К сожалению, вместе с появлением Интернета, который во многом в положительную сторону изменил нашу жизнь, появились и мошенники, пытающиеся похитить деньги у пользователей сети. О мерах безопасности рассказывают сотрудники полиции.

Чтобы не дать себя обмануть, нужно знать, схемы, по которым могут действовать мошенники. Одна из самых распространенных – рассылка электронных писем, с помощью чего злоумышленники пытаются получить персональные данные, пароли, сведения о банковском счете. Эта информация впоследствии используется для взлома аккаунта.

Также в подобных письмах могут содержаться различные рекомендации по заработку «легких» денег. Например, якобы если положить деньги на определенный счет, вам вернется сумма, в десятки раз превосходящая стартовую. Верить этим обещаниям не стоит.

Еще одна очень распространенная схема – это псевдорекомендации на форумах. Например, вы ищете какой-нибудь файл. На форуме открывается тема, в которой другой пользователь ищет то же самое. Админ скидывает ему ссылку и пишет, что нужно всего лишь принять смс. Затем пользователь размещает массу восторженных отзывов за помощь. Однако на самом деле, вероятнее всего, вы направите деньги злоумышленнику, а файл так и не получите.

Проявляйте осторожность при совершении покупок в интернет-магазинах. Всегда изучайте отзывы о подобных ресурсах. Не доверяйте тем, кто обещает брендовые товары по копеечной стоимости. Обратите внимание на срок существования сайта: если ему всего несколько дней, а в сети множество восторженных отзывов и ни одного негативного, то от покупки лучше воздержаться.

Еще один распространенный вид мошенничества – кардинг, то есть незаконное использование чужих банковских карт. Существует огромное количество способов получения персональных данных – от ложных сайтов до личных звонков. Например, вам могут позвонить и представиться сотрудником банка, попросив сообщить данные, указанные на карте. Ни в коем случае не делайте этого, если не хотите лишиться своих средств.

Если же вы стали жертвой мошенников, то немедленно обратитесь с заявлением в полицию. Чем быстрее вы оповестите органы внутренних дел о совершенном в отношении вас преступлении, тем выше вероятность задержания подозреваемого по горячим следам.

Стоп, мошенник! Не дай себя обмануть!

Полицейские рассказывают простые правила, чтобы не стать жертвой мошенников.

Сотрудники полиции призывают жителей Ростовской области быть бдительными! Видов мошенничества немного, но их вариаций достаточное количество, причем все они выгодны для мошенников. Даже при небольших финансовых потерях конкретного человека (15-150 рублей) срабатывает эффект масштаба, когда жертвами становятся тысячи людей. Один из самых распространенных видов мошенничества – телефонное. По телефону злоумышленники говорят, что родственник или другой близкий человек попал в беду:

- он попал в серьезное ДТП;

- совершил преступление и находится в правоохранительных органах;

- попал в больницу и ему прямо сейчас требуется дорогостоящая операция.

После того, как жертва ошарашена плохой новостью, мошенники продолжают давить на нее и предлагать прямо сейчас «решить вопрос» и спасти близкого. Нередко для подтверждения своих слов трубка передается «родственнику», который плачет и просит спасти его. Большинство людей, пострадавших от таких ситуаций, потом уверяли, что это

был голос их близкого человека. На самом деле мошенники используют состояние шока, в котором находится потенциальная жертва.

Затем преступники называют сумму, которую необходимо передать посреднику, перевести на карту или положить на номер телефона.

Так, например:

Неизвестный человек позвонил женщине-пенсионеру, 1933 года рождения, и сообщил, что ее сын убил человека и для «решения вопроса» ей необходимо передать 450 тысяч рублей. В назначенное время подъехал водитель и забрал указанную сумму. Через некоторое время, связавшись с сыном, женщина поняла, что с ним все в порядке и он находится дома, после чего написала заявление в полицию. Сейчас по данному факту возбуждено уголовное дело по части 3 статьи 159 УК РФ «Мошенничество». Полицейские проводят комплекс оперативно-розыскных мероприятий, направленный на установление и задержание участников противоправной деятельности.

