Эстафета Мои финансы

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

ГАЙД

ТОП-5 САМЫХ АКТУАЛЬНЫХ ИНТЕРНЕТ-СХЕМ МОШЕННИКОВ

СХЕМА 1
Вам открытка!

Мошенники маскируют вредоносный код под открытку или картинку и рассылают ее по электронной почте. При нажатии на них пользователь скачивает на гаджет вирусную программу, которая похищает его персональные данные.

***Не доверяйте** сообщениям от неизвестных людей. Если вы знаете отправителя, с настороженностью отнеситесь к нестандартным сообщениям, в том числе с вложением фото или картинки без предпросмотра. Уточните у него через другой способ связи, что во вложении.*

СХЕМА 2
Очень выгодное предложение!

Мошенники подделывают сайт маркетплейса и присылают пользователю на почту электронное письмо с промокодом на определенную сумму. Для его получения нужно перейти на сайт, там добавить товары в корзину, ввести реквизиты банковской карты, а подаренная сумма якобы зачтется.

***Не переходите** по ссылкам из электронных писем. Проверяйте акции, промокоды и другую информацию на официальном сайте интернет-магазинов.*

СХЕМА 3
Инвестиционный проект с высоким доходом

Лжеброкеры рассылают письма на электронную почту с рекламой крупного инвестиционного проекта. При минимальных вложениях они обещают высокий доход в ближайшее время.

***Не верьте** обещаниям про легкое и быстрое обогащение! Прежде чем вложить деньги в такой проект, соберите информацию о нем, прочитайте отзывы, уточните контакты брокерской компании.*

СХЕМА 4
Предлагаем работу!

Мошенники публикуют объявления об удаленной работе. Условия привлекательные, зарплата высокая. Они предлагают человеку оформить банковскую карту на свое имя и передать ее курьеру, получить деньги на собственную банковскую карту, часть передать доверенному лицу или перевести кому-то, а вознаграждение оставить себе или стать администратором лотереи и рассылать победителям выигрыши. Подобные предложения — замаскированная схема дропперства.

***Не соглашайтесь** на сомнительные предложения о легком заработке. Помните, что, участвуя в такой схеме, вы становитесь участником преступления и несете уголовную ответственность.*

СХЕМА 5
Получите выплату!

Мошенники под видом специалиста портала «Госуслуги» или СФР рассылают письма на электронную почту и сообщают пользователю о назначении дополнительной выплаты. Для ее получения необходимо перейти по ссылке, ввести паспортные данные и указать реквизиты банковской карты, на которую переведут деньги.

***Внимательно проверяйте** адрес отправителя электронного письма. Помните, что информация о выплатах и льготах отображается в личном кабинете на «Госуслугах». Не переходите по ссылкам из подобных писем и не оставляйте свои данные на сомнительных ресурсах.*

Подробнее на портале **моифинансы.рф**

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

ГАЙД

ТОП-5 САМЫХ АКТУАЛЬНЫХ СХЕМ ТЕЛЕФОННЫХ МОШЕННИКОВ

СХЕМА 1. Меняем медицинский полис

Мошенник под видом сотрудника страховой компании сообщает, что у вас истек срок действия медицинского полиса. Документ нужно заменить. Для этого назовите код из смс, который придет на телефон.

***Работники страховых компаний не просят** устанавливать приложения или называть им коды из смс и данные.*
А медицинский полис действует бессрочно, и его не нужно менять.

СХЕМА 2. Вам цветы, примите доставку!

Мошенник под видом курьерской службы сообщает, что вам отправили букет, уточняет, куда и когда его привезти. После получения букета курьер просит назвать код из смс, чтобы подтвердить доставку заказа.

***Курьерские службы не просят** коды из смс для подтверждения доставки. Свяжитесь с отправителем подарка и уточните детали.*
Если это сделать не удается — не принимайте презент.

СХЕМА 3. Получите письмо!

Мошенник под видом сотрудника «Почты России» сообщает, что вам пришла посылка/заказное письмо. Для его получения надо воспользоваться несуществующим чат-ботом и ввести код из смс.

***Сотрудники «Почты России» никогда не звонят** клиентам и не запрашивают код из смс.*
Вы можете самостоятельно подключить или отказаться от услуг сервиса на его официальном сайте или в приложении.

Подробнее на портале **моифинансы.рф**

СХЕМА 4. Заканчивается договор сотовой связи

Мошенник под видом оператора сотовой связи сообщает, что у вас заканчивается контракт на мобильную связь. Его нужно продлить, иначе вы не сможете звонить, отправлять смс и пр.
Это можно сделать через «Госуслуги»: просто продиктуйте код из смс.

