РЕКОМЕНДАЦИИ

КАК ИЗБЕЖАТЬ УЛОВОК МОШЕННИКОВ ВО ВРЕМЯ ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

https://www.rospotrebnadzor.ru/activities/recommendations/details.php?ELEMENT_ID=16761

В связи со сложившейся неблагоприятной эпидемиологической обстановкой в мире, большого количества противоречивой информации о новой коронавирусной инфекции в средствах массовой информации, в том числе и сети интернет, появились мошенники, которые используют разнообразные схемы, связанные с пандемией с целью обмана граждан и наживы.

Условно, все схемы можно разделить на несколько групп:

1. Предложения о продаже несуществующих товаров, услуг, социальных льготах.

В интернете появилось огромное количество сайтов, предлагающих купить очиститель воздуха или другие «чудо-средства», удаляющие возбудитель вируса из воздуха и препятствующие заражению коронавирусом. Документы на данные приборы, как правило, отсутствуют или же оказывается, что Вам пытаются продать обычный увлажнитель воздуха, медицинскую маску с фильтром по цене, превосходящей в десятки раз аналогичные предложения на рынке. Иногда, за сопроводительные документы пытаются выдать обычные вкладыши-распечатки о чудодейственном средстве, которые сами обманщики и печатают на обычном принтере. Мошенники могут не только размещать свою информацию на сайте, но и звонить, или осуществлять поквартирный обход.

Предложения о покупке лекарств или пищевых добавок, якобы помогающих от коронавируса.

Будьте бдительны! Правильным решением будет не вступать в контакт с лицами, предлагающими купить «волшебный прибор» или «чудо-таблетку». Как правило, мошенники прекращают общение, если начать более подробно расспрашивать о фирме-продавце и производителе прибора, протоколах клинических исследований лекарства. Обязательно надо предупредить, что перед покупкой Вы обязательно свяжетесь с представителями фирмы изготовителя, с целью уточнения характеристик товара. И помните, любые лекарственные средства назначает только врач и самостоятельно или по совету посторонних людей принимать их не следует.

Предложение покупки индивидуальных средств защиты известных и надежных производителей с обязательной предоплатой. После получения денег товар не поставляется.

Предложения или звонки с информацией о контакте с подтвержденным носителем вируса, с требованием проведения платного анализа на дому. Ни в коем случае не переводите деньги и не предоставляйте свои личные данные

случайным людям. Платные лаборатории могут провести анализ на дому только по Вашему запросу, и такие лаборатории имеют лицензию на осуществляемый ими вид деятельности и не являются «безымянными» - всю информацию о них можно узнать на сайтах и в других открытых источниках.

Запросы конфиденциальных личных данных для предоставления мифической господдержки, компенсации ущерба от вируса – сотрудники государственных служб не запрашивают данную информацию по телефону и не осуществляют поквартирные обход. А всю информацию о полагающихся льготах можно узнать на официальных сайтах государственных организаций.

Фишинговые рассылки (просят пройти по ссылке. с целью кражи данных карты) – например, про то, как в квартире избавиться от возбудителя вируса с помощью фена.

Мошенники могут предлагать провести на дому бесплатное тестирование, вакцинацию от коронавируса или дезинфекцию квартиры. Как правило, цель такого визита – квартирная кража. Ни под каким предлогом не открывайте дверь посторонним людям.

2. Лжеблаготворительные акции

Мошенники могут попросить принять участие в благотворительных акциях, например, пожертвовать деньги на помощь пожилым людям или соотечественникам, оставшимся за рубежом, объявить сборы на лечение детей или взрослых, заболевших коронавирусом. Переведенные в таком случае деньги, скорее всего, вернуть не удастся. Следует тщательно проверять такие обращения.

3. Ложные предложения о работе

Фейковые предложения об удаленной работе под прикрытием корпоративных рассылок. Такие сообщения могут иметь вид приглашения принять участие в Zoom-конференции. Таким образом, мошенники заставляют перейти по небезопасным ссылкам.

Предложения по удаленной работе. Для того, чтобы к ней приступить, мошенники заявляют о необходимости предварительно купить методические материалы.

С целью получения достоверной информации о коронавирусной инфекции и способов борьбы с ней, получения государственной поддержки в период пандемии, доверяйте только официальным сайтам – Роспотребнадзор, Минздрав, ВОЗ, сайты Правительства и портал Государственных услуг. Однако, и в этом случае следует проявлять бдительность, поскольку известны факты, когда мошенники создают вирусные интернет-сайты, распространяющие вредоносное программное обеспечение, для кражи личных данных или данных банковской карты, которые маскируются под официальные порталы реальных организаций.

Что важно знать пожилым людям, чтобы защититься от мошенников

Распространенные виды обмана

- Проникновение в жилище под видом работников разных госслужб.
- Посещение квартир с сообщениями о надбавке к пенсии, перерасчете квартплаты, обмене денег "для ветеранов и пенсионеров".
- Продажа дорогостоящих товаров, которые не соответствуют требованиям к качеству.

Будьте бдительны!

- ✕ Не принимайте незнакомых людей, когда вы одни.
- ✕ Не отдавайте в руки чужим людям паспорт.
- ✕ Не сообщайте ПИН-код и CVV банковской карты.
- ✕ Не пересчитывайте деньги при незнакомцах.

Позвонили в дверь: что происходит и что делать

Пришли представители служб, которых вы не вызывали.

↓

Позвоните в учреждение, от которого якобы пришли незнакомцы.

Вы почувствовали потенциальную опасность от незнакомцев.

↓

Сообщите в полицию и предупредите о ситуации родных.

Вам предлагают совершить покупку на дому с большой скидкой.

↓

Скорей всего, это мошенники. Не совершайте такие покупки без обсуждения с близкими.

Повесьте на видное место телефоны важных служб, банка, соседей и родственников.

8 (800) 100-29-26
горячая линия по вопросам нарушений прав потребителей финансовых услуг.

02, 102 — полиция.

https://www.rospotrebnadzor.ru/activities/recommendations/details.php?ELEMENT_ID=12561

Горячая линия по вопросам нарушений прав потребителей финансовых услуг 8 800-100-29-26

Часто граждане, особенно в силу преклонного возраста, доверчивы и порой наивны. На это и рассчитывают нечестные на руку люди, которые проникают в квартиры под различными предлогами. После визитов многие отдают свои последние сбережения за некачественные товары или услуги.

Ассортимент товаров и услуг, реализуемых такими способами широк – косметическая продукция, медицинские приборы, пылесосы, БАДы, фильтры для очистки воды, посуда, замена и поверка приборов учета и др.

Нередко продавцы берут на себя роль представителей органов государственной власти, используя фальшивые удостоверения и апеллируя тем, что пенсионер попал под действие некой государственной программы адресной помощи.

Чтобы обезопасить себя, близких и не оказаться жертвой мошенников, Роспотребнадзор рекомендует придерживаться нескольких правил:

1. Бережно относитесь к своим персональным данным и документам. Не следует отдавать в руки чужим людям паспорт, никогда никому не называть данные банковской карты: пин-код и CVV (трехзначный код на обратной стороне карты).

2. Если Вы получили СМС-сообщение о блокировке карты или списании денежных средств, не перезванивайте по указанному в СМС номеру! Чтобы узнать обо всех операциях, перезвоните по номеру, указанному на ВАШЕЙ банковской карточке, сходите в банк лично и проверьте баланс через банкомат/онлайн-банк.

3. Если Вам дают заполнить анкету или опросный лист - внимательно изучите их содержание, а своих пожилых или, наоборот, слишком юных родственников и знакомых предупредите, что прежде чем что-либо подписать, необходимо внимательно ознакомиться с содержанием и связаться с Вами.

4. С осторожностью приобретайте у людей, занимающихся квартирным сетевым маркетингом, продукты, мелкую бытовую технику – товары могут не соответствовать обязательным требованиям, а их цена, как правило, завышается в десятки раз. С осторожностью посещайте бесплатные демонстрации косметологических услуг (массаж, «пилинг», уход за волосами

и т.д.) с настойчивыми рекомендациями «местного» врача, презентации косметики с «исключительными» свойствами. Продавцы таких товаров и услуг, услышав о недостатке денежных средств, убеждают граждан заключать кредитные договоры на крупные суммы. Документация по таким сделкам часто сложная и запутанная, напечатанная мелким шрифтом. Продавцы настойчивы и торопят с подписанием договора.

Внимательно изучите документы, не подписывайте, не прочитав и не поняв предварительно их содержание.

Прежде, чем приобрести товар или услугу следует:

- продумать вопрос о необходимости покупки;

- ознакомиться с инструкцией;

- внимательно изучить все имеющиеся у продавца документы;

- потребовать от распространителя демонстрации его работы;

- проконсультироваться с сотрудниками компетентных организаций;

- посоветоваться с родными и близкими.

Помните, что потребитель свободен в заключении договора, а понуждение к заключению договора не допускается.

Если Вы или Ваши близкие всё же подписали договор с недобросовестными продавцами или исполнителями услуг, то следует помнить, что за защитой своих прав Вы можете обратиться в Роспотребнадзор.

Самое главное – не только рассказать пожилым людям и юному поколению о способах мошенничества и мерах предосторожности, но и оказать поддержку. Пусть Ваши близкие не стесняются звонить Вам в подобных ситуациях. Будьте всегда на связи.

О РЕКОМЕНДАЦИЯХ КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

https://www.rospotrebnadzor.ru/about/info/news/news_details.php?ELEMENT_ID=14979

Роспотребнадзор совместно с экспертами и партнерами проекта Министерства финансов Российской Федерации «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации» разработал памятку для потребителей с описанием часто встречающихся случаев мошенничества. В памятке содержится информация о схемах, которые часто используют мошенники, в том числе, новые методы обмана в связи с распространением коронавирусной инфекции COVID-19, а также рекомендации как не стать жертвой мошенников.

Помните, если вы получили СМС о переводе, которого не совершали, позвоните в банк по официальному номеру (указанному на карте), не стоит возвращать деньги самостоятельно:

►не сообщайте никому логины и пароли от банковских приложений, коды из СМС, данные банковских карт;

►не совершайте никаких операций с картой или счетом, если вам диктуют действия по телефону или в чате; прервите разговор и сами перезвоните в банк по официальному номеру и уточните информацию;

►будьте крайне внимательны и осторожны при переходе по ссылкам и при звонке по номеру телефона, указанным в получаемых от банка сообщениях; убедитесь, что отправитель – именно ваш банк;

►если ваш друг или родственник просит срочно перевести деньги, особенно другому человеку, задайте несколько личных вопросов и убедитесь, что вы общаетесь не с мошенником, а лучше – перезвоните человеку по тому номеру, который сохранен у вас в записной книжке;

►отказывайтесь от сомнительных предложений заработать деньги или участвовать в «успешном» проекте с обязательным первоначальным взносом или быстрым авансом за еще не сделанную работу;

►проверяйте информацию о благотворительных акциях на официальных страницах известных вам благотворительных организаций;

►проверяйте на официальных сайтах государственных органов информацию о мерах поддержки – например, в разделе на сайте Роспотребнадзора.

Помните: работники банка никогда не запрашивают коды безопасности, логины и пароли от банковских приложений, коды из СМС.

МИНФИН РОССИИ

Дружи с финансами

РОСПОТРЕБНАДЗОР

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ

Памятка для потребителей

МОШЕННИКИ ВСЕГДА ИСПОЛЬЗУЮТ ОСОБЕННОСТИ ЧЕЛОВЕЧЕСКОГО ВОСПРИЯТИЯ И ПОВЕДЕНИЯ

- Вам **предлагают легкое решение насущной проблемы** – заработок, ремонт в доме, защиту от коронавируса, получение компенсации или пособия, снижение штрафа, списание задолженности и т.д.
- На вас **давят, используют ваше стрессовое состояние,** часто созданное самими мошенниками, ведь в стрессе сложно принимать взвешенные решения. На ваши вопросы отвечают уклончиво.
- У вас **создают чувство нехватки времени** – решение надо принять прямо здесь и сейчас, иначе выгодное предложение уйдет, деньги со счета пропадут, штраф выпишут, компенсацию не дадут и т.д. У вас нет возможности хорошо обдумать ситуацию.
- Вам **не дают советоваться** с близкими и друзьями, упирая на срочность вопроса, доверие к говорящему, закрытость информации, технические проблемы.
- Вам предлагают что-то бесплатное и эксклюзивное – это снижает бдительность, поскольку вроде бы не надо платить; растет чувство собственной значимости.

Помните: даже бесплатные товары и услуги (помощь соцработников, осмотр домовых сетей коммунальными службами и т.д.) или полагающиеся вам выплаты (например, в связи с коронавирусом или рождением ребенка) могут быть получены только по вашему заявлению. Вам надо обратиться в соответствующую организацию или ведомство лично, по телефону, через сайт или Госуслуги.

ЦЕЛЬ МОШЕННИКОВ – НЕ ТОЛЬКО ВАШИ ДЕНЬГИ!

Хотя деньги мошенников, безусловно, интересуют, потерять их можно не только в результате кражи, но и **оплачивая навязанные товары** и услуги, часто низкого качества и по завышенной цене.

Мошенники собирают **информацию о своих жертвах**: прежде всего паспортные данные, номер телефона, данные банковской карты и счета. С их помощью мошенники могут «стать вами» и, например, получить заем или кредит, либо похитить ваши деньги позднее.

Злоумышленники с помощью вредоносных программ могут получить **контроль над вашим телефоном или компьютером**. Под угрозой оказываются личные данные, от вашего лица могут проводиться платежные операции (покупки в интернет-магазинах, платежи в мобильном банке). Зараженное устройство может использоваться **для мошеннических действий против других людей** (спам-рассылки, взлом других компьютеров, атаки на сайты).

Мошенники могут **использовать вас для ухода от ответственности** и «запутывания следов», предоставляя другой своей жертве номер вашей карты для совершения платежа – например, за товар в интернете.

В КРИЗИС МОШЕННИКИ РАБОТАЮТ В ТРИ СМЕНЫ*

- **более чем на 30%** выросло число случаев мошенничества за время пандемии;
- появились **десятки** вариантов мошеннических схем, эксплуатирующих тему коронавируса;
- **на 30%** выросло количество рассылок, выманивающих данные пользователя и направляющих его на мошеннические сайты (фишинг);
- возникли **тысячи интернет-ресурсов**, связанных с коронавирусом, из которых, по некоторым оценкам, до **70%** созданы мошенниками.

* По данным Лаборатории Касперского, Positive Technologies, Group-IB, участников финансового рынка.

Не стоит радоваться внезапному переводу на карту, особенно от незнакомого человека. **Самостоятельно возвращать эти средства рискованно**, особенно если отправитель позвонил вам и просит вернуть «ошибочный перевод» **на другой счет**. Возможно, номер вашей карты был указан мошенником при продаже несуществующего товара на интернет-площадке ничего не подозревающему покупателю. **Обратитесь в свой банк и попросите вернуть перевод отправителю как ошибочный.**

Актуально во время коронавируса!

Перепроверяйте информацию, если сомневаетесь в услугах или товарах, которые вам предлагают в связи с эпидемией:

звоните на горячую линию по коронавирусу **8-800-2000-112**

изучите специальный портал **стопкоронавирус.рф**

заходите на сайт **Роспотребнадзора** www.rospotrebnadzor.ru/region/korono_virus/punkt.php

МОШЕННИКИ ВОРУЮТ ДАННЫЕ БАНКОВСКИХ КАРТ, ЧТОБЫ ОПЛАТИТЬ ТОВАРЫ И УСЛУГИ В ИНТЕРНЕТ-МАГАЗИНАХ, ОТПРАВИТЬ ПЕРЕВОДЫ СВОИМ СООБЩНИКАМ, СНЯТЬ НАЛИЧНЫЕ В БАНКОМАТЕ

МОШЕННИЧЕСТВО ПРИ ОНЛАЙН-ПЛАТЕЖАХ

Как действуют мошенники:

- создают копии сайтов банков, интернет-магазинов, благотворительных организаций с полями для ввода платежных данных;
- перехватывают платежную информацию, отправленную через незащищенный вайфай;
- при переходе по ссылке внедряют на устройство пользователя вирус.

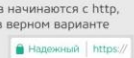
КАК РАБОТАЕТ ФИШИНГ

Пользователь переходит по **ссылке** или нажимает **кнопку** в письме и **переходит на мошеннический сайт**, выглядящий «как настоящий», и/или на его телефон/компьютер **устанавливается вредоносная программа**. Так мошенники могут:

- получить доступ к данным банковских карт, мобильного банка;
- рассылать сообщения с вирусными ссылками на номера из записной книги.

Признаки подозрительных сайтов и фишинговых рассылок:

- адреса сайтов начинаются с http, а не с https (в верном варианте добавляется «s» в конце);



- отсутствует контактная информация и отзывы или, наоборот, есть большое количество негативных отзывов;
- много мелких грамматических ошибок, опечаток и нестыковок;
- слишком низкие цены на товары и услуги;
- есть призывы к срочным действиям, нагнетание, запугивание, восклицательные знаки;
- предлагают быстро/легко заработать.

Подробнее см. лекцию на Семейном финансовом фестивале в июне 2020 г.: www.youtube.com/watch?v=204CDukwNzw

Как не стать жертвой мошенников:

- если собираетесь вводить **личные/платежные данные в интернете** – проверьте, что **адрес начинается с https**, (в конце обязательно должна быть буква «s»);

- **читайте отзывы** об онлайн-магазине/приложении до оплаты покупки;
- заведите **отдельную карту для онлайн-платежей** и храните на ней небольшую сумму;
- настройте в мобильном банке и почте **вход не только по постоянному паролю, но и по одноразовому коду**, который присылается по СМС или генерируется приложением (многофакторная система авторизации);
- старайтесь не производить онлайн-платежи через **незащищенный вайфай**, особенно в общественных местах (транспорт, торговые центры, кафе);
- **старайтесь не оплачивать** товары и услуги **переводом на карту** или по **номеру телефона**, особенно если вы не знакомы с получателем;
- скачивайте мобильные приложения только **в официальных магазинах** (App Store и Google Play);
- **не переходите по коротким ссылкам** вида bit.ly и goo.gl, если не доверяете источнику;
- регулярно **обновляйте программное обеспечение и антивирус** телефона и компьютера;
- **добавьте официальные сайты** магазинов и банков, где вы регулярно вводите данные, **в закладки** браузера.

Актуально во время коронавируса!

Мошенники создают сайты, где продают поддельные товары и услуги: псевдолекарства, псевдотесты и псевдовакцины от коронавируса; поддельные больничные листы с информацией о перенесенном COVID-19; псевдодезинфекцию квартиры и др.

МОШЕННИЧЕСТВО ПУТЕМ МАНИПУЛИРОВАНИЯ ЧЕРЕЗ ТЕЛЕФОННЫЕ ЗВОНКИ, СОЦИАЛЬНЫЕ СЕТИ И МЕССЕНДЖЕРЫ

Как действуют мошенники:

- **вводят в заблуждение и требуют срочного решения**: могут сообщать о близких, которые якобы попали в беду, и просить срочно перевести деньги;
- **присылают сообщение якобы от имени банка** о подозрительных операциях с вашими деньгами или о блокировке счета; просят сообщить код из СМС, перезвонить по указанному номеру или перейти по ссылке (на фальшивую страницу), крадут ваши данные и/или заражают ваше устройство вирусом, который даст им доступ к данным банковских карт и банковским приложениям;
- **взламывают страницы друзей и родственников в социальных сетях**, пишут от их имени и просят перевести деньги;
- **предлагают «выгодную» работу** и требуют зарегистрироваться на неизвестном сайте или предоставить данные банковской карты под предлогом зачисления «аванса»;
- **предлагают упростить** процедуру личного банкротства, быстрее/легче получить кредитные или ипотечные каникулы, помочь оформить пособия, справки 2-НДФЛ;
- **организуют псевдоблаготворительные акции** (в том числе для пострадавших от COVID-19), забирая собранные средства себе.

КЕМ МОЖЕТ ПРЕДСТАВИТЬСЯ МОШЕННИК?

- **родственником** или **другом**, якобы попавшим в беду;
- **сотрудником Пенсионного фонда России** или других официальных организаций, которые оформляют льготы и путевки, пенсии и пособия;
- **сотрудником службы занятости**, кадрового агентства или известной компании, которые предлагают удаленную работу и при этом просят **оплатить регистрационный взнос**;
- **сотрудником банка**, который сообщает о подозрительных операциях с вашей картой и для их отмены требует продиктовать данные карты или код из СМС;
- **сотрудником благотворительного фонда** или **волонтером**, который собирает деньги на срочное лечение или иную благородную цель;
- **покупателем** вашего товара, который хочет узнать данные вашей карты или код из СМС, **чтобы якобы перевести вам деньги**.

Как не стать жертвой мошенников:

- если вы получили **СМС о переводе**, которого не совершали, **позвоните в банк** по официальному номеру (указанному на карте), не стоит возвращать деньги самостоятельно;
- **не сообщайте** никому **логины и пароли** от банковских приложений, **коды** из СМС, **данные** банковских карт;
- **не совершайте** никаких **операций** с картой или счетом, если вам диктуют действия по телефону или в чате; прервите разговор и сами перезвоните в банк по официальному номеру и уточните информацию;
- будьте крайне внимательны и осторожны при **переходе по ссылкам и при звонке по номеру телефона**, указанным в получаемых от банка сообщениях; **убедитесь, что отправитель – именно ваш банк**;

Помните: работники банка никогда не запрашивают коды безопасности, логины и пароли от банковских приложений, коды из СМС!

- если ваш друг или родственник **просит срочно перевести деньги**, особенно другому человеку, **задайте** несколько **личных вопросов** и убедитесь, что вы общаетесь не с мошенником, а лучше – перезвоните человеку по тому номеру, который сохранен у вас в записной книжке;
- **отказывайтесь от сомнительных предложений заработать деньги** или участвовать в «успешном» проекте с обязательным первоначальным взносом или быстрым авансом за еще не сделанную работу;
- **проверяйте информацию о благотворительных акциях** на официальных страницах известных вам благотворительных организаций;
- **проверяйте** на официальных сайтах государственных органов информацию о **мерах поддержки** – например, на сайте Роспотребнадзора www.rospotrebnadzor.ru/region/korono_virus/zachit_prav.php

МОШЕННИЧЕСТВО ПУТЕМ ПОЛУЧЕНИЯ ФИЗИЧЕСКОГО ДОСТУПА К БАНКОВСКОЙ КАРТЕ

Как действуют мошенники:

- **крадут или находят потерянные банковские карты**, получая доступ к написанной на них информации (номер, имя владельца, срок действия, CVC-код) и к информации на магнитной полосе/чипе;
- **устанавливают на банкоматы** незаметные **устройства для считывания данных** с магнитной полосы/чипа карты.

КАК МОШЕННИКИ ИСПОЛЬЗУЮТ ТЕМУ КОРОНАВИРУСА

- присылают сообщения о выписанных штрафах (в т.ч за нарушение самоизоляции) и просят сразу оплатить его переводом на карту или по номеру телефона;
- сообщают о контакте с больным коронавирусом и требуют провести платный анализ;
- предлагают оформить компенсацию ущерба от COVID-19, в т.ч. из-за перерыва в работе, действий интернет-мошенников, пропавших туристических путевок и билетов, а также предлагают «оформить» возврат налогов.

Как не стать жертвой мошенников:

- для каждой карты **создавайте в банкомате отдельный ПИН-код**, известный только вам;
- **не записывайте ПИН-код**, не храните информацию о нем вместе с картой, никому не сообщайте его;
- **никому не показывайте CVC/CVV-код**, расположенный на обороте карты;
- при оплате **старайтесь не выпускать карту из рук** и тем более – из поля зрения, не позволяйте уносить ее куда-либо;
- при наборе ПИН-кода **прикрывайте клавиатуру рукой**;
- используйте **банкоматы, расположенные в хорошо охраняемых, просматриваемых местах** с постоянным видеонаблюдением – например, в отделениях банков;
- **подключите СМС-уведомление от банка**: вам будет приходить информация обо всех операциях по карте;
- **запомните телефонный номер вашего банка** и храните его не только в телефоне, но и записанным на бумаге – отдельно от карт и денег;
- в случае **потери карты немедленно звоните в банк** для ее блокировки.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ?

- Если мошенники использовали вашу банковскую карту, заблокируйте ее в мобильном приложении или позвоните в банк по официальному номеру.
- Сообщите о мошенничестве в ваш банк через официальный сайт, по номеру телефона, указанному на банковской карте, или через мобильное приложение.
- Оставьте заявление о действиях мошенников по телефону горячей линии МВД России 8-800-222-74-47, через портал **https://мвд.рф/request_main** (если это интернет-мошенничество, обратитесь в управление «К» МВД России) или в отделение полиции по месту жительства.

Дружи с финансами

Подготовлено в рамках совместного проекта Минфина России и Всемирного банка «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации» по контракту № FEFLP/QCBS-2.18 «Развитие и укрепление сообщества профессионалов в области финансовой грамотности за счет расширения функционала портала вашифинансы.рф» Институтом национальных проектов в сотрудничестве с проектом «Финшок».

вашифинансы.рф www.rospotrebnadzor.ru zpp.rospotrebnadzor.ru

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ, ПОКУПАЯ ТОВАРЫ В ИНТЕРНЕТЕ

Как не стать жертвой мошенников, покупая товары в интернете

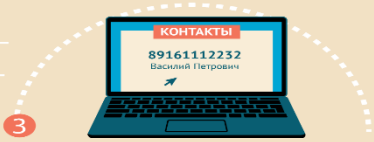
Признаки потенциально опасного интернет-магазина

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 вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара.

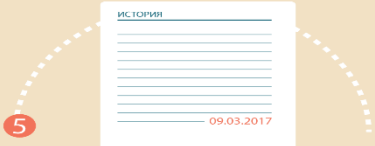


3 **Отсутствие контактной информации и сведений о продавце:**

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.

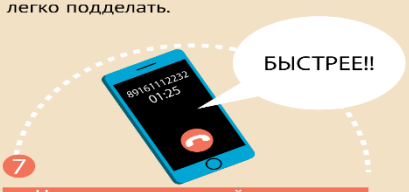


5 **Отсутствие истории у продавца или магазина**

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.

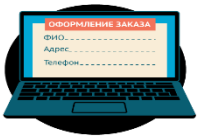
8 **Требование предоплаты продавцом**

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.

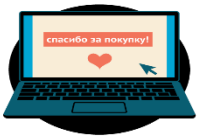
Ошибки самого покупателя

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

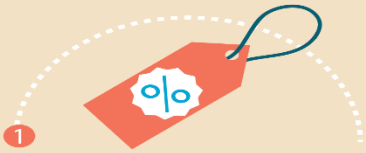
Стоит помнить: желательно заранее изучить отзывы о магазине или продавце, просмотреть характеристики товаров на других сайтах, провести замеры, внимательно оформлять заказ

По рекомендациям Роспотребнадзора

Редактор: Анна Шатохина
Дизайнер: Юлия Осинцева

Как не стать жертвой мошенников, покупая товары в интернете

Признаки потенциально опасного интернет-магазина



1

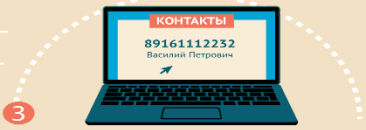
Низкая цена

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 вносить предоплату за услуги транспортной компании. Злоумышленники могут предоставить поддельные квитанции об отправке товара.



3

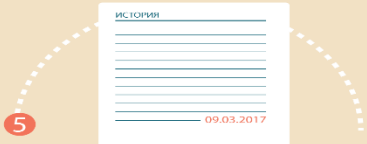
Отсутствие контактной информации и сведений о продавце:

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

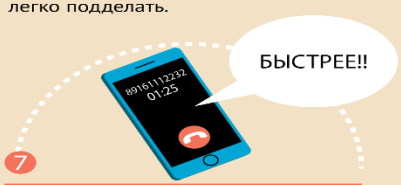
Отсутствие истории у продавца или магазина

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

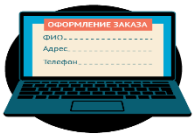
Требование предоплаты продавцом

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.

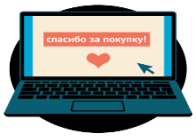
Ошибки самого покупателя

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

По рекомендациям Роспотребнадзора

Редактор: Анна Шатохина
Дизайнер: Юлия Осинцева

Особенностью розничных интернет-продаж является то, что у покупателя отсутствует возможность непосредственного ознакомления с товаром в момент принятия решения о покупке. Такая схема торговли определена ст. 497 ГК РФ. Отношения же с покупателями интернет-магазина регулируются Постановлением Правительства РФ от 27 сентября 2007 г. № 612 «Об утверждении правил продажи товаров дистанционным способом» и ст. 26.1 закона РФ «О защите прав потребителей».

Ошибки самого покупателя:

Самой часто встречающейся причиной разочарования в интернет-покупках, как ни странно, являются ошибки самого покупателя. Чаще всего это бывает связано либо с недостаточными знаниями покупателя об особенностях заказываемого товара, либо с банальной невнимательностью и поспешностью при оформлении заказа.

Например, если речь идет о покупке одежды или обуви, купленная вещь может просто не подойти — по размеру, фасону и т. д. К счастью, эта проблема обычно легче всего решается. Вероятность такой ошибки тем меньше, чем внимательнее и дотошнее покупатель относится к выбору товара и чем больше покупок он делает. Многочисленные покупки дают опыт и знания об особенностях размерного ряда того или иного бренда, о качестве вещей конкретной марки и других нюансах. Очень помогают избежать-таки ошибок таблицы соответствия размеров на сайтах магазинов и производителей. Огромным подспорьем являются и тематические ресурсы, форумы и блоги, изучив которые, можно также узнать много полезной информации о выбранном товаре. Поэтому новичкам перед совершением покупки желательно потратить немного времени и постараться найти побольше информации о выбранном товаре.

Бывают, как уже говорилось, и ошибки при оформлении заказа. Достаточно невнимательно отнестись к выбору опций при оформлении заказа, чтобы получить, например, вещь ненужного размера или не того цвета, или купить привязанный к определенному мобильному оператору сотовый телефон, который не будет работать в отечественных сетях связи, или вообще оправить собственную посылку по неверному адресу.

Поэтому главное при оформлении любого заказа — внимание и неторопливость. Изучите рейтинг магазина, в котором вы собрались делать покупку, описание понравившегося товара и отзывы о нем, поищите информацию об особенностях размерного ряда данного бренда, внимательно заполните сведения об адресе доставки и платежные реквизиты — и рис ошибок на этом этапе будет сведен к минимуму.

Не всеми товарами можно торговать дистанционно. Не допускается продажа дистанционным способом алкогольной продукции, а также товаров, свободная реализация которых запрещена или ограничена законодательством РФ (психотропных, сильнодействующих и ядовитых веществ, наркотических средств) (п. 5 Правил продажи товаров дистанционным способом от 27.09.2007 № 612).

Учитывая, что при дистанционной продаже покупатель лишен возможности осмотреть товар и получить о нем исчерпывающую информацию, законодатель обязывает Продавца до заключения договора розничной купли-продажи предоставить покупателю информацию об основных потребительских свойствах товара и адресе (месте нахождения) продавца, о месте изготовления товара, полном фирменном наименовании (наименовании) продавца, о цене и об условиях приобретения товара, о его доставке, сроке службы, сроке годности и гарантийном сроке, о порядке оплаты

товара, а также о сроке, в течение которого действует предложение о заключении договора (п. 8 правил), о порядке и сроках возврата товара (п. 4 ст. 26.1 Закона РФ «О защите прав потребителей»).

Если приобретаемый покупателем товар был в употреблении или в нем устранялся недостаток (недостатки), покупателю должна быть предоставлена информация об этом (п.10 настоящих правил).

Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег мы рекомендуем вам обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов.

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

На что следует обратить внимание? Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.

На что следует обратить внимание? Создание Интернет-магазина – дело нескольких часов, изменение его названия и переезд на другой адрес – дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

На что следует обратить внимание? Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия.

На что следует обратить внимание? Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы сделки. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие.

На что следует обратить внимание? Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

ВЫВОД: Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки.

Если под их описание подходят два или более признака, мы настоятельно рекомендуем вам воздержаться от контактов с данным продавцом или магазином.

КАК НЕ СТАТЬ ЖЕРТВОЙ СМС-МОШЕННИЧЕСТВА

http://04.rospotrebnadzor.ru/index.php/otdel-zpp/org/141-280410.html

«Уважаемые потребители, сегодня почти каждый из жителей Республики Алтай является абонентом сотовой связи, которым приходят СМС сообщения с различной информацией, чаще всего рекламного характера. Среди них поступают СМС с предложениями об участи в розыгрыше, о получении регулярной информации о погоде, курсе валют, предложения о стабильной работе. Особенно популярны смс-сообщения о проведении различных акций, о возможности выиграть приз.

Например, абонент получает сообщение об акции, проводимой его оператором. По условиям «акции», абонент до конца недели (месяца, года, жизни) получает возможность осуществлять бесплатные звонки по стране. Для этого ему необходимо всего лишь отослать в службу информационной поддержки (телефоны прилагаются) «оператора» коды нескольких карт оплаты. Естественно, выясняется, что оператор никаких акций не проводил, а карты оплаты пополнили счета мошенников.

Для того, чтобы не стать жертвой мошенничества, хотелось бы дать несколько ответов потребителям услуг связи.

Прежде, чем принимать какое-либо решение по поводу пришедших СМС-сообщений от неизвестных абонентов:

Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.

Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученных посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию. Поспешные действия могут привести к финансовому ущербу.

Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку телефона или компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.

Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.

Не торопитесь давать телефон на «1 звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.

Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения - то и от известных. С развитием функциональности мобильных телефонов, карманных персональных компьютеров и коммуникаторов хакеры стали уделять больше внимания созданию вредоносного программного обеспечения для этих устройств. По возможности, установите на мобильное устройство одну из многих антивирусных программ, которые вы можете найти на сайтах известных производителей антивирусного программного обеспечения.

Если вы считаете, что стали жертвой мошенника, обратитесь в правоохранительные органы и оставьте информацию в абонентской службе своего оператора связи. Они подскажут, что делать, дадут нужные телефоны и контакты.

Если Вы абонент «**Билайн**», вы можете прослушать рекомендации, позвонив с мобильного телефона по бесплатному номеру **0611 и 6-99-99**.

Если Вы абонент «**МТС**», вы можете прослушать рекомендации, позвонив с мобильного телефона по бесплатному номеру **0890 и 8-800-333-08-90**.

Если Вы абонент «**Мегафона**», вы можете прослушать рекомендации, позвонив с мобильного телефона по бесплатному номеру **0500 и 8-800-333-0500.**

При обращении к оператору Вы можете сообщать номера телефонов, с которых были сделаны звонки или присланы SMS сомнительного содержания, чтобы к правонарушителям были приняты соответствующие меры.