Наиболее распространенные виды мошенничеств и меры противодействия им

1. Звонок от службы безопасности банка, силовых структур, портала «Госуслуги»: «Неизвестные пытаются оформить на ваше имя кредит», а также другие мошенничества с банковскими картами.

В дежурную часть УМВД России по г. Йошкар-Оле с заявлением обратился 46-летний житель Медведевского района с заявлением о мошенничестве. Ему поступали звонки, якобы от сотрудника правоохранительных органов и банка. Звонившие убедили, что на его имя третьи лица пытаются оформить кредит. Для предотвращения операции неизвестные рекомендовали исчерпать кредитный лимит, оформив займ в банке, а полученные денежные средства перевести на «безопасные счета». Мужчина, потерявший бдительность, оформил кредит в банке, а также часть личных сбережений перевел посредством банкомата на продиктованные мошенниками реквизиты. Только спустя время он понял, что стал жертвой обмана. Сумма ущерба составила 2.3 млн. руб.

Меры противодействия: При поступлении звонка якобы из банка под предлогом предотвращения несанкционированного списания денежных средств или нелегального оформления кредита необходимо сразу же прекратить диалог и набрать номер телефона, который размещен на банковской карте. Ни в коем случае не передавайте содержание поступющих SMS-уведомлениях, не переходите по присылаемым ссылкам в мессенджерах, не устанавливайте по совету собеседников на компьютеры и смартфоны программы, не выполняйте никаких манипуляций со своими счетами под диктовку неизвестных, кем бы они ни представлялись. Все это может привести к хищению денежных средств с ваших счетов.

2. Инвестиционное мошенничество.

В полицию с заявлением обратился 41-летний местный житель. Он рассказал, что с января по февраль этого года пытался заработать денежные средства с помощью инвестирования. С ним связался неизвестный и предложил заработать в сети Интернет. Суть работы заключалась в том, чтобы открыть счет, вкладывать денежные средства и следить за растущим балансом. Мужчина оформлял кредиты на сумму более 8 миллионов рублей и отправлял на различные банковские счета, указанные в ходе общения.. Когда потерпевший захотел вывести свои денежные средства, у него это не удалось. Тогда он понял, что стал жертвой аферистов.

Меры противодействия: Чтобы обезопасить свои деньги, важно критически относиться к любой поступающей информации и проверять ее. Инвестировать денежные средства можно, только на заслуживающей доверия платформе и обладая хотя бы минимальными знаниями по этой теме. Брокеры, для того, чтобы осуществлять свою деятельность на территории Российской Федерации, должны иметь лицензию на осуществление брокерской деятельности, которую выдает ЦБ РФ. Поэтому первое, что вы должны сделать при выборе брокера, - проверить наличие у него лицензии. Сделать это можно на сайте Банка России. Если у компании, которая обещает вам огромную прибыль, нет лицензии Банка России – осторожно, это мошенники.

На что еще следует обратить внимание:

1. Навязчивые звонки в любое время суток. Помните: профессиональный и честный брокер никогда не станет навязывать свои услуги по телефону. Хорошего специалиста клиенты ищут сами.

2. Обещание брокером баснословной прибыли от вложенных денежных средств. Важно помнить, что ни один брокер не может гарантировать 100-процентное получение прибыли.

3. Отказ назвать адрес сайта брокерской компании, отсутствие информации о ней в Интернете или на сайте компании нет сведений о собственнике компании, юридического адреса и контактных данных.

4. Брокер предлагает быстро открыть счет без проверки ваших документов и заверяет, что достаточно оформить личный кабинет на сайте.

3. Смена тарифного плана сотового оператора, интернет заявка на смену газового или электросчетчика, согласие на получение или отправку почтового отправления, электронная запись к врачу, замена страхового полиса, доставка товаров или иные предлоги получения SMS-сообщения.

