

## ПАМЯТКА

о порядке действий при обнаружении признаков дистанционного мошенничества и склонении к коррупционному поведению

Злоумышленники постоянно изменяют формы и методы совершения дистанционных мошенничеств.

В том числе ими практикуются телефонные обращения к руководителям государственных/муниципальных, бюджетных учреждений и организаций с информацией о предстоящих проверках надзорных органов, органов исполнительной власти или вышестоящих организаций и предложением повлиять на их результаты с помощью «вознаграждения» или подарков проверяющим.

При обращении мошенники чаще всего представляются должностными лицами исполнительных органов государственной власти автономного округа.

В телефонном разговоре мошенники:

ссылаются на некие имеющиеся предварительные договоренности с руководством, наличие поручений должностных лиц органов власти, называя анкетные данные реальных лиц;

демонстрируют осведомленность в вопросах организации антитеррористической защищенности объектов, обеспечения противопожарной безопасности, специфики деятельности конкретного учреждения, организации;

ограничивают сроки выполнения поставленной «задачи», исполнения «поручения», подчеркивая, что для реализации необходимо принятие оперативных мер, выходящих за рамки действующих служебных регламентов;

заверяют, что в последующем понесенные при выполнении «поручения» издержки и затраты будут компенсированы;

подключают к разговору других лиц, участвующих в мошенничестве и выдающих себя за сотрудников правоохранительных, надзорных органов, коллег, руководителей и т.д.

В связи с изложенным, предлагается при обнаружении признаков телефонного мошенничества:

1. Письменно зафиксировать фамилию, имя, отчество, должность звонившего, содержание телефонного разговора;
2. Уточнить у звонившего номер(а) телефона(ов) обратной связи;
3. Осуществить аудиозапись телефонного разговора (при наличии технической возможности) и обеспечить ее сохранение;
4. Завершить телефонный разговор;
5. По официальным каналам связи получить от должностных лиц органов власти, называемых в разговоре, подтверждение либо опровержение поступившей информации;
6. Доложить непосредственному руководителю о факте поступления телефонного звонка и его содержание;
7. При выдвижении со стороны звонившего преступных требований по переводу денежных средств, приобретения подарков, организации досуга и т.д., направить сообщение в территориальный орган МВД России.

Внимание! Содействие мошенническим действиям неустановленных лиц, а также несообщение в установленном порядке руководителю и в правоохранительные органы о совершении мошенничества либо покушении на его совершение, является основанием для расторжения трудового контракта.

Государственные и муниципальные служащие, работники учреждений (организаций) обязаны уведомлять представителя нанимателя (работодателя), органы прокуратуры или другие государственные органы обо всех случаях обращения к ним каких-либо лиц в целях склонения его к совершению коррупционных правонарушений (ст.9 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции», пункт 3 Типового положения информирования работниками работодателя о случаях склонения их к совершению коррупционных нарушений и порядке рассмотрения таких сообщений, утвержденного распоряжением Правительства автономного округа от 14.08.2014 № 449-рп).

Невыполнение данной обязанности является правонарушением, влекущим увольнение либо привлечение к иным видам ответственности в соответствии с законодательством Российской Федерации.

# ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

**МОШЕННИК** МОЖЕТ ПРЕДСТАВИТЬСЯ: И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:



- сотрудником Банка;
  - сотрудником службы безопасности Банка;
  - сотрудником Росфинмониторинга;
  - сотрудником больницы;
  - сотрудником благотворительной организации;
  - родственником.
- ваша карта заблокирована;
  - в отношении вашей карты предпринимаются мошеннические действия;
  - вашему родственнику нужна помощь или лечение;
  - вам положена отсрочка по кредиту или пособие.

ОН МОЖЕТ ПОПРОСИТЬ:

Данные карты:



- номер карты;
- CVV/CVC-код;
- PIN-код;
- срок действия карты.

Пароль:



- от интернет-банка;
- из SMS-сообщения  
(для входа в интернет-банк или подтверждения операции).

Перевести деньги:



- на специальный счет или карту, где они будут в безопасности.

# НЕ

- сообщайте никому данные карты;
- сообщайте никому пароли и коды из SMS;
- выполняйте действия с банковской картой по просьбе третьих лиц.



номер карты    владелец карты    срок действия



последние три цифры - код безопасности CVV/CVC

**УМВД РОССИИ ПО ХМАО - ЮГРЕ ПРЕДУПРЕЖДАЕТ  
БУДЬТЕ БДИТЕЛЬНЫ!**

## ЗАЩИТА СТАРШЕГО ПОКОЛЕНИЯ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

### ЛИЧНЫЙ КОНТАКТ



**КАК ЭТО ОРГАНИЗОВАНО:** Вам лично (придя домой, подойдя на улице или в другом месте) предлагают приобрести товар, услугу «с большой скидкой», «по акции». Вас ограничивают во времени, торопят, заставляют совершать какие-либо действия в спешке. Мошенникам крайне важно не дать вам шанса хорошо подумать над их предложением.

