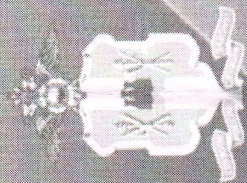


СТОП! **- МОШЕННИК -**



Не дай себя обмануть!
Звоните в полицию
102 или 112 !



ГУ МВД России по Ростовской области

! Подумай, кому
□ переводить деньги
! Будь внимателен
□ и бдителен
! Не дай себя обмануть
□

ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА

МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ СОВЕРШАЮТСЯ В ОСНОВНОМ ПУТЕМ СООБЩЕНИЯ ГРАЖДАНАМ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ.



Вам сообщают, что кто-то из близких попал в ДТП, больницу, совершил преступление, и ему срочно нужны деньги, после чего просят передать их лично или куда-либо перевести.

Поступает звонок или SMS от якобы сотрудника службы безопасности банка. Вам сообщают о блокировке карт, аресте счетов, незаконном списании средств с вашей карты и т.п., после чего просят сообщить им реквизиты карты и ваши персональные данные.

Вы получаете SMS или звонящий сам сообщает, что вы стали обладателем приза или победителем конкурса, далее следует просьба перечислить ему деньги под благовидным предлогом, как гарантию того, что награда попадет именно к Вам.

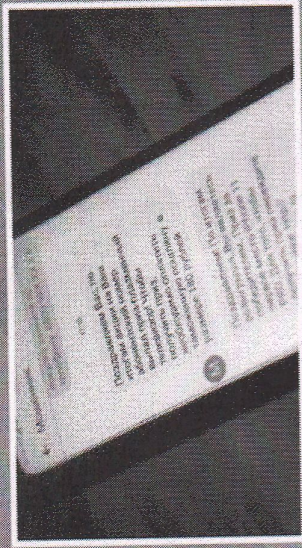
ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Позвоните своему близкому человеку, в больницу, в органы внутренних дел и проверьте информацию

Никогда не передавайте и не переводите деньги неизвестным людям

КИБЕРМОШЕННИЧЕСТВО

ВИРУСНОЕ ЗАРАЖЕНИЕ ПК ИЛИ СМАРТФОНА ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ДАННЫМ СИСТЕМ ОНЛАЙН БАНКИНГА И ПОХИЩЕНИЯ ДЕНЕГ С ВАШЕГО СЧЕТА;



На Ваш смартфон или компьютер поступает сообщение, либо письмо с любой информацией, которая способна Вас заинтересовать, при этом в данном сообщении содержится ссылка, по которой необходимо перейти.

Вы сами устанавливаете на свой смартфон или компьютер нелегитимное программное обеспечение. При этом не обращаете внимание, что предоставляете этой программе доступ к сети интернет, отправке SMS и т.д.

Вы теряете свой мобильный телефон с подключенной услугой «Мобильный банк».

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по SMS, MMS, электронной почте, мессенжерам, в том числе от имени банка

В случае потери мобильного телефона с подключенной услугой «Мобильный банк», следует срочно обратиться в контактный центр банка для блокировки услуги.

МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

МОШЕННИЧЕСТВА ПРИ ПОКУПКАХ ИЛИ ПРОДАЖАХ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ (ОНЛАЙН МАГАЗИНЫ, СОЦ СЕТИ, РЕСУРСЫ ОБЪЯВЛЕНИЙ).



Мошенники создают сайты-клоны торговых площадок с отличной репутацией (копируют интерфейс оригинального сайта), с небольшим отличием в доменном имени сайта. Вы отдаете деньги мошенникам, думая что покупаете товар.

Мошенники создают собственные интернет-магазины, как правило с товарами по цене существенно ниже среднерыночной, либо с большими скидками.

Вы размещаете в сети интернет объявление о продаже какого-либо товара.

Вам звонит мошенник и сообщает о своем намерении купить ваш товар, при этом просит сообщить данные вашей банковской карты для перевода на нее денежных средств.

ЧТО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДЕНЬГИ

Проверьте правильно ли Вы написали доменное имя сайта. Зайдите в раздел сайта, где размещены контактные данные сайта. Если указан лишь адрес электронной почты или телефон, воздержитесь от покупки. Проверьте дату регистрации сайта, если продавец работает недавно, лучше найти альтернативу.

Никому не сообщайте данные своей банковской карты.

«Осторожно, мошенники!»