***Сотрудники оператора могут отключить связь,** если вы не оплачиваете услуги или ваши персональные данные, указанные в договоре, необходимо актуализировать. Но это произойдет не сразу. Вы можете обновить данные не только через «Госуслуги», но в салоне связи.*

СХЕМА 5. Зафиксирована подозрительная операция по вашей карте!

Мошенник под видом сотрудника банка сообщает, что по вашей карте зафиксирован подозрительный перевод или кто-то пытается оформить кредит на ваше имя. Для отмены этих финансовых операций вы должны назвать код из смс, который направит специалист.

***Сотрудники банков, правоохранительных органов и государственных ведомств не звонят** гражданам и не запрашивают у них персональные данные, коды из сообщений. Положите трубку и позвоните в организацию, по номеру с ее официального сайта.*

БУДЬТЕ БДИТЕЛЬНЫ! Если вас просят назвать код из СМС, не поддавайтесь на уговоры. Мошенники могут придумывать разные предлоги, чтобы выманить его. Этот код дает доступ к вашим персональным данным и банковским счетам

Эстафета Мои финансы

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап **«Финансовая безопасность для всей семьи: защити свои деньги»**

ИНСТРУКЦИЯ. ВЗЛОМАЛИ СТРАНИЦУ В СОЦСЕТИ?

Воспользуйтесь нашей инструкцией, чтобы быстро вернуть контроль над своим аккаунтом.

ДЕЙСТВИЕ 1
Предупредите друзей и близких

Свяжитесь с ними через другие каналы связи — телефон, электронную почту, другие соцсети. Предупредите, что ваш аккаунт взломан. Попросите их не переходить по ссылкам, не отвечать на сообщения, отправленные с вашего взломанного аккаунта.

ДЕЙСТВИЕ 2
Попробуйте восстановить доступ самостоятельно

Каждая из социальных сетей имеет свой алгоритм восстановления пароля. Следуйте ему. Если доступ сохранился или его удалось восстановить, поменяйте пароль и завершите активные сессии на других устройствах (это можно сделать в настройках соцсети).

ДЕЙСТВИЕ 3
Сообщите о взломе в службу поддержки социальной сети

Найдите форму обратной связи в разделах «Помощь», «Поддержка» или «Связаться с нами». Подробно опишите ситуацию и следуйте инструкции службы поддержки. Возможно, вам потребуется предоставить дополнительные документы, подтверждающие личность.

ДЕЙСТВИЕ 4
Попросите друзей пожаловаться на вашу страничку в соцсетях и отметить публикации как спам

Это поможет заблокировать аккаунт. Такой способ подойдет, если действия 2 и 3 не помогли, а мошенники продолжают использовать ваш аккаунт в преступных целях.

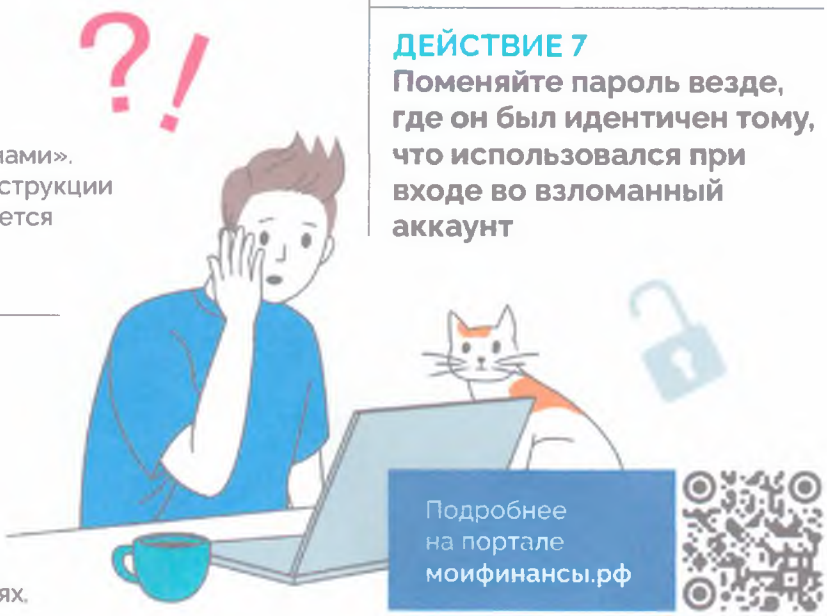
ДЕЙСТВИЕ 5
Обратитесь в банк или платежный сервис, если к учетной записи была привязана карта

Заблокируйте ее до тех пор, пока не вернете доступы к своему аккаунту в социальных сетях. Мошенники, получив доступ к нему, могут переводить с вашей карты деньги на счета других пользователей сети, а также оплачивать товары и услуги.

