

ТОРЖОКСКАЯ МЕЖРАЙОННАЯ
ПРОКУРАТУРА

МО МВД РОССИИ «ТОРЖОКСКИЙ»

A black rectangular warning sign with a white border. At the top left is a white triangle containing a black exclamation mark. To the right of the triangle are three white icons: a speech bubble with 'SMS', an envelope with '@', and a telephone handset with a diagonal slash through it. Below the icons is the Russian text 'ОСТОРОЖНО, МОШЕННИКИ!' in white capital letters.

ОСТОРОЖНО, ТЕЛЕФОННЫЕ МОШЕННИКИ!

В повседневной жизни используется множество разнообразных высокотехнологичных устройств — пластиковых карт, мобильных телефонов и компьютеров.

Постоянно появляющиеся новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определенных навыков и знаний. Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

Предлагаем Вам понятию и полезную памятку. Внимательно ознакомьтесь с ее содержанием и следуйте нашим рекомендациям. Они защитят Вас от действий мошенников и сэкономят Ваши средства.

Телефонное мошенничество

Чаще всего в сети телефонных мошенников попадают пожилые или доверчивые люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

Основные схемы телефонного мошенничества:

Обман по телефону: требование выкупа
КАК ЭТО ОРГАНИЗОВАНО:
Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинен в совершении того или иного преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжелых телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции.

Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привести в оговоренное место или передать какому-либо человеку.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕ:

В организации обмана по телефону с требованием выкупа участвуют несколько преступников.

Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набрата телефонного номера наврал, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама случайно подпадает под его о ком она волнуется.

Если жертва преступления поддается на обман и согласилась привести указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопроводжают жертву лично.

Мошенники стараются заставить жертву не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег.

После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщает, где он может увидеть своего родственника или знакомого.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ.

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идет речь. Если телефон отключен, позвоните связаться с его коллегами, друзьями и родственниками для уточнения информации.

Хотя большинство за родственника или близкого человека мешать мыслить здраво, следует понимать: если незнакомого человека звонит Вам и требует привести на некий адрес денежную сумму — это мошенник.

Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и, если

звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба.

Если вы разговариваете якобы с представителем правоохранительных органов, спросите, на каком он отделе находится. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

Обращайте ваше внимание на то, что требование взятки является преступлением.

SMS-проблема о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Такую вариацию мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительно опасность представляют упрощенные схемы перевода денег на счет.

КАК ЭТО ОРГАНИЗОВАНО:

Абонент получает на мобильный телефон сообщение: «У меня проблема, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друзь» или другие.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ.

Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Телефонный номер-трайблеть

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Пробоя может быть обоснована любой причиной — помощь другу, изменение тарифов связи, *проблема со связью или с Вашей банковской картой* и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь, — и оказывается, что с Вашего счета списаны крупные суммы.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕ:

Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный.

Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ.

Не звонить по неизвестным номерам. Это единственный способ обезопасить себя от телефонных мошенников.

Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения перейдите по ссылке...».

При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер ... для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства.

Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счет они снимаются с телефона.

Не следует звонить по номеру, с которого отправлен SMS — вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

Существует множество вариантов таких мошенничеств. Будьте бдительны!

Выигрыш в лотерею

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей.

«Вы победили, сообщите код карты экспресс-оплаты»
Карты экспресс-оплаты упростили процедуру зачисления денежных средств на счет, но одновременно и открыли новые возможности для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерею, организованной радиостанцией и оператором мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию.

Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры:

- просит предоставить и назвать год рождения;
- грамотно убеждает в честности акции (никаких взносов, персигровок и т.д.);
- спрашивает, может ли абонент перевести на свой номер денежные средства с карты экспресс-оплаты на определенную сумму (от 300 долларов и выше);
- объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер, куда надо перезвонить;

- поочередно поручает последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Если по каким-то причинам абонент не сможет в течение часа купить экспресс-карту, то все равно должен позвонить для согласования дальнейших действий.

Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переклочении на оператора — сообщить свои коды. Любая ошибка приводит к отмене номера, а призовой отгол контролирует правильность его действий, после чего присваивает ему персональный номер, с которым «победитель» должен ехать за призом.

Но если Вы предложите самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании, то это обяжет нарушением прав радиостанции.

