Приложение

Основные схемы мошенничеств

1. Звонок от службы безопасности банка «По вашему счету происходит несанкционированные операции...», а также другие мошенничества с банковскими картами.

57-летняя местная йошкаролинка лишилась 3.8 миллиона рублей. Потерпевшая рассказала, что в конце августа ей позвонил неизвестный мужчина, который представился сотрудником службы безопасности банка. Звонок поступил с номера, начинающегося на «+7499….» Звонивший убедил женщину в том, что с ее банковских карт происходит попытка снятия денежных средств. Для того, чтобы обезопасить сбережения, необходимо перевести их на резервный счет. Далее собеседник переключил йошкаролинку на другую сотрудницу банка, которая попросила продиктовать номера всех банковских карт, сроки действия и три цифры, расположенные на оборотах. Как только женщина сделала это, с ее счетов произошли списания денежных средств на общую сумму 107 тысяч рублей. Но на этом мошенники не остановились. Далее злоумышленница сообщила своей жертве, будто неизвестные оформили на ее имя несколько кредитов на общую сумму 10 миллионов рублей и необходимо погасить их, взяв несколько займов в финансовых учреждениях. При этом собеседница уверила горожанку, что все деньги, которые она потратит на погашение кредитов, банк вернет. В результате в течение нескольких дней потерпевшая в трех банках оформила кредиты на общую сумму около трех миллионов, которые обналичила и перевела на указанные злоумышленницей реквизиты. Кроме того, в микрофинансовой организации женщина взяла 200 тысяч рублей под залог своего автомобиля, а также закрыла все свои вклады на общую сумму около 660 тысяч рублей. Все полученные денежные средства она также перевела на счета аферистов. Спустя некоторое время йошкаролинка поняла, что ее обманули, и обратилась в полицию. Причиненный ущерб составил более 3,8 млн. рублей.

Меры противодействия: помните главное: банки никогда не звонят своим клиентам с просьбой представиться, назвать номер карты и CUV-код. Все возникшие неисправности банк устраняет самостоятельно, не привлекая клиентов. Не вступайте в беседы с незнакомцами, которые представляются работниками службы безопасности банка, не выполняйте их поручения, полученные по телефону. В случае возникновения вопросов необходимо обратиться в ближайшее отделение банка, либо позвонить по телефону «горячей линии», который указан на оборотной стороне каждой банковской карты.

Ни в коем случае не сообщайте КОДЫ и ПАРОЛИ подтверждения операции, приходящие в смс-сообщениях

2. Мошенники звонят, используя сервис подмены номеров МВД

В дежурную часть отдела полиции №2 УМВД России по г. Йошкар-Оле обратилась 34-летняя местная жительница, которая сообщила о том, что неизвестный путем обмана похитил у нее около 200 тысяч рублей. Полицейским заявительница рассказала, что накануне на ее мобильный телефон поступил звонок. Незнакомец представился сотрудником банка и сообщил, что неизвестные лица подали заявку от ее имени на кредит на сумму 250 тысяч рублей. По словам собеседника, чтобы мошенники не смогли завершить процедуру оформления займа, ей необходимо взять еще один кредит и таким образом исчерпать весь потенциал предыдущего, то есть того, который намереваются заполучить злоумышленники. По окончании всех операций, как обещал лже-банкир, все кредиты аннулируются. Далее он сообщил женщине, что в ближайшее время с ней свяжется сотрудник полиции. Вскоре ей, действительно, с номера +78362680000 позвонил незнакомец, который представился сотрудником МВД по Республике Марий Эл. Для того, чтобы йошкаролинка перестала сомневаться, он посоветовал ей сверить номер телефона с тем, который указан на официальном сайте МВД республики. Женщина так и поступила, номер телефона совпал с указанным на странице правоохранительного ведомства. Затем «страж порядка» снова позвонил ей и после беседы с ним она начала выполнять все указания «специалиста банка». Под диктовку аферист она оформила кредит на сумму около 200 тысяч рублей, обналичила их и через банкомат перевела на 7 различных абонентских телефонных номеров.

Меры противодействия: Если вам позвонили с официальных номеров финансовых, правоохранительных, государственных структур, инициативно перезвоните по этим номерам, заново набрав их, а не перезванивая, чтобы убедиться, что они действительно имеют принадлежность к конкретной официальной организации. Пытаясь завладеть вашими денежными средствами, мошенники используют имеющиеся технические возможности, маскируя телефонные звонки под номера банков и правоохранительных структур.

