представившись сотрудником службы безопасности выманить данные Вашей карты, рассказав, например, о взломе вашей карты и попытках несанкционированного списания денежных средств, а потом уже узнать у вас всю нужную информацию.

Пожалуйста запомните, мошенники могут подставить ЛЮБОЙ номер. Если вы видите при входящем звонке номер вашего банка, страховой компании, государственной организации, друга или родственника, это НЕ ОЗНАЧАЕТ, что вам звонит действительно тот, чей это номер. Будьте осторожны!

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и самостоятельно перезвонить на абонентский номер близкого человека. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. В случаи если звонили со стационарного номера телефона банка, для того чтобы убедиться, что Вашим деньгам ничего не угрожает достаточно позвонить в клиентскую службу поддержки банка или обратиться лично в банк.

«УДАЛЕННЫЙ ДОСТУП»

Это когда жертва в телефонном режиме, под руководством мошенников установила приложение и предоставила злоумышленникам удаленный доступ к мобильному устройству, и тем самым дают возможность беспрепятственно завладеть персональной информацией и в последующем похитить деньги со счетов через мобильный банк.

КАК ЭТО ОРГАНИЗОВАНО:

Преступник представляется сотрудником банка и сообщает о выявлении вредоносного программного обеспечения на мобильном устройстве клиента. Сообщает, что для его устранения нужно предоставить доступ к устройству. Жертве необходимо скачать на мобильный телефон программу удаленного доступа – TeamViewer, Anydesk или другую, после установки лжесотрудник банка просит клиента назвать код, отображающийся в приложении. Мошенник вводит этот код в программу на своем устройстве. После того как жертва предоставляет все разрешения, злоумышленник получает полный доступ к персональным данным мобильного устройства в том числе и к личному кабинету мобильного банка, и от лица жертвы осуществляет операции по банковским счетам, в том числе имеет возможность оформления онлайн заявки и в последующем получения кредита.

Поэтому нужно запомнить, что настоящие сотрудники банка никогда не попросят:

- Сообщить им код подтверждения операции.
- Установить программы на мобильный телефон, тем более с функцией удаленного доступа.
- Перевести или через банкомат внести ваши деньги на счета третьих лиц.

«РОДСТВЕННИК В БЕДЕ»

КАК ЭТО ОРГАНИЗОВАНО:

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких 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 перечислить на счет либо привезти в оговоренное место и передать какому-либо человеку.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

занять деньги в долг, либо под различными предлогами выясняют реквизиты Вашей карты, пароли и коды из СМС-сообщений. После того как Вы сообщили преступникам реквизиты своей карты и пароли они получает доступ к Вашим счетам.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Следует связаться со знакомыми или родственниками по телефону и выяснить действительно ли им нужна помощь. Ни в коем случае не сообщайте реквизиты Вашей банковской карты.

«ВРЕДОНОСНАЯ ПРОГРАММА (ВИРУС)»

В данном случае преступники используют вредоносную программу, как способ завладения Вашими деньгами. Данная программа устанавливается на телефон при получении СМС или ММС сообщений с различными ссылками, а также при входе на различные сайты в интернете. Особо следует обратить внимание на то, что подобные сообщения могут приходить от знакомых, родственников, которые записаны в Вашей телефонной книге, а также в сообщениях может быть указано Ваше имя или другие персональные данные.

КАК ЭТО ОРГАНИЗОВАНО:

На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». Или другой пример «Алексей, привет! Выложила наши фотографии здесь…., посмотри». При переходе по указанному адресу на телефон скачивается вирус. Либо заражение может произойти при посещении различных сайтов в интернете.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУЦИИ:

Следует установить на телефоне антивирусное программное обеспечение, не следует открывать сообщения с вложениями, перезванивать на номер, указанный в полученном сообщении.

«ОШИБОЧНЫЙ ПЕРЕВОД»

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS-сообщение о поступлении средств на счет. Сразу после этого поступает звонок от мошенников, которые излагают легенду, что они по ошибке перевели деньги и просят их вернуть.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Мошенники пытаются таким образом завладеть Вашими деньгами. Естественно никакой ошибки не было. Денег Вам не присылали.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Советуем Вам не поддаваться на обман. Если Вас просят перевести, якобы, ошибочно переведённую сумму, напомните, что для этого используется чек.

«СМС-ПРОСЬБА О ПОМОЩИ»

СМС-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

КАК ЭТО ОРГАНИЗОВАНО:

Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» и т.д.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Следует запомнить, что на СМС с незнакомых номеров реагировать нельзя, это могут быть мошенники.

