Профилактика мошенничества

Виды мошенничеств в сетях сотовой и проводной связи и в сети Интернет

1. Мошенничества совершаемые с использованием мобильной и проводной связи:

а) сотовый и проводной телефон используется как средство передачи голосовой информации, подвиды, типы:

- «ваш сын попал в аварию..»,

- «мама/папа у меня проблемы..»,

- «это из банка/соцзащиты и пр..»

б) сотовый телефон используется для передачи СМС с ложной информацией:

-«мама, кинь мне на этот номер денег, потом все объясню»,

-«ваша карта заблокирована подробности по тел..»,

-«с вашего счета списано 5000 рублей, подробности по тел...»;

Самая актуальная схема мошенничества:

в) сотовый телефон и ваше объявление в сети Интернет (сайт Avito) используется мошенником для получения от вас данных карты и привязки карты к мобильному телефону мошенника:

- « я по вашему объявлению на авито (о продаже, о сдаче в аренду), сообщите мне данные с вашей карты и код на обратной стороне я вам отправлю деньги...»;

- « я хочу отправить деньги вам на карту за товар на авито, предоплату за аренду, у вас карта привязана к мобильному банку, если нет идите к банкомату я вас проинструктирую как подключить мобильный банк».

При получении сообщения не нужно перезванивать на указанные номера. Мошенники могут потребовать передать деньги курьеру, перечислить их на карту, номер мобильного телефона, попытаются получить от вас сведения о Вашей банковской карте, предложить пройти к банкомату и совершить какие-либо операции у банкомата, попросят сообщить коды которые приходят к Вам на телефон. В случае получения входящего звонка необходимо прекратить разговор, даже если собеседник вселяет уверенность в своей правдивости. Мошенники обладают психологическими приемами введения в заблуждение, либо обладают информацией о потерпевшем и его

близких. Аналогичные случаи мошенничества встречаются и в сети Интернет, но сообщение о помощи передается посредством сообщения в социальной сети с ложной страницы родственника.

При сомнении 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.

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.

Гражданам имеющим престарелых родственников, соседей, знакомых необходимо разъяснить им, какие способы мошенничества существуют, как вести себя при получении звонков и сообщений мошеннического характера, а именно не вести диалоги с мошенниками, прекратить разговор и позвонить родственникам. Если пожилой человек получает пенсию на банковскую карту, то предложите свою помощь в снятии с карты денежных средств, либо предложите родственнику передать карту Вам. Во многих случаях в ходе общения с престарелыми людьми сообщники мошенников находятся в районе проживания пожилого человека, либо у его дома, подъезда. При получении мошеннического звонка необходимо немедленно сообщить о данном факте в полицию.

Если при мошенничестве, в ходе телефонного разговора преступником была получена информация о банковской карте, то необходимо позвонить по телефону указанному на карте и заблокировать карту. В день совершения мошенничества необходимо обратиться в банк с заявлением о возврате денежных средств на карту, так как банк обязан возвратить денежные средства если операция была оспорена владельцем карты в день операции.

Для предотвращения мошенничеств так же рекомендуем не распространять в сети Интернет сведения о мобильных номерах с их привязкой к анкетным данным, не указывать мобильные номера на социальных страницах, в подаваемых в сети объявлениях не указывать рядом с номером сотового телефона Имя и Фамилию, 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».

Последнее время получают распространение мошенничества совершенные в отношении пользователей сети Интернет продающих товары на сайтах бесплатных объявлений. Продавцу поступает звонок от якобы покупателя. Мошенник под видом покупателя сообщает, 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. Другой вариант когда на телефон продавца поступают коды от банка и мошенник просит сообщать их якобы для перевода денег, в этот момент мошенник подключает к телефону потерпевшего, либо к своему телефону услугу «Мобильный банк» и похищает деньги с карты. Третий вариант когда мошенник, выступающий в роли «покупателя» предлагает продавцу пройти к банкомату и якобы произведя некоторые операции получить деньги, в трех указанных случаях мошенник похищает денежные средства продавца.

г) сотовый телефон используется мошенниками для передачи СМС сообщения, сообщений через мессенджеры Viber, WhatsApp с вредоносной информацией. Типы сообщений: «здесь наши с тобой фото http:\\\\...», , «ваш акакунт, страница «вКонтате» взломаны, пройдите регистрацию http:\\\\...», «вы выиграли автомобиль, подробности http:\\\\...”

Новый тип сообщений с вредоносной ссылкой:

«я по вашему объявлению, согласны ли на обмен на это http:\\\\foto3.inc...»

