**ГРАЖДАНЕ, БУДЬТЕ БДИТЕЛЬНЫ!**

**УБЕРЕГИТЕ СЕБЯ, СВОИХ РОДНЫХ И ЗНАКОМЫХ ОТ ПОСЯГАТЕЛСЬТВ МОШЕННИКОВ!**

Проведенный анализ сотрудниками полиции свидетельствует о том, что в последнее время на территории ЗАТО Сибирский, а в целом и на территории Российской Федерации существенно осложнилась оперативная обстановка связанная с мошенничествами и совершением хищения денежных средств, с банковских карт и счетов граждан, данные преступления совершаются с использованием средств сотовой связи и Интернет-ресурсов.

В настоящее время используются следующие схемы совершения мошенничеств:

1. ***«Ваш родственник попал в беду»***. При совершении мошенничеств по данной схеме преступники находят потерпевших путем «прозвона» домашних телефонов. В ходе разговора представляются от имени родственников, либо сотрудников правоохранительных органов, сообщая заведомо ложную информацию о том, что их родные совершили тяжкое уголовное преступление, при этом выясняя все данные самого потерпевшего и его родственника, предлагая вариант о не привлечении к ответственности за определенную сумму. Денежными средствами мошенники завладевают следующими способами: через терминалы оплаты - путем пополнения абонентских счетов, путем денежных переводов «Блиц» через отделения банков, а также путем личного принятия, либо передачи через привлекаемых ими же лиц, которыми зачастую выступают водители такси. Указанная схема используется лицами, содержащимися в исправительных колониях Самарской и Новосибирской областях.

2. ***«Вы выиграли приз»***, данная схема имеет следующий порядок совершения преступления: исполнитель путем рассылки ряда СМС-сообщений на абонентские номера граждан сообщает заведомо ложную информацию о том, что данный абонентский номер выиграл ценный приз, которым может являться автомобиль, либо дорогая бытовая, электронная техника и в редких случаях денежные средства. После того как потерпевший перезванивает на указанный в сообщении абонентский номер, между ним и неизвестным осуществляется беседа. В ходе, которой мошенник представляется от имени ведущего радио, оператора сотовой компании, сообщает о выигрыше и предлагает вариант по перечислению денежной суммы равной стоимости выигранного приза, когда потерпевший соглашается, то со стороны мошенника поступает предложение о переводе части суммы на абонентские номера в виду взыскания государственного налога. В данном случае денежные средства попадают в пользование преступника практически во всех случаях посредствам перевода их через терминал оплаты услуг сотовой связи, но иногда мошенники запрашивают реквизиты банковской карты для использования их при подключении к услуге операторов сотовых компаний «Мобильный кошелек». Указанная схема используется жителями Самарской области.

3. ***«Ваша банковская карта заблокирована»*** для совершения мошенничества по обозначенной схеме, исполнитель рассылает СМС-сообщения на абонентские номера граждан, от имени службы безопасности банка и указывает контактный абонентский номер для обратной связи. В процессе звонка с потерпевшим происходит беседа с мнимым сотрудником службы безопасности банка, который в свою очередь поясняет, что произошел сбой системы и ряд банковских карт заблокировано, и для устранения неполадок предлагает потерпевшему при помощи банкомата произвести следующую операцию: «вставить банковскую карту – ввести пин-код – зайти в меню «оплата услуг» – выбрать «платежи» – далее «Билайн» – ввести абонентский номер – выбрать позицию «без оплаты» - забрать карту», которая в последствии приводит к автоматическому подключению услуги операторов сотовой связи «Мобильный кошелек», затем разговор заканчивается. После чего мошенник осуществляет перевод денежных средств имеющихся на карте на абонентский номер, который самим же потерпевшим и был введен ранее. Также мошенники при использовании данной схемы просят потерпевших назвать реквизиты своей банковской карты, с которой в последующем происходит перечисление денежных средств на абонентские номера по услуге «Мобильный кошелек». Указанная схема используется как жителями Самарской, так и Курганской областей.

