|  |
| --- |
| **SMS -  мошенничество.  Популярные схемы** |

**Обман, основанный на доверии, самый распространенный вид мошенничества. Только бдительность поможет защититься от обмана. Бдительность и знание  методов, которые используют мошенники в своих схемах. О некоторых из них речь идет ниже. Зная их, вы сможете защитить себя от обмана!**

Тема мобильного мошенничества привлекает все большее внимание потребителей сотовой связи. Около 10 млн. абонентов считают себя в той или иной мере пострадавшими от действий мобильных мошенников.

**Подарок от «Кати»**Вам приходит SMS интригующего содержания: «Отправлена ММS-открытка или получен ММS-подарок от «Катя» для абонента с номером +7...» И далее вы видите свой номер и ссылку для скачивания. Не спешите. При нажатии на ссылку на телефон скачивается и автоматически запускается java-приложение, содержащее вредоносное ПО, которое отсылает смс с переводом средств на номера мошенников. Затем злоумышленники в течение короткого времени выводят средства со своих мобильных счетов.

***Совет:*** используйте правило защиты от СПАМа: старайтесь не переходить по ссылкам, пришедшим с неизвестных номеров.

**Бесплатно только 24 часа**Вы хотите получить доступ к интересному контенту, например, нашли в Интернете фильм или книгу, которую давно искали. Получить ее легко и просто - отправить SMS с кодом активации.  
**ИЛИ**Вам предлагают загрузить новинки кинопроката, установить местонахождение абонента или получить сумасшедшие скидки! Все, что нужно, - отправить SMS с кодом активации. Казалось бы, это просто и так удобно! Но время идет, а доступ не активируется, кроме этого с баланса мобильного телефона начинают списываться деньги.

Следует быть внимательными к условиям получения сервиса, напротив которых вы установили галочку «согласен», не ознакомившись с ними подробно. Как правило, в таких случаях указано, что сервис является «тестовым» и предоставляется бесплатно только в первый день пользования, а затем стоимость доступа к контенту указана посуточно и для отказа от него нужно отписаться, позвонив в центр поддержки клиентов или зайдя на тот же сайт.

***Рекомендации:*** перед тем, как отправить SMS на короткий номер и подписаться на какую - либо услугу, прочитайте условия предоставления этой услуги, обращая особое внимание на условия оплаты.

**Вирус - блокиратор (Trojan Winlock)**  
В настоящее время отмечен всплеск мошенничеств, связанных с модификацией вируса Trojan Winlock. Во время работы за компьютером вместо необходимых страничек пользователи Windows обнаруживают на экране объявление примерно следующего содержания: "Ваш Windows заблокирован. Microsoft установил некорректное пользование Интернетом с вашего компьютера. Вы просматривали сайты, содержащие ненадлежащую информацию/имеющие порнографический контент. Попытка перезагрузить ваш компьютер приведет к необратимым последствиям. Если не принять мер, в течение 12 часов после получения данного сообщения все данные, включая Windows и Bios, будут полностью удалены. Для устранения блокировки вы должны в течение 12 часов внести 300 рублей на телефон "Билайн" номер х-ххх-ххх-хх-хх (указан частный номер). Вы можете сделать это в ближайшем пункте приема платежей. После этого на ваш телефон придет сообщение коде/ либо на чеке об оплате будет указан код, по которому сможете разблокировать ваш Windows".

***Рекомендация:*** Ни в коем случае не стоит выполнять указания мошенников и пополнять счет неизвестного абонента. Для того, чтобы мы смогли заблокировать телефонный номер мошенника, просьба сообщить его в центр поддержки клиентов "Билайн" по номеру 0611. Для разблокировки компьютера следует обратиться в центр технической поддержки своего интернет- провайдера или к одному из разработчиков антивирусного ПО, например Dr.Web и Лаборатория Касперского. После того, как баннер исчезнет с рабочего стола, обязательно проверьте компьютер на наличие вирусов.

**Ваш выигрыш - автомобиль!**Абоненту поступает звонок или смс якобы от крупного автосалона с информацией о том, что в рамках празднования годовщины салона он выиграл автомобиль.

