

ТОП-5

онлайн-инструментов, которые помогут обезопасить ваши сбережения от мошенников

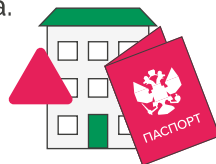
1 ОФОРМИТЕ САМОЗАПРЕТ НА ПОЛУЧЕНИЕ КРЕДИТОВ И ЗАЙМОВ

Устанавливается через
«Госуслуги» или МФЦ.
**Мошенники не смогут
набрать кредитов** на ваше
имя.



2 УСТАНОВИТЕ ЗАПРЕТ НА СДЕЛКИ С ВАШЕЙ НЕДВИЖИМОСТЬЮ БЕЗ УЧАСТИЯ СОБСТВЕННИКА

Устанавливается через
«Госуслуги» или МФЦ.
Мошенники украли данные
паспорта и сделали
фальшивую доверенность?
Теперь **они не смогут
заключить сделку** без
вашего ведома.



3 ПОДКЛЮЧИТЕ СЕРВИС «ВТОРОЙ РУКИ»

Устанавливается в банке.
Если вы склонны слишком
доверять людям, выберите
среди своих родственников
или близких доверенное
лицо, которое будет
подтверждать ваши крупные
денежные переводы. Либо
сами станьте таким лицом,
например для своих
пожилых родителей.

4 УСТАНОВИТЕ ЛИМИТ ТРАТ ПО КАРТАМ И СЧЕТАМ

Устанавливается через
приложение банка или
в отделении банка. Так вы
ограничите сумму, которую
можно вывести со счета
под влиянием мошенников.



5 ИСПОЛЬЗУЙТЕ ПРОВЕРЕННЫЙ БРАУЗЕР И МЕНЕДЖЕР ПАРОЛЕЙ ДЛЯ ПРОВЕРКИ БЕЗОПАСНОСТИ ВАШИХ ДАННЫХ В ИНТЕРНЕТЕ

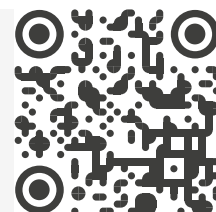
Устанавливается самостоятельно через настройки
браузера. Это хороший способ выявить утечки, взломы
и скомпрометированные учетные записи.

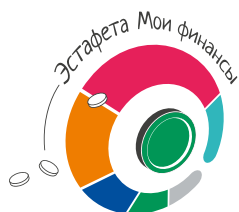


ВНИМАНИЕ!

Эти простые меры значительно
усложняют работу мошенникам
и повысят вашу финансовую
безопасность.

ПОДРОБНЕЕ НА ПОРТАЛЕ
«МОИФИНАНСЫ.РФ» →





ИНСТРУКЦИЯ

«ГОСУСЛУГИ»: КАК РАСПОЗНАТЬ ВЗЛОМ И КАК ВОССТАНОВИТЬ АККАУНТ

Как понять, что ваш личный кабинет на «Госуслугах» взломали?



Сработала двухфакторная аутентификация

Вы не входили в аккаунт, но получили код из СМС.



Не получилось войти в аккаунт

Пароль, который вы всегда использовали, внезапно перестал работать.

Пришло уведомление о подозрительной активности

Вы не заходили в личный кабинет, но ресурс зафиксировал посещение с новых устройств, попытку смены пароля или редактирования персональных данных.

Что делать, чтобы восстановить доступ к учетной записи

ШАГ 1. Восстановите доступ к учетной записи

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 создания 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 выполните действия для подтверждения учетной записи на «Госуслугах».

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

Если мошенники **ИЗМЕНИЛИ** контактные данные

Лично в центре обслуживания

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



ШАГ 2. Проверьте настройки безопасности

Выйдите из учетной записи на «Госуслугах» со всех устройств, кроме текущего. Для этого следуйте алгоритму:

«Безопасность» → вкладка «Действия в системе» → «Выйти». Повторите тоже самое во вкладке «Мобильные приложения».

ШАГ 3. Проверьте, что изменили мошенники в вашей учетной записи

Обратите внимание на номер телефона, сим-карты, банковские карты, счета, электронные подписи, согласия и доверенности, заявления, связанные аккаунты.