В дежурную часть УМВД России по г. Йошкар-Оле с заявлением обратилась 52-летняя местная жительница. Она рассказала, что ей позвонил незнакомец, который представился сотрудником сотовой компании. Звонивший, под предлогом дистанционной записи для продления действия договора с сотовой компанией, попросил продиктовать код из SMS который должен поступить с портала «Госуслуг». При этом звонивший убеждал, что если это не сделать то SIM-карта заблокируется и потеряется доступ ко всем приложениям. Женщина выполнила требуемое. После чего мошенники получили доступ к личному кабинету. В последующем незнакомец убедил, что третьи лица пытаются оформить займ на имя горожанки, и для предотвращения несанкционированной операции злоумышленник рекомендовал исчерпать кредитный лимит, оформив займ, и таким образом, якобы третьи лица не успеют завершить операцию до конца. Потерпевшая выполнила требуемое, оформив кредит, и перевела посредством банкоматов на продиктованные счета более 800 тыс. рублей.

Меры противодействия:

Ни когда нельзя сообщать поступающие SMS-сообщения в ходе телефонного разговора третьим лицам. Все SMS-сообщения поступающие от портала «ГосУслуги» в тексте содержат предостережение о запрете передачи кода третьим лицам.

4. На популярном интернет-сервисе поиска попутчиков водитель предлагает внести предоплату за поездку по ссылке.

Так в дежурную часть ОМВД России по Моркинскому району обратилась 28-летняя йошкаролинка, которая сообщила о том, что стала жертвой телефонных мошенников при бронировании поездки. Полицейские выяснили, что заявительница посредством мессенджера в группе нашла поездку из Моркинского района до города Йошкар-Олы и откликнулась на объявление. Псевдо-водитель попросил для обсуждения условий поездки перейти из чата в мессенджер «WhatsApp». После чего мошенник убедил перевести предоплату. Для этого он сбросил девушке ссылку. После перехода по этой ссылке девушке предложили ввести полные данные карты, включая секретные. Потерпевшая ввела данные банковской карты своей мамы. Сразу после несложных операций со счета пропало более 4 тыс. рублей. После этого лже-водитель сообщил, что на имя её мамы оформлен кредит, для того, чтобы его закрыть он рекомендовал перевести имеющиеся денежные средства на «специальный счет». Девушка знала, что у неё действительно есть кредит, поверила мошенникам и перевела заемные средства на продиктованные реквизиты. Связаться с водителем она уже не смогла, поскольку тот заблокировал ее на всех ресурсах. Причиненный ущерб составил 42 тыс. рублей.

Меры противодействия: Необходимо оплачивать товары и услуги онлайн только на ресурсах, которым вы доверяете. Если от вас хотят оплаты через конкретный сервис, не

переходите по ссылкам в сообщениях. Обращайте внимание на URL-адрес страницы: если он содержит ошибки и неуместные слова или расположен в странной доменной зоне – велика вероятность, что это мошеннический сайт.

5. Мошенничество на сайтах бесплатных объявлений.

Полиция призывает граждан к бдительности при общении через Интернет с незнакомыми людьми. Невнимательность и полное доверие к чужим людям позволяют аферистам обманывать граждан, принуждая их к передаче денежных средств либо сведений, позволяющих похитить сбережения с электронного счета.

В полицию с заявлением обратился 58-летний йошкаролинец. Он рассказал, что на сайте бесплатных объявлений нашел подходящее предложение о продаже лодочного мотора. После чего обсудил условия сделки с псевдо-продавцом и перевел предоплату в сумме 95 тыс. рублей через приложение на абонентский номер. После получения денег мошенник перестал выходить на связь, а товар горожанин так и не получил.

Меры противодействия. Признаки мошенничества со стороны продавца при покупках в Интернете:

1. Отсутствует адрес и телефон, все общение предлагается вести через электронную почту или программы обмена мгновенными сообщениями.

2. Отсутствует реальное имя продавца, человек прячется за «ником».

3. Продавец зарегистрирован на сервисе недавно, объявление о продаже - единственное его сообщение.

