



МИНФИН РОССИИ



Дружи с финансами



РОСПОТРЕБНАДЗОР

ФИНАНСОВАЯ КИБЕРГРАМОТНОСТЬ И БОРЬБА С МОШЕННИЧЕСТВОМ

Памятка для потребителей

**ПАНДЕМИЯ КОРОНАВИРУСА УСКОРИЛА ПЕРЕХОД В ОНЛАЙН,
ПОРОДИВ НОВЫЕ РИСКИ. БУДЬТЕ БДИТЕЛЬНЫ
И НЕ ЗАБЫВАЙТЕ О ПРАВИЛАХ КИБЕРБЕЗОПАСНОСТИ**

ЦИФРОВИЗАЦИЯ: УДОБНО, БЫСТРО, БЕЗОПАСНО?



**БОЛЬШЕ ПОКУПАЕТЕ
ТОВАРОВ И УСЛУГ
ОНЛАЙН?**

**ПОМНИТЕ О «ЦИФРОВОМ СЛЕДЕ»:
ЗНАНИЯ О ВАШЕЙ ПОЛЬЗОВАТЕЛЬСКОЙ
АКТИВНОСТИ МОГУТ ИСПОЛЬЗОВАТЬСЯ
ПРИ (НЕ)ПРЕДОСТАВЛЕНИИ
СЛЕДУЮЩЕЙ УСЛУГИ, В Т. Ч.
ФИНАНСОВОЙ.**



**ВСЕ БОЛЬШЕ ЗАКЛЮЧАЕТЕ
ДОГОВОРОВ ОНЛАЙН?
ЭТО ЖЕ ЛЕГКО – ДОСТАТОЧНО
НЕСКОЛЬКИХ КЛИКОВ!**

**ПРОВЕРЯЕТЕ ЛИ ВЫ, С КЕМ ИМЕННО
ЗАКЛЮЧАЕТЕ ДОГОВОР,
КТО НЕПОСРЕДСТВЕННЫЙ ПРОДАВЕЦ?
ПОНЯТНЫ ЛИ ВАМ ВСЕ УСЛОВИЯ?
ПОМНИТЕ, ОНЛАЙН ПРОЩЕ НЕ
ТОЛЬКО ЗАКЛЮЧИТЬ ДОГОВОР,
НО И ИЗМЕНИТЬ ЕГО УСЛОВИЯ
(НАПРИМЕР, ПОСТАВЩИКУ УСЛУГИ
ПО ДЛЯЩЕМУСЯ СОГЛАШЕНИЮ).**



**ПОЛЬЗУЕТЕСЬ ЦИФРОВЫМИ
ПЛАТФОРМАМИ? ОНИ ЖЕ
ОКАЗЫВАЮТ СТОЛЬКО ПОЛЕЗНЫХ –
ОСОБЕННО В НЫНЕШНИХ
УСЛОВИЯХ – СЕРВИСОВ:
СВЯЗЬ, КИНО И МУЗЫКА,
ДОСТАВКА ПРОДУКТОВ,
ТАКСИ, КАРШЕРИНГ!**

**НЕ ЗАБЫВАЙТЕ, ПЛАТФОРМЫ
ЗНАЮТ О ВАС ОЧЕНЬ МНОГО
И МОГУТ МАНИПУЛИРОВАТЬ ВАШИМ
ПОТРЕБИТЕЛЬСКИМ ПОВЕДЕНИЕМ
(С ПОМОЩЬЮ ПРОГРАММ
ЛОЯЛЬНОСТИ, КОНТЕКСТНОЙ
РЕКЛАМЫ, ИНТЕРФЕЙСА), А СПОРИТЬ
С ПЛАТФОРМАМИ СЛОЖНО.**

ЦИФРОВИЗАЦИЯ – ЭТО РОСТ УЯЗВИМОСТИ ПОТРЕБИТЕЛЯ

- Недостаточная **цифровая** и **правовая** грамотность, снижение бдительности из-за стресса, связанного с пандемией и снижением дохода.
- Продажа/предоставление **некачественных (или не тех)** товаров и услуг, **непоставка** оплаченных товаров, **непредоставление** оплаченных услуг.
- **Навязывание** ненужных товаров и услуг, неправомерное **использование персональных данных** потребителя.
- **Манипуляции** с условиями программ **лояльности**: сгорание/конфискация баллов, сложность их использования.
- **Одностороннее изменение** условий обслуживания (в заключаемых договорах), **взимание дополнительной** неоговоренной или неочевидной **платы** (скрытые комиссии).
- Сложность в отстаивании прав потребителя **при конфликте** – особенно в отсутствие **прямого контакта** с контрагентом.
- Рост **цифрового мошенничества**: фишинг, вишинг, фейковые сайты, псевдопомощь в решении трудных ситуаций, кража денег и «квазиденег» (баллы в программах лояльности), персональных данных.
- **Заключение договоров от имени потребителя** без его ведома в интересах третьего лица (кредиты и займы).



Как работает ФИШИНГ

Мошенник пытается выманить ваши личные или платежные данные: например, 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.**



Как работает ВИШИНГ

Мошенник **звонит по телефону** и, представляясь сотрудником банка, покупателем и т.д., **выманивает данные вашей банковской карты, пароли и коды из СМС**, подталкивает к совершению выгодных ему действий: сделать перевод, пройти по ссылке из СМС, сообщить секретный код.

ПОДРОБНЕЕ СМ. В ПАМЯТКЕ
«КАК ЗАЩИТИТЬСЯ
ОТ МОШЕННИКОВ»

скачать в pdf



НАРУШЕНИЯ ПРАВ ПОТРЕБИТЕЛЯ ФИНАНСОВЫХ ОНЛАЙН-УСЛУГ



Кредитование:

- **навязывание ненужного кредита/займа** при продаже товара или услуги;
- предоставление **неполной информации** о кредите – часть сведений «спрятана» в дальних разделах договора;
- **скрытые комиссии**, спрятанные в «тарифном плане»;
- **займы**, взятые **посторонним на ваше имя**;
- «порча» **кредитной истории**: финансовая организация «забывает» сообщить в бюро кредитных историй о закрытом обязательстве;
- **отказ в реструктуризации кредита** на заявленных условиях;
- **недобросовестные кредитные брокеры и псевдоброкеры**, взимающие оплату без оказания услуг;
- **псевдопомощники**: обещают «исправление» кредитной истории, поиск «законного» способа не платить долги», но только выманивают деньги и усугубляют положение.



Страхование:

- включение в полисы **условий, снижающих вероятность получения страхового возмещения**;
- **блокирование заключения договоров в электронном виде**, если они невыгодны страховщику;
- **невнесение** агентом **полиса в базу** компании и присвоение денег страхователя;
- продажа накопительного **инвестиционного страхования** жизни под **видом депозита**;
- **занижение** суммы страховой выплаты.



Инвестирование:

- предложение **сложных продуктов** (структурные облигации, производные финансовые инструменты) без надлежащего разъяснения их сути и рисков;
- сложно структурированные тарифы, подталкивающие к **избыточной торговой активности**;
- **некачественные консультации**, в т. ч. данные роботом-советником («робоэдвайзинг»);
- «**автоследование**» (автоматическое повторение сделок) за неумелым «инвестиционным гуру»;
- **возможность кражи** части денег или ценных бумаг в случае **недобросовестности брокера** или **управляющего**.

ОСТОРОЖНО! ФИНАНСОВЫЕ КИБЕРМОШЕННИКИ!

- **Финансовые пирамиды** отлично освоились в цифровом пространстве и работают по старому принципу: постоянное привлечение денег новых участников без ведения реальной экономической деятельности, обещание огромных доходов, в т.ч. за привод новых клиентов.
- **«Троянское обучение»**: бесплатное «обучение» инвестированию на фондовом рынке с обещанием высокого дохода и стимулирование открыть счет у нелегального брокера, что приводит к потере денег. Работает за счет **бесплатности «обучения»** и доверия людей «псевдоконсалтингу».
- **Продажа несуществующих финансовых инструментов** – псевдотокенов и псевдокриптовалют. Работает за счет привлекательности и «модности» темы.

Проверяйте на официальных сайтах государственных органов информацию о **мерах поддержки населения** – например, на сайте Роспотребнадзора www.rospotrebnadzor.ru/region/korono_virus/zachit_prav.php



АКТУАЛЬНО ВО ВРЕМЯ
КОРОНАВИРУСА!

МОШЕННИКИ МОГУТ:



создавать сайты для продажи поддельных товаров и услуг: псевдoleкарства, псевдотесты и псевдовакцины от коронавируса; поддельные больничные листы с информацией о перенесенном COVID-19; псевдодезинфекция квартиры и др.;



присылать сообщения о выписанных штрафах (в т.ч. за нарушение самоизоляции) и просить сразу оплатить его переводом на карту или по номеру телефона;



сообщать о контакте с больным коронавирусом и требовать сделать платный псевдоанализ;



предлагать 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;



рассылать фишинговые псевдопросветительские рассылки о коронавирусе;



создавать вирусные сайты, маскирующиеся под сайты реальных организаций – Минздрава, Пенсионного фонда России, – и под порталы, оформляющие электронные пропуска;



рассылать информацию с ложными предложениями о работе с просьбой предоставить персональные данные для зачисления «аванса»;



запускать ложные благотворительные акции или кампании по сбору средств на разработку вакцины.

КАК СНИЗИТЬ ОНЛАЙН-РИСКИ

Риск

Действия

Навязывание на основании известной о вас информации товара или услуги, в которых вы не нуждаетесь (мисселлинг)

- по возможности **не допускайте утечки персональной информации** в публичное пространство;
- **критически относитесь** к предлагаемой в Интернете **стоимости товара/услуги** – узнавайте среднюю стоимость аналогов, проверяйте цену, заходя на страницу в режиме «инкогнито», при необходимости – запрашивайте перерасчет стоимости;
- внимательно **изучайте доступную информацию** о новых товарах/услугах, критически и рационально подходите к выбору необходимых опций;
- **не соглашайтесь** на неизвестный товар/услугу, **не изучив** самостоятельно его характеристики/условия;
- **не торопитесь – берите «паузу»**, чтобы лучше разобраться, точно ли вам необходим этот товар/услуга.

Навязывание новых товаров/услуг с не до конца понятными характеристиками и несовершенным регулированием

- до того, как нажмете кнопку «купить», **подумайте, что будете делать, если «что-то пойдет не так»;**
- по возможности **страхуйте риски;**
- **не вкладывайте** в новые финансовые продукты **больше, чем готовы потерять.**

Дистанционное заключение договора



- **убедитесь**, что имеете дело с **законным представителем** нужной вам **организации** – самостоятельно звоните по официальным номерам организаций; пишите письма на адреса, указанные на их официальных сайтах, проверяйте физический адрес организации на онлайн-картах;
- при заключении договора с неизвестным вам контрагентом **проверьте информацию** о нем в Интернете – отзывы, а также соответствие данным о видах деятельности юридического лица (egrul.nalog.ru, rusprofile.ru, fek.ru);
- **читайте** тексты заключаемых договоров и принимаемых согласий на обработку и передачу персональных данных;
- **проверяйте** наличие на сайте **пользовательских соглашений** и отсутствие в них ссылок на сторонние компании;
- **сохраняйте файлы договоров** в электронной форме, **скриншоты** Интернет-страниц организации с описанием ключевых условий;
- для договоров, по которым вы делаете регулярные выплаты, ставьте напоминания и **отслеживайте обновления условий** и изменения тарифов.

Онлайн-платежи

- проверяйте, что **адрес Интернет-страницы безопасен, т.е. начинается с https** – в конце **обязательно должна быть буква «s»;**
- **используйте отдельную банковскую карту** с ограниченным объемом средств для оплаты покупок в Интернете;
- **проверяйте все данные и назначение платежа;**
- проводите платежи, используя только **проверенные системы оплаты**, при переходе на страницу оплаты обращайте внимание на логотипы платежных систем (Master Card SecureCode, Verified by Visa и MirAccept).



Надежный

https://

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ

- установите **антивирус** на телефон и компьютер;
- используйте **защищенный вайфай**;
- **скачивайте мобильные приложения** только в **официальных магазинах** (App Store и Google Play);
- установите **двухфакторную аутентификацию**, где возможно;
- **используйте защищенные папки** на устройствах для персональной информации;
- **не открывайте вложения** в письмах от **незнакомых адресатов**, **не предоставляйте** в ответных письмах **персональную информацию**;
- **перед покупкой** проверяйте **подлинность** Интернет-магазина;
- **используйте отдельную карту** для покупок онлайн;
- **подключите СМС-оповещения** от банка обо всех операциях по карте;
- используйте **приложения для определения незнакомых номеров**;
- **не передавайте платежные данные, пароли и коды** подтверждений **третьим лицам**; не храните их в одном месте;
- **не публикуйте персональные данные** (например, номера телефона);
- используйте **разные пароли** для разных сервисов и устройств; периодически **обновляйте** их.
- **не совершайте никаких операций** с картой или счетом, **если вам диктуют действия по телефону** или **в чате** – **прервите разговор и перезвоните в банк** по официальному номеру для уточнения информации;
- **не поддавайтесь на слишком выгодные предложения**, тем более на обещания неожиданного обогащения;
- **не спешите принимать важные решения** – не верьте тем, кто заставляет вас действовать второпях;
- не покупайте продукты/услуги, в т. ч. финансовые, которые **вам непонятны**;
- **обращайте внимание на грамотность** текстов – не верьте тем, где много ошибок;
- **следите** за информацией о **новых видах мошенничества** и **принципах цифровой гигиены**.

КУДА ОБРАЩАТЬСЯ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ

- **МВД России** – оставить заявление о действиях мошенников можно по телефону 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.
- **Роспотребнадзор** (www.rospotrebnadzor.ru) – за бесплатной консультацией, с жалобой на обман, навязывание дополнительных услуг, несправедливые условия договора, с просьбой вступить в судебное дело или подготовить групповой иск.
- **Банк России** – для проведения проверок, требований к финансовой организации об устранении нарушений. Форма подачи жалобы: <https://cbr.ru/Reception/Message/Register?messageType=Complaint>.
- **Финансовый уполномоченный** (finombudsman.ru) – для досудебного урегулирования спора с финансовой организацией (МФО, но не банком).
- **Прокуратура** – для рассмотрения жалоб на нарушение законов.

