размере 45 000 рублей. Заявитель перевел денежные средства в размере 20 000 рублей на указанный в сообщении расчётный счёт «Озон Банка» и только позднее получил сообщение от знакомого, что его телефон взломан и сообщение с просьбой заёма денежных средств последний не отправлял.

2) В дежурную часть ОМВД России по г. Магадану в августе 2024 года от работника одного из предприятий в сфере торговли поступило заявление о том, что по мессенджеру «Телеграмм» от якобы брата заявителя поступила просьба занять денежные средства в сумме 50 000 рублей. Потерпевший перевел 5 000 рублей через мобильное приложение «Т-Банк» на банковскую карту Яндекс-Банка. В дальнейшем установлено, что злоумышленник получил неправомерный доступ к телефону родственника.

3. Мошеннический способ **«покупка-продажа» имущества (предоставление услуг) через сайты объявлений также один из самых распространённых**.

Несмотря на меры безопасности для клиентов, внедряемые на интернет-сервисах с объявлениями («Авито», «Юла» и другие), мошенники по-прежнему находят способы их обойти. Как правило, это происходит по вине самих потерпевших, которые поддаются порыву срочно купить товар с большой скидкой, пренебрегая элементарными правилами безопасности.

Здесь, как правило, применяются ***три рабочих схемы мошенничества***:

- при оплате товара (услуги) или оформлении заказа используется фишинговая ссылка на сайт, схожий по названию с известными торговыми и почтовыми сервисами («Авито», CDEK и т.д.), где размещается форма оформления заказа, где продавцу якобы нужно ввести данные своей карты для совершения оплаты. Получив нужную информацию, мошенники списывают деньги со счёта продавца;

- происходит простое выманивание платёжных данных: при продаже или покупке онлайн с вами на связь выходит другой пользователь и якобы для совершения сделки просит продиктовать ему CVV/CVC-код банковской карты или код из СМС-сообщения от банка. Если мошенникам удастся получить подобную информацию, они без труда заходят в личный кабинет банка потерпевшего, чтобы вывести деньги с карты либо получают возможность совершить покупки в Интернете за ваш счёт;

- самая распространённая схема – мошенники выставляют на продажу востребованный товар, как правило, с низким ценником (чаще всего, продажа смартфонов, автомобилей, запчастей к автомобилям, одежда и т.д.). Покупателя торопят и уговаривают перевести предоплату, полную или чаще – частичную, на свой счёт в интернет-банке или по поддельной ссылке на оплату. Получив деньги, «продавец» пропадает из поля зрения, а покупателя добавляет в чёрный список.

Справочно:

1) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление от неработающего жителя г. Магадана о том, что неустановленное лицо под предлогом продажи автомобиля через сервис объявлений «Юла», введя заявителя в заблуждение последнего, убедило перечислить денежные средства в размере 200 000 рублей. Получив предоплату, мошенник на связь больше не выходил, его контактный номер заблокирован.

2) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление от неработающего жителя областного центра о том, что неустановленное лицо посредством размещения объявления в социальной сети «ВКонтакте» под предлогом продажи запчасти для автомобиля «Хонда-Прелюд» путём обмана завладело денежными средствами потерпевшего в размере 6 500 рублей. После получение денежных средств, переведённых через онлайн-приложение МТС-банка, «продавец» на связь выходить перестал, товар заявителю не поступил.

3) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление от работника одного из учреждений в сфере культуры областного центра о том, что неустановленное лицо, используя мессенджер «Телеграмм» через ссылку на фейковый аккаунт магазина под предлогом продажи заявителю 3 часов и 5 БПЛА, совершило хищение денежных средств «Д» в сумме 380 448 руб. При этом указанная сумма переводилась на протяжении месяца неоднократно частями на различные номера сотовых операторов и счета банков.

4. Часто жертвами мошенников становятся граждане, пытающиеся **заработать на фейковых биржах, якобы осуществляющих брокерскую и инвестиционную деятельность.**

Справочно:

1) В дежурную часть ОМВД России по г. Магадану в октябре 2024 года поступило заявление от работника одного из горнодобывающих предприятий региона о том, что заявитель на протяжении нескольких дней переводил неустановленным лицам под предлогом заработка на бирже «Газинвест» денежные средства в сумме 257 300 рублей. Для связи злоумышленники использовали абонентские номера сотовой компании ПАО «Мегафон» и мессенджер Whatsapp.

2) В дежурную часть ОМВД России по г. Магадану в октябре 2024 года поступило заявление от работника одного из учреждений социального обслуживания о том, что злоумышленники, контактируя с ней через мессенджер «WhatsApp» и мобильное приложение «Skype», под предлогом оказания помощи инвестирования через онлайн-биржу в течение месяца похитили денежные средства заявительницы в сумме 4 325 500 рублей, взятые ею в кредит в ПАО «Сбербанк», а также с кредитной карты «Тинькофф-Банка».

