Приложение №1

Методические рекомендации
о предупреждении наиболее распространенных видов мошенничеств

Основные распространенные виды мошенничества:

Мошенничества в банках:

1. Мошенничество при кредитовании - зачисление сумм, предназначенных для погашения долга на другие счета, оформление кредитов на несуществующих заемщиков, оформление кредитов без ведома клиентов; оплата страхового взноса по несуществующему кредиту,

Мошенничество при рассчетно-кассовом обслуживании - несанкционированное списание сумм со счета, подмена купюр фальшивыми, вытягивание банкнот из пересчитанной пачки;

2. Мошенничество с депозитами - изъятие внесенных средств, преуменьшение сумм в документах, списание средств без ведома клиента.

Большинство банковских махинаций осуществляются в филиалах и отделениях банков, где меньше контроля, а не в крупных головных офисах. В таких условиях сотрудников меньше, но они вовлечены в большее количество бизнес-процессов, что открывает более широкие возможности для незаконной деятельности.

Мошенничества, совершаемые с использованием мобильной и проводной связи:

1. ***Просьбы о помощи от лица друзей или родственников*** с помощью СМС, в которых указывается примерно следующее: «Привет. Это Саша. Положи мне, пожалуйста, 1000 рублей на телефон. Срочно!». Более сложная схема - звонок от человека, который может представиться кем угодно, вплоть до сотрудника правоохранительных органов. В большинстве случаев «полицейский» сообщает, что кто-то из родственников стал участником ДТП с тяжелыми последствиями, и чтобы избежать уголовной ответственности, предлагает решить ситуацию с помощью денег, которые необходимо передать любым возможным способом.

2. ***Звонок или сообщение на платные номера.*** Человеку звонят с неизвестного номера, но затем сбрасывают еще до того момента, как абонент возьмет трубку. Человек из любопытства перезванивает на входящий ему номер, после чего ему отвечает либо автоответчик, либо он слышит длинные гудки. И в том, и в другом случае звонок платный и деньги со счета любопытного владельца сотового телефона переходят на счета мошенника.

Не менее часто случаи телефонного мошенничества связаны с различными «выгодными предложениями», которые ежедневно получают тысячи граждан через СМС, в котором указывается, что якобы владелец сотового телефона выиграл в лотерею большую сумму денег, либо поездку на курорт, машину и т.д. Для получения более подробной информации о том, как можно забрать свой приз, необходимо отправить либо ответное СМС на этот номер, либо перевести небольшую сумму денег на указанный счет.

Не менее опасно переходить по указанным в СМС ссылкам. Вместо розыгрыша призов и прочих «акций» можно легко попасть на сайт мошенников и получить вирус, крадущий с телефона абонента не только деньги, но и всю имеющуюся информацию.

Иногда мошенники обращаются к прохожим на улице с просьбой одолжить сотовый телефон, чтобы позвонить. После одного или нескольких звонков отзывчивый владелец мобильника обнаруживает, что баланс значительно меньше.

3. ***Платный код.*** Поступает звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

4. ***Штрафные санкции оператора.*** Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды.

5. ***Проблемы с банковской картой (счетом).*** Самые примитивные телефонные мошенничества банковскими картами или счетами рассчитаны на страх человека лишиться денежных накоплений и начинаются примерно одинаково: на телефон приходит СМС от «банка» или звонят мошенники, представляясь его сотрудниками. Информация может быть самой неприятной, например, о том, что заблокирована банковская карта или имеется задолженность по кредиту. В лучшем случае для разъяснения ситуации владельцу телефона предлагают позвонить оператору «банка». Те, кто после этого перезванивают, попадают на платный номер и теряют большую сумму со счета телефона.

Гораздо худшие последствия наступают, если по просьбе «банка» владелец телефона сообщает мошенникам номер карты и её пин-код, пароль от «Личного кабинета» интернет-версии банка, персональные данные и прочую информацию, которую следовало бы держать в секрете. В такой ситуации деньги с банковского счета обманутого абонента действительно бесследно исчезают.

6. ***«Мобильный банк»*** - приложение, которое позволит управлять вашим счетом. Участились случаи мошенничеств с использованием услуги «Мобильный банк», позволяющей управлять счетами через мобильное устройство. Данная услуга «привязывает» банковский счет к номеру телефона клиента банка.

Для предотвращения мошенничеств рекомендуем не распространять в сети Интернет сведения о мобильных номерах с их привязкой к анкетным данным, не указывать мобильные номера на социальных страницах, адрес жительства и другую личную информацию. Не использовать в сети Интернет номера своих мобильных телефонов к которым привязаны банковские карты и номера мобильных телефонов, которые используются для работы в «Мобильном банке». В случае если с Вашего телефона, банковской карты похитили денежные средства необходимо немедленно обратиться в банк и заблокировать ваш счет, запретить перевод денежных средств с вашего счета на другие счета, приостановить

обслуживание счетов, на которые были перечислены ваши денежные средства. После получения ответа от банка обратиться в полицию.

