Дружи с финансами

КАК ЗАЩИТИТЬ СЕБЯ 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 ваш стресс** – часто созданный 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 в заявительном порядке. 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. И **рискованно самостоятельно возвращать** эти средства, 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 одной из популярных интернет-площадок ничего не подозревающему покупателю. **Лучше обратиться в свой банк и попросить вернуть перевод отправителю как ошибочный.**

Актуально во время коронавируса!

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

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

заходите на специально созданный 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

СХЕМЫ, КОТОРЫЕ ИСПОЛЬЗУЮТ МОШЕННИКИ 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: псевдо-лекарства, псевдо-тесты и псевдо-вакцины от коронавируса; поддельные больничные листы с информацией о перенесенном COVID-19; псевдо-дезинфекцию квартиры и др.

МОШЕННИКИ ПЫТАЮТСЯ МАНИПУЛИРОВАТЬ ЛЮДЬМИ, ИСПОЛЬЗУЯ ТЕЛЕФОН, СОЦИАЛЬНЫЕ СЕТИ И МЕССЕНДЖЕРЫ

Как действуют мошенники:

- **вводят в заблуждение и требуют срочного решения**: могут сообщать о родственниках, 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), получают 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 псевдо-благотворительные 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

СХЕМЫ, КОТОРЫЕ ИСПОЛЬЗУЮТ МОШЕННИКИ, ПОЛУЧИВ ДОСТУП К БАНКОВСКОЙ КАРТЕ ФИЗИЧЕСКИ

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.