ДЕЙСТВИЕ 6
Вспомните все сервисы, которые привязаны к взломанному аккаунту, и «отвяжите» их

Например, в ВКонтакте можно авторизоваться в мини-приложении «Госуслуги». Взломав аккаунт соцсети, злоумышленники могут получить доступ и к нему.

ДЕЙСТВИЕ 7
Поменяйте пароль везде, где он был идентичен тому, что использовался при входе во взломанный аккаунт



Подробнее на портале моифинансы.рф

ВАЖНО! При взломе аккаунта игнорируйте любые предложения незнакомых лиц, якобы готовых помочь за вознаграждение. Это мошенники!

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

ИНСТРУКЦИЯ. ВЗЛОМАЛИ «ГОСУСЛУГИ»: ЧТО ДЕЛАТЬ

Вы обнаружили, что ваш аккаунт на «Госуслугах» взломан. Что делать? Следуйте шагам, описанным в нашей инструкции, чтобы защитить свои данные.

ШАГ 1. Восстановите доступ к учетной записи и замените пароль

Злоумышленники рассылают сообщения от имени государственных и финансовых организаций, интернет-магазинов, организаторов лотерей и даже родственников и близких. Их цель — заманить жертву на фишинговый сайт, чтобы украсть ее личные данные, информацию о банковской карте и деньги.

Если мошенники ИЗМЕНИЛИ контактные данные

Лично в центре обслуживания

Предоставьте специалисту МФЦ паспорт, СНИЛС и номер телефона. Он поможет восстановить доступ к «Госуслугам».

Подробнее на портале моифинансы.рф

Если мошенники НЕ ИЗМЕНИЛИ контактные данные

Онлайн на «Госуслугах»

На странице входа в аккаунт нажмите *«Восстановить доступ»*. Выберите, куда придет код подтверждения для смены пароля:

- на номер телефона → 4 цифры в смс,
- на электронную почту → ссылка для подтверждения на создание нового пароля.

Сервис может запросить данные для подтверждения личности: паспорт, ИНН или СНИЛС.

Онлайн через банки Сбер, Почта Банк или РНКБ, если вы являетесь их клиентом.

Зайдите на сайт или в приложение банка и пройдите шаги по подтверждению учетной записи на «Госуслугах».

Важно: данные паспорта на «Госуслугах» должны совпадать с данными в банке.

ШАГ 2. Выйдите из учетной записи на «Госуслугах» со всех устройств, кроме текущего

В личном кабинете выберите раздел *«Безопасность» → вкладка «Действия в системе» → «Выйти»*. Повторите то же самое во вкладке *«Мобильные приложения»*, нажмите *«Выйти»* из тех приложений, в которые вы не входили.

ШАГ 3. Проверьте, где мошенники могли использовать учетную запись

В личном кабинете выберите раздел *«Безопасность» → вкладка «Действия в системе»*. Если злоумышленники успели подать заявления в МФО, отзовите их.

ШАГ 4. Убедитесь, что на вас не оформили кредит

Выберите услугу «Получение информации о хранении вашей кредитной истории» и закажите отчет в бюро кредитных историй (БКИ). В присланных документах посмотрите, какие заявки на кредиты подавались от вашего имени.

Важно: Если на вас взяли кредит — срочно обратитесь в банк или МФО и сообщите, что заявку на кредит подали мошенники.

ШАГ 5. Защитите свою учетную запись

Вы можете выбрать один из дополнительных способов или подключить все три:

- Настройте вход с дополнительным способом подтверждения, помимо пароля: добавьте одноразовый код или вход с помощью биометрии.
- Установите контрольный вопрос.
- Подключите уведомление с помощью письма на электронную почту о входе в личный кабинет.

ШАГ 6. Обратитесь в МВД

Сообщите полиции, что вашу учетную запись взломали. Подать заявление можно лично или онлайн на сайте МВД.