ШАГ 4. Убедитесь, что на вас не оформили кредит

Это нужно сделать, если у вас не установлен самозапрет на кредиты. Для проверки 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:

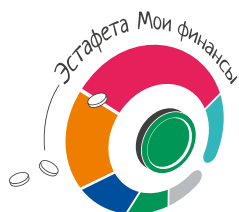
- вход с дополнительным способом подтверждения, помимо пароля;
- контрольный вопрос;
- уведомление о входе в личный кабинет с помощью письма на электронную почту.

ЕСЛИ ВАШ АККАУНТ ЗАБЛОКИРОВАН И ВЫ НЕ МОЖЕТЕ ВОССТАНОВИТЬ ЕГО (см. шаг 1):

- Обратитесь в службу поддержки «Госуслуг»: позвоните на горячую линию **8 800 100 70 10** либо напишите в онлайн-чат через мобильное приложение.
- Подайте заявление в МВД лично или онлайн через интернет-приемную на сайте вашего территориального органа. Укажите все известные вам подробности, включая контактные данные, которые злоумышленники могли использовать вместо ваших. Сохраните копию заявления в полицию и талон-уведомление о его приеме.



Подробнее на портале
моифinanсы.рф



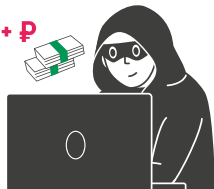
7 ВАЖНЫХ РЕКОМЕНДАЦИЙ

РОДИТЕЛЯМ! КАК НАУЧИТЬ РЕБЕНКА ЗАЩИЩАТЬСЯ ОТ МОШЕННИКОВ В ИНТЕРНЕТЕ

1 МОШЕННИКИ В СЕТИ:

изучайте то, как они
обманывают детей в Сети

Распознать мошенника
легче, когда
вы знаете, как
он действует.



2 ИСТОРИИ ОБМАНА:

регулярно обсуждайте
их с ребенком

Спрашивайте, как бы
ребенок действовал в этих
ситуациях. Это поможет
донести, что риск быть
обманутым в интернете
выше, чем кажется.

3 ПЕРСОНАЛЬНЫЕ ДАННЫЕ:

объясните, что это и почему
их надо хранить в секрете

Если мошенник перехватит
реквизиты карты,
пароли, коды
для подтверждения
операций, семья может
потерять все свои деньги.

4 КАРТА РЕБЕНКА:

подключите ее к своему счету

Так вы быстро заметите
подозрительные покупки
и переводы.



7 БЮДЖЕТ СЕМЬИ:

говорите с ребенком о том,
как он устроен

Так ребенок быстрее поймет
ценность денег.

5 ДЕНЕЖНЫЕ ПЕРЕВОДЫ:

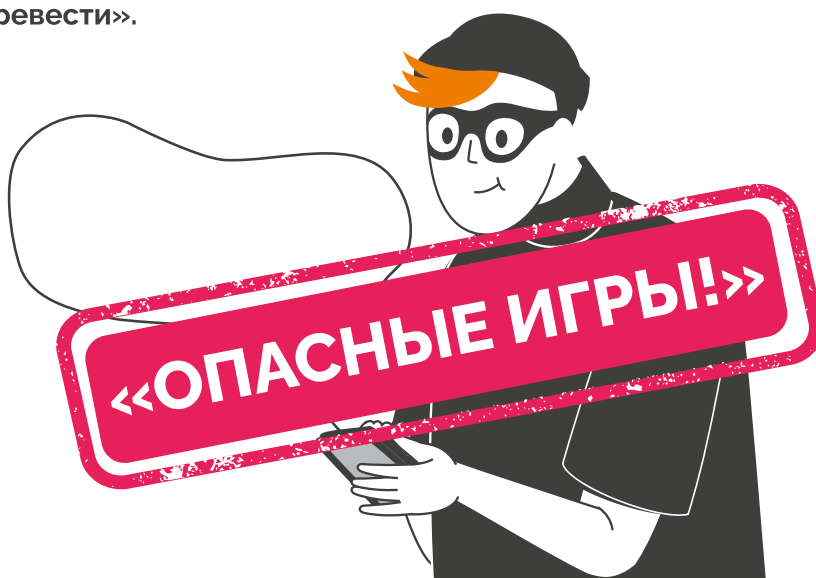
объясните, как делать
их безопасно

Нельзя переводить деньги
незнакомцам. Сначала
проверьте имя получателя
и только потом нажимайте
«Перевести».