В последнее время начинают активизироваться новые схемы совершения преступлений:

4. ***«Приобретение автомобиля через средства Интернет»,*** неустановленные лица размещают в официальных Интернет-сайтах объявления по продаже автомобиля, по заниженной цене, ссылаясь на объективные причины указанной цены, приводят описание продаваемого автомобиля и контактный абонентский номер. В ходе разговора между потерпевшим и неизвестным оговариваются условия расчета за автомобиль, при этом неизвестный просит предоплату и сообщает расчетный счет, на который необходимо перевести денежные средства. Через некоторое время на абонентский номер покупателя приходит смс-сообщения о том, что сделка не состоится, либо используемый мошенником абонентский номер отключается. Данной схемой пользуются жители Европейской части России – это Краснодарский край, Московская область.

5. ***«Вам полагается компенсация»*** мошенничества данного вида совершаются в отношении престарелых граждан, т.к. последние зачастую приобретают посредствам сетевого маркетинга в пользование различные препараты, аппараты, предлагаемые под видом медицинских. Неизвестные в ходе беседы с потерпевшим выясняют приобретал ли он какой-нибудь товар из сферы сетевого маркетинга, помог ли он потерпевшему. В ходе разговора мошенник представляется от имени работника прокуратуры и поясняет, что проводилась прокурорская проверка, либо работников данной организации привлекают к уголовной ответственности и товар который был реализован является не сертифицированным, а лицам, приобретавшим его полагается компенсация в довольно крупном размере, при этом поясняет, что для получения денежных средств необходимо внести определенную сумму на расчетный счет, для проведения операции, открытия индивидуальной ячейки и т.д. После чего неизвестным оставляются либо абонентские номера якобы службы безопасности банка, либо просто номер расчетного счета. Перечисление денежных средств совершается в несколько этапов. Зачастую мошенничества совершенные указанным видом имеют большую латентность, т.к. потерпевшие ожидают обещанной компенсации и длительное время не обращаются в правоохранительные органы, а лишь спустя 2-3 месяца. Описываемая схема получила распространение с территории Московской области.

6. ***«Вам в сотовый телефон системы «Андроид» автоматически поступает вирус -*** хищения денежных средств данного вида совершаются в отношении граждан, которые пользуются услугами мобильный банк и интернет ресурсами со своего сотового телефона, т.е. у вас имеется банковская карта, на которой подключена услуга мобильный банк. Данная услуга подключается на абонентский номер вашего сотового телефона и вам после проведения, каких либо банковских операций по карте поступают смс оповещения. В дальнейшем вы пользуетесь на своём сотовом телефоне Интернет-ресурсами, в один из дней вам понадобились обновления приложений системы «Андроид», которые вы закачиваете с интернета, совместно с приобретенными вами приложениями на ваш сотовый телефон автоматически поступает вирусная программа, вы на первый взгляд не определите о том, что она имеется у вас в наличии. Но в дальнейшем данная вирусная программа делает своё дело, она собирает всю информацию о вашей банковской карте, которая привязана на ваш абонентский номер сотового телефона и в дальнейшем вся собранная информация смс-сообщением отправляется с вашего сотового телефона на телефон преступника. После чего преступнику становится известны все ваши коды по банковской карте, что ему позволяет без всяких трудностей в системе интернет при помощи мобильного банка и вашего личного кабинета совершить операции по вашей банковской карте т.е совершить хищение денежных средств со всех банковских счетов, которые у вас имеются. При совершении преступником хищения денежных средств, с вашей банковской карты, вам на сотовый телефон смс-оповещение о проведении операций по карте не поступают, как правило вам становиться это известно только после того, как вы обратитесь к сотрудникам банка.