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап **«Финансовая безопасность для всей семьи: защити свои деньги»**

ИНСТРУКЦИЯ «10 ШАГОВ К НАДЕЖНОМУ ПАРОЛЮ»

Банковские счета, социальные сети, личная переписка — все это требует надежной защиты в цифровом пространстве. Чтобы сохранить свои данные и деньги от мошенников, выполните 10 простых шагов и создайте надежный пароль!

Шаг 1. Задействуйте больше 12 символов

Чем длиннее пароль, тем сложнее его взломать.

- «Ялюблюгулять»
- «Ялюблюгулятьвпаркевечером»

Шаг 2. Смешивайте регистры

Используйте заглавные и строчные буквы в случайном порядке.

- «Ялюблюгулять»
- «ЯЛюблюГулятьВПарке»

Шаг 3. Добавьте спецсимволы и цифры

Размещайте их в разных частях пароля. При выборе букв, знаков и цифр избегайте последовательности.

- «Qwerty123»
- «65ЯЛюблю!Гулять$ВПарке!2»

Шаг 4. Используйте пароль-фразу

Запоминается легко, взламывается сложно. Это могут быть преобразованные предложения, строчка из песни, комбинация случайных слов или буквы каждого слова известной фразы.

- «ILoveYou2025»
- «Во поле березка стояла» → «VpoleBcSt01!»

Шаг 5. Забудьте о личной информации

Никаких имен, дат рождения, кличек питомцев, адресов или других персональных данных. Мошенники могут найти эту информацию в ваших социальных сетях и использовать ее для взлома.

Шаг 6. Создавайте уникальный пароль для каждого аккаунта

Если вы используете один и тот же пароль для нескольких аккаунтов и один из них взломан, злоумышленники получают доступ сразу ко всему.

Шаг 7. Используйте менеджер паролей

Это сервис, который создает, хранит и автоматически подставляет сложные пароли для каждого сайта.

Шаг 8. Устанавливайте двухфакторную идентификацию

В таком случае для входа в аккаунт мошеннику нужно преодолеть два «шлюза»: первый — введение логина и пароля, второй — специальный код, который отправляется по SMS или электронной почте.

Шаг 9. Правильно храните пароли

- Записывать пароль на листочек, хранить в телефонных заметках или на вложенном в паспорт стикере.
- Запоминать пароль в уме. Придумайте ассоциацию, которая позволит легко воспроизвести код. Например, «Mountain!TriP2019#» может ассоциироваться с походом в горы.

Шаг 10. Обновляйте пароли

Оптимально менять пароль раз в 3–6 месяцев, особенно для важных аккаунтов — электронной почты, онлайн-банкинга, социальных сетей. Это поможет защитить ваши данные и деньги от возможных утечек.

Подробнее на портале **моифинансы.рф**

ПОМНИТЕ! Надежный пароль — это не просто набор символов, а ваша защита от цифровых угроз. Следуйте этой инструкции, и ваши аккаунты будут в безопасности!

ПАМЯТКА

Я ДРОППЕР?

Проверьте, не попали ли вы в ловушку финансовых мошенников

ДРОППЕР — это человек, которого мошенники используют для вывода и обналичивания похищенных денег.

ЧТО ДЕЛАЕТ ДРОППЕР

- Оформляет на себя банковские карты и отдает доступ к ним мошенникам.
- Переводит деньги на разные счета по указанию преступников.
- Снимает и вносит в банкоматы украденные деньги.
- Предлагает работу с «дополнительным» взносом, который нужно перечислить «работодателю».
- Делает «ошибочные» денежные переводы гражданам.
- Рассылает сообщения о выигрыше, который якобы выпал потенциальной жертве мошенников.

ГДЕ ПРЕСТУПНИКИ ВЕРБУЮТ ДРОППЕРОВ

Рассылают предложения о трудоустройстве:

- В социальных сетях.
- В мессенджерах.
- По электронной почте.
- Расклеивают объявления и раздают листовки в общественных местах.

В зоне риска подростки и студенты, которые хотят быстро заработать!

ВНИМАНИЕ! Дроппером можно стать случайно!

КАК НЕ СТАТЬ ДРОППЕРОМ

- Будьте осторожны с предложениями о работе, связанными с переводами денег.
- Будьте осторожны с вакансиями, которые предлагают легкую прибыль без усилий, навыков и образования.
- Не открывайте банковские карты по просьбе незнакомых людей.
- Не передавайте никому реквизиты своей карты.
- Не возвращайте деньги, которые пришли на ваш счет или телефон «по ошибке», а отправитель требует вернуть их на другой счет.
- Не верьте звонкам от «сотрудников» правоохранительных органов или Банка России.