Не дайте себя обмануть!

Столкнувшись с подобной ситуацией, необходимо соблюдать простые правила:

- никогда и никому не отправляйте и не передавайте деньги;

- позвоните своему близкому человеку;

- позвоните в органы внутренних дел, больницу и проверьте полученную по телефону информацию.

Если вы все-таки стали жертвой мошенников, незамедлительно обратитесь в ближайший отдел полиции.

Стоп, мошенник! Представляясь службой безопасности банка…

Сотрудники полиции напоминают о том, как не попадаться на уловки злоумышленников.

Еще одна разновидность телефонного мошенничества - «Ваша карта заблокирована». На мобильный телефон приходит СМС о блокировке карты, начислении денежных средств либо о списании комиссии за неуплату кредита. Для подтверждения или отмены операции необходимо связаться по указанному в сообщении номеру. На том конце провода трубку снимает мошенник. Основная его цель напугать жертву и заставить скорее совершить нужное действие, мошенники придумывают разные сценарии. Говорят, что банк заблокировал счет, начислил штраф за кредит или что проведена подозрительная операция. Далее злоумышленник просит продиктовать номер карты и трехзначный код, указанный на обратной стороне. После чего на номер телефона жертвы поступает СМС с кодом. Преступник, поторапливая ни о чем не подозревающего гражданина, просить назвать полученный код. В некоторых случаях телефонные мошенники просят абонента подойти к банкомату и там совершить несколько манипуляция, в результате которых со счета жертвы будут похищены деньги.

В других случаях мошенник сам звонит жертве. Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка». Мошенник сообщает о сомнительном переводе денежных средств с банковской карты либо о сбое системы. Преступник спрашивает у абонента подтверждение по данному переводу. Получив отказ, он предлагает отменить данную операцию, однако для этого он просит у вас полные данные карты, CVV- или CCV-код, код из СМС или пароли от Сбербанк Онлайн. Это нужно якобы «для сохранности ваших денег».

Результат в обоих случаях не заставит себя долго ждать – деньги с карты перейдут на счет мошенников.

В полицию обратилась жительница города Батайска. В своем заявлении она пояснила, что ей на телефон позвонил неизвестный и представился сотрудником одного из банков. После чего сообщил, что с банковской карты гражданки пытаются похитить деньги и для их сохранности необходимо продиктовать код из смс-сообщения, которое поступит на ее абонентский номер. Следуя инструкциям незнакомца, женщина сама перевела 52 тысячи рублей со своей банковской карты на неизвестные счета.

По данному факту следственными органами возбуждено уголовное дело по пункту «г» части 3 статьи 158 УК РФ «Кража». Полицейские проводят мероприятия по установлению лиц, причастных к противоправной деятельности.

Чтобы избежать подобного рода преступлений необходимо:

- при поступлении подобных смс ни в коем случае не сообщайте персональные данные неизвестным лицам. Даже если они представляются сотрудниками банка;

- при получении сообщений от банков, мобильных операторов о проблемах со счетом, обязательно перезвоните по официальному номеру банка и уточните нужные сведения. Банк никогда не запрашивает подобным образом информацию.

- не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам;

- сразу завершайте разговор. Сотрудник банка никогда не попросит у вас данные карты или интернет-банка.

Если вы все-таки стали жертвой мошенников, незамедлительно обратитесь в ближайший отдел полиции.

Стоп, мошенник! «Вы выиграли приз…»

В Ростовской области продолжается проект донской полиции «Стоп, мошенник!».