При получении данного сообщения откажитесь от прохождения по указанной ссылке и активации полученных ссылок. По возможности проверьте есть ли в сети Интернет в поисковых системах сведения о данных ссылках и возможных мошенничествах. Сообщите пользователям сети Интернет, что данная ссылка мошенническая. Удалите указанное сообщение если убеждены, что оно не нанесло вред Вашему устройству.

Вредоносные программы создаются и усовершенствуются мошенниками регулярно и при работе с телефоном 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.

В случае заражения мобильного устройства рекомендуем определить угрозы и последствия получения доступа хакера к Вашему мобильному устройству.

Признаками заражения мобильного устройства могут быть блокирование операционной системы, блокирование входящих СМС сообщений, отправка искусственно сгенерированных мобильным устройством сообщений. Зараженный мобильный телефон следует немедленно выключить. Сим-карту перевыпустить у оператора, а телефон сохранить для последующего изучения полицией, если было совершено мошенничество, либо передать в сервисный центр, если деньги похищены не были.

Если к данному мобильному устройству привязана банковская карта, банковские услуги такие как «Мобильный банк», «Онлайн Банк», «Интернет-банк», то необходимо срочно связаться с банком заблокировать карту и приостановить обслуживание по счетам. Если с помощью телефона это не удается сделать, то необходимо обратиться в ближайшее отделение банка. Если мобильное устройство используется для доступа к страницам в социальных сетях, то необходимо с другого устройства либо компьютера выйти в социальную сеть и сменить привязанный номер телефона.

Зараженное мобильное устройство так же является источником распространения вредоносной информации по контактам, содержащимся в телефоне. Для предотвращения рассылки необходимо уведомить максимальное количество знакомых о Вашей проблеме и о возможно приходящих от Вашего имени вредоносных сообщениях.

В случае если с Вашего телефона, банковской карты похитили денежные средства необходимо в день совершения хищения обратиться в банк с требованием вернуть денежные средства, 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, с выпиской по счету обратиться в полицию.

Одним из распространенных мобильных мошенничеств так же является использование дубликата сим-карты для доступа к системам дистанционного управления банковским счетом. Признаком использования дубликата Вашей сим-карты является блокирование доступа мобильной связи. В этом случае

необходимо срочно обратиться к мобильному оператору и перевыпустить сим-карту. В случае подтверждения мобильным оператором факта несанкционированной замены Вашей сим-карты необходимо написать претензию в сотовую компанию и обратиться в полицию.

Можно избежать участи жертвы данных мошенничеств если следовать следующим рекомендациям:

-Для работы с банковскими картами, системами «Мобильный банк», «Банк-онлайн», «Интернет-банк» и др. использовать отдельное мобильное устройство не предназначенное для разговоров и развлечения в сети Интернет;

-Не указывать номера мобильных устройств, используемых для работы с банковскими картами и дистанционного управления банковским счетом, как контактных в сети Интернет, в объявлениях и на страницах соц. сетей;

-Приобрести и установить на мобильное устройство лицензионное антивирусное программное обеспечение из официальных источников;

-Указать в договоре с банком, либо в иной форме согласовать с банком что управление банковским счетом и проведение операций по карте может осуществляться только с одного мобильного устройства с одним IMEI, ограничить круг операций, установить лимит, который можно переводить с помощью мобильного устройства.

-Запретить перевод всего объема денежных средств с карты, счета.

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

а) мошенничества при продаже товаров в сети Интернет по предоплате (распространенные виды : продажа Iphone, цифровой, бытовой техники, одежды, обуви, автомобилей, автозапчастей);

б) получение от интернет магазина, продавца товара не соответствующего заявленному;

Развитие данных видов мошенничества обусловлено человеческими факторами, такими как желание сэкономить, отсутствие близко расположенных магазинов с таким товаром, полное отсутствие предложений на рынке. Основными приобретаемыми товарами являются предметы роскоши-дорогая цифровая техника, автомобили, шубы, брендовые вещи. Исключены полностью факты приобретения товаров первой необходимости. Желание сэкономить приводит зачастую к потере всех денежных средств, в

связи с чем первая и основная рекомендация - приобретать вещи за их реальную стоимость и не искать предложений с 30-50 % выгодой, так как это противоречит в целом принципам рынка, либо присланный товар окажется подделкой, неисправным, либо не удовлетворяющим запросам покупателя. Не стоит приобретать товары в интернет магазинах позиционирующих себя как российские, но имеющие сайты в доменных зонах .com .org .biz .net .info .tv .mobi .