3. В социальных сетях проводится акция от имени крупных финансовых учреждений

В дежурную часть отделения полиции №10 МО МВД России «Советский» обратилась 40-летняя жительница п. Новый Торъял, которая сообщила о хищении с ее банковского счета 10 тысяч рублей. Полицейские выяснили, что заявительница в популярной социальной сети увидела группу, якобы созданную одним из крупных банков России. Руководство паблика

обещало финансовую поддержку. Чтобы получить ее, достаточно выполнить бесхитростные условия: подписаться на аккаунт, поставить «лайк» на пост с розыгрышем и сделать репост записи на свою страницу. Если участник выполнит условия, то через 24 часа ему переведут 1000 рублей. После того, как женщина выполнила требуемое, она написала организатору, который для перевода денег запросил у нее номер банковской карты. Далее мошенник попросил продиктовать код из смс-сообщения от банка, якобы для регистрации в проводимой акции. Потерпевшая сообщила необходимую информацию, после чего обнаружила, что со счета банковской карты списаны 10 тысяч рублей. Денежные средства в сумме 67 тысяч рублей, хранящиеся на счетах двух других банковских карт, злоумышленник похитить не успел, так как банк заблокировал их.

Меры противодействия: Для того чтобы не стать жертвой злоумышленников, никогда не совершайте действия, на которые указывает неизвестное лицо по телефону. Ни в коем случае не сообщайте незнакомцам: срок окончания действия карты, трехзначный CVC-код на обороте карты, одноразовые смс-пароли для подтверждения интернет-операций. Не доверяйте им, даже если они обращаются к вам по фамилии, имени и отчеству.

4. Мошенничества на «Авито» и других 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.

31-летний житель г. Йошкар-Олы в сети Интернет нашел объявление о продаже сидений для автомобиля и решил купить их. Для совершения сделки мужчина перечислил незнакомцу 6 тысяч рублей и ожидал доставки товара через транспортную компанию. Однако этого не произошло, а лжепродавец удалил объявление с сайта и не выходил больше на связь.

В г.Йошкар-Оле 34-летняя потерпевшая нашла на сайте объявление о продаже автомобильных дисков и перевела продавцу 20 тысяч рублей. Однако в назначенное время свою посылку она не получила. При этом, телефон продавца перестал отвечать, а объявление было удалено.

Выставив объявление на Авито о продаже земельного участка, денежных средств лишилась 69-летняя йошкаролинка. По объявлению позвонил неизвестный и сообщил, что готов внести задаток за продаваемый объект. Для этого ему нужно было продиктовать номер банковской пластиковой карты и код, пришедший в смс-сообщении. Пенсионерка выполнила его условия. Через некоторое время злоумышленник сообщил женщине, что перевел ей на 49,5 тысяч рублей больше и попросил вернуть их. Потерпевшая зачислила их на несколько абонентских номеров. Как выяснилось, получив доступ к мобильному банку пенсионерки, он увидел, что

на ее счету в банке лежат 49,5 тысяч рублей. А йошкаролинка, будучи обманутой, сняла свои деньги и перевела их мошеннику.

37-летняя жительница г. Йошкар-Олы лишилась 30 тысяч рублей в надежде сдать квартиру в аренду. Она разместила на «Авито» объявление и ждала звонков. К ней позвонил неизвестный и выразил желание арендовать квартиру на 2,5 года. При этом, мужчина готов был внести предоплату, чтобы арендодательница сняла объявление с сайта. Женщина согласилась и продиктовала незнакомцу всю запрашиваемую им информацию: номер карты, трехзначный код с оборотной стороны, кроме того, она назвала пин-коды из смс-сообщений, которые поступили на ее телефон.Когда со счета потерпевшей стали списываться денежные средства, она поняла, что ее обманули. Ущерб от действий злоумышленника составил 30 тысяч рублей.

35-летний йошкаролинец лишился 14 тысяч рублей, продавая диван через Интернет. Лже-покупатель предложил внести предоплату на карту собственнику имущества. Мужчина согласился, и по указанию аферист прошел к банкомату, на котором под диктовку выполнил ряд некоторыхопераций. После этого со всех счетов потерпевшего были списаны сбережения.

В настоящее время мошенники широко используют сайты-двойники с помощью которых им удается похищать денежные средства. Жертва в переписке с аферистом получает ссылку, перейдя по которой попадает на сайт-двойник. Далее вводит данные карты и вместо того чтобы получить деньги переводит мошеннику деньги.

