КАК РАСПОЗНАТЬ ТЕЛЕФОННОГО МОШЕННИКА

МВД по НЕФТЕЮГАНСКУ ПРЕДУПРЕЖДАЕТ!

ЕСЛИ ВАМ СООБЩИЛИ ПО ТЕЛЕФОНУ, ЧТО:

- ваша банковская карта заблокирована...
- необходимо пополнить баланс неизвестного номера телефона...
- нужны деньги, чтобы спасти попавшего в беду родственника
- вы выиграли приз...
- вам полагается компенсация...

ПОМНИТЕ: ЭТО ОРУДУЮТ ТЕЛЕФОННЫЕ МОШЕННИКИ!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

ОСТОРОЖНО! МОШЕННИКИ!
БУДЬТЕ БДИТЕЛЬНЫ, КОГДА ВАС ТОРОПЯТ!

ВАМ ПОЗВОНИЛИ И ПРЕДСТАВИЛИСЬ СОТРУДНИКОМ БАНКА, ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

СООБЩИЛИ О ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЯХ ПО БАНКОВСКИМ КАРТАМ

ПРОСЯТ НАЗВАТЬ НОМЕР БАНКОВСКОЙ КАРТЫ, КОД-ПОРОЛЬ ИЗ СМС СООБЩЕНИЙ

ЧТО ДЕЛАТЬ?

-ПРЕРВИТЕ РАЗГОВОР
-ПОЗВОНИТЕ НА ГОРЯЧУЮ ЛИНИЮ БАНКА

ПОМНИТЕ:

-РАБОТНИК БАНКА НИКОГДА **НЕ БУДЕТ** СПРАШИВАТЬ И УТОЧНЯТЬ РЕКВИЗИТЫ БАНКОВСКИХ КАРТ
-СОТРУДНИКИ ПОЛИЦИИ **НЕ ЗВОНЯТ** ГРАЖДАНАМ С ПРЕДЛОЖЕНИЕМ ПРИНЯТЬ УЧАСТИЕ В СЛЕДСТВЕННЫХ МЕРОПРИЯТИЯХ ПО ПОИМКЕ МОШЕННИКОВ ПОД УГРОЗОЙ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ОТКАЗ В УЧАСТИИ

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

SMS-просьба о помощи

Требование перевести определённую сумму на указанный номер, используется обращение «мама», друг», «сынок» и т.п..

Обман по телефону

Требование выкупа или взятки за освобождение из отделения полиции знакомого или родственника.

Телефонный номер-«грабитель»

Платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую, якобы, проводит радиостанция или оператор связи

Вас просят приобрести карты экспресс-оплаты и сообщить коды, либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Простой код от оператора связи

Предложение услуги – достаточно ввести код, который на самом деле заблокирует Вашу sim-карту

Штрафные санкции и угроза отключения номера

Якобы, за нарушение договора с оператором Вашей мобильной связи

ПОМНИТЕ! Чтобы не стать жертвой телефонных мошенников

- отметьте в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
- не реагируйте на SMS без подписи с незнакомых номеров;
- осторожно относитесь к звонкам с незнакомых номеров.

Если Вы сомневаетесь, что звонивший - действительно ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

Будьте бдительны и внимательны!

Ошибочный перевод средств

Просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы, позволяющая получить доступ к SMS и звонкам другого человека.

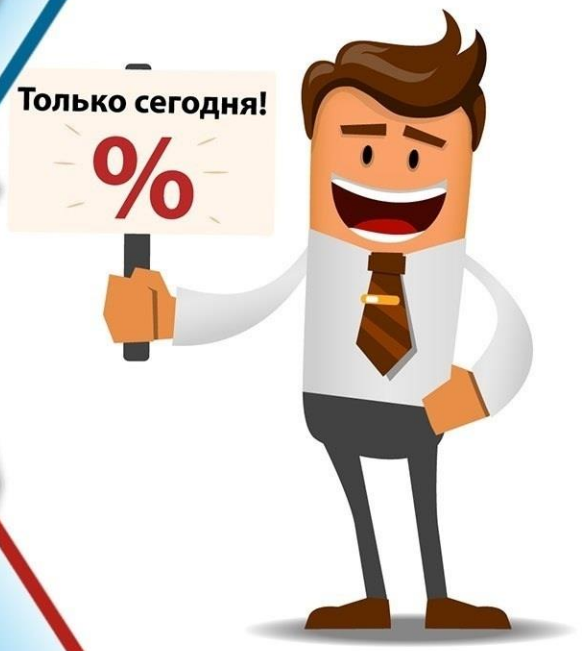
ЛИЧНЫЙ КОНТАКТ

ЗАЩИТА СТАРШЕГО ПОКОЛЕНИЯ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

Вам настойчиво предлагают приобрести товар/услугу «с БОЛЬШОЙ скидкой»?