ВАЖНО! **Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.**

«КРИК О ПОМОЩИ»

Один из самых цинничных способов хищения денежных средств, является выкладываемая в социальных сетях душераздирающих историй о борьбе с болезнью малолетних детей за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Мы не призываем отказывать в помощи всем, кто просит! Но! Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

Указанный список не является исчерпывающим, так как возможны иные способы и виды мошенничеств, а также их изменение или комбинирование. Во всех случаях обращения с мобильными устройствами, банковскими картами и компьютерами необходимо соблюдать меры предосторожности, которые помогут обезопасить себя и своих близких от мошенников.

Вы получили электронное сообщение о том, что вы выиграли приз и вас просят перевести деньги для получения его получения?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по привлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

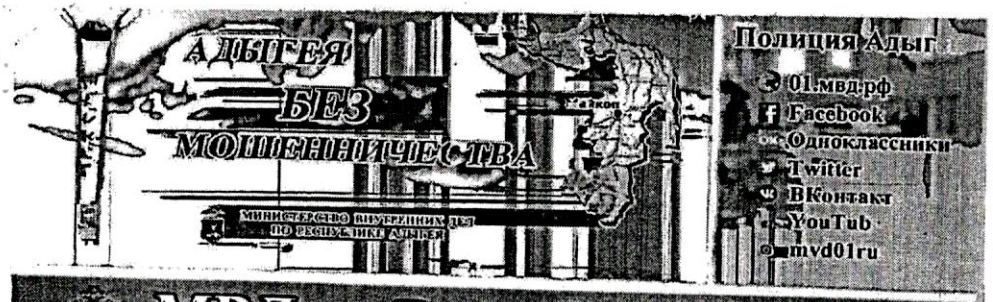
На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах?

НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности продавца.

Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.

Вы хотите приобрести авиабилеты, туристические путевки, через Интернет?

НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов.



Полиция Адыг
01.мвд.рф
Facebook
Одноклассники
Twitter
ВКонтакте
YouTub
mvd01ru

МВД по Республике Адыгея предупреждает!!!

ТЕЛЕФОННЫЕ АФЕРИСТЫ

ВНИМАНИЕ МОШЕННИКИ!

➡ НЕ ВЫПОЛНЯЙТЕ УКАЗАНИЯ НЕЗНАКОМЫХ ЛИЦ!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Мошенники звонят либо рассылают сообщения о блокировке карты и в разговоре предлагают перевести ваши деньги на безопасный счет, либо на номер телефона, просят сообщить им номер карты, ПИН-код и трехзначный номер на обратной стороне карты. Это - ОБМАН!

КОМПЕНСАЦИЯ ЗА НЕКАЧЕСТВЕННЫЙ ТОВАР

Мошенники сообщают, что вам положена компенсация за ранее приобретенные некачественные товары (БАДы). Вас просят оплатить комиссию, налог или пошлину. Это - ОБМАН!

Сотрудники банков никогда не спрашивают пин-коды и пароли!

РОДСТВЕННИК В БЕДЕ

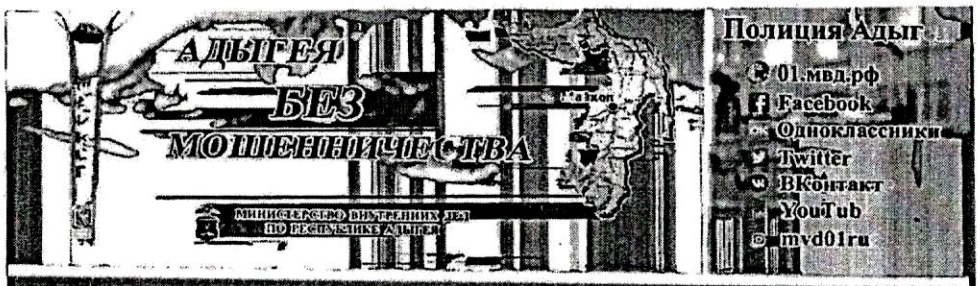
Мошенник представляется вашим родственником и сообщает, что задержан за совершение преступления. Далее, якобы сотрудник правоохранительных органов предлагает разрешить проблему за деньги. Это - ОБМАН!

IP-ТЕЛЕФОНИЯ

Мошенники, при звонке с IP-телефонии, могут эмитировать любые телефонные номера (банков, организаций, учреждений и знакомых). Нужно прервать разговор и позвонить в указанные учреждения, либо знакомым.

Возможны иные способы и виды мошенничества. БУДЬТЕ БДИТЕЛЬНЫ!!!