Так, в полицию с заявлением о мошенничестве обратилась 50-летняя йошкаролинка. Женщина рассказала, что хотела приобрести кофемашину на сайте бесплатных объявлений «Авито». В ходе переписки со злоумышленником она обговорила все условия сделки, после чего последний прислал ей ссылку на сайт, на странице которого она ввела реквизиты своей карты и оформила перевод. В результате женщина лишилась 4.5 тысяч рублей так и не получив желаемый товар.

28-летняя жительница лишилась 75 тысяч рублей. Полицейские выяснили, что заявительница на популярном сайте бесплатных объявлений опубликовала информацию о продаже своего макбука. Вскоре ей написал один из пользователей, который сообщил о своем намерении приобрести его. Они договорились о том, что женщина отправит компьютер через сервис доставки, который действует на интернет-сайте. И злоумышленник через мессенджер сбросил ей ссылку, перейдя по которой потерпевшая увидела уведомление о якобы покупке товара и оплате доставки покупателем. После чего она отнесла посылку на почту и отправила ее. Однако перевода денег на свою карту йошкаролинка так и не дождалась. Она обратилась в полицию. Выяснилось, что ссылка вела на сайт-двойник.

У йошкаролинца 47-летнего местного жителя неизвестный с помощью сайта-двойника похитил более 20 тысяч рублей.

Предварительно установлено, что потерпевший в одной из групп социальной сети увидел информацию о продаже лодки. Перейдя по ссылке, он попал на страницу, на которой после оформления заказа для проведения оплаты ввел реквизиты банковской карты. После чего с его счета списались более 20 тысяч рублей. Однако вскоре сайт, через который была совершена покупка, оказалась заблокированной.

По предварительным данным, мошенники создали, так называемый сайт-двойник официального сайта, в названии которого имеется незаметная разница в знаках.

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»;

- 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.

Ни в коем случае не сообщайте коды и пароли подтверждения операции приходящие в смс-сообщениях

Меры противодействия: помните, что предоплату за товар вы вносите на свой страх и риск, 100%-ой гарантии получения товара не существует. При заказе товаров внимательно проверяете 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.

5. Займ денежных средств в социальных сетях

38-летней жительнице Звениговского района в социальной сети «Одноклассники» написала подруга, которая попросила о помощи. Женщина спросила ее, что случилось,а та в ответ попросила взаймы 14 тысяч рублей.Женщина, не раздумывая, перевела деньги на счет банковской карты, который указал злоумышленник.После этого подруга вновь попросила деньги, однако у потерпевшей не оказалось запрашиваемой суммы и она решила позвонить ей. Выяснилось, что страницу подруги в социальной сети взломали, а потерпевшая перечислила денежные средства мошенникам.

Меры противодействия: запомните главное правило – в первую очередь связаться с родственниками, знакомыми от чьего имени у Вас просят денежные средства!

6. Мошенничества, которые совершаются от имени органов государственной власти.

Так, директору одной из школ Медведевского района позвонил неизвестный и представился районным прокурором. Далее аферист сообщил о необходимости прийти в прокуратуру, ознакомиться с документами и поставить подписи. Через некоторое время ей снова позвонили якобы из прокуратуры и попросили по пути приобрести в салоне связи две экспресс карты сотового оператора и зачислить на них по три тысячи рублей.

Заявитель ничего не подозревая, выполнила просьбу. Женщина поняла, что обманута, когда прибыла в прокуратуру и там выяснилось, что ей никто из сотрудников не звонил.

В полицию обратилась юрисконсульт одного из заводов в Звениговском районе. Женщина рассказала сотрудникам полиции, что на электронную почту завода поступило письмо из «Министерства промышленности, экономического развития и торговли Республики Марий Эл» с просьбой оказать спонсорскую помощь малоимущим детям и сиротам. Директор завода позвонил по указанному в письме номеру, ему ответил мужчина, который представился сотрудником министерства. В ходе беседы аферист убедил жертву, что деньги необходимы на закупку мебели, сантехники и иного товара в детский дом.

Директор, не подозревая обмана, согласился оказать финансовую помощь и перевел на указанный мошенником счет более 120 тысяч рублей. После чего, желая получить документы для отчетности предприятия, он позвонил по данному номеру телефона, но абонент был уже не доступен.

7. Выигрыш приза в размере N суммы рублей или иного имущества

23-летней йошкаролинкена одном из интернет-сайтов поступило сообщение о том, что она выиграла в конкурсе сотовый телефон. В ходе

переписки девушке сообщили, что для его получения необходимо оплатить доставку товара. Девушка, не подозревая обмана и желая получить приз, решила заплатить запрашиваемую сумму. Но на этом злоумышленник не остановился и под предлогом оплаты страховки, налога, выманил у потерпевшей еще деньги. В результате йошкаролинкалишилась 122 тысяч рублей.

