ЛИСТОВКА

ОСТОРОЖНО МОШЕННИКИ!!!

Обращаемся к гражданам пенсионного возраста в первую очередь!!!

Если кто-то позвонил и просит деньги от имени родственников, не передавайте их, пока не уточните информацию у родственников по их личным номерам телефонов.

Не передавайте и не переводите деньги:

- за лекарства пока не согласуете информацию с лечащим врачом и не убедитесь, что это жизненно Вам необходимо;
- если позвонит кто-то представившись сотрудником правоохранительных органов;
- за снятие порчи.

По всем вышеуказанным фактам обращайтесь в «02».

ЛИСТОВКА

Полиция предупреждает!!!

Мошенники постоянно изыскивают все новые и новые варианты хищения чужого имущества! Будьте осторожны!!!

Не открывайте незнакомым людям, даже если они представляются работниками социальных служб, ЖКХ, поликлиники, и тд. До того как открыть дверь незнакомцу, позвоните в названную им организацию и уточните, направляли ли оттуда к вам специалиста. **Запишите все нужные телефоны заранее.** Телефоны социальных служб можно узнать в единой бесплатной справочной службе 09.

Не доверяйте, если Вам сообщают, что ваш родственник или знакомый попал в беду, и срочно нужна финансовая помощь. Это обман! Техника сегодня позволяет даже подделать голос человека. **Обязательно перезвоните близкому человеку или его окружению, узнайте все ли у него в порядке.** Позвоните в полицию, больницу, уточните, действительно ли родственник находится там. Сообщите о попытке мошенничества в полицию.

Вам поступил телефонный звонок или смс-сообщение, в которых сообщается о выигрыше, блокировке банковской карты, просьбе перечислить деньги знакомому, внести предоплату, отправить смс-сообщение для перехода на более выгодный тариф. **Не перезванивайте на номер звонившего, не принимайте никаких мер, не связавшись с официальными представителями указанной организации! Не открывайте в телефоне сомнительные ссылки из сообщений, используйте антивирусные программы!**

Будьте бдительны!!!

ПАМЯТКА
по профилактике мошеннических действий

Сеть Интернет, являясь крупнейшим средством обмена информац
то же время порождает стремительный рост преступлений, связан
использованием информационных технологий.

***Признаки мошенничества со стороны покупателя при прода
Интернете:***

1. Покупатель не особо интересуется товаром, быстро демонстр
свое желание сделать покупку и переходит к разговору о способе оплат
2. Покупатель просит вас назвать полные реквизиты карты, вкл
фамилию-имя латиницей, срок действия и CVC-код. При помощи
данных он сам легко сможет расплатиться вашей картой в Интернете.
3. Покупатель просит вас сообщить ему различные коды, кот
придут к вам на мобильный телефон, якобы необходимые ему
совершения платежа.

***Признаки мошенничества со стороны продавца при покупк
Интернете:***

1. Отсутствует адрес и телефон, все общение предлагается вести ч
электронную почту или программы обмена мгновенными сообщениями.
2. Отсутствует реальное имя продавца, человек прячется за «ником»
3. Продавец зарегистрирован на сервисе недавно, объявлени
продаже – единственное его сообщение.
4. Объявление опубликовано с ошибками, составлено небрежно,
знаков препинания, заглавными буквами и т. д.
5. Отсутствует фото товара, либо же приложен снимок из Интер
(это можно определить, используя сервисы поиска дубликатов картинок).
6. Слишком низкая цена товара в сравнении с аналогами у дру
продавцов.
7. Продавец требует полную или частичную предоплату (наприме
качестве гарантии, что вы пойдете получать товар на почте с опла
наложенным платежом).
9. Продавец принимает оплату только на анонимные реквизи
электронные кошельки, пополнение мобильного телефона или на
другого человека (родственника, друга и т. д.).