Информацию о розыгрыше можно посмотреть на официальном сайте автосалона, подробности - получить по телефонам, указанным на том же сайте. Сайт, который вы вслед за этим посещаете, сделан качественно. Телефоны работают исправно. Тем не менее, он фальшивка. На ваш вопрос, откуда у звонившего ваш номер телефона, вы слышите, что ваш оператор связи является партнером акции и, соответственно, поделился вашими контактами с автосалоном. В другом варианте "развода" вам предельно четко объясняют механику акции и просят не торопиться с принятием решения, все обдумать и перезвонить в салон чуть позже. Когда вы звоните, то самостоятельно представляетесь, называете свой номер телефона и слушаете рекомендации оператора по дальнейшему участию в акции.

В любом случае, в конечном итоге вы услышите, что для выдачи приза требуется внести взнос за выигрыш/участие через терминал оплаты. Какой-то странный способ вручить вам выигрыш, не правда ли?

***Рекомендации:*** даже если вам кажется правдоподобными информация на сайте и разговор с оператором, настораживающим моментом должна стать сама просьба проследовать к терминалу оплаты для выполнения каких - либо действий.

**Лже-звонок от технической службы оператора**Наиболее распространенная в последнее время схема обмана такова: раздается звонок, приятный голос сообщает (как вариант - приходит смс), что происходит перенастройка сети и необходимо перенастроить телефон на новые параметры, соответственно, нужно набрать комбинацию цифр и знаков. Иногда диктуют, иногда присылают в смс. После набора комбинации со счета списываются денежные средства.

Эта схема мошенничества, которую мы называем "лже-звонком от технической службы оператора", сегодня одна из самых распространенных. В большинстве случаев эта схема осуществляется с помощью услуги "Мобильный перевод". Распознать мошенников достаточно просто - они действуют очень настойчиво и требуют незамедлительного выполнения их действий. Абоненту любого оператора связи следует знать, что у оператора миллионы абонентов, и настройки на сети совершаются таким образом, чтобы быть незаметными пользователям.

В связи с тем, что пользователь совершает перевод средств добровольно, то оператор связи, к сожалению, не имеет юридического права вернуть ему переведенные на другой счет средства.

Основная наша рекомендация: не выполнять указания неизвестного лица и не вводить под диктовку коды на своем телефоне. Необходимо проверить информацию, перезвонив в абонентскую службу своего оператора связи.

**Мошенническая подписка на платные сервисы**Не так давно возник новый вид мобильного мошенничества, при котором у абонентов сотовых операторов ежедневно снимаются деньги за сервисы, которые они не заказывали. При выяснении причин возникшей проблемы, оказывается, что они вводили на каком-либо Интернет-сайте номер своего сотового телефона и код активации на пробный день подписки на какую-либо услугу. При этом правила пользования услугой и информация о том, что от нее необходимо отписаться в случае нежелания ее использовать в дальнейшем, представлена на сайте в неявном виде. Таким образом, абоненты, не прочитав правила о необходимом отказе от этой услуги, на следующий день автоматически оказывались подписанными на сервис, в результате чего происходило ежедневное списание средств с их телефонных счетов.

***Рекомендации:*** Всегда внимательно читайте условия и стоимость предоставления сервисов, которыми пользуетесь, не ставьте автоматически галочку напротив строки "Я согласен". Иначе Вы можете добровольно подписаться на сервисы, которые не заказывали, и при этом с Вас будут списываться суммы, о которых Вы не подозреваете.

**Интернет-баннер**Новый вид мошенничества, успевший стать достаточно распространенным в короткие сроки. Суть обмана заключается в том, что во время пользования Интернетом на вашем компьютере неожиданно появляется рекламный баннер, который довольно сложно закрыть рядовому пользователю ПК (хотя специальные команды на компьютере позволяют это сделать). Чтобы убрать этот мешающий работе баннер, вам предлагается отправить SMS на платный короткий номер и получить код для его удаления, однако баннер может не исчезнуть, а средства спишутся с вашего счета.

Рекомендации: Если у Вас не получается удалить навязчивую рекламу самостоятельно, Вы можете зайти по ссылке [**http://www.freedrweb.com/cureit/**](http://www.freedrweb.com/cureit/) и воспользоваться бесплатной программой разработчика антивирусного ПО "Доктор Веб" - Dr.Web CureIt! Или обратиться за технической помощью в центр поддержки клиентов своего Интернет-провайдера.

**Ваша кредитная карта заблокирована!**В последнее время мошенники разнообразили схемы обмана абонентов, включив в свой арсенал финансовые учреждения. Так, участились случаи получения абонентами SMS, содержащих текст: "Ваша банковская карта заблокирована" и номер телефона, на который нужно перезвонить. После того, как абонент звонит по номеру, мошенники ему сообщают, что на банковском сервере произошел сбой и просят сообщить реквизиты банковской карты для устранения неполадок. Затем мошенники используют полученные реквизиты банковской карты для покупок через Интернет.