Сотрудники полиции в очередной раз объясняют гражданам, как не стать жертвой мошенников. Еще одна уловка, к которой прибегают преступники – сообщение о якобы полученном выигрыше (путевки, квартиры, бытовая техника, компьютеры и различные гаджеты). Суть его состоит в том, что совершаются e-mail или смс-рассылки с текстом о получении адресатом ценной вещи. Важная деталь, которая сразу же обращает на себя внимание - для получения выигрыша организаторы просят сделать перевод некоторого количества денег либо перейти по ссылке для заполнения анкеты.

В качестве причины могут называть:

- выплату налогов;

- уплату таможенной пошлины;

- компенсацию транспортных расходов;

- проверку подлинности личности, работоспособности карты или электронного кошелька.

В сравнении со стоимостью приза размер требуемой к переводу суммы выглядит незначительным. После ее получения мошенники перестают оставаться на связи либо входят во вкус и предлагают совершить дополнительный платеж для оформления ценного выигрыша.

В полицию обратилась жительница города Таганрога и сообщила, что стала жертвой мошенников. Гражданка пояснила, что ей на телефон пришло смс-сообщение. В нем говорилось о том, что женщина стала победителем мобильной лотереи. Чтобы забрать приз, нужно было позвонить по номеру, указанному в сообщении. Когда потерпевшая позвонила по данному номеру телефона, ей сообщили, что для получения призовых денег в сумме 1 500 000 рублей, нужно оплатить таможенную пошлину в размере 75 тысяч рублей. После перечисления денег, злоумышленники перестали выходить на связь.

По данному факту следственные органы возбудили уголовное дело по части 2 статьи 159 УК РФ «Мошенничество». Полицейские проводят мероприятия по установления подозреваемых в совершении данного преступления.

Меры, чтобы себя обезопасить:

При получении сообщения о внезапном крупном выигрыше стоит вспомнить, подавали ли вы заявку на участие.

Не нужно говорить «организаторам» данные своих банковских карт или спешить переводить деньги за якобы оплату членского взноса, оформления документов или чего-то другого.

Не переходите по ссылкам в полученных электронных письмах и смс.

Если вы столкнулись с подобными мошенническими схемами, незамедлительно обратитесь в полицию.

Стоп, мошенник! Вирусная рассылка сообщений

Сотрудники ГУ МВД России по Ростовской области в рамках проекта «Стоп, мошенник!» продолжают предостерегать граждан от различных махинаций, к которым прибегают кибер-мошенники. Нередко злоумышленники для похищения денег используют номера телефонов с сайтов по продаже товаров и услуг либо нелегально покупают базы номеров. В дальнейшем, используя специальную программу, мошенники рассылают смс-сообщения с определенной ссылкой, переходя по которой устройство заражается вредоносной программой. «Вредонос» собирает и передает своему владельцу данные необходимые для хищения денег с банковского счета либо со счета мобильного оператора.

Мошенники придумывают разнообразные предлоги, чтобы подтолкнуть ни о чем не подозревающего человека перейти по предложенной ссылке. Например, «ваша карта заблокирована, перейдите по ссылке для ее разблокировки», «мне прислали твою фотографию, я и не мог подумать, что ты так поступишь (далее следует текст ссылки)», «меня заинтересовало твое предложение о продаже (платья, дивана, телевизора и т.д.) далее следует ссылка».

Подобную мошенническую схему похищения денег использовали семеро участников организованной группы, которых задержали сотрудники уголовного розыска. Причиненный ущерб превысил 18 миллионов рублей. Сейчас в отношении подозреваемых возбуждено уголовное дело по статье 159 УК РФ «Мошенничество».

Единственное правило, которому следует придерживаться гражданам, чтобы обезопасить свои сбережения, это не переходить по сомнительным ссылкам в сообщениях.

Если в отношении вас были совершены противоправные действия незамедлительно обратитесь в ближайший отдел полиции.

