**Наиболее распространенные виды мошенничеств**

Полиция напоминает гражданам о необходимости быть бдительными в общении с незнакомцами – в телефонном разговоре, посредством сети Интернет и при личном контакте.

Основные распространенные виды мошенничества:

1. Мошенничества совершаемые с использованием мобильной и проводной связи:

1.1. 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.

Так, в 2016 году следователем ГСУ ГУ МВД России по Новосибирской области направлено в суд уголовное дело по факту мошеннических действий, совершенных организованной группой.

В ходе следствия установлено, что мужчина, отбывая наказание в одной из исправительных колоний Новосибирской области, создал организованную группу, состоящую из его жены и троих знакомых.

Свою деятельность они осуществляли по следующей схеме: организатор совместно с участником организованной группы, путем случайного набора номера осуществляли телефонные звонки гражданам, проживающим на территории РФ.  Представлялись их родственниками и сотрудниками правоохранительных органов, после чего путем обмана якобы за освобождение родственника от ответственности за совершения преступления убеждали граждан переводить денежные средства на различные номера сим-карт и через систему электронных платежей.

От действий мошенников пострадали жители Приморского края, Ростовской, Иркутской, Тульской, Владимировской, Московской и Нижегородской областей.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. 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.

В сентябре 2016 года следователем СО ОМВД России по г. Бердску возбуждено уголовное дело по факту хищения денежных средств с банковской карты, принадлежащей жительнице г. Бердска.

Установлено, что супругу потерпевшей на телефон пришло СМС -сообщение о том, что банковская карта заблокирована. Женщина незамедлительно позвонила на номер, указанный как контактный. Трубку взял мужчина, представился сотрудником службы безопасности банка. Мужчина спросил у нее, знает ли она Полякова. Она ответила, что не знает. Мужчина сказал, что данный человек пытался снять денежные средства с банковской карты мужа, в связи с чем служба безопасности заблокировала данную карту. Для того, чтобы разблокировать карту, мужчина сказал, что необходимо назвать номер карты и цифры на обороте карты. Женщина сообщила данные карты. После этого на ее абонентский номер и номер её мужа стали приходить СМС - сообщения с кодами, которые она также сообщила «сотруднику» банка. После этого с карты ее мужа были списаны денежные средства в сумме 10 тысяч рублей, а также с ее карты списаны 22 тысячи рублей.

1.6. «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.

Следователем ГСУ ГУ МВД России возбужденно уголовное дело по факту хищения денежных средств с банковской карты.

Установлено, что к банковской карте потерпевшего была подключена услуга «Мобильный банк». Решив оплатить коммунальные услуги, мужчина вошел в приложение «Мобильный банк» по ссылке, которой постоянно пользовался, но не обратил внимание, что при входе в строке, где пишется адрес входа, что-то поменялось. Ему пришло сообщение с одноразовым паролем для в хода в приложение «Мобильный банк». Он ввел код, после чего на странице появилось слово «СПАСИБО», больше страница не открывалась. Нажав повторно на ссылку страница вновь открылась. Впоследствии со его счета были похищены денежные средства в сумме 6 800 рублей.

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.

1.7. 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.

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

2.1. 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.

2.2. 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.

3. Способы и виды мошенничеств на сайтах объявлений:

3.1. 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.

  3.2. 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 так же 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.

В производстве следователя ГСУ ГУ МВД России по Новосибирской области находится уголовное дело, возбужденное по факту хищения денежных средств с банковской карты.

Установлено, что житель Новосибирской области разместил на одном из сайтов объявлений информацию о продаже дома в Республике Бурятия. На его абонентский номер позвонил мужчина, который сказал, что хочет приобрести дом, готов перевести ему денежные средства на его банковскую карту в счет предоплаты. После этого позвонила женщина, которая представилась бухгалтером, и сказала, что готова внести предоплату за дом. Потерпевший назвал ей номер своей карты, а после того, как пришли СМС - сообщения с кодами подтверждения, назвал коды, не прочитав текст сообщений, в которых было указано, что одноразовые коды нельзя сообщать никому, даже сотрудникам банка. После этого с банковской карты потерпевшего были списаны денежные средства в сумме 63 000 рублей.

4.  Другие виды мошенничества в Интернете.

4.1. 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.

4.2. Инвестирование.

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

4.3.  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».

ГУ МВД России по Новосибирской области предупреждает! 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!