Описываемая схема получила распространение в Центральной части РФ и республике Украина. Помимо указанного способа попадания вирусного программного обеспечения, имеются иные способы – например, посредством направления на Ваш сотовый телефон ммс-сообщения, содержащего ссылку, под видом картинки, при переходе по которой посредством Интернет-браузера происходит скачивание вируса. В последнее время распространена рассылка ммс-сообщением под предлогом обмена или просмотра товара по размещенному объявлению на Интернет-ресурсах размещения объявлений о продаже различных товаров – «Авито», «Юла» и т.п.

7. ***«Вы самостоятельно сообщаете номера банковских карт преступнику в системе интернет на сайте социальных страниц «Одноклассники, Вконтакте и иных сайтах интернет ресурсов»*** хищения денежных средств данного вида совершаются следующим образом, вы используете свою банковскую карту, для оплаты в социальных сетях «Одноклассники, Вконтакте» покупаете ОК т.е покупаете различные подарки своим близким и друзьям, или осуществляете какую либо покупку вещей на различных сайтах в интернете например на сайте «Али Экспресс» но при этом вы не знаете о том, что данный сайт может быть взломан мошенниками и когда вы производите оплату на данном сайте то номера карт или номера операций по вашей банковской карте становятся известны злоумышленникам так, как в компьютерных технологиях память проведенных операций имеет свойство сохраняться тем самым злоумышленнику вы самостоятельно сообщаете номера своих банковских карт, в дальнейшем злоумышленник пользуется данной информацией и без всяких трудностей имеет доступ к вашим банковским счетам, через интернет ресурсы он вскрывает ваш личный кабинет в системе мобильный банк, после чего осуществляет любые операции по перечислению денежных средств с ваших счетов.

**8. «Задаток за покупку покупаемой вещи по Вашему объявлению».** В последнее время является одним из самых распространенных способов хищения денежных средств. Хищение денежных средств происходит следующим образом – Вы размещаете объявление на сайтах продаж товаров вторичного использования ( «Авито», «Юла», «LetGo» и т.п.). Через некоторое время – как правило в течении нескольких дней, Вам поступает звонок, в ходе разговора злоумышленник сообщает, что ему очень понравился продаваемый Вами товар, он хотел бы приобрести его, однако в настоящее время за пределами Алтайского края, ввиду чего просит «придержать» данный товар, предлагая Вам перевести задаток на Вашу банковскую карту – как правило открытую в ПАО «Сбербанк России». После получения номера банковской карты сообщает Вам, что, по неизвестным причинам, у него не получается произвести операцию перевода, просит сообщить дополнительные реквизиты карты – дату действия карты, наименование собственника карты (указанное на лицевой стороне карты», CVV-код карты (указан на обратной стороне карты, как правило состоит из 3 цифр), а также просит сообщить коды, которые пришли Вам в смс-сообщении в ходе разговора. После сообщения Вами указанных сведений, злоумышленник получает доступ к сервису «Сбербанк Онлайн» по Вашей карте (даже в случае, если Вы никогда указанным сервисом никогда не пользовались), подключает услугу «Мобильный Банк» к своему сотовому номеру (с целью отключить Вас от информирования о проводимых по Вашим карта и счетам операциям), после чего осуществляет перевод всех имеющихся денежных средств на Ваших счетах и картах ПАО «Сбербанк России» на имеющиеся в его распоряжении банковские карты как этого банка, так и других банков – чаще всего АО «Альфа Банк», АО «Тинькофф Банк».

**9. «Компенсация за услуги связи».** В последнее время указанный вид хищения денежных средств начинает приобретать популярность в преступной среде. Хищение денежных средств происходит следующим образом – Вам на сотовый телефон поступает звонок, в ходе разговора звонящий представляется сотрудником одной из сотовых компаний – ПАО «Вымпелком», ПАО «МТС», ПАО «Мегафон», ООО «Т2 Мобайл» и т.п., сообщает Вам, что с баланса Вашего сотового номера ранее были необоснованно списаны денежные средства за услуги связи, в связи с чем предлагает Вам вернуть указанные денежные средства посредством пополнения баланса Вашей банковской карты, чаще всего открытой в ПАО «Сбербанк России». Далее получает доступ к карте и совершает хищение описанной в предыдущем пункте алгоритмом.

**Как не стать жертвой подобных преступлений и защитить своих близких от данного посягательства?** Прежде всего, не следует быть слишком доверчивым. Если вам позвонили от лица какого-либо серьезного ведомства или любой другой организации и потребовали деньги, не бойтесь перезвонить по официальным телефонам учреждения и выяснить, соответствует ли полученная вами информация действительности. Также, узнав о новом способе, применяемом аферистами в мобильной сфере, обязательно расскажите о нем всем своим знакомым. Часто преступники пользуются не информированностью населения.

Жажда легкой наживы— одна из тех человеческих слабостей, которые используются мошенниками в первую очередь. Легкие деньги, выигрыши в лотерею, обман платежной или иной системы — все эти схемы обмана построены одинаково: «Сначала вы дадите нам немножко денег, зато потом получите миллионы». Очевидно, что никакого «потом» не бывает. Нужно хорошо помнить, что бесплатный сыр бывает только в мышеловке. Еще одно естественное человеческое чувство, на которое рассчитывают злоумышленники, — это страх. Чаще всего мобильные мошенники апеллируют жизнью и безопасностью наших родных и близких людей, присылая SMS, либо оповещая нас посредством мобильной и стационарной связи о травмах, авариях и других чрезвычайных происшествиях с участием близких нам людей. Подобные телефонные звонки, мотивирующие человека выполнить определенные действия немедленно, не задумываясь, направлены на игру именно на этом чувстве, не сумев, трезво оценить ситуацию, приняв голос чужого человека за мольбу о помощи близкого родственника, люди перечисляют на счет мошенников крупные суммы денежных средств. Сотрудники полиции советуют в таких случаях немедленно прервать разговор и положить трубку, Если контакт уже налажен, то постарайтесь задать собеседнику как можно больше уточняющих вопросов. Если на Ваш телефонный номер поступил подобный звонок в первую очередь, свяжитесь с родственниками и выясните, где они находятся, действительно ли они попали в беду. Затем сообщите о случившемся в дежурную часть ближайшего отделения полиции по телефону 02, либо на «телефон доверия» полиции ГУ МВД России по Алтайскому краю на телефон 128 (звонок бесплатный).

 Время не стоит на месте, и мошенничество подстерегает нас везде: на просторах Интернета, в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Случаи Интернет-мошенничества имеют место быть в нашей жизни, ведь большинство граждан для своего удобства пользуются предложениями в сфере товаров и услуг в сети Интернет. Однако не всегда случаи Интернет-мошенничества люди могут распознать «с ходу». К сожалению, не редко жители нашего края, а также жители ЗАТО Сибирский попадаются на уловки аферистов и в итоге такие истории заканчиваются плачевно. Летнее время считается временем отпусков и каждый мечтает провести свой отпуск красочно и запоминающим. Большинство турагентств и авиакомпаний предлагают приобрести путевки не выходя из дома посредством сети Интернет. Прежде чем переводить свои денежные средства за авиабилеты или за какой-либо товар, услугу, убедитесь, что данный сайт не является «фирмой-однодневкой», прочитав все отзывы о данном сайте. Не торопитесь, перед тем как совершить какие-либо необратимые действия, подумайте, только сам пользователь сети может сделать свою жизнь в виртуальном пространстве безопасной. «Предупрежден-значит вооружен», — гласит поговорка. Это справедливо по отношению к защите от мошенничества.

 Также МО МВД России по ЗАТО Сибирский просит всех, кому известно о случаях мошенничеств, а также при попытках совершения в отношении Вас или Ваших близких преступлений указанной сферы, обращаться в МО МВД России по ЗАТО Сибирский по указанным телефонам – ДЧ: 8 (38532) 50 002, тел. сотрудника уголовного розыска по линии мошенничеств и хищений денежных средств с банковских карт: 8 (38532) 50 334, 8-913-026-88-45.

С.В. Самойлов, заместитель начальника полиции

по охране общественного порядка