Используются и другие варианты мошенничества

Вам может поступить звонок от якобы представителя вашей сотовой компании, который предложит пополнить счет карточной экспресс-оплаты. Но прежде чем совершить оплату, Вы должны будете сообщить оператору личный ПИН-код, персональный номер, номер радиостанции.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕ:

Задача мошенников — выудить у Вас купит карты экспресс-оплаты на крупную сумму и сообщить личный код с этих карт. Это позволит злоумышленникам присвоить средства с этих карт. Приз и «победа» — приманка, призванная уделить ваше внимание и бдительность.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ.

Активировать карточки экспресс-оплаты следует исключительно через специальные короткий номер, указанный на карточке, а личный код никому никогда не сообщается.

Вед это указано на карте экспресс-оплаты – и в первую очередь надо следовать этим правилам.

Если Вы поступили предложение от радиостанции активировать карточки экспресс-оплаты – не верьте.

Радиостанция никогда не требует активировать карточки экспресс-оплаты при проведении лотереи. «Вы выигрываете машину, нужны деньги для ее оформления». Выигрывать приз может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон – как правило, в ночное время – приходит SMS-сообщение, в котором говорится о том, что в результате проведенной лотереи Вы выигрываете автомобиль.

Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров.

Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уполнить посылочнику и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного телефона 30 тысяч рублей, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения (кода регистрации).

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполнили заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

Простой код от оператора связи

КАК ЭТО ОРГАНИЗОВАНО:

Вам поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными:

- предложение подключить новую эксклюзивную услугу;

- для перерегистрации во избежание отключения связи из-за технического сбоя;

- для улучшения качества связи;

- для защиты от СПАМ-рассылок;

- предложение принять участие в акции от вашего сотового оператора. Вам предлагается собрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Код, который Вам предлагают отправить, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только вы его наберете, Ваш счет будет опустошен. Никакая услуга не будет подключена.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Любая упрощенная процедура изменения тарифных планов выигрывает доверительно. Не ленитесь перевзвонивать своему мобильному оператору для уточнения условий. SMS-сообщения могут быть самыми разными. Советуем Вам критически относиться к таким сообщениям и не спешить

выполнить то, о чем просят. Лучше позвоните оператору связи, узнайте, каков сумма списывается с вашего счета при отправке SMS или звонок на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

Штрафные санкции и угроза отключения номера

КАК ЭТО ОРГАНИЗОВАНО:

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что произошло нарушение условий договора.

- абонент сменил тарифный план, не оповестив оператора;

- не внес своевременно оплату;

- воспользовался услугами роуминга без предупреждения и так далее.

Чтобы предотвратить отключение номера, Вам предлагается:

- купить карту экспресс-оплаты и сообщить их коды;

- перевести на свой номер сумму штрафа и набрать код.

- перевести средства на указанный номер.

После этого Вы якобы сможете доказать свою невиновность и при этом сохранить свой номер.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Пользуясь тем, что телефон Вам нужен постоянно и потеря номера может стать для Вас критической, мошенник заигрывает Вас. В результате он получает возможность присвоить себе Ваши средства – с карт экспресс-оплаты либо напрямую со счета телефона.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Перезванивая своему мобильному оператору для уточнения условий. Помните, что у Вас, как у потребителя услуг связи, есть права, которые защищаются законом. Никакой оператор связи не может требовать выплачивать ему штрафы до тех пор, пока Ваша вина не будет доказана.

Ошибочный перевод средств

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счета.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Чтобы во второй раз списать сумму с Вашего счета, злоумышленник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер. Тот есть первый раз Вы переводите деньги по его просьбе, а во второй раз он получает их по правилам возврата средств.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерял» скорее всего свидетельствует о том, что с Вами общается мошенник.

Мошенничество с банковскими картами

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счете, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит сообщение о том, что «Ваша банковская карта заблокирована». Предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карт, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Для хищения злоумышленникам нужен лишь номер Вашей карты и ПИН-код. Как только Вы их сообщите, деньги будут сняты с Вашего счета.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Не торопитесь сообщать реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступающую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не произошло, а Ваша карта продолжает обслуживаться банком.

Еще раз напомним: держателем карт одно из основных правил безопасности: никто не имеет права интересоваться вашим ПИН-кодом, он должен быть известен только держателю карты.