Стоп, мошенник! Срочно переведи деньги, потом объясню

Сейчас практически каждый человек имеет страничку в различных социальных сетях. Однако смекалка мошенников находит все новые комбинации для незаконного обогащения. Злоумышленники взламывают аккаунты пользователей социальных сетей, изучают переписки и стили общения человека со знакомыми. А затем производят рассылку друзьям потерпевшего с просьбой занять определенную сумму денег на один день. В любой из социальных сетей вам может прийти сообщение от знакомого, где он рассказывает драматичную историю, которая вызывает желание помочь (попал в ДТП, тяжело болен сам или родственник и т.д.). Как правило, информацию проверять не спешат, воздействуют на эмоции, пользователь верит, что нужна помощь и ее оказывает, пересылая деньги мошенникам.

Так, в полицию обратилась жительница Тарасовского района Ростовской области. Девушка рассказала полицейским, что в одной из популярных сетей ей написала подруга. В сообщении она сказала, что ее матери требуется срочная дорогостоящая операция и попросила одолжить 25 тысяч рублей. Заявительница не задумываясь отправила деньги, на присланный номер банковской карты. Через некоторое время она решила позвонить подруге, однако оказалось, что с ее мамой все в порядке, а страницу взломали и писали от ее имени.

Сейчас полицейские занимаются поиском злоумышленников. Возбуждено уголовное дело по статье 159 УК РФ.

Способ разоблачения подобных махинаций – это проверка информации. Не поленитесь потратить время, чтобы совершить звонок знакомому, который обратился за помощью. Либо вы можете задать контрольный вопрос, который будет знать только этот человек.

Если вас все-таки обманули, обратитесь в полицию. Чем быстрее вы оповестите органы внутренних дел о совершенном в отношении вас преступлении, тем выше вероятность задержания подозреваемого по горячим следам.

! СТОП !
МОШЕННИК !

ТЕЛЕФОННЫЕ МОШЕННИЧЕСТВА

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

Вам поступает звонок якобы сотрудника правоохранительных органов (ФСБ, СК, прокуратура, полиция). Звонящий сообщает, что вы стали жертвой мошенника и требует оказать помощь в их поимке, угрожая уголовной ответственностью за отказ или разглашение информации. Под страхом наказания запрещают говорить о случившемся даже родственникам и близким. Следующий звонок поступает уже от якобы сотрудника банка, он предлагает произвести операции для поимки мошенников: перечислить деньги на безопасный счет, оформить кредит, пока на вас его не оформили злоумышленники и др.

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 СМС 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 СМС 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 проверьте информацию
Никогда не передавайте и не переводите деньги незнакомым людям. Не верьте в безопасный счет – это уловка

КИБЕРМОШЕННИЧЕСТВО

ВИРУСНОЕ ЗАРАЖЕНИЕ ПК ИЛИ СМАРТФОНА ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ДАННЫМ СИСТЕМ ОНЛАЙН БАНКИНГАИ 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 не лицензионное программное обеспечение.
При этом не обращаете внимание, что предоставляете этой программе доступ к сети интернет, отправке СМС 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 СМС, ММС, электронной почте, мессенжерам, в том числе от имени банка

МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

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

В сети широко распространена реклама биржевых площадок, обещающих крупные заработки от инвестиций в короткие сроки. Стоит зарегистрироваться и ввести данные, как вам сразу же позвонит лжеброкер и расскажет о том, как много вы можете заработать не выходя из дома. Причем заработок будет тем больше и быстрее, чем больше средств вы внесете на свой счет на торговой площадке. Как только вы перечислите средства на якобы ваш счет, вы их не сможете вернуть обратно. И виртуальные заработки на бирже так и останутся виртуальными

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. Никому не сообщайте данные своей банковской карты. Относитесь с осторожностью к предложениям получения прибыли в короткие сроки, таким предлогом пользуются аферисты, пытающиеся похитить деньги!

БУДЬТЕ БДИТЕЛЬНЫ!
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Если вам поступают звонки
от службы безопасности банка,
различных правоохранительных органов
о небходимости перевода
денежных средств
на другие лицевые счета,

ЗНАЙТЕ - ЭТО МОШЕННИКИ!