**ПАМЯТКА ПО ПРОФИЛАКТИКЕ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ**

Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает стремительный рост преступлений, связанных с использованием информационных технологий.

**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.

**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, без знаков препинания, заглавными буквами и т.д.
5. Отсутствует фото товара, либо же 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).

9. Продавец принимает оплату только на анонимные реквизиты: электронные кошельки, пополнение мобильного телефона или на имя другого человека (родственника, друга и т.д.).

**Как не стать жертвами телефонных мошенничеств:**

* При телефонном звонке от имени якобы родственников и сообщении о трудной ситуации следует дозвониться до родных и близких, о которых идет речь, выяснить подробности случившегося, а не переводить и не отдавать деньги незнакомым людям;
* Перезвонить (а лучше всего подойти) в любое отделение банка, от имени которого пришло сообщение о проблемах обслуживания по расчетному счету/карте, и решить все возникшие вопросы. Можно также позвонить своим близким, которые хорошо разбираются в современных технологиях, рассказать о поступившем сообщении и спросить совета. Следует запомнить: ни один банк не будет просить владельца карты совершать какие-либо действия по телефону или сообщать реквизиты карты;
* Не сообщать незнакомым людям (как при личном контакте, так и по телефону или интернет-переписке) данные о себе, своих близких, родственниках, банковских картах, то есть любую конфиденциальную (личную)информацию;
* Не осуществлять предоплату за товар или обещанную выплату (услугу), производить оплату только при их фактическом получении.

**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 являются 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 (посылать по электронной почте) информацию о своих пластиковых картах. Преступники могут воспользоваться их реквизитами и произвести, например, различные покупки.

**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...».

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 Avito (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 Avito, 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: ее номер, код на обратной стороне, Ф.И.О. владельца карты и срок еѐ 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 также 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 якобы от 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 «вКонтакте» взломаны, пройдите регистрациюhttp:\\...»,

«вы выиграли автомобиль, подробности http:\\...” Новый тип сообщений с вредоносной ссылкой:

«я по вашему объявлению, согласны ли вы 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 небыли.

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 или 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 также 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 социальных 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.