Прежде, чем участвовать в «заманчиво выгодных» сделках, проконсультируйтесь с родственниками

Мошенники часто выдают себя за сотрудников социальных служб, государственных учреждений, работников ЖКХ или медицинских работников. Если подобные сотрудники пришли к вам без предупреждения или вызова, это повод насторожиться.



Отдел МВД России по г. Нефтеюганску

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей
- Задайте звонящему вопросы личного характера, помогающие отличить близкого Вам человека от мошенника
- Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте, все ли у них в порядке

Вам позвонили/прислали SMS «из банка» с неизвестного номера

- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка
- Незамедлительно обратитесь в правоохранительные органы

Вам прислали MMS или ссылку с неизвестного номера

- Не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков
- Защитите свой телефон, подключите БЕСПЛАТНУЮ услугу «Стоп-контент»

Вы заподозрили интернет-продавца в недобросовестности

- Необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки
- Встречаться с продавцом в общественном месте, так как это наиболее безопасный и гарантированный способ покупки. Следует передавать деньги продавцу лично в руки сразу после получения товара
- Никогда не переводить незнакомым лицам деньги в качестве предоплаты

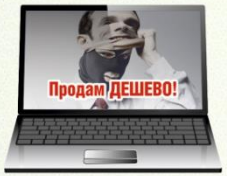
УМВД России по ХМАО - Югре предупреждает

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

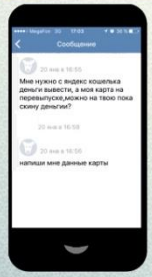
ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

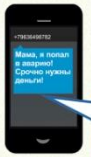


СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

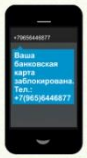
ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

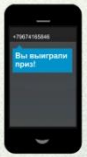
Мама, я попал в аварию!



БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

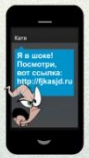
Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)



Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ



Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

Если вам звонят незнакомые люди
и пытаются получить доступ к вашей карте –

ЭТО МОШЕННИКИ!

УСЛОВНО ПРИЕМЫ МОШЕННИКОВ МОЖНО РАЗБИТЬ НА ГРУППЫ:

- финансовые операции
- покупка/продажа товаров/ услуг через Интернет
- инвестиции

ФИНАНСОВЫЕ ОПЕРАЦИИ:

Лже-сотрудник банка может позвонить с сообщением, что ваша карта заблокирована или неизвестные лица пытаются оформить кредит.

Мошенники представляются сотрудниками правоохранительных органов и подтверждают информацию.

Предлагают оформить кредит и перевести деньги на безопасный счёт.

ЧТО НУЖНО ДЕЛАТЬ:

Прервать разговор, позвонить в банк либо лично посетить ближайший офис банка.

Помните, что сотрудники правоохранительных органов не звонят по подобным вопросам.

ИНВЕСТИЦИИ:

«Менеджеры» предлагают быстрый доход от вложений, предлагая инвестировать деньги в ценные бумаги

ЧТО НУЖНО ДЕЛАТЬ:

Проверить, имеется ли лицензия на ведение брокерской деятельности на сайте Банка России.

Помните, что брокерская компания не может предложить быстрый и высокий доход.

ПОКУПКИ В ИНТЕРНЕТ:

«Покупатели» готовы отправить деньги за товар, но для этого им требуются данные карты и код из SMS.

«Продавцы» отдают товар или предоставляют услуги почти даром, но требуют 100% или частичную предоплату.

ЧТО НУЖНО ДЕЛАТЬ:

Совершать покупки только с проверенных сайтов.
Вносить оплату только после получения.

Не верьте на слово невидимым собеседникам, проверяйте любую информацию.

Не сообщайте мошенникам никакой информации: номер карты, ПИН-код, CVC2-код (три цифры с обратной стороны карты), код из SMS.

Эти цифры – доступ к вашим деньгам!

МВД РОССИИ

ВНИМАНИЕ! МОШЕННИКИ!

ТОП-4 САМЫХ ПОПУЛЯРНЫХ СПОСОБОВ ОБМАНА

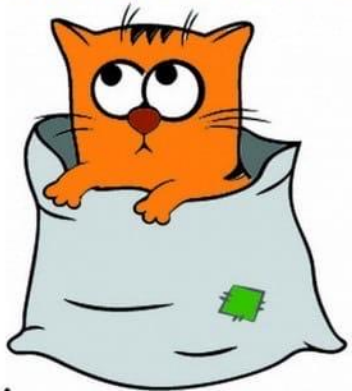
Вы планируете приобрести товар в Интернете

Вы нашли в Интернете подходящий товар по привлекательной цене, но продавец просит внести предоплату или оплатить товар полностью.