Мошенники обладают психологическими приемами введения в заблуждение, либо обладают информацией о потерпевшем и его близких. В случае сомнения в правдивости полученной информации следует перезвонить близким от имени кого пришло сообщение, позвонить в банк по указанному на карте, либо в договоре телефону, посетить ближайшее отделение банка. Запомните! Банк никогда не запрашивает по телефону сведения о карте клиента её номер, код на обратной стороне, Ф.И.О. владельца карты и срок её действия, а тем более пин-код, если собеседник пытается получить от вас такую информацию, либо просит сообщить коды, которые пришли на Ваш телефон от банка, прекратите с ним разговор. Доведите эти рекомендации до своих пожилых родителей и других родственников, что ни в коем случае не следует идти на поводу у незнакомцев. Настаивайте на том, чтобы пенсионеры всегда советовались с вами, прежде чем осуществлять любые операции с наличностью. Составьте для них специальный список экстренных телефонов: в нем должны быть номера полиции (дежурной части и участкового вашего района), аварийной службы, ближайшей поликлиники, социальной службы, ЖЭКа, банка, мобильного оператора и т. д.

7. Мобильный телефон используется мошенниками для передачи СМС-сообщений через мессенджеры Viber, WhatsApp с вредоносной ссылкой. Например, «здесь ваши фото…», «ваш акакунт, страница в «Одноклассниках» взломаны - пройдите регистрацию, «вы выиграли автомобиль, подробности ...» и т.д. Не стоит проходить по данной ссылке, т.к. риск заражения вашего телефона вредоносной программой очень высок. Кроме того, вы можете столкнуться с видом вредоносных программ которые не требуют Вашей активности и самостоятельно могут быть загружены на Ваше мобильное устройство через уязвимости операционной системы.

При заражении мобильного устройства происходит блокировка операционной системы, входящих СМС-сообщений, отправка искусственно сгенерированных мобильным устройством сообщений. Зараженный мобильный телефон следует отключить. Обратиться к оператору за новой сим-картой, а телефон передать в сервисный центр. В случае, если мошенникам удалось похитить денежные средства - немедленно обратиться в полицию и предоставить телефон для изучения компетентными сотрудниками.

Мошенничества, совершаемые в сети Интернет и с помощью сети Интернет:

1. Мошенничества при продаже товаров в сети Интернет по предоплате. Продавец отказывается встречаться лично и готов продать вам товар только посредством пересылки его по почте при условии полной или частичной предоплаты. Рекомендуем воспользоваться услугами уже проверенного продавца или магазина.

2. Получение от интернет-магазина, продавца товара, не соответствующего заявленному.

При совершении покупки дистанционным способом, необходимо проверить давно ли был создан сайт магазина, уделить внимание отзывам в сети Интернет по данному интернет-магазину, продавцу. Если в сети вы общаетесь с магазином, то

потребуйте сообщить сайт магазина в сети Интернет, юридический и фактический адрес.

Убедительно рекомендуем не осуществлять «слепые» покупки в социальных сетях. Администрация соц.сетей исключила разделы объявлений с сайтов и не несет ответственность за совершаемые с использованием сети действия пользователей.

При покупке железнодорожных и авиабилетов не приоретайте дешевые билеты на сомнительных сайтах, тем более расположенных в доменных зонах .com, .mobi, .org, .biz, .net, .info, .tv. и других не связанных с российским интернет-пространством. Осуществляйте покупку билетов на официальных сайтах компаний перевозчиков.

Способы и виды мошенничеств на сайтах объявлений:

1. Вам приходит SMS от имени сайта объявлений с предложением отправить текст на короткий номер в связи с тем, что вам поступили отклики по объявлению, или же ваш аккаунт был заблокирован. Впоследствии с вашего счета будут сняты деньги. Вернуть их будет невозможно. Рекомендуем не отвечать на подобные сообщения и обратиться в службу поддержки или к оператору мобильной связи с жалобой.

2. Мошенник под видом покупателя сообщает вам, что желает приобрести товар, но проживает в другом городе и предлагает оплатить товар путем перечисления денежных средств на карту продавца. Для этого он просит продавца назвать номер карты, владельца карты, срок действия карты, код на обратной стороне, а также сотовый номер привязанный к карте, либо по умолчанию использует номер, указанный в объявлении. После получения этих сведений мошенник использует данные о карте для оплаты покупок в сети Интернет.

Другие виды мошенничества в Интернете

1. На некоторых сайтах можно зарегистрироваться только, указав свой номер телефона, на который якобы должен прийти код для регистрации. Но если код не приходит в течение 5 минут (а он и не придет), вам самостоятельно необходимо отправить СМС на определенный номер. Не делайте этого! С вашего счета будут списаны денежные средства.