4. Объявление опубликовано с ошибками, составлено небрежно, с использованием транслитерации, без знаков препинания, заглавными буквами и т.д.

5. Отсутствует фото товара либо приложен снимок из Интернета (это можно определить, используя сервисы поиска дубликатов картинок).

6. Слишком низкая цена товара в сравнении с аналогами у других продавцов.

7. Продавец требует полную или частичную предоплату (например, в качестве гарантии, что вы пойдете получать товар на почте с оплатой наложенным платежом).

8. Продавец принимает оплату только на анонимные реквизиты: электронные кошельки, пополнение мобильного телефона или на имя другого человека (родственника, друга и т.д.).

Признаки мошенничества со стороны покупателя при продажах в Интернете:

1. Покупатель не особо интересуется товаром, быстро демонстрирует свое желание сделать покупку и переходит к разговору о способе оплаты.

2. Покупатель просит вас назвать полные реквизиты карты, включая фамилию-имя латиницей, срок действия и cvc-код. При помощи этих данных он сам легко сможет расплатиться вашей картой в Интернете.

3. Покупатель просит вас сообщить ему различные коды, которые придут к вам на мобильный телефон, якобы необходимые ему для совершения платежа.

Как не стать жертвой Интернет-мошенничества:

- следует внимательно изучить информацию Интернет-сайта, отзывы, сравнить цены за интересующий товар. Отсутствие информации, запутанная система получения товара зачастую является признаками мошенничества.

- получить максимум сведений о продавце или магазине, адреса, телефоны, историю в социальных сетях, наличие службы доставки и т.п. Действующие легально Интернет-магазины или розничные продавцы размещают полную информацию и работают по принципу «оплата товара после доставки»;

- пользуйтесь проверенными интернет-магазинами, заранее изучайте отзывы других покупателей. Если у вас закрались сомнения по поводу благонадежности продавца, откажитесь от покупки. Если же решили заказать товар, то требуйте от продавца, чтобы посылку оформлял с описью вложения. Если посылка имеет опись вложения, то она

вскрывается до оплаты, содержимое проверяется согласно перечню, подписывается акт, посылка оплачивается, и адресат ее забирает.

- нельзя сообщать (а уж тем более посылать по электронной почте) информацию о своих пластиковых картах. Преступники могут воспользоваться их реквизитами и произвести, например, различные покупки.

Помните, что предоплату за товар вы вносите на свой страх и риск, 100%-ой гарантии получения товара не существует. При заказе товаров внимательно проверяйте название сайта в адресной строке браузера, чтобы не попасть на сайт-двойник. Пользуйтесь услугами Интернет-магазинов, работающих длительное время и заслуживших положительную репутацию покупателей, читайте отзывы покупателей о работе данных Интернет-магазинов.

6. Мошенничества под предлогом оцифровки данных, посредством групповых чатов в мессенджерах «Telegram», «WhatsApp», «VK Мессенджер».

В дежурную часть УМВД России по г.Йошкар-Оле с заявлением обратился 60-летний местный житель. Мужчина рассказал, что был добавлен в чат мессенджера «Telegram» организации в которой он ранее осуществлял трудовую деятельность. Чат не вызывал опасений так как в качестве фото значился логотип компании, а в участников и администратора значились руководители с фотоизображением, при этом в чате имитировалась переписка с других аккаунтов и часто сообщалось о срочности действий. Бухгалтером был указан список сотрудников, которым требовалось пройти оцифровку данных, для чего необходимо было пройти по ссылке, которая перенесла беседу в отдельный чат где необходимо было прописать код из смс-сообщения. После этого поступило смс-сообщение с информацией о взломе личного кабинета портала «Госуслуги» с указанием контактных номеров (мошенников). Связавшись по одному из указанных номеров лжесотрудница «Минцифры» сообщила о неправомерном доступе к порталу «Госуслуги» и переключила на лжесотрудников «Центрального банка России», ФСБ России. Под предлогом перевода денежных средств на «безопасный счет» мужчина перевел 230 тыс. рублей через приложение на абонентский номер. В определенный момент заявитель догадался, что стал жертвой мошенников, и обратился в полицию.