Подробнее о дропперах читайте на моифинансы.рф

ВНИМАНИЕ! Участие в дропперской схеме — уголовно наказуемое преступление, ответственность за которое граждане несут с 14 лет. Незнание своей вовлеченности в преступление не освобождает от ответственности за него.

ПАМЯТКА

ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛ ДРОППЕРОМ

Дроппер может не знать, что он стал соучастником преступления. Если вы вдруг поняли, что стали дроппером, сделайте следующие 7 шагов. Они помогут минимизировать неприятные последствия.

ШАГ 1

Заблокируйте карту или счет,

которые использовались в мошеннических операциях.

ШАГ 2

Не общайтесь с мошенниками

Прекратите любые действия, связанные с мошеннической схемой. Не выполняйте больше никаких поручений и не передавайте деньги или данные.

ШАГ 3

Сообщите в банк

Свяжитесь с вашим банком и объясните ситуацию, расскажите о подозрительных операциях. Сотрудники примут меры, чтобы вернуть деньги пострадавшим.

ШАГ 4

Обратитесь в правоохранительные органы

Напишите заявление в полицию. Предоставьте доказательства: записи разговоров, сообщения, данные о переводах.

ШАГ 5

Проконсультируйтесь с юристом

Он разъяснит, какие правовые последствия могут быть и как действовать.

ШАГ 6

Подготовьтесь к проверке

Будьте готовы предоставить правоохранительным органам всю необходимую информацию и сотрудничать с расследованием.

ШАГ 7

Не повторяйте ошибок

В будущем будьте более осторожны с предложениями о легком заработке, особенно если они связаны с банковскими операциями или передачей денег.

Подробнее о дропперах читайте на моифинансы.рф

ПОМНИТЕ! Своевременные действия помогут избежать серьезных проблем и привлечь мошенников к ответственности.

Минфин России

мои финансы

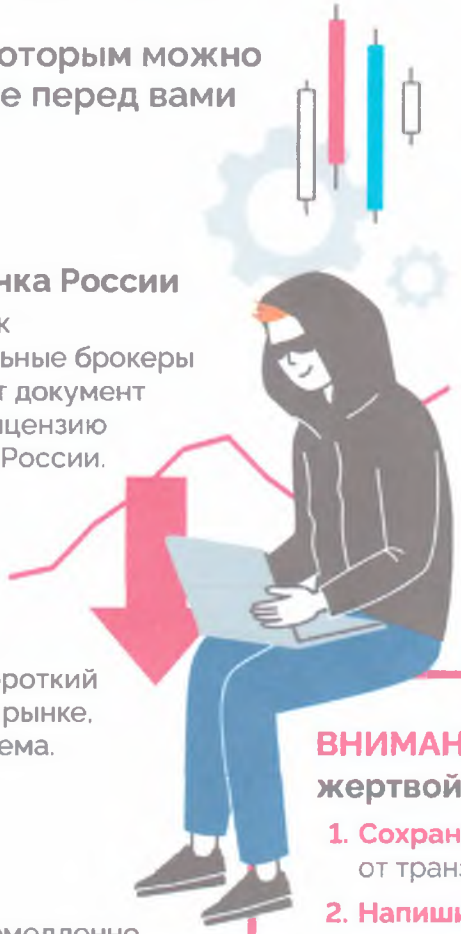
Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

ИНСТРУКЦИЯ

КАК РАСПОЗНАТЬ ЛЖЕБРОКЕРОВ

6 главных признаков, по которым можно легко понять, что на бирже перед вами не брокер, а мошенник.



Признак 1

У брокера нет лицензии Банка России

ВНИМАНИЕ! Это главный признак мошеннической компании! Легальные брокеры обязаны получить лицензию. Этот документ в отрытом доступе. Проверить лицензию у брокера можно на сайте Банка России.

Признак 2

Гарантирует прибыль

Если компания обещает высокую фиксированную доходность за короткий срок, независимо от ситуации на рынке, перед вами — мошенническая схема.

Признак 3

Давит, создает спешку

Звонки, письма с требованием немедленно внести деньги, любые попытки ускорить ваше решение в инвестициях должны насторожить.

Признак 4

Есть проблемы с выводом средств

Перед началом сотрудничества изучите условия брокерского обслуживания: комиссии, сроки перечисления денег, проценты по займам. Если условия не прозрачны, откажитесь от дальнейших действий.

