



ГУ МВД России по Ростовской области

О Т Д Е Л
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по БАГАЕВСКОМУ РАЙОНУ
(ОМВД России по Багаевскому району)

ул. Трюта, 9, Багаевская, 346610

30 ИЮН 2023 № 6019

на № _____ от _____

Главе Багаевского
сельского поселения
Д.Н. Лазарец

Багаевский район
ст. Багаевская
ул. Красноармейская, 5

В рамках выполнения указания ГУ МВД России по Ростовской области о принятии мер по профилактике и противодействию преступлениям, совершенным с использованием информационно-телекоммуникационной сети «Интернет» прошу Вас, поручить довести до работников организации способы хищения денежных средств а также мошеннических действий:

ВНИМАНИЕ - ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО!!!

Основные схемы телефонного мошенничества - обман по телефону:

ТРЕБОВАНИЕ ВЫКУПА

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму — это мошенник. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону.

Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов.

ОПАСНОСТЬ ПРЕДСТАВЛЯЮТ УПРОСТИВШИЕСЯ СХЕМЫ ПЕРЕВОДА ДЕНЕГ НА СЧЁТ.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД РФ настоятельно советует не звонить по незнакомым 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 пройдите 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.

ВЫИГРЫШ В ЛОТЕРЕЕ

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»

Карточки экспресс-оплаты упростили процедуру зачисления денежных средств на счет, но одновременно и открыли новые возможности для мошенников.

ИСПОЛЬЗУЮТСЯ И ДРУГИЕ ВАРИАНТЫ МОШЕННИЧЕСТВА.

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

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД РФ напоминает, что активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер, указанный на карточке, а личный код никому никогда не сообщается. Всё это указано на карте экспресс-оплаты – и в первую очередь надо следовать этим правилам.

Если Вам поступило предложение от радиостанции активировать карточки экспресс-оплаты – не верьте. Радиостанции никогда не требуют активировать карточки экспресс-оплаты при проведении лотереи. «Вы выиграли машину, нужны деньги для её оформления»

Выигрыши приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД РФ предупреждает: если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли 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-рассылки; предложение принять участие в акции от вашего сотового оператора.

Вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД РФ обращает Ваше внимание, что любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Не ленитесь перезванивать 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, какая сумма списется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшем 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 карты 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 сохраните свой номер.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД РФ рекомендует перезванивать 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 счёта.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД РФ советует Вам не поддаваться на обман. Если Вас просят перевести якобы ошибочно переведённую сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян» скорее всего свидетельствует о том, что с Вами общается мошенник. Доступ к SMS и звонкам

Многие люди хотя бы раз в жизни испытывали любопытство по отношению к частной жизни своих родственников и знакомых. Мобильная связь, фиксируя SMS и звонки, даёт ложное ощущение, что каждый может стать шпионом. И мошенники пользуются этим.

КАК ЭТО ОРГАНИЗОВАНО:

В Интернете или прессе публикуется объявление, в котором Вам предлагается изучить содержание SMS-сообщений и список входящих и исходящих звонков интересующего Вас абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

МВД России предупреждает: предложение о предоставлении данной услуги является мошенничеством, так как такая услуга может оказываться исключительно операторами сотовой связи и в установленном законом порядке!

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, 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 карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

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

МВД РЕКОМЕНДУЕТ!

Владельцам пластиковых банковских карт как защититься от мошенников. В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

- ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ
- Никогда и никому не сообщайте ПИН-код Вашей карты.
- Лучше всего его запомнить.
- Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.
- Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.
- ВАША КАРТА – ТОЛЬКО ВАША
- Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошёлёк, не пересчитывая сумму в нём.
- НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ ПРИ ЕЕ УТЕРЕ

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей.

Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Набирая ПИН-код, прикрывайте клавиатуру рукой.

Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Если вы столкнулись с подобными мошенническими схемами, незамедлительно обратитесь в полицию. Чем быстрее вы оповестите органы внутренних дел о совершенном в отношении вас преступлении, тем выше вероятность задержания подозреваемого по горячим следам.

ССЫЛКИ НА ВИДЕО РОЛИК

<https://yadi.sk/i/LzQtTKeG4gnUcw> (ссылка на яндекс диск), <http://media.mvd.ru/files/video/1843629> (ссылка на медиабанк МВД), <https://багаевский.61.МВД.РФ>

О принятых мерах сообщить в адрес ОМВД России по Багаевскому району в срок 10 суток, эл.почта: avlasenko27@mvd.ru, факс 886357-33-0-66, почтовый адрес: 346610, ул. Трюта, 9 ст.Багаевская

С уважением!

Начальник

подполковник полиции

И.М. Бакало