**КАК ПОСТУПИТЬ:** Прежде чем участвовать в «заманчиво выгодных» сделках, проконсультируйтесь с родственниками, скажите, что вам нужно подумать. Сегодня нет такого уникального товара или услуги, которые бы продавались только «здесь и сейчас» и только в одном месте.

### ПРИГЛАШЕНИЕ НА БЕСПЛАТНОЕ МЕДИЦИНСКОЕ ОБСЛЕДОВАНИЕ



**КАК ЭТО ОРГАНИЗОВАНО:** Вас приглашают в салоны красоты или медицинские центры на бесплатные процедуры или обследование. В данном учреждении «медиками» ставится «страшный диагноз», и прямо на месте вам предлагают пройти необходимое лечение по «новейшей методике» или с применением «уникальных средств». На самом деле никакого «страшного диагноза» нет, это приманка, чтобы продать процедуры по завышенной цене и навязать кредит.

**КАК ПОСТУПИТЬ:** Не посещайте сомнительные медицинские центры и не соглашайтесь ни на какие процедуры, пока не посоветуетесь с врачом из вашей поликлиники, вашими родными. Не подписывайте никаких кредитных договоров.

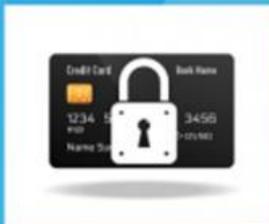
### НАЧИСЛЕНИЕ НЕСУЩЕСТВУЮЩЕЙ СУБСИДИИ



**КАК ЭТО ОРГАНИЗОВАНО:** Звонящий часто представляется сотрудником пенсионного фонда, банка и под предлогом перевода денежной субсидии или выплаты просит назвать ФИО, номер карты и цифры на обратной стороне, якобы для того, чтобы убедиться, что это именно тот человек, которому нужно перевести деньги, просит назвать код, который придет в СМС на телефон. В итоге мошенники воруют средства с карты.

**КАК ПОСТУПИТЬ:** Никому ни при каких обстоятельствах не называйте данные своей карты, в особенности три цифры на обратной стороне карты и код, который приходит вам в СМС.

### БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ



**КАК ЭТО ОРГАНИЗОВАНО:** Мошенники, представляясь сотрудниками вашего банка или сотрудниками Центрального банка, говорят о том, что с вашей картой совершаются мошеннические действия, просят отправить СМС на номер, проследовать к ближайшему банкомату и провести некие операции с картой. В результате вы переводите свои деньги на счета мошенников.

**КАК ПОСТУПИТЬ:** Сотрудники банка никогда не попросят вас проследовать к банкомату для разблокировки или блокировки карты. Свяжитесь с вашим банком, сообщите о случившемся. Заранее запишите контактные телефоны вашего банка.

### ТЕЛЕФОННЫЙ ЗВОНОК/СМС-СООБЩЕНИЕ



**КАК ЭТО ОРГАНИЗОВАНО:** Вам с неизвестного номера звонит человек и представляется вашим сыном, внуком или другим родственником. Говорит, что попал в беду, не может долго разговаривать, плохая связь и передает трубку своему «другу», «сотруднику полиции», «врачу». Далее, вам сообщают, что родственнику срочно нужны деньги, и необходимо их отдать курьеру или продиктовать данные карты.

**КАК ПОСТУПИТЬ:** Попросите еще раз передать трубку родственнику. Если трубку передали, то удостоверьтесь, что это именно он, задав ему уточняющие личные вопросы.





## Как не стать жертвой мошенников, покупая товары в интернете

### Признаки потенциально опасного интернет-магазина



#### 1 Низкая цена

Стоимость товаров в магазине мошенников зачастую существенно ниже, чем в других. Не следует поддаваться на слова «акция», «количество ограничено», «спешите купить» и т.д.



#### 2 Отсутствие курьерской доставки и самовывоза

В этом случае нередко приходится внести предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара.



#### 3 Отсутствие контактной информации и сведений о продавце

Если на сайте прописаны только форма обратной связи и мобильный телефон продавца, такой магазин может представлять опасность. Перед обращением сюда следует почитать отзывы в интернете.



#### 4 Подтверждение личности продавца посредством направления покупателю скана его паспорта

Документ, особенно отсканированный, легко подделать.



#### 5 Отсутствие истории у продавца или магазина

Потенциально опасными являются страницы, зарегистрированные пару дней назад.



#### 6 Неточности и несоответствия в описании товаров

Желательно почитать описания такого же товара на других сайтах.



#### 7 Чрезмерная настойчивость продавцов и менеджеров

Если представитель продавца начинает торопить с оформлением заказа или его оплатой, стоит отказаться от покупки. Мошенники часто используют временной фактор, чтобы нельзя было оценить все нюансы сделки.



#### 8 Требование предоплаты продавцом

Особенно должно насторожить предложение перевести деньги через анонимные платежные системы, электронные деньги, банковским переводом на карту частного лица. В таком случае нет гарантий возврата или получения товара.

### Ошибки самого покупателя

Разочарование от покупки в интернет-магазине нередко наступает и по вине самого покупателя. Ошибки происходят из-за:



Недостаточных знаний об особенностях заказываемого товара: не совпадает размерный ряд, не подходит фасон и т.д.



Невнимательности при оформлении заказа



Поспешности

Потребитель вправе отказаться от покупки, совершенной в интернете, в течение семи дней после получения товара, при этом оплатив обратную доставку товара

Стоит помнить: желательно заранее изучить отзывы о магазине или продавце, просмотреть характеристики товаров на других сайтах, провести замеры, внимательно оформлять заказ



# УМВД России по ХМАО - Югре предупреждает

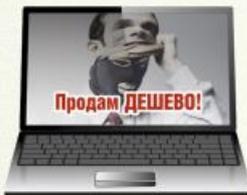


## ОСТОРОЖНО: МОШЕННИКИ!

### 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) sms-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



### СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страницей 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 предложениями.

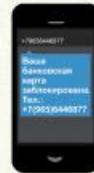
#### ТЕЛЕФОННЫЕ МОШЕННИКИ

### ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



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

**Мама, я попал в аварию!**

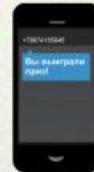


### БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

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 переходите по сомнительным ссылкам.

**НЕ ДОВЕРЯЙТЕ СООБЩЕНИЯМ С НЕЗНАКОМЫХ НОМЕРОВ**

Если Вам приходит информация от имени Вашего родственника о том, что у него COVID-19, он попал больницу и нужно срочно перевести деньги на указанный номер - не отвечайте на сообщение сразу. Позвоните родственнику, уточните информацию.

**ЗАЩИТИТЕ СВОИ ПОКУПКИ В ИНТЕРНЕТЕ**

CVC/CVV код - это дополнительная защита Вашей карты. Он нужен только для оплаты покупок через Интернет. В период самоизоляции совершайте онлайн-покупки только на известных сайтах и через защищенное соединение. О безопасности контакта говорит изображение замка слева от адреса сайта.

**НЕ ПУСКАЙТЕ НЕЗНАКОМЫХ ЛЮДЕЙ К СЕБЕ ДОМОЙ**

Если в Вашу квартиру звонит человек и представляется сотрудником поликлиники/социальной службы/санэпидстанции и предлагает прививку/дезинфекцию от коронавируса - не открывайте ему дверь. Сначала позвоните в названную им организацию и уточните, направляли ли к Вам этого сотрудника.

**ВОСПРИНИМАЙТЕ ИНФОРМАЦИЮ КРИТИЧЕСКИ**

Если Вам сообщают о единовременной выплате от государства, как мере поддержки в период пандемии коронавируса, не отвечайте и не перезванивайте - это условия мошенников. Обратитесь на единую горячую линию 8-800-200-01-12.

**НЕ ОТДАВАЙТЕ СВОИ ДЕНЬГИ МОШЕННИКАМ**

Не отвечайте на электронные письма или sms-рассылки от имени официальных организаций или благотворительных фондов с просьбой о пожертвованиях. Мошенники часто используют такие приемы.

**ОСТОРОЖНО: МОШЕННИКИ!**

**НЕ РАЗГОВАРИВАЙТЕ С МОШЕННИКАМИ**

Если Вам звонят и представляются сотрудниками банка и предлагают «кредитные каникулы» - лучше прекратите разговор. Со всеми предложениями банка Вы можете ознакомиться на его официальном сайте или получить информацию по номеру телефона, указанному на Вашей банковской карте.

**ЗАВЕДИТЕ ОТДЕЛЬНУЮ КАРТУ ДЛЯ ПОКУПОК**

Совершайте удаленные финансовые операции через отдельную карту, не привязанную к основному счету. Переводите на карту небольшие суммы для совершения платежей. Очень легко через приложение банка открыть виртуальную карту и пополнять ее непосредственно перед оплатой товаров и услуг через Интернет.

**СОВЕРШАЙТЕ ПОКУПКИ В ПРОВЕРЕННЫХ МЕСТАХ**

Если Вам предлагают приобрести товары первой необходимости или средства защиты от коронавируса - не поддавайтесь на уловки аферистов. Уточните информацию в официальных источниках.

**БУДЬТЕ ВНИМАТЕЛЬНЫ**

Если Вам сообщают о выигрыше в лотерею, перерасчете квартплаты, блокировке банковской карты, неожиданной единовременной выплате от государства - не выполняйте указания говорящего. Подобные сообщения - распространенные уловки мошенников.

**защитите себя и своих близких**