Меры противодействия:

- запомните, что нет понятия «безопасный счет», безопасным является счет, на котором хранятся ваши сбережения, ответственность за сохранность которых несет банк, которому вы их доверили. Никогда не переводите деньги по указанию звонящих, даже если они представляются сотрудниками банка или правоохранительных органов. Это мошенники;

- свяжитесь по обычной сотовой связи с действующим сотрудником компании или учреждения для проверки действительности необходимых действий и предоставлении каких либо сведений;

- не проходите по сомнительным ссылкам, не зависимо от того кем именно она была направлена;

- ни под каким предлогом никому не сообщайте код из SMS-сообщения, а так же анкетные данные, данные расчетных счетов и сумме денежных средств, хранящихся на них, не пересылайте фотоизображение ваших документов.

7. Займ денежных средств в социальных сетях и мессенджерах от имени знакомых/родственников.

В дежурную часть УМВД России по г.Йошкар-Оле с заявлением обратилась 55-летняя местная жительница. Она рассказала, что в мессенджере от имени приятельницы ей пришло сообщение с просьбой одолжить денежные средства. Введенная

в заблуждение потерпевшая, будучи уверенная, что общается со своей знакомой, посредством мобильного приложения перевела почти 16 тыс. рублей. Только спустя некоторое время она узнала, что общалась с мошенниками, которые писали от имени приятельницы.

Меры противодействия: запомните главное правило – необходимо по телефону связаться с родственниками, знакомыми, от чьего имени у Вас просят денежные средства, и убедиться в том, что они, действительно, нуждаются в помощи!

8. Отдельно стоит обратить внимание на острую проблему использование молодых людей в качестве «Дропов»

Для совершения мошеннических действий преступникам необходимо содействие так называемых «Дропов». Это лица осуществляющие первичный прием денежных средств на подготовленные ранее банковские реквизиты (карты, счета) с целью дальнейшего перевода или обналичивания денежных средств. Как правило указанные лица являются граждане молодого возраста, и в том числе граждане не достигшие возраста 18 лет (несовершеннолетние) которых привлекает быстрый заработок, как от продажи или передачи банковской карты или доступа к электронным средствам платежа (Он-лайн банкингу) своей карты.

С 5 июля 2025 года начали действовать изменения, внесенные в статью 187 Уголовного кодекса Российской Федерации «Неправомерный оборот средств платежей», так называемое Дроперство, соучастие в схемах мошенников, которое выражается в содействии при переводе и обналичивании похищенных денежных средств.

- В частности, вводиться ответственность для тех, кто за денежное вознаграждение передают свои банковские карты для криминальной деятельности либо сами совершают незаконные операции из корыстной заинтересованности по указанию третьих лица. Максимальное наказание за это – лишение свободы сроком на 3 года.

- За приобретение карты для передачи другому лицу, которое замыслило совершить противоправные действия, грозит наказание вплоть до лишения свободы на срок до 6 лет со штрафом от 100 до 500 тысяч рублей.

Похожее наказание – лишение свободы на срок до 6 лет со штрафом в размере от 300 тысяч до 1 млн рублей - предусматривается за осуществление неправомерных операций с использованием чужих банковских карт или электронных кошельков.

МВД настоятельно требует: Не передавайте свою банковскую карту или реквизиты доступа к ней тем людям, которым вы не доверяете. Не предоставляйте посторонним возможность использовать приложения банков на своем компьютере или смартфоне. Внимательно относитесь к переводам на ваши счета от неизвестных, особенно если они связаны с просьбами их обналичить или перенаправить. «Дроп» будет обязан вернуть все украденные деньги пострадавшим, поступившие ему на банковские карты.

МВД по Республике Марий Эл