Признак 5

Требует перевести деньги на карту физлица

Легальные брокеры никогда не требуют предоплаты на карту «личного менеджера», а все расчеты проходят только через брокерский счет.

Признак 6

Нет реального офиса. Контакты скрыты

Брокеры-мошенники в большинстве случаев строят все общение через соцсети и телефон. А на сайте компании все ссылки на контакты ведут на сторонние ресурсы или на главную страницу.

ВНИМАНИЕ! Если вы стали жертвой мошенников на бирже

1. **Сохраните** переписку и чеки от транзакций.
2. **Напишите** заявление в банк, через который отправляли деньги, и попросите вернуть деньги (чарджбэк).
3. **Напишите** заявление в полицию.

Подробнее на портале **моифинансы.рф**

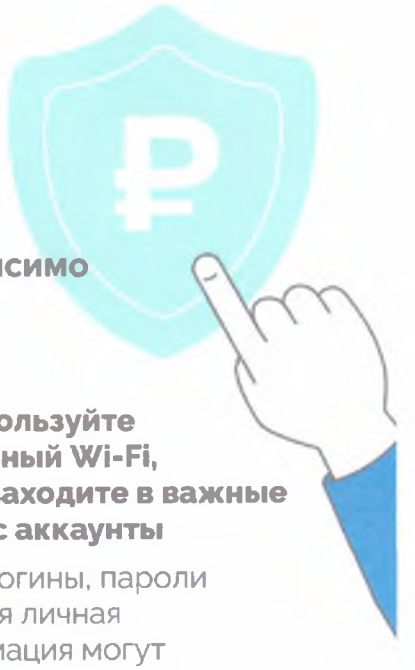
Всероссийская просветительская Эстафета
по финансовой грамотности
Этап — «**Финансовая безопасность для всей семьи: защити свои деньги**»

Минфин России

мои финансы

ЗАЩИТИТЕ СВОИ ДЕНЬГИ!

7 базовых правил финансово-цифровой безопасности, которые помогут вам защитить свои данные и деньги, независимо от того, какую схему решат использовать злоумышленники.



1

Не сообщайте коды из СМС-сообщений — никому и никогда

Код из СМС — часть системы двухфакторной аутентификации, которая защищает доступ к вашим персональным данным и банковским счетам.

2

Не совершайте финансовые операции по инструкции от незнакомых, кем бы они ни представлялись

Незнакомцы могут предлагать схемы, направленные на кражу ваших денег.

3

Остерегайтесь фишинга

Будьте внимательны к сайтам, которые требуют вводить личные данные.

4

Не используйте публичный Wi-Fi, когда заходите в важные для вас аккаунты

Ваши логины, пароли и другая личная информация могут оказаться в руках преступников.

5

Не возвращайте деньги, присланные по ошибке неизвестными

Такие переводы могут быть связаны с мошенническими схемами.

6

Не спешите реагировать на тревожные звонки и сообщения

Мошенники манипулируют эмоциями, которые притупляют бдительность.

7

Не делитесь персональными данными с посторонними

Не сообщайте свои пароли, PIN-коды, данные банковских карт, паспортные данные и другую конфиденциальную информацию.

На портале **моифинансы.рф** рассказываем больше про финансово-цифровую безопасность →

Всероссийская просветительская Эстафета по финансовой грамотности.
Этап — **«Финансовая безопасность для всей семьи: защити свои деньги»**

Минфин России

мои финансы

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА!

Аферисты постоянно находят новые способы украсть деньги или личные данные. Но какими бы хитрыми ни были их схемы, есть пять признаков, по которым легко их разоблачить.

Признак 1

НА ВАС ВЫХОДЯТ САМИ

У мошенников много личин. Помните, что инициатору контакта всегда от вас что-то нужно.

Признак 2

ВАС ВЫВОДЯТ ИЗ РАВНОВЕСИЯ

Радуют или пугают, чтобы сбить вас с толку и притупить бдительность.

Признак 3

ВАС ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Преступников интересуют коды из СМС, пуш-уведомлений, данные банковской карты, персональные данные.

Признак 4

ВАС ТОРОПЯТ

Преступникам важно, чтобы вы действовали импульсивно.

Признак 5

ВАШИ ВОПРОСЫ ИГНОРИРУЮТ

Мошенник будет стараться следовать своему сценарию.

На портале
моифинансы.рф

рассказываем больше про финансово-цифровую безопасность

ВНИМАНИЕ! Кладите трубку в разговоре с незнакомцем, если распознаете хотя бы два из этих признака. Помните, что цель любой схемы мошенников — получить от жертвы сведения, достаточные для доступа к ее деньгам. БУДЬТЕ ВНИМАТЕЛЬНЫ И ОСТОРОЖНЫ!