Скорее всего это МОШЕННИК!

Не переводите деньги за кота в мешке!

Пользуйтесь только проверенными сайтами по рекомендации Ваших друзей (родственников).



МВД РОССИИ

Вы разместили в Интернете объявление о продаже товара

По Вашему объявлению позвонил (отправил сообщение) покупатель и попросил сообщить реквизиты банковской карты и sms-код, чтобы перевести деньги за товар. Это МОШЕННИК!

Прекратите разговор или переписку и ни в коем случае не сообщайте данные банковской карты и sms-код.

Сообщение в социальной сети

МВД РОССИИ

Ваш друг (родственник, знакомый) пишет в социальной сети личное сообщение с просьбой одолжить денег.

Скорее всего это МОШЕННИК!

Перезвоните другу (родственнику, знакомому) и лично перепроверьте полученную информацию.

Возможно, страницу «взломали», а её владелец не подозревает об этом!

Блокировка банковской карты

Вам поступил звонок о блокировке банковской карты или о подозрительных операциях по счету.

Прекратите разговор – это МОШЕННИК!

Позвоните на горячую линию банка (номер телефона указан на обороте карты) или обратитесь в ближайшее отделение банка лично.

МВД РОССИИ

Чтобы не стать жертвой мошенников, соблюдайте меры предосторожности

Не сообщайте никому код из СМС, даже если представляются банком

Никому не разглашайте данные своей банковской карты: ПИН-код, срок действия, код-безопасности (CVV-код – три цифры с оборотной стороны карты)

Незамедлительно уведомите банк о смене номера телефона, особенно если старый - был привязан к действующей карте

Незамедлительно уведомите банк о подозрении на мошеннические действия по карте, постарайтесь как можно скорее заблокировать карту

Не устанавливайте на смартфон, где установлен мобильный банк или используется интернет-банк, приложения к которым нет доверия

Установите на смартфон лицензионный антивирусник

Если необходимо сообщить номер карты, для того чтобы на карту перевели деньги, ни в коем случае не фотографируйте карту, а просто напишите её номер (только номер)

Самые распространенные виды телефонного мошенничества

Случай с родственником

Если Вам звонят и сообщают, что **Ваш родственник попал** в аварию, за решетку, в больницу или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку. **ЭТО ОБМАН!**

Заблокирована банковская карта

Вам поступил звонок из банка или пришло сообщение о блокировке банковской карты или о несанкционированных операциях со счетом.

НЕ ОТВЕЧАЙТЕ и НЕ ПЕРЕЗВАНИВАЙТЕ, ЭТО МОШЕННИКИ! Обратитесь в отдел банка.

БАДы

Если Вам звонят и представляются сотрудниками медицинских учреждений, дистанционно ставят диагноз, при этом сразу назначают **курс лечения препаратов** и предлагают тут же его приобрести. Не спешите отдавать свои сбережения. Скорее всего это **МОШЕННИКИ!**

Выплата компенсаций

Вам позвонили или пришло СМС сообщение с предложением получить выплату компенсаций за страхование, медобслуживание, коммунальные и прочие услуги, но для этого Вам необходимо **перевести некую сумму в качестве комиссии**. Будьте осторожны, скорее всего **ЭТО ОБМАН!**

Выигрыш в лотерее

Вам сообщили, что Вы выиграли приз, но для его получения необходимо **перевести сумму** денег на незнакомый Вам счет.
НЕ торопитесь следовать инструкциям! Проверьте информацию! Вполне возможно, что с Вами общаются **МОШЕННИКИ!**

Перевод денежных средств

Если для перевода Вам денежных средств на банковскую карту просят сообщить 3 цифры с оборота карты (код CVC), Вы столкнулись с мошенником!
НИКОМУ не сообщайте **3-значный код** проверки подлинности карты, а также пароль для списания средств!

ОМВД России по г.Нефтеюганску
Телефон Дежурной части: 8(3463) 29-56-10

ВНИМАНИЕ МОШЕННИКИ!

Вам звонит "сотрудник МФЦ" и сообщает, что с Вашего номера пришел запрос о смене пароля или номера телефона - ЭТО МОШЕННИКИ!

Для отмены данной операции звонящий попросит продиктовать коды подтверждения из смс от портала Госулуг. Таким образом мошенник получит доступ к личному кабинету Госулуг и личным данным. С их помощью не составит труда оформить кредит на Ваше имя.