6 ДРУЗЬЯ В ВИРТУАЛЬНЫХ ИГРАХ:

обсуждайте их с ребенком

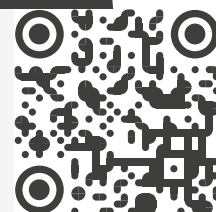
Притворяться в интернете
другим человеком гораздо
проще, чем в реальной жизни.

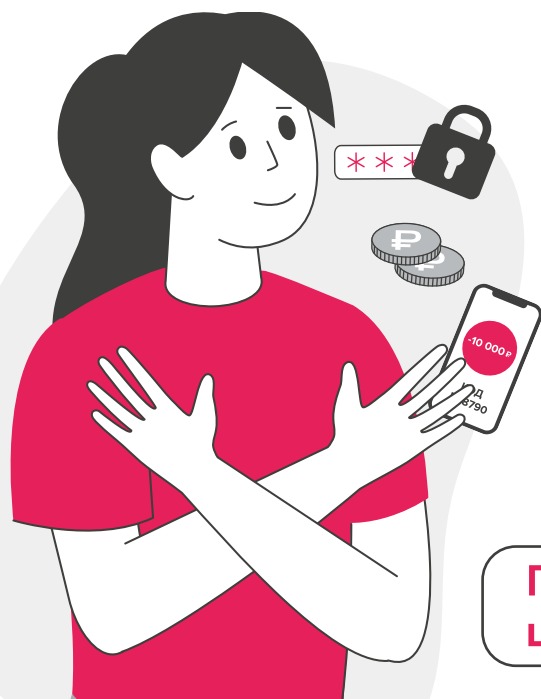
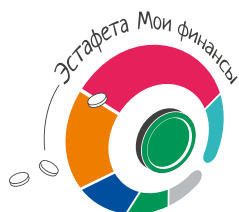


ПОМНИТЕ:

Финансовая безопасность ребенка
в интернете – это не только процесс
воспитания, но и атмосфера доверия!

ПОДРОБНЕЕ НА ПОРТАЛЕ
«МОИФИНАНСЫ.РФ» →





ИНТЕРНЕТ-МОШЕННИКИ:

5 ПРАВИЛ «НЕ», ЧТОБЫ ЗАЩИТИТЬ ДЕНЬГИ ОТ АФЕРИСТОВ!

Правила помогут вам обойти уловки
цифровых мошенников.

1 НЕ СООБЩАЙТЕ

незнакомым коды из СМС

Код из СМС — часть системы
защиты ваших данных
и денег.

Его спрашивают
только мошенники.



2 НЕ ПЕРЕВОДИТЕ

свои деньги по инструкции
незнакомых лиц, кем бы они
ни представлялись.

! Это может
быть кража.



3 НЕ ПОДДАВАЙТЕСЬ

просьбам незнакомцев
вернуть деньги,
присланные «по ошибке»

Это может быть преступная
схема по отмыванию денег.
Сообщите в банк о странном
переводе.



4 НЕ ДЕЛИТЕСЬ

персональными данными с посторонними

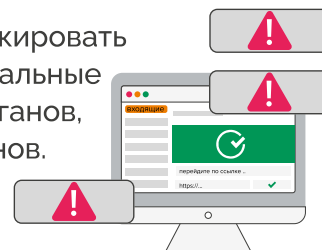
Не сообщайте пароли,
PIN-коды, данные банковских
карт, паспортные данные
и другую конфиденциальную
информацию.



5 НЕ ЛЕНИТЕСЬ

проверять подлинность сообщений и уведомлений

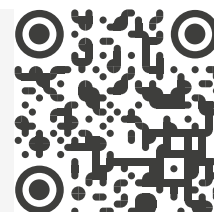
Мошенники могут маскировать
сообщения под официальные
уведомления от госорганов,
банков и даже магазинов.

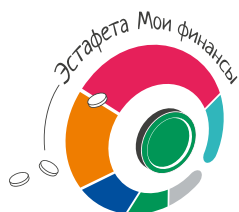


ПОМНИТЕ:

мошенники всегда используют ваши
эмоции и невнимательность в своих
интересах!