Всероссийская просветительская Эстафета
по финансовой грамотности.
Этап — **«Финансовая безопасность для всей семьи: защити свои деньги»**

Минфин России

мои финансы

КАК НАУЧИТЬ РЕБЕНКА ЗАЩИЩАТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

10 важных рекомендаций родителям

1 **Сделайте разговоры с ребенком о мошенниках регулярными**

Обсудите реальные случаи мошенничества, спрашивайте, как бы ребенок действовал в этих ситуациях. Это поможет донести, что риск быть обманутым в интернете выше, чем кажется.

2 **Изучите сами как мошенники обманывают детей**

Распознать мошенника легче, когда знаешь, как он действует.

3 **Расскажите, что такое личные данные и почему их надо хранить в секрете**

Реквизиты карты, пароли, коды для подтверждения операций — перехватив их, мошенник может лишить семью финансов.

4 **Убедитесь, что ребенок пользуется проверенными приложениями и сайтами**

Это важно, чтобы избегать фишинговых ресурсов.

5 **Объясните, как безопасно делать денежные переводы**

Переводы по номеру телефона безопаснее, чем по номеру карты. При отправке средств со счета одного банка на карту другого не видно имя владельца карты.

6 **Подключите карту ребенка к своему счету**

Так вы быстро заметите подозрительные покупки и переводы.

7 **Помогайте ребенку искать подработку в интернете**

За обещаниями легких и быстрых денег могут стоять преступные схемы, которые родителям легче распознать.

8 **Обсуждайте с ребенком его виртуальных друзей**

Притворяться в интернете другим человеком гораздо проще, чем в реальной жизни.

9 **Обозначьте правило: если кто-то в интернете просит деньги, нужно убедиться, что это не мошенник**

Даже если сообщение пришло от друзей и знакомых.

10 **Чаще говорите с ребенком о финансах в целом**

Так он быстрее поймет ценность денег.

На портале **моифинансы.рф** рассказываем больше про финансово-цифровую безопасность

ПОМНИТЕ! Финансовая безопасность ребенка в интернете — это процесс воспитания. Поддерживайте с ними открытость и доверие!

Эстафета Мои финансы

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

Подробнее на портале **моифинансы.рф**

ПРОВЕРЬ, СУМЕЕШЬ ЛИ ТЫ СДЕЛАТЬ ПОКУПКИ В ИНТЕРНЕТЕ И НЕ ПОТЕРЯТЬ ДЕНЬГИ?

Пройдите по шагам в нашем чек-листе, узнайте 6 правил онлайн-покупок и наслаждайтесь безопасным интернет-шопингом.

СТАРТ

Вы нашли сайт интернет-магазина или скачали официальное приложение самостоятельно, а не по ссылке из e-mail, смс или сообщения в мессенджере.

ДА

НЕТ

Мошенники под видом магазинов и маркетплейсов рассылают такие ссылки, чтобы украсть личные данные, информацию о банковской карте и деньги.

Вы проверили адрес сайта: в нем нет лишних символов и цифр, нет ошибок, а контакты заполнены.

ДА

НЕТ

Неточности в оформлении интернет-ресурса, опечатки в домене сайта, отсутствие реквизитов продавца — признаки поддельного сайта.

Вы прочитали отзывы перед покупкой и проанализировали стоимость товара

ДА

НЕТ

Помните, что неоправданно низкие цены — одна из уловок злоумышленников. Перед покупкой почитайте отзывы о магазине и сравните цену на товар на других ресурсах.

Вы не подключаетесь к публичному WiFi при оплате товара.

ДА

НЕТ

Мошенники могут использовать дубли точек доступа к общественному WiFi, чтобы похитить ваши данные и получить доступ к банковским приложениям и деньгам.

Вы используете отдельную банковскую карту для онлайн-шопинга и переводите на нее только ту сумму, которую собираетесь потратить.

ДА

НЕТ

Если мошенники получат доступ к отдельной банковской карте, то завладеют только теми средствами, которые есть на ней.

Вы получили после оплаты чек на адрес электронной почты или телефон и сохранили его до получения покупки.

ДА

НЕТ

Электронный чек — доказательство совершения покупки и оплаты товара. Если возникнут проблемы с заказом, вы можете предъявить этот документ.

Вы подключили уведомления банка об операциях по вашей карте.