Меры противодействия: запомните главное правило – «халявы» не бывает! Не задумываясь удаляйте из телефона полученные сообщения о выигрыше BMW, Mercedes, Apple, IPhone и т.д.!

8. Под видом работников газовых и социальных служб

В сентябре злоумышленницы похитили у 75-летней йошкаролинки золотые украшения. К ней в квартиру постучались три незнакомки, которые представились сотрудниками газовой службы. Пенсионерка впустила их к себе домой. Две женщины прошли с хозяйкой на кухню для осмотра газовой плиты, а третья осталась в комнате. После их ухода бабушка обнаружила пропажу из шкатулки золотых колец на общую сумму 14 тысяч рублей.

Меры противодействия: не впускайте в жилище посторонних, требуйте представить документы, подтверждающие принадлежность к той или иной организации. Не поленитесь позвонить в данную организацию и уточнить, работает, ли там сотрудник и действительно ли вам положены какие-либо выплаты, для этого рекомендуется заранее записать телефоны управляющих компаний, учреждений социальной защиты, пенсионного фонда, здравоохранения, коммунальных служб и т.д., а не звонить по телефонам которые Вам диктуют прибывшие «представители» той или иной организации, учреждения.

9.Под предлогом оказания помощи в получении кредита

В последнее время в полицию поступают заявления от жителей республики о потере денег после общения с аферистами, выдающими себя за сотрудников банков.

Так, 29-летняя йошкаролинка обратилась в полицию с заявлением о том, что мошенники похитили у нее крупную сумму денег. Позже выяснилось, что женщина на разных интернет-сайтах оставляла заявки о выдаче кредита. Через некоторое время ей позвонил неизвестный, который представился сотрудником банка и сообщил, что запрошенный ею кредит одобрен. Для его получения необходимо оплатить 5 тысяч рублей. Потерпевшая перевела требуемую сумму. Далее лжеконсультант неоднократно просил деньги на оплату страховки и различные услуги. В результате ничего не подозревавшая женщина перевела незнакомцу порядка 77 тыс. рублей.

Еще одной жертвой мошенников стала 63-летняя йошкаролинка. Она рассказала полицейским, что к ее подруге поступил телефонный звонок от якобы специалиста банка, который сообщил, что ей одобрена сумма кредита в 500 тысяч рублей и деньги будут привезены к ней домой сразу после оплаты страховки и возмещения затрат за работу специалистов. Женщина, желая получить займ, позвонила подруге и попросила в долг необходимую сумму денежных средств. Женщина, долго не раздумывая, перевела деньги незнакомцу. Получив желаемое, лжебанкир отключил мобильный телефон. Таким образом, ущерб составил 82 тысячи рублей.

Одним из важных факторов в противодействии мошенничествам является адекватность действий граждан (либо наоборот отказ от необдуманных шагов), реакция и самообладание при тех или иных обстоятельствах.

Престарелые граждане не всегда могут правильно оценить обстановку, поэтому МВД по Республике Марий Эл обращается к их детям и внукам – как можно чаще предупреждайте своих родителей о возможной опасности.

Если в отношении граждан все же было совершено мошенничество, следует незамедлительно обратиться в полицию, сообщив обстоятельства произошедшего и предоставив имеющиеся документы (расчетные чеки, распечатки звонков и т.п.).

10. Использование чужой банковской карты

В дежурную часть МО МВД России «Козьмодемьянский» с заявлением о краже обратилась 60-летняя местная жительница. Она рассказала полицейским, что с ранее утерянной ею банковской карты списаны около 1500 рублей на оплату товаров в различных торговых точках города. В ходе проведения оперативно-розыскных мероприятий сотрудниками уголовного розыска установлена личность предполагаемого злоумышленника. Им оказался 60-летний местный житель. Он признался в содеянном. Банковская карта была изъята.

Сотрудники полиции напоминают, если вы нашли чужую банковскую карту, то расплачиваться ею категорически нельзя! Пластиковая карта принадлежит банку, денежные средства на счете карты принадлежат ее владельцу. Если вы обнаружили чужую карточку, рекомендуется позвонить в банк (номер бесплатной горячей линии указан на внутренней стороне карты), и объяснить ситуацию. Финансовое учреждение заблокирует карту и

свяжется с ее владельцем. Ответственность за хищение денежных средств с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса) предусмотрена пунктом «г» части 3 статьи 158 УК РФ. По данной статье предусмотрено максимальное наказание в виде лишения свободы на срок до шести лет.