Как не стать жертвами телефонных мошенничеств:

– При телефонном звонке от имени якобы родственников и сообще
о трудной ситуации следует дозвониться до родных и близких, о котор
идет речь, выяснить подробности случившегося, а не переводить и
отдавать деньги незнакомым людям;

— Перезвонить (а лучше всего подойти) в любое отделение банк имени которого пришло сообщение о проблемах обслуживани расчетному счету/карте, и решить все возникшие вопросы. Можно т позвонить своим близким, которые хорошо разбираются в совреме технологиях, рассказать о поступившем сообщении и спросить со Следует запомнить: ни один банк не будет просить владельца к совершать какие-либо действия по телефону или сообщать реквизиты ка

— Не сообщать незнакомым людям (как при личном контакте, так телефону или интернет-переписке) данные о себе, своих бли родственниках, банковских картах, то есть любую конфиденциал (личную) информацию;

— Не осуществлять предоплату за товар или обещанную вы (услугу), производить оплату только при их фактическом получении.

Как не стать жертвой интернет - мошенничества:

— Следует внимательно изучить информацию интернет-сайта, отз сравнить цены за интересующий товар. Отсутствие информации, запута система получения товара зачастую являются признаками мошенничеств

— Получить максимум сведений о продавце или магазине: ад телефоны, историю в социальных сетях, наличие службы доставки и Действующие легально интернет-магазины или розничные прода размещают полную информацию и работают по принципу «оплата то после доставки»;

— Нельзя сообщать (посылать по электронной почте) информаци своих пластиковых картах. Преступники могут воспользоваться реквизитами и произвести, например, различные покупки.

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

1. Мошенничества, совершаемые с использованием мобильно проводной связи:

а) Сотовый и проводной телефон используется как средс передачи голосовой информации, подвиды, типы: «ваш сын попа аварию...», «мама/папа у меня проблемы...», «это из банка/соцзащит пр...».

б) Сотовый телефон используется для передачи СМС с ложн информацией: «мама, кинь мне на этот номер денег, потом все объясн «ваша карта заблокирована подробности по тел..», «с вашего счета спис 5000 рублей, подробности по тел...».

в) Сотовый телефон и ваше объявление в сети Интернет

Avito) используется мошенником для получения от вас данных кар привязки карты к мобильному телефону мошенника:

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

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

При получении сообщения не нужно перезванивать на указа номера. Мошенники могут потребовать передать деньги кур перечислить их на карту, номер мобильного телефона, попытаются полу от вас сведения о Вашей банковской карте, предложить пройти к банком совершить какие-либо операции у банкомата, попросят сообщить которые приходят к Вам на телефон.

В случае получения входящего звонка необходимо прекра разговор, даже если собеседник вселяет уверенность в своей правдивс Мошенники обладают психологическими приемами введения в заблужде либо обладают информацией о потерпевшем и его близких. Аналогич случаи мошенничества встречаются и в сети Интернет, но сообщени помощи передается посредством сообщения в социальной сети с ложн страницы родственника.

При сомнении в правдивости полученной информации след перезвонить близким от имени кого пришло сообщение, позвонить в бан указанному на карте, либо в договоре телефону, посетить ближай отделение банка. Банк никогда не запрашивает по телефону сведения о ка клиента: ее номер, код на обратной стороне, Ф.И.О. владельца карты и с её действия, а тем более пин-код. Если собеседник пытается получить от такую информацию, либо просит сообщить коды, которые пришли на Е телефон от банка, прекратите с ним разговор.

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

Если при мошенничестве, в ходе телефонного разговора преступник была получена информация о банковской карте, то необходимо позвонить

телефону указанному на карте и заблокировать карту. В день совер мошенничества необходимо обратиться в банк с заявлением о воз денежных средств на карту, так как банк обязан возвратить дене средства, если операция была оспорена владельцем карты в день операц

Для предотвращения мошенничеств также рекомендуем распространять в сети Интернет сведения о мобильных номерах привязкой к анкетным данным, не указывать мобильные номер социальных страницах, в подаваемых в сети объявлениях не указывать р с номером сотового телефона Имя и Фамилию, адрес жительства и др личную информацию. Не использовать в сети Интернет номера с мобильных телефонов, к которым привязаны банковские карты и но мобильных телефонов, которые используются для работы в «Мобил банке».