ДА

НЕТ

Уведомления по карте позволят увидеть списания с карты и понять, куда уходят деньги. При необходимости вы сможете оперативно позвонить в банк.

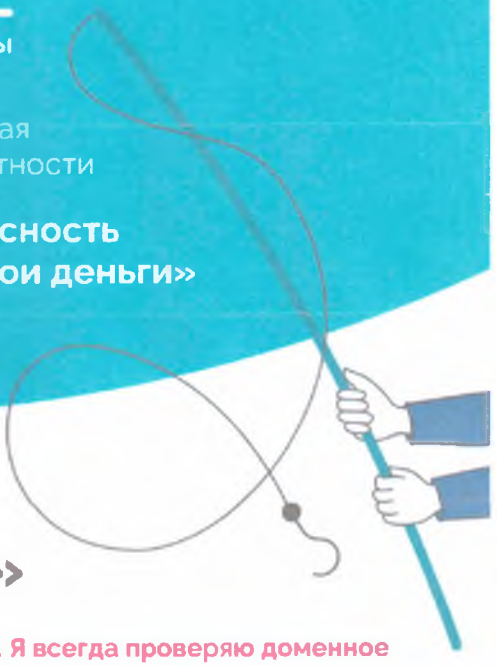
ФИНИШ

Минфин России

мои финансы

Всероссийская просветительская
Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**



ЧЕК-ЛИСТ

«ПРОВЕРЬ, СМОЖЕШЬ ЛИ ТЫ ОБОЙТИ ФИШИНГОВЫЙ САЙТ»

Фишинговый сайт — вид мошенничества, цель которого обманом завладеть персональными данными человека и получить доступ к его деньгам. Термин «фишинг» происходит от английского fishing — рыбная ловля. Проверьте, сможете ли вы отличить настоящий сайт от поддельного.

Если все пункты будут отмечены как «ДА» — поздравляем, вы готовы к встрече с фишинговыми сайтами и сможете защитить свои данные!

1. Я не перехожу по ссылкам из почты, соцсетей и мессенджеров, которые сам не запрашивал

Злоумышленники рассылают сообщения от имени государственных и финансовых организаций, интернет-магазинов, организаторов лотерей и даже родственников и близких. Их цель — заманить жертву на фишинговый сайт, чтобы украсть ее личные данные, информацию о банковской карте и деньги.

◯ ДА ◯ НЕТ

2. Я не нажимаю на всплывающие рекламные баннеры на сайтах

Чтобы не скачать вредоносное ПО и не попасть на поддельный сайт через рекламный баннер, лучше проверить информацию об акции на официальном сайте компании.

◯ ДА ◯ НЕТ

3. Я не игнорирую предупреждение браузера о том, что посещение сайта небезопасно

Уведомление появится, если у ресурса нет SSL-сертификата, который подтверждает подлинность сайта. Это значит, что информация, которую пользователь вводит на сайте, не защищена. Чаще всего если SSL-сертификат есть — в адресной строке отображается значок замка.

◯ ДА ◯ НЕТ

4. Я обращаю внимание на оформление интернет-ресурса

Мошенники торопятся и допускают орфографические и пунктуационные ошибки, используют устаревшие дизайн, логотипы, изображения плохого качества. Это один из признаков фишингового сайта.

◯ ДА ◯ НЕТ

5. Я установил антивирус на свой гаджет и пользуюсь им

Такая программа вовремя предупредит о том, что вы пытаетесь перейти на вредоносную страницу и заблокирует угрозу.

◯ ДА ◯ НЕТ

6. Я всегда проверяю доменное имя сайта, на который зашел

Доменное имя или адрес сайта отображается в браузере в адресной строке. Отличить поддельный домен от настоящего непросто: разница между ними может быть в одной букве или символе.

◯ ДА ◯ НЕТ

7. Я проверяю юридическую информацию и контакты

Настоящие компании и ресурсы размещают название, описание деятельности, реквизиты, способы связи и другие важные документы.

◯ ДА ◯ НЕТ

8. Я сохраняю в «Избранное» сайты, которые чаще всего посещаю

Это позволит быстро перейти на ресурс по правильному адресу. Сохраняя сайт в «Избранное», пользователь запоминает, как выглядит ресурс. Если он случайно попадет на фишинговый сайт, то, скорее всего, заметит разницу во внешнем виде и адресе и вовремя распознает обман.

◯ ДА ◯ НЕТ

Подробнее на портале **моифинансы.рф**