В современном мире средства коммуникации развиваются стремительно. Они делают нашу жизнь комфортнее, многие вещи становятся доступнее и проще. Но любую технологию можно применить не только во благо. Мошенники не отстают от прогресса, совершенствуют свои методы «работы» и с удовольствием используют всемирную сеть интернет и мобильную связь для своих целей.

В нашем районе звонки или сообщения от мошенников поступали чуть ли не каждому второму жителю. Наивно предполагать, что жертвами этих злоумышленников становятся только пожилые люди, это далеко не так. Как поясняют сотрудники правоохранительных органов, на удочку криминальных элементов может попасть абсолютно каждый.

Рассмотрим типовые схемы мошеннических проявлений:

СМС рассылка.

В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

Оградить себя от подобного рода преступлений предельно просто. Прежде всего, необходимо быть благоразумным. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов? Знакома ли вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны ваши контактные данные? Если вы не можете ответить хотя бы на один из этих вопросов, рекомендуем вам проигнорировать поступившее сообщение.

Взятка.

Звонит телефон. Собеседник на другом конце провода представляется сотрудником правоохранительных органов, как правило, высокого звания и сразу в лоб заявляет, что сын/дочь/муж попал в дорожно-транспортное происшествие или сбил человека. Конкретики никакой. Чаше всего в процессе разговора жертва сама называет имя своего родственника. Затем поддается панике, что играет на руку мошенникам. Что называется, «берут в оборот».

Лжесотрудник даже может передать трубку другому человеку, который представится родственником и подтвердит вышесказанное, вот только долго поговорить не дадут. Если на этом этапе человека удалось ввести в заблуждение и тот начинает верить, то ему предлагают заплатить некую сумму денег, если такой суммы нет, то следует вопрос: «А сколько у вас есть?», в итоге мошенник соглашается на предложенные деньги. А дальше дело техники и индивидуального подхода к собеседнику.

В таком случае необходимо прекратить разговор и попытаться связаться с якобы попавшим в беду родственником. Стоит также отметить, что законодательством предусмотрена уголовная ответственность за дачу взятки должностному лицу.

Покупки в интернет-магазине.

Один из популярных способов мошенничеств, основанных на доверии, связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Как правило, мошенники привлекают своих жертв заниженными ценами и выгодными предложениями и требуют перечисления предоплаты путем перевода денежных средств на электронный кошелек.

Благодаримие поможет и здесь.

Внимательно изучите объявление, посмотрите информацию о лице, разместившем его. Если торговая площадка имеет систему рейтингов продавцов, изучите отзывы, оставленные другими покупателями, не забывая, однако, о том, что преступники могут оставлять положительные отзывы о себе, используя дополнительные учетные записи. Воспользуйтесь Интернет-поиском.

Иногда достаточно ввести в форму поиска телефонный номер или сетевой псевдоним продавца для того, чтобы обнаружить, что эти данные уже использовались в целях хищения денежных средств и обмана покупателей.

Неизвестные ссылки.

Если вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или какой-нибудь программы, не спешите открывать её. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто-то из знакомых вам людей, будет не лишним дополнительно убедиться в этом, ведь сообщение могло быть отправлено с зараженного телефона без его ведома. Если отправитель вам не знаком, не открывайте его.

Звонки и СМС из банка.

Самый лакомый объект — данные банковской карты, благодаря которой можно лишиться сразу всей суммы на счету. Например, поступает звонок или СМС от якобы сотрудника банка, что у вас заблокирована карта. При этом выливает поток абсолютно ненужной информации, не давая опомниться, и в процессе разговора вы сами диктуете необходимые данные или совершаете нужные манипуляции, находясь у банкомата.

В таких ситуациях необходимо игнорировать полученное сообщение, а состояние банковской карты или счета проверить, обратившись непосредственно в отделение банка либо используя официальный телефон службы поддержки клиентов.

В заключении статьи перечислим основные правила, соблюдение которых поможет Вам избежать обмана и не стать жертвой мошенников:

- Проверьте и убедитесь в достоверности информации, которую Вам сообщили по телефону, в СМС.
- Не торопитесь выполнить действия, которые от Вас требуют неизвестные.
- Не отправляйте СМС на короткие номера, указанные в СМС сообщении.
- Не открывайте файлы и ссылки, пришедшие в СМС сообщениях с неизвестных номеров.