3) В дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление пенсионерки о том, что неустановленное лицо под предлогом получения пассивного заработка на инвестициях похитило её

денежные средства в сумме 905 000 рублей (кредит, взятый в ПАО «Промсвязьбанк»).

5. <u>Преступная схема, предусматривающая фейковые розыгрыши призов</u>.

В настоящее время Интернет заполонили порталы с фейковыми розыгрышами призов. Схема мошенничества проста: пользователям предлагают поучаствовать в лотерее, по результатам участия в которой можно получить приз. В других случаях доверчивым гражданам сразу сообщают, что они уже выиграли приз. После чего «победитель» должен дать согласие на получение подарка и ввести реквизиты банковской карты, на которую будет переведена сумма, эквивалентная стоимости подарка. После ввода данных пользователя просят оплатить некую комиссию, связанную с конвертацией выигрыша в рубли. В итоге деньги и платежная информация уходят к мошенникам, а никакого приза жертва не получает. В худшем случае злоумышленники получают несанкционированный доступ к персональным данным жертв, которые используются в преступных схемах.

Наиболее показательным является следующий пример.

*Так, в дежурную часть ОМВД России по г. Магадану в сентябре 2024 года поступило заявление от пенсионера о том, что неустановленное лицо, воспользовавшись его персональными данными, оформило на его имя потребительский кредит в сумме 350 000 рублей в **<u>АО «Почта Банк»</u>**, после чего похитило указанную сумму денежных средств с банковского счета АО «Почта Банк» путём осуществления 9 переводов через систему быстрых платежей на банковские счета ПАО «Сбербанк».*

В дальнейшем установлено, что перед оформлением на имя потерпевшего кредита, он в мобильном приложении «Почта-Банк» во вкладке «сообщения», увидел входящее сообщение с текстом: «Начался розыгрыш денежных призов. Подписывайтесь на нашу группу в Одноклассниках pochtabank.ru/ok/gift». Затем перешел по данной ссылке и зарегистрировался. При регистрации в приложении «Одноклассники» ввёл

последние 4 цифры со своей банковской карты АО «Почта Банк», после чего его сотовый телефон стали приходить смс-уведомления об одобрении кредита в АО «Почта Банк».

6. Преступная схема «родственник в беде».

Сегодня данная схема не так распространена, как ещё несколько лет назад, но всё же в редких случаях доверчивые граждане, как правило, пожилые люди, попадаются на уловки мошенников.

Например, в дежурную часть Отд МВД России по Хасынско району в октябре т.г. поступило заявление от пенсионерки, проживающей в пос. Палатка, о мошеннических действиях в отношении неё. Органами внутренних дел установлено, что злоумышленник, представившись сотрудником полиции, сообщило по сотовому телефону заявителю о том, что её дочь попала в аварию, сбив на автомобиле человека, и для решения вопроса о невозбуждении уголовного дела необходимо перевести на указанный мошенником банковский счёт денежные средства в размере 200 000 рублей. После этого потерпевшая попыталась перевести 20 000 рублей (все имеющиеся у неё на тот момент деньги), однако банк неоднократно блокировал онлайн-операции, указав, что банковская карта, на которую осуществляется перевод средств, заблокирована и числится в базе «Мошенники». Будучи в состоянии стресса, несмотря на предупреждения банка, потерпевшая уточнила у злоумышленника новые банковские реквизиты и перевела на другой расчётный счёт 20 000 рублей.

Учитывая вышеизложенное, 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 родственника, знакомого, руководителя (коллег по работе) 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, **САМОСТОЯТЕЛЬНО СВЯЖИТЕСЬ С ТЕМ, КТО ПРОСИТ ОКАЗАТЬ ПОМОЩЬ, И УТОЧНИТЕ СИТУАЦИЮ**.

5. ОБРАТИТЕ ВНИМАНИЕ! НЕ СОЗВАНИВАЮТСЯ С КЛИЕНТАМИ:

- сотовые компании – с целью ***продления услуг мобильной связи*** (работа ведётся исключительно через официальное мобильное приложение операторов связи);

- Отделение Фонда пенсионного и социального страхования Российской Федерации по Магаданской области (его филиалы) – с предложением ***услуг по перерасчёту размера пенсии и трудового стажа***;

- АО «Магаданэнергосбыт» – для оказания содействия ***по замене счётчика электроэнергии либо настройки личного кабинета*** на сайте компании;

- медицинские организации – об оказании услуги по дистанционной записи в очередь ***на замену полиса обязательного медицинского страхования***.