***Рекомендации:*** Не поддаваться первому импульсу и стараться проверять информацию, поступившую от неизвестных лиц. Стоит помнить, что сотрудникам банков запрещено пытаться узнать информацию о реквизитах банковских карт клиентов. Получив подобное сообщение, постарайтесь проверить поступившую от неизвестных информацию, позвонив в call-центр своего банка.

**Случай с родственниками**Мошенник представляется родственником, другом или сослуживцем Вашего родственника и взволнованным голосом сообщает, что с ним приключилась беда (попал в аварию, сбил человека). Беда, как известно, не приходит одна. Вот и у пострадавшего во время аварии сломался телефон (сели батарейки, отобран бандитами, потерялся) и приходится звонить с чужого. Предстоит еще очень много звонков, поэтому необходимо пополнить человеку баланс. Находясь в стрессовом состоянии или замешательстве, люди легко соглашаются помочь. Мошенники начинают раскручивать своих "родственников" на наличные. После пополнения баланса они перезванивают и с облегчением сообщают, что конфликт улажен - от пострадавших в ДТП сторон удалось откупиться. Нужно лишь в условленном месте передать посредникам деньги. Передавая необходимую сумму, человек и не подозревает, что делает очередное добровольное пожертвование.

***Рекомендация:*** для того чтобы распознать обман и не лишиться крупной суммы денег, постарайтесь связаться с родственником напрямую либо через друзей и знакомых; попросите звонящего описать внешность Вашего родственника и ответить на вопросы личного характера.

**Ложный приз**На мобильный телефон абонента звонит лже-ведущий известной музыкальной радиостанции и поздравляет с выигрышем ценного приза. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию. Дозвонившегося поздравляют, он передает приветы, заказывает песню и узнает еще одну приятную новость: он не просто получит приз - телефон - его сразу же подключат, нужно лишь срочно купить карту пополнения счета вышеназванной компании и сообщить ее данные диджею. Заплатив деньги и придя через несколько дней за подарком, обманутый абонент узнает, что на радиостанции никто подобного конкурса не проводил, так что долгожданного телефона он не получит. Да и купленная карточка уже не пригодится - "награждающие" давно перевели с нее деньги на свои счета.

***Рекомендация:*** радиостанции обычно проводят розыгрыши призов в прямом эфире - включите радиостанцию и проверьте информацию о розыгрыше.

**Лже-работа**Новый вид мошенничества: объявления с предложением стабильной работы с жильем и высокой зарплатой. Для получения информации о работе в них предлагается отправить SMS или позвонить на короткий номер (повышенная стоимость SMS или платный автоответчик).

***Рекомендация:*** как правило, крупные агентства по подбору персонала, от имени которых действуют мошенники, предоставляют информацию обо всех вакансиях бесплатно и, скорее всего, после отправки смс вам придет информация о вакансии, размещенной в свободном доступе в интернете.

**СМС-просьба**Абоненты сотовых операторов получают смс с просьбой: "У меня проблемы, позвони по такому-то номеру. Если номер не отвечает, положи на него деньги и перезвони". Некоторые абоненты, особенно люди пенсионного возраста, пополняют счет мошенников, думая, что пишет кто-то из близких людей.

***Рекомендация:*** если Вы подумали, что помощь требуется Вашему родственнику, знакомому, другу, - постарайтесь связаться с ним по известному Вам номеру.

**Жизнь без спама**Абоненту приходит SMS с предложением отписаться от рекламной SMS-рассылки. Для того чтобы отписаться, предлагается отправить "бесплатное" SMS определенного содержания (чаще всего это набор цифр) на один из коротких номеров и перейти по полученной в ответ ссылке, чтобы исключить номер из списка рассылки рекламных сообщений.

***Рекомендация:*** не верьте подобного рода сообщениям. Отписаться от предложений, присылаемых вам различными компаниями, в которых вы оформляли дисконтные карты, оставляли контактные данные с согласием получать информацию рекламного характера и т.п. вы можете либо самостоятельно, либо с помощью оператора, позвонив в центр поддержки клиентов.

**Ошибочный перевод средств**Человек получает SMS, оповещающее о поступлении средств на его счет, переведенных якобы с помощью услуги "Мобильный перевод". Сразу же после этого ему звонит мошенник, который утверждает, что только что перевел деньги на его номер ошибочно и просит вернуть деньги обратно тем же "Мобильным переводом".

***Рекомендация:*** проверьте баланс Вашего счета, убедитесь, что он был пополнен на указанную незнакомым человеком сумму, после этого принимайте решение.

**Спасение от компьютерного вируса**Последнее время активизировался новый тип компьютерного вируса Trojan.Winlock и его модификация (Trojan.Winlock.origin), который блокирует работу компьютера и за разблокировку просит отправить смс на короткий номер. После отправки смс, разблокировки, естественно, не происходит, при этом у абонента со счета списывается большая сумма средств.

***Наши рекомендации:*** необходимо позвонить в Центр поддержки клиентов по номеру 0611 и назвать короткий номер для отправки смс, который используется хакерами. Это поможет оперативно заблокировать этот короткий номер и принять меры в отношении недобросовестного партнера, которому этот номер принадлежит.

**Открытка - подписка**Человек получает от мошенников SMS, оповещающее его о том, что он может посмотреть присланную ему поздравительную открытку со своего сотового телефона, пройдя по указанной ссылке. После перехода по ссылке абонент автоматически подписывается на один из платных сервисов или "цепляет" вирус, в результате чего в последующем происходит ежедневное списание средств с его телефонного счета.

***Рекомендации:*** Наша рекомендация - получив SMS или MMS от неизвестного отправителя с предложением перейти по ссылке, отнеситесь к этому с осторожностью. Вряд ли кто-то из ваших друзей и знакомых станет делать Вам анонимные подарки.

**Голосовое письмо/поздравление**Схема обмана такова: абонента информируют о том, что он получил голосовое поздравление с праздником, прослушать которое он может, набрав определенный код. Этот код на самом деле является не чем иным, как зашифрованной командой на мобильный перевод средств со счета абонента или звонком на платный номер.

***Рекомендации:*** Голосовое письмо является бесплатным для получателя. Идентифицировать настоящее голосовое письмо достаточно просто. Система присылает SMS с номером, начинающимся на #00…., набрав который можно прослушать голосовое письмо. Отправитель - идентифицируется. Вряд ли кто-то из Ваших близких станет отправлять поздравления анонимно, и, если номер друга не указан, знайте - это очередная уловка мошенников.

**Вирус для мобильных устройств**В России появились новые вирусы для смартфонов и коммуникаторов, которые инициируют рассылку SMS на платные номера. Вирус может попасть в мобильное устройство через MMS, Интернет или через программы, скачанные из непроверенных источников. После заражения смартфона он начинает рассылать огромное количество SMS на специальные платные короткие номера, принадлежащие мошенникам.

***Рекомендации:*** Поскольку смартфоны и коммуникаторы также стали уязвимы, с точки зрения вирусных атак, не следует открывать MMS от неизвестного отправителя, переходить по ссылкам в Интернете, пришедшим с неизвестных номеров, а также устанавливать на мобильное устройство неизвестное программное обеспечение.

**Пожертвуйте деньги на благотворительность!**В поисках наживы мошенники прибегают даже к таким методам, как выкачивание денег из людей, готовых помочь нуждающимся. Так, например, происходит рассылка сообщений с указанием платного номера, на который абоненту нужно позвонить или отправить SMS, чтобы внести свой благотворительный вклад. Очень часто мошенники используют широко освещаемые в СМИ трагедии. Например, после взрывов в московском метро в марте 2010 года участились случаи обращения мошенников к абонентам с призывом "собрать деньги в помощь жертвам терактов".

***Рекомендации:*** Мы советуем обязательно уточнить информацию о проведении подобных благотворительных акций - по бесплатному номеру Центра поддержки клиентов "Билайн" 0611 или на сайте [**www.safe.beeline.ru**](http://www.safe.beeline.ru/). Если информация поступила не с короткого, а с частного номера, советуем в обязательном порядке перепроверять данные через Интернет или известные благотворительные фонды.

**Отправь SMS и перейди на более выгодный тариф!**Данный метод обмана достаточно популярен среди мошенников. Абонент, не обращая внимания на то, что отправителем сообщений является не их оператор, откликается на предложение из разряда "Отправь SMS на короткий номер, чтобы перейти на более выгодный тариф! Все локальные звонки - теперь безлимитные!". В итоге он остается с прежним тарифом, но теряет деньги, так как номер, на которой он отправлял SMS, был платным.

**Платный код или «Акции» оператора**Абонент получает сообщение об акции, проводимой его оператором. По условиям "акции", абонент до конца недели (месяца, года, жизни) получает возможность осуществлять бесплатные звонки по стране. Для этого ему необходимо всего лишь отослать в службу информационной поддержки (телефоны прилагаются) "оператора" коды нескольких карт оплаты. Естественно, выясняется, что оператор никаких акций не проводил, а карты оплаты пополнили счета мошенников.

***Рекомендация:*** не выполняйте действий под диктовку неизвестного Вам человека, как бы правдоподобно он не описывал условия акции. Перезвоните в абонентскую службу Вашего оператора связи и проверьте информацию.

**Кражи, разбой и фальшивые аппараты**  
Огромное количество мобильных телефонов, выпускающихся в наше время, привело к тому, что случаи потерь и краж мобильных телефонов приобрели массовый характер. Количество краж мобильных телефонов превышает показатели любого другого вида краж, в том числе и квартирных. Этот вид хищения поражает огромным количеством способов отъема средств связи у владельцев. Как основные виды можно выделить обман, игру в доверие, кражу и разбой.

Обман происходит очень просто. На улице к вам подходят с просьбой позволить перезвонить больной матери или детям домой, ссылаясь на севший аккумулятор и срочность звонка. Вы проявляете понимание, и через минуту телефон возвращается к Вам, а вот количество наличных на счету сильно уменьшается - либо звонок совершается на платный номер, либо набирается определенная комбинация цифр, позволяющая перевести средства на счет другого абонента

Порой жертвы после кражи сами поражаются своей наивности. Допустим, на остановке к вам обращаются с просьбой дать мобильный телефон, дескать, срочно нужно позвонить. Вы проявляете понимание, и злоумышленник во время разговора отдаляется от вас и определенный момент садиться в машину соучастника и уезжает с вашим телефоном.

Игра в доверие является разновидностью обмана. Преступник, сославшись на разряженную батарею телефона, просит вставить в ваш аппарат свою сим-карту, чтобы сделать срочный звонок. Потом просит подождать, пока сходит в машину за номером, а свой телефон оставляет вам в залог. После долгих ожиданий вы понимаете, что у вас в руках остался искусно сделанный муляж. Такие же муляжи зачастую продают любителям приобрести технически продвинутую модель за небольшие деньги.

***Рекомендация:*** Не отдавайте телефон в руки незнакомца. Если Вы хотите помочь, предложите самостоятельно набрать нужный номер и передать информацию.

**Проверка пластиковой карты через банкомат**Суть мошенничества заключается в следующем: абонентам приходит СМС-сообщение следующего содержания (дословно, с сохранением орфографии и пунктуации): «(bank) Заявка с карты 5.500р. Принята. Инфо 8(ххх) ххх-хх-хх». При этом в сообщении могут быть указаны другие суммы и номера телефонов. Естественно, обеспокоенный абонент перезванивает на указанный, якобы, информационный номер, где трубку берет мужчина и представляется «службой финансового контроля». На вопрос, о чем идет речь, собеседник отвечает, что, скорее всего это ошибка, с которой будет разбираться «служба безопасности банка». Но для того чтобы избежать перевода денег, необходимо отправиться к банкомату, перезвонить снова и выполнить несколько действий с пластиковой картой под диктовку мнимого сотрудника банка.

В данном случае следуя указаниям мошенников, абонент совершает процедуру перевода денег на счет чужого мобильного телефона со своего личного банковского счета, привязанного к пластиковой карте. Причем при этом абонент сознательно выбирает опцию «оплатить услуги сотовой связи».

***Рекомендация:*** Абонента должна изначально насторожить просьба незнакомого человека выполнить какие – либо действия со своей платежной картой и при помощи банкомата. Мы хотели бы еще раз напомнить, что ни сотрудники банка, ни сотрудники оператора никогда не предлагают осуществить «проверку карты» подобным образом. Если вам приходит подобного рода сообщение, советуем связаться непосредственно с банком по указанному на карте номеру для проверки информации по последнему списанию средств. Скорее всего, сотрудник банка опровергнет информацию, содержащуюся в смс-сообщении якобы от «службы финансового контроля».

*По материалам сайта*[***http://safe.beeline.ru***](http://safe.beeline.ru/)

https://www.potrebitel-russia.ru/?id=573