Последнее время получают распространение мошенниче совершенные в отношении пользователей сети Интернет продающих то на сайтах бесплатных объявлений. Продавцу поступает звонок якоб покупателя. Мошенник под видом покупателя сообщает, что же приобрести товар, но проживает в другом городе и предлагает опла товар путем перечисления денежных средств на карту продавца. Для этог просит продавца назвать номер карты, владельца карты, срок действия ка код на обратной стороне, а так же сотовый номер, привязанный к карте, к по умолчанию использует номер, указанный в объявлении. После получ этих сведений мошенник использует данные о карте для оплаты покуп сети Интернет. Другой вариант, когда на телефон продавца поступают к от банка и мошенник просит сообщать их якобы для перевода денег, в момент мошенник подключает к телефону потерпевшего, либо к сво телефону услугу «Мобильный банк» и похищает деньги с карты. Тре вариант, когда мошенник, выступающий в роли «покупателя» предла продавцу пройти к банкомату и, якобы произведя некоторые опера получить деньги, в трех указанных случаях мошенник похищает денеж средства продавца.

г) Сотовый телефон используется мошенниками для перед СМС сообщения, сообщений через мессенджеры Viber, WhatsAp вредоносной информацией.

Типы сообщений: «здесь наши с тобой фото http:\\...», «ваш акаку страница «вКонтакте» взломаны, пройдите регистрацию http:\\...», выиграли автомобиль, подробности http:\\..."

Новый тип сообщений с вредоносной ссылкой:

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

При получении данного сообщения откажитесь от прохождения указанной ссылке и активации полученных ссылок. По возможно проверьте есть ли в сети Интернет в поисковых системах сведения о данн

ссылках и возможных мошенничествах. Сообщите пользователям Интернет, что данная ссылка мошенническая. Удалите указанное сообщ если убеждены, что оно не нанесло вред Вашему устройству.

Вредоносные программы создаются и усовершенству мошенниками регулярно, и при работе с телефоном Вы можете столкнут видом вредоносных программ, которые не требуют Вашей активнос самостоятельно могут быть загружены на Ваше мобильное устройство уязвимости операционной системы.

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

Признаками заражения мобильного устройства могут блокирование операционной системы, блокирование входящих сообщений, отправка искусственно сгенерированных мобил устройством сообщений. Зараженный мобильный телефон сле немедленно выключить. Сим-карту перевыпустить у оператора, а тел сохранить для последующего изучения полицией, если было соверш мошенничество, либо передать в сервисный центр, если деньги похищен были.

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

Зараженное мобильное устройство так же является источни распространения вредоносной информации по контактам, содержащимс телефоне. Для предотвращения рассылки необходимо уведом максимальное количество знакомых о Вашей проблеме и о возмо приходящих от Вашего имени вредоносных сообщениях.

В случае если с Вашего телефона или банковской карты похит денежные средства необходимо в день совершения хищения обратитьс банк с требованием вернуть денежные средства, заблокировать ваш с запретить перевод денежных средств с вашего счета на другие сч приостановить обслуживание счетов на которые были перечислены ва денежные средства. После получения ответа от банка, с выпиской по сч обратиться в полицию.

Одним из распространенных мобильных мошенничеств также являе использование дубликата сим-карты для доступа к системам дистанционн управления банковским счетом. Признаком использования дубликата Ваш сим-карты является блокирование доступа мобильной связи. В этом слу необходимо срочно обратиться к мобильному оператору и перевыпусти

сим-карту. В случае подтверждения мобильным оператором несанкционированной замены Вашей сим-карты необходимо нап претензию в сотовую компанию и обратиться в полицию.

Можно избежать участи жертвы данных мошенничеств, следовать следующим рекомендациям:

- Для работы с банковскими картами, системами «Мобильный б «Банк-онлайн», «Интернет-банк» и др. использовать отдельное моби устройство, не предназначенное для разговоров и развлечения в Интернет;
- Не указывать номера мобильных устройств, используемых для ра с банковскими картами и дистанционного управления банковским сч как контактных в сети Интернет, в объявлениях и на страницах социал сетей;
- Приобрести и установить на мобильное устройство лицензио антивирусное программное обеспечение из официальных источников;
- Указать в договоре с банком, либо в иной форме согласова банком, что управление банковским счетом и проведение операций по к может осуществляться только с одного мобильного устройства с одним П ограничить круг операций, установить лимит, который можно переводи помощью мобильного устройства;
- Запретить перевод всего объема денежных средств с карты, счета.