2. Инвестирование. На просторах Интернета существует множество сайтов, которые предлагают вложить свои деньги под определенный процент. Но многие из этих ресурсов обычный обман.

3. Методики, обучающие заработку в интернете. Вам предлагают приобрести руководство по заработку в сети Интернет (или методики иного характера), где дается подробная инструкция, как можно заработать определенную, как правило, большую сумму денег в день. Вам необходимо купить диск, оплатить пересылку и т.п. На самом вы приобретете «пустышку».

4. Фишинг - кража персональных данных (пароля, логина) с целью похищения средств с банковской карты. В основном для фишинга используют почтовую рассылку, содержащую ссылку на фальшивые сайты.

Мошенничества с наличными купюрами:

1. Самым простым и распространенным является мошенничество путем замены настоящих купюр в пачке на фальшивые (в основном, сверху и снизу - настоящие, посередине - фальшивые или обычная бумага).

2. «Недостача» - из уже пересчитанной пачки купюр вытягивается несколько банкнот.

3. Мошенничество с помощью банкомата при попытке снять наличность, на котором устанавливается датчик, считывающий персональные данные.

Чтобы не стать жертвой мошенников:

-не открывайте дверь незнакомым людям, даже если они представляются работниками социальных служб, полиции, поликлиники, ЖКХ и т.д. Перезвоните в организацию и уточните, направляли ли к Вам этого специалиста;

- если незнакомые люди предлагают приобрести продукты или товары по неправдоподобно низким (льготным) ценам, не верьте! Это обман!

- проявляйте осторожность, если с вами пытаются заговорить на улице незнакомые люди, не соглашайтесь на их предложения, ни в коем случае не приглашайте их к себе домой.

Если Вы стали жертвой мошенника, незамедлительно обращайтесь в органы внутренних дел. Вовремя поступивший сигнал о деятельности преступников повышает шансы установить личности злоумышленников «по горячим следам». Будьте бдительными!

Мошенничества, совершаемые в отношении пожилых граждан

В Новосибирской области наиболее распространены мошенничества, совершаемые под предлогом «снятия порчи», под видом сотрудников пенсионного фонда, социальных или коммунальных служб, медицинских учреждений. Отдельно можно выделить категории так называемых «телефонных мошенничеств» и мошенничеств в сети Интернет (обман при покупках на сайтах).

«Снятие порчи». Преступники, обращаясь к пожилому человеку, говорят, что он болен, либо на нем есть «порча», в связи с чем он и болеет, предлагая свои услуги по «исцелению». Жертвами таких мошенников становятся и молодые люди. Вступая в разговор с «целителем», жертва добровольно передает ему деньги или украшения для проведения «магического обряда», либо просто впускает в дом мошенников, которые, отвлекая жертву (например, попросив стакан воды) совершают тайное хищение имущества.

Другие мошенники обходят квартиры, где проживают пожилые люди, поясняя, что в ближайшее время будет реформа (либо дефолт), все накопления обнулятся, в связи с чем их необходимо поменять. Пенсионерам при этом могут показать якобы «удостоверение», чему пожилые люди как правило верят. Жертва показывает все свои накопления, которые хранятся дома, а после ухода «соцработников» обнаруживает вместо денежных купюр билеты «банка приколов». Понять, в какой именно момент произошла подмена купюр, потерпевшие не всегда могут.

Нередко мошенничества совершаются под видом компенсации за лекарственные препараты или какие-либо услуги: преступники приходят в квартиру к пожилым людям, завязывают разговор, в дальнейшем выясняя все условия проживания. В ходе беседы они сообщают, что пенсионеру полагается компенсация за когда-то приобретенное дорогостоящее лекарство, но для ее получения необходимо перевести некий «процент» в счет погашения той или иной задолженности. В ходе разговора преступники манипулируют психологическим состоянием пожилых людей.

«Телефонные мошенничества» на сегодняшний день остаются одним из наиболее распространенных видов мошенничеств. На домашний (мобильный) телефон гражданину звонят неустановленные лица, представляясь родственником и сообщая легенду о «ДТП с пострадавшим», драке, доставлении в полицию и.т.д, при этом требуя денег «на лечение пострадавшего», либо «для непривлечения к уголовной ответственности».

Преступники (как правило, мужчины) искажают свой голос (картавят, шепелявят), имен при этом не называют. Если пострадавший сразу же называет имя, звонящий подтверждает, что это он. Чтобы человек, которому позвонили, не смог позвонить никому из родственников, его просят не отключаться и ведут с ним разговор до тех пор, пока он не перечислит денежные средства на абонентский номер либо на банковскую карту, номер которой также диктуют по телефону.

Правительство Новосибирской области

Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

-Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;

-Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;

-Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные;

-Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

-Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;

-Сотрудник банка может запросить у клиента только контрольное слово, ФИО;

-При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие- либо операции с картой или счетом;

-Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

-При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

-Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

-Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

-Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.