ПОДРОБНЕЕ НА ПОРТАЛЕ
«МОИФИНАНСЫ.РФ» →





Всероссийская просветительская Эстафета
по финансовой грамотности «Мои финансы»



МИНФИН
РОССИИ

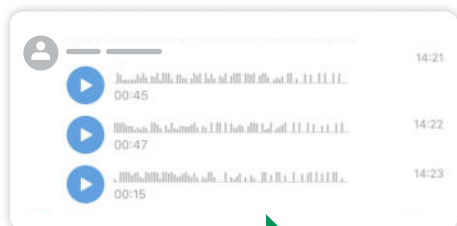
мои финансы

Этап IX: «Безопасность денег в цифровой среде»

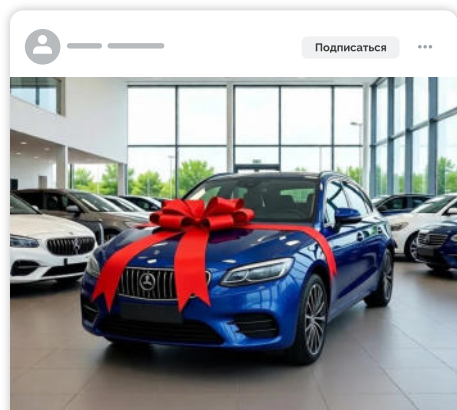
ПАМЯТКА

КАК НАС ВИДЯТ МОШЕННИКИ В СЕТИ!

Посмотри на себя в интернете глазами преступников



Отличная биометрия
для дипфейка: можно
сгенерить голос и ви-
део через ИИ, отправить
родственникам
и потребовать денег.

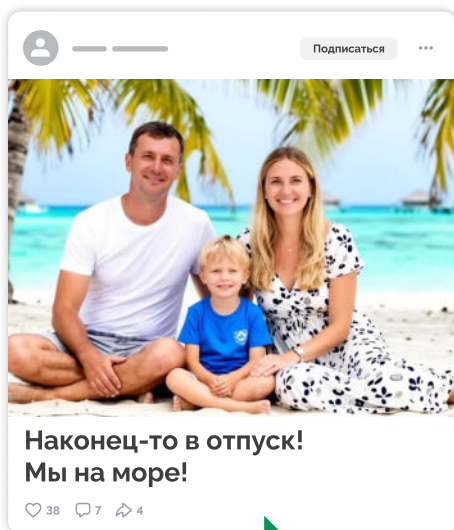


Принимаю поздравления! 🚗
Мой новый конь с полным
приводом! 📺



Здесь все хорошо
с финансами!

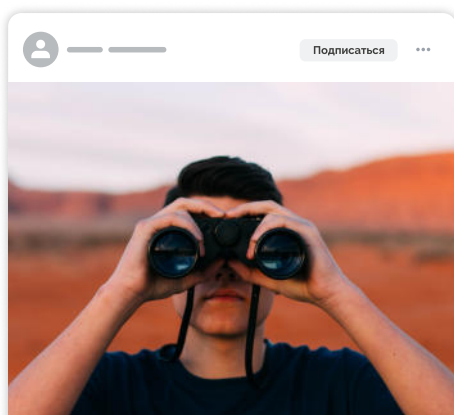
ВНИМАНИЕ! Большую часть информации о себе мы размещаем в социальных сетях сами. Этим пользуются мошенники! Их цель — собрать как можно больше персональных данных, чтобы шантажировать вас и вымогать деньги.



Наконец-то в отпуск!
Мы на море!



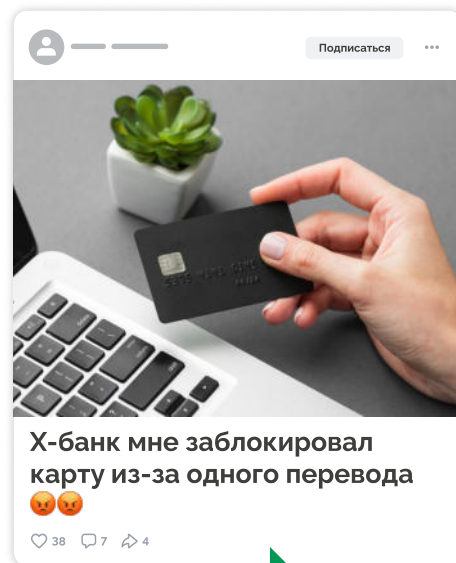
Квартира пустует —
пора «в гости»!



Друзья, буду благодарен
за репост. Ищу работу
копирайтером, удаленка,
резюме скину в личных
сообщениях.



Ему нужна работа,
а мне — дроппер,
чтобы вывести деньги.
Предложу «легкий
заработок».