Особое внимание следует уделить отзывам в сети Интернет по данному интернет-магазину, продавцу. Проверить когда был создан магазин, сайт. Создан ли он год и более назад. Если сайт существует меньше месяца, то стоит отказаться от покупки. Можно проверить наличие офиса у данного магазина, удостовериться в сети Интернет, что такой дом существует, посмотреть его на карте, фото снимках, панорамах Яндекс, Гугл. Убедиться что на доме есть вывеска магазина, либо имеются офисные помещения. На снимках так же можно узнать названия, телефоны близко расположенных организаций, позвонить им и выяснить достоверность информации. В интернет справочниках найти телефоны администратора офисного центра, ресепшена, убедиться, что такой магазин, индивидуальный предприниматель существуют и осуществляют свою деятельность в данном здании. Полученную информацию следует использовать при общении по телефону с сотрудниками магазина. Если магазин, продавец отказываются звонить по телефону предлагают другие способы общения такие как Viber, Skype, WhatsApp и другие, либо телефона магазин не имеет, следует отказаться от покупки. В ходе общения по телефону можно сообщить, что находитесь в городе продавца, магазина и предложите забрать товар самовывозом и оплатить наличными в офисе. В случае категоричного отказа следует отказаться от покупки.

При приобретении дорогостоящих вещей таких как автомобиль, дорожная техника, строительные материалы, рекомендуем потратить деньги на дорогу до города продавца и удостовериться в наличии продавца и товара. Либо найти в городе продавца знакомых и попросить их проверить достоверность предложения в сети Интернет. Если же такой возможности нет, то оплатить услуги юриста, сотрудника автофирмы, занимающейся в городе продавца продажей и скупкой авто и за символическую плату предложить ему встретиться с продавцом и осмотреть авто и документы. То же касается приобретения стройматериалов и металла, обратитесь к услугам юриста в городе продавца. Любые присланные Вам по Интернету

фотографии, сканы документов и автомобиля мошенники с легкостью подделывают.

В настоящее время большинство интернет магазинов работаю по 100 % предоплате, при соблюдении указанных рекомендаций можно совершить удачную покупку.

Настоятельно 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.

В случае необходимости приобрести товар через социальную сеть необходимо тщательно проверить продавца, обязательно связаться с ним по телефону, расспросить подробности о товаре , потребовать фотографии товара в деталях, предложить отправить товар курьерской службой и наложным платежом, обговорить возможность возврата товара, возможность самовывоза.

Проверить отзывы и оставленные комментарии в группе и на странице продавца. Если несколько пользователей сети размещают сплошь хвалебные отзывы и рекомендации, то стоит просмотреть страницы этих пользователей, не являются ли они «фейковыми», есть ли у них на страницах личные фотографии, большое количество друзей. Данную информацию можно просмотреть и на странице продавца. Страница продавца должна быть активной, на ней регулярно должны размещаться личные фотографии, обновляться альбомы, должны быть сведения о месте учебы и работы, а в друзьях должны быть «живые» и активные пользователи. Можно уточнить где находится продавец, в каком городе, предложить забрать товар якобы вашим знакомым, находящимся в данном городе и оценить реакцию продавца. Если в сети вы общаетесь с магазином, то потребуйте сообщить сайт магазина в сети Интернет, юридический и фактический адрес. При любом сомнении откажитесь от приобретения товара со 100% предоплатой через соцсеть.

Широкое распространение в сети Интернет так же приобретают мошенничества с привлечением средств пользователей для их приумножения в финансовых пирамидах, кооперативах, микрофинансовых организациях, биржах, букмекерских конторах, рынках электронных валют. Правоохранительные органы настоятельно рекомендуют не вступать в какие-либо отношения с такими организациями и лицами, предлагающими такие услуги, так как многие компании и интернет сайты данных компаний

находятся за рубежом, организации работают по законам других государств, либо изначально мошеннические и вернуть затраченные на данные проекты деньги практически невозможно.

в) сайты «подделки» , а так же фишинговые сайты

Данный вид мошенничества предполагает, что жертва посчитает сайт знакомым и приобретет на нем товар, услугу, либо укажет данные своей банковской карты.

Единственной рекомендацией может быть проявление внимательности. Необходимо обратить внимание на адресную строку сайта, название сайта, есть ли какие-либо добавочные символы или названия в адресной строке, расположен ли сайт в доменной зоне «ru». Скопировать название сайта из адресной строки и проверить в поисковой системе. Не стоит доверять сайтам имеющим в названии знакомые слова, но расположенные в доменных зонах .com .org .biz .net .info .tv .mobi и других не связанных с российским интернет пространством.

Проверьте неоднократно сайты в разделах которых, планируете указать данные о своей банковской карте, по дате создания сайта, по телефонам указанным на сайте, по отзывам в сети Интернет, следует уточнить нет ли сайта в различных блек листах сети Интернет. Помните мошеннику достаточно номера карты и кода на обратной стороне карты (CVV код состоящий из четырех цифр) для покупок и оплаты услуг в сети Интернет. Другие данные, то как срок действия карты, он может подобрать, а имя и фамилию владельца узнать от вас либо из сети Интернет с ваших личных страниц.