6. ПРИ СОВЕРШЕНИИ ОНЛАЙН-ПОКУПОК ИЛИ ПРОДАЖ НА ИНТЕРНЕТ-ПЛОЩАДКАХ ОБЪЯВЛЕНИЙ следуйте следующим рекомендациям:

- изучите карточку продавца, его рейтинг и отзывы. Насторожитесь, если продавец имеет слишком низкий рейтинг и большое количество отрицательных отзывов;

- мошенники часто используют фишинговые сайты, замаскированные под реально существующие онлайн-ресурсы торговых площадок (доменное имя при этом может отличаться всего лишь одним символом). Ссылки на фишинговые сайты, как правило, оставляют в мессенджерах, поэтому общайтесь с пользователями только через чат интернет-площадки размещения объявлений. В большинстве случаев в таких чатах блокируется рассылка ссылок. Если ресурс не блокирует ссылки, отправляемые пользователям, просто не переходите по ним;

- мошенники часто пытаются увести вас с интернет-ресурса. Следует настороженно отнестись к просьбам продолжить общение в WhatsApp, Viber, Telegram. Вас могут убеждать в том, что функционал сайта работает некорректно, и сделку лучше совершить в обход ресурса. Никогда не поддавайтесь на подобные уговоры. Оплату проводите только через платёжные сервисы, которые предлагает выбранная вами интернет-площадка. В таком случае вы можете быть уверены в безопасности оплаты и в сохранности денежных средств на вашей карте. Поскольку сервисы безопасной оплаты предполагают блокирование денег на виртуальном счету торговой площадки, в случае неполучения товара или получения товара ненадлежащего качества денежные средства вернутся на ваш счёт. Только при подтверждении получения нужного вам заказа и отсутствии претензий к его качеству торговая площадка направляет денежные средства продавцу.

- не отправляйте предоплату за товар или услугу;

- при общении в чате мошенники под самыми разными предлогами могут попытаться получить информацию, позволяющую совершать

несанкционированные операции с вашей банковской картой. Поэтому ни при каких обстоятельствах не сообщайте пользователям код на оборотной стороне карты (CVV/CVC-код), а также коды из СМС-сообщений для совершения оплаты, приходящих на номер вашего сотового телефона.

- если вы всё же успели ввести номер своей карты на поддельном сайте или передать свои платежные данные мошенникам и только потом поняли – что-то не так, нужно немедленно позвонить в банк, заблокировать карту и подать заявление на её перевыпуск. Если успеете сделать это до того, как мошенники воспользуются вашими данными, потери денег удастся избежать.

7. ЗАЩИТИТЕ СВОЙ СМАРТФОН!

- не устанавливайте на свой смартфон никаких программ по указанию неизвестных;

- 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», Т2 – «Антиспам для звонков» и другие).

8. Не следует доверять звонкам и сообщениям, о том, что **РОДСТВЕННИК ИЛИ ЗНАКОМЫЙ ПОПАЛ В АВАРИЮ**, **ЗАДЕРЖАН 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.

7. Чтобы **НЕ ДОПУСТИТЬ НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП В ВАШ ЛИЧНЫЙ КАБИНЕТ НА САЙТЕ «ГОСУСЛУГИ»,** необходимо соблюдать ряд простых правил кибербезопасности, которые изложены на официальном этого сайта (ссылка: https://www.gosuslugi.ru/help/faq/personal_data/100465). Особое внимание

специалисты по кибербезопасности обращают внимание на создание уникального пароля для входа в личный кабинет из 12 символов (ссылка: https://www.gosuslugi.ru/life/details/how_to_create_strong_passwords).

Ещё несколько общих советов. **В СЛУЧАЕ ВОЗНИКНОВЕНИЯ В ОТНОШЕНИИ ВАС МОШЕННИЧЕСКИХ ДЕЙСТВИЙ НЕЗАМЕДЛИТЕЛЬНО 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;

- 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.

Также напоминаем, что о действующей в регионе **горячей линии по профилактике совершений мошеннических действий с использованием информационно-телекоммуникационных технологий**. **Кол-центр** действует на основе **единого бесплатного регионального номера 122.**

Специалисты кол-центра с целью предотвращения правонарушений в их отношении окажут вам консультации, а также помогут оперативно предоставить информацию о необходимых действиях в случаях обращений к вам мошенников, в том числе если:

- с вашей банковской карты списали деньги;

- если вы получили тревожное смс-сообщение или звонок с незнакомого номера от «родственников», сомнительное сообщение из «банков» или государственных учреждений о блокировке банковской карты или поступлении денежных средств по ошибке, а также уведомление о назначении компенсации или выигрыша и так далее

Также по горячей линии можно проконсультироваться по вопросу безопасности персональных данных.

Узнать о работе кол-центра можно на сайте Правительства Магаданской области и в социальных сетях по ссылкам:

- https://www.49gov.ru/press/press_releases/index.php?id_4=92297,
- https://t.me/gov49/9911;
- https://t.me/gov49/9433.

_____