НИКОГДА НЕ ПРЕДОСТАВЛЯЙТЕ НЕИЗВЕСТНЫМ ДАННЫЕ ИЗ СМС И ИНФОРМАЦИЮ О СВОИХ БАНКОВСКИХ КАРТАХ И СЧЕТАХ!

МОШЕННИКИ ТАКЖЕ МОГУТ:

- предлагать “компенсацию” за приобретенные лекарства или фальсифицированные товары;
- попросить перевести предоплату за покупаемый товар;
- попросить оплатить покупку на сомнительном сайте, переведя деньги на указанный ими счёт.

ВАЖНО!

Телефон ОМВД России по г.Нефтеюганску: 8(3463)29-56-10 или 102

ОМВД России по г.Нефтеюганску
предупреждает

ОСТОРОЖНО!

МОШЕННИКИ!

Вам поступил звонок от "представителя сотового оператора"

ПРИЗНАКИ

1. "Он утверждает, что срок действия Вашей сим-карты истекает
2. Чтобы исправить эту ситуацию, просит назвать коды, приходящие на сотовый телефон.
3. Ни в коем случае не передавайте данную информацию!
4. С вашего счета произойдет списание денежных средств! Будьте бдительны!

МОШЕННИЧЕСТВО НА «ГОСУСЛУГАХ»

Мошенники звонят жертве

Приветливый голос представляется сотрудником «Госуслуг» и сообщает, что ваш личный кабинет пытаются взломать, изменив номер телефона, который привязан к порталу.

Важно!!! Новая мошенническая схема строится именно на номере телефона, который привязан к личному кабинету!

УМВД России по Ханты-Мансийскому автономному округу - Югре

ЧТО ЗАСТАВЛЯЕТ ЖЕРТВУ ПОТЕРЯТЬ БДИТЕЛЬНОСТЬ И ПОВЕРИТЬ СОБЕСЕДНИКУ?

Лжесотрудник «Госуслуг» говорит убедительно и предлагает задать любые уточняющие вопросы, на которые уверенно отвечает.

Безошибочно называет ваши персональные данные: номер паспорта, ИНН или информацию о наличии штрафов ГИБДД.

УМВД России по Ханты-Мансийскому автономному округу - Югре

ГДЕ МОШЕННИКИ ВЗЯЛИ ВАШИ ДАННЫЕ?

– Номера телефонов часто привязаны к социальным сетям, там же имеются фотографии автомобилей с государственными регистрационными знаками.

– ИНН можно получить, введя ФИО жертвы на сервисе проверки контрагентов.

– Персональные данные также могут утечь от недобросовестных организаций, из различных служб доставки или сервисов лояльности в магазинах.

УМВД России по Ханты-Мансийскому автономному округу - Югре

КАК МОШЕННИК ПОЛУЧАЕТ ДОСТУП К ЛИЧНОМУ КАБИНЕТУ?

- Аферист убедил вас, что действительно является сотрудником «госуслуг»

- Вы называете коды восстановления доступа к «Госуслугам», которые приходят в смс-сообщении.

Важно!!! Получив код, мошенники блокируют вам доступ к личному кабинету и похищают информацию, которая в нем хранится.

УМВД России по Ханты-Мансийскому автономному округу - Югре

ЧТО МОГУТ СДЕЛАТЬ МОШЕННИКИ, ПОЛУЧИВ ДОСТУП К ЛИЧНОМУ КАБИНЕТУ?

– Получить доступ к мобильному банку карты, привязанной к «Госуслугам»

– Оформить кредит на ваше имя в микрофинансовой организации

– С помощью электронной цифровой подписи оформить ИП на ваше имя.

– Продать ваши персональные данные в даркнете, чтобы заработать

– Переоформить ваше имущество на себя.

УМВД России по Ханты-Мансийскому автономному округу - Югре

ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛИ ЖЕРТВОЙ МОШЕННИКА?

Необходимо действовать максимально быстро, пока вашими данными не успели воспользоваться.

Позвоните в банки и заблокируйте карты, которые привязаны к личному кабинету.

Посетите МФЦ и восстановите доступ к личному кабинету, сообщив о том, что стали жертвой мошенников.

УМВД России по Ханты-Мансийскому автономному округу - Югре

КАК ИЗБЕЖАТЬ ОБМАНА?

– Никогда не сообщайте никакие данные по телефону: номера карт, коды из смс-сообщений, логины, пароли и кодовые слова.

– Посетите МФЦ и узнайте, все ли с вашим аккаунтом в порядке.

– Установите двухфакторную аутентификацию на сайте, чтобы вы могли войти в личный кабинет только после ввода пароля и дополнительного кода, который придет по смс.

УМВД России по Ханты-Мансийскому автономному округу - Югре