Если вы стали жертвой такого сайта и заметили это после проведения операции, покупки, заблокируйте карту и обратитесь в банк в день проведения операции для её отмены и возврате денежных средств.

При покупке авиа, жд. билетов не ищите очень дешевые билеты на сомнительных сайтах, тем более расположенных в доменных зонах .com .org .biz .net .info .tv .mobi . Доступные по цене билеты желательно приобретать на официальных сайтах компаний перевозчиков.

ПРИМЕРЫ МОШЕННИЧЕСТВ

30.05.2014г. в адрес отдела «К» ГУ МВД России по Челябинской области поступила оперативная информация о личностях Ш.а, 27.09.1990 г/р., уроженца г.Миасса Челябинской области, проживающего по адресам: и

М., прож. г. Челябинск ул. Бейвеля, , которые могут быть причастны к созданию и распространению вредоносных программ.

В ходе анализа информации, полученной в ходе мероприятий в отношении Ш.а В.И., сотрудниками управления «К» МВД России было достоверно установлена причастность к созданию и распространению вируса «Trojan-Banker.AndroidOS.Svpeng.a» Ш.а В.И., а так же к управлению бот-сетью зараженных мобильных устройств.

Хищение денежных средств осуществлялось следующим образом: в начале 2014г. на одном из зарубежных серверов Ш. В.И. разместил созданную им программу контрольно-административную панель «бот-сети», для управления зараженными мобильными устройствами-«ботами». Ш.В.И. расширял сеть зараженных устройств, путем размещения вредоносной программы «Trojan-Banker.AndroidOS.Svpeng.a» на различных интернет-ресурсах, внешне схожих с официальными ресурсами поддержки устройств на операционной системе «Андройд», под видом лицензионного программного обеспечения для Андройд-устройств, в виде обновлений к приложениям, играм, которые создавал сам, либо брал в аренду.

Используя контрольно-административную панель «бот-сети» Ш. В.И. выбирал несколько скомпрометированных устройств находящихся на тот момент в сети, после чего подавал группе зараженных устройств команду на проверку баланса и тем самым выяснял привязку мобильного устройства к банковскому счету, сформировав СМС-сообщение на короткий номер «900» с текстом «баланс», ответ на указанную команду поступал в виде текстового файла содержащего денежные суммы на банковской карте пользователя скомпрометированного устройства. Выбрав одного из клиентов чей баланс составлял больше 15 тысяч рублей Ш. В.И. формировал денежный перевод в виде СМС-сообщения с текстом в котором указывался «абонентский номер телефона» и «сумма» в размере 3 тысячи рублей, при этом указанные денежные средства поступали на лицевой счет абонентского номера зараженного телефона. Далее формировалось следующее СМС-сообщение с текстом «перевод» и «абонентский номер телефона» и «сумма» в размере 8 тысяч рублей. Указывались именно такие суммы переводов в связи с суточными лимитами переводов установленные ОАО «Сбербанк России». Денежные средства переводились в дальнейшем на QIWI-кошельки, с которых в дальнейшем перечислялись на сервис по обмену Биткоинов («Bitcoin», «BTC» - виртуальная интернет валюта, разработанная в «Силиконовой долине» США, не имеющая центра по обработке и хранению информации). В дальнейшем денежные средства переводились снова с

Биткоинов на расчетные счета мобильных телефонов, привязанных к пластиковым картам ОАО «Сбербанк России» № 42767, оформленной на имя К., № 4279, выданной в ОСБ на территории Республики Чувашии на Петрова Владимира Витальевича, 27.01.1978 г.р., зарегистрированного по адресу: Р.Чувашия, Чебоксарский район, ул., а также на банковскую карту ОАО «Альфа-Банк» №415482, выданной на имя Павла Л., так же Ш. В.И. использовал банковскую карту The Global Blue Card 308604. Дальнейшие действия по обналичиванию денежных средств поступивших на вышеуказанные реквизиты, осуществлялись знакомыми Ш.а В.И.- К., 12.03.1989 г.р., прож.: г. Миасс, М., 27.07.1993 г.р., А. 18.05.1994 г.р. которые в дальнейшем передавали полученные денежные средства через посредников, либо лично при встрече Ш.у В.И. получая свой процент.

25.03.2015г. следственно-оперативной группой управления «К» МВД России следователями СЧ ГСУ ГУ МВД России по Свердловской области по уголовному делу №150038120 проведено 6 обысков по адресам фигурантов.