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

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

б) Получение от интернет магазина, продавца товара, соответствующего заявленному.

Развитие данных видов мошенничества обусловлено человеческ факторами, такими, как желание сэкономить, отсутствие бли расположенных магазинов с таким товаром, полное отсутствие предложе на рынке. Основными приобретаемыми товарами являются предм роскоши: дорогая цифровая техника, автомобили, шубы, брендовые ве Исключены полностью факты приобретения товаров первой необходимо Желание сэкономить приводит зачастую к потере всех денежных средст связи с чем, первая и основная рекомендация - приобретать вещи за реальную стоимость и не искать предложений с 30-50% выгодой, так как противоречит в целом принципам рынка, либо присланный товар окаже подделкой, неисправным, либо не удовлетворяющим запросам покупателя.

Не стоит приобретать товары в интернет-магазинах позициониру себя как российские, но имеющие сайты в доменных зонах com .org .b .info .tv .mobi.

Особое внимание следует уделить отзывам в сети Интернет к да интернет-магазину, продавцу. Проверить когда был создан магазин, Создан ли он год и более назад. Если сайт существует меньше месяц стоит отказаться от покупки. Можно проверить наличие офиса у да магазина, удостовериться в сети Интернет, что такой дом сущест посмотреть его на карте, фото-снимках, панорамах Яндекс, Гугл. Убеди что на доме есть вывеска магазина, либо имеются офисные помещени снимках также можно узнать названия, телефоны близко расположе организаций, позвонить им и выяснить достоверность информаци интернет-справочниках найти телефоны администратора офисного це ресепшена, убедиться, что такой магазин или индивидуал предприниматель существуют и осуществляют свою деятельность в да здании. Полученную информацию следует использовать при общени телефону с сотрудниками магазина. Если магазин или прод отказываются звонить по телефону и предлагают другие способы обще такие как Viber, Skype, WhatsApp и другие, либо магазин телефона не им следует отказаться от покупки. В ходе общения по телефону мо сообщить, что находитесь в городе продавца, магазина и предложите заб товар самовывозом и оплатить наличными в офисе. В случае категорич отказа следует отказаться от покупки.

При приобретении дорогостоящих вещей, таких как автомоб дорожная техника, строительные материалы, рекомендуем потратить де на дорогу до города продавца и удостовериться в наличии продавца и тов Либо найти в городе продавца знакомых и попросить их провер достоверность предложения в сети Интернет. Если же такой возможно нет, то оплатить услуги юриста, сотрудника автофирмы, занимающейс городе продавца продажей и скупкой авто и за символическую пл предложить ему встретиться с продавцом и осмотреть авто и документы. касается и приобретения стройматериалов и металла – обратитесь к услу юриста в городе продавца. Любые присланные Вам по Интерн фотографии, сканы документов и автомобиля мошенники с легкост подделывают.

В настоящее время большинство интернет магазинов работаю по 10 предоплате, при соблюдении указанных рекомендаций можно соверш удачную покупку.

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

В случае необходимости приобрести товар через социальную необходимо тщательно проверить продавца, обязательно связаться с н телефону, расспросить подробности о товаре, потребовать фотог товара в деталях, предложить отправить товар курьерской служб наложенным платежом, обговорить возможность возврата т возможность самовывоза.

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

Широкое распространение в сети Интернет также приобрет мошенничества с привлечением средств пользователей для их приумноже в финансовых пирамидах, кооперативах, микрофинансовых организац биржах, букмекерских конторах, рынках электронных вал Правоохранительные органы настоятельно рекомендуют не вступать в ка либо отношения с такими организациями и лицами, предлагающими та услуги, так как многие компании и интернет сайты данных компа находятся за рубежом, организации работают по законам других государ либо изначально мошеннические, и вернуть затраченные на данные прое деньги практически невозможно.

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

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

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

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

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

При покупке авиа, железнодорожных билетов не ищите очень деш
билеты на сомнительных сайтах, тем более расположенных в домен
зонах .com .org .biz .net .info .tv .mobi . Доступные по цене билеты желате
приобретать на официальных сайтах компаний-перевозчиков.

ГУ МВД России по Волгоградской области