Полиция Адыгеи: 02 (102/112 - с мобильного)



Полиция Адыгеи
01.мвд.рф
Facebook
Одноклассники
Twitter
ВКонтакт
YouTub
mvd01ru

МВД по Республике Адыгея предупреждает!!!

ПАМЯТКА ДЛЯ ПОЖИЛЫХ ЛЮДЕЙ

ВНИМАНИЕ МОШЕННИКИ!

➡ОБЯЗАТЕЛЬНО ПОЗВОНИТЕ РОДНЫМ И В ПОЛИЦИЮ!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Мошенники звонят либо рассылают сообщения о блокировке карты и в разговоре предлагают перевести ваши деньги на безопасный счет, либо на номер телефона, просят сообщить им номер карты, ПИН-код и трехзначный номер на обратной стороне карты. Это - ОБМАН!

РОДСТВЕННИК В БЕДЕ

Мошенник представляется вашим родственником и сообщает, что задержан за совершение преступления. Далее, якобы сотрудник правоохранительных органов предлагает разрешить проблему за деньги. Это - ОБМАН!

Всегда советуйтесь с родными и близкими!

КОМПЕНСАЦИЯ ЗА НЕКАЧЕСТВЕННЫЙ ТОВАР

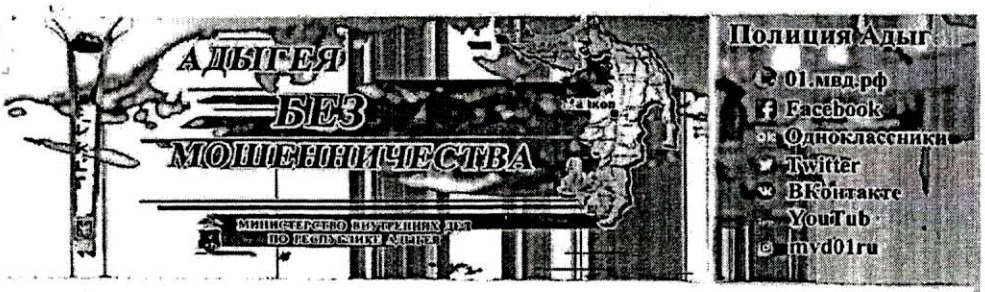
Мошенники сообщают, что вам положена компенсация за ранее приобретенные некачественные товары (БАДы). Вас просят оплатить комиссию, налог или пошлину. Это - ОБМАН!

КУПЛЯ-ПРОДАЖА ТОВАРОВ В ИНТЕРНЕТЕ

Мошенники сообщают, что готовы купить (продать) товар. Для осуществления сделки просят сообщить реквизиты банковской карты, ПИН-код и пароль из СМС-сообщения. Это - ОБМАН!

Возможны иные способы и виды мошенничества. БУДЬТЕ БДИТЕЛЬНЫ!!!

Полиция Адыгеи: 02 (102/112 - с мобильного)



МВД по Республике Адыгея предупреждает!!!

ОБМАН В ИНТЕРНЕТЕ

ВНИМАНИЕ МОШЕННИКИ!

➡ ЗАПОМНИТЕ САМИ и РАССКАЖИТЕ БЛИЗКИМ!

КУПЛЯ-ПРОДАЖА ТОВАРОВ В ИНТЕРНЕТЕ

Мошенники сообщают, что готовы купить (продать) товар. Для осуществления сделки просят сообщить реквизиты банковской карты, ПИН-код и пароль из СМС-сообщения. Это - ОБМАН!

ВЗЛОМ СТРАНИЦЫ В СОЦИАЛЬНЫХ СЕТЯХ

Мошенники путем взлома получают доступ к странице ваших родственников или друзей в соцсетях. От их имени просят занять деньги либо выясняют реквизиты вашей карты. Это - ОБМАН!

Не сообщайте реквизиты банковских карт чужим людям!

САЙТ-ДВОЙНИК

Мошенники используют сайт, адрес которого и оформление идентичны официальному сайту, например банка или по продаже товаров. Не торопитесь, почитайте отзывы и не осуществляйте сделки, через непроверенные сайты.

ФИНАНСОВЫЕ ПИРАМИДЫ

Мошенники маскируют финансовые пирамиды под инвестиционные компании или коммерческие организации, с высокой доходностью. Помните, что вложив деньги в сомнительную компанию, вы соглашаетесь с условиями оферы и можете потерять свои деньги.

Возможны иные способы и виды мошенничества. БУДЬТЕ БДИТЕЛЬНЫ!!!

Полиция Адыгеи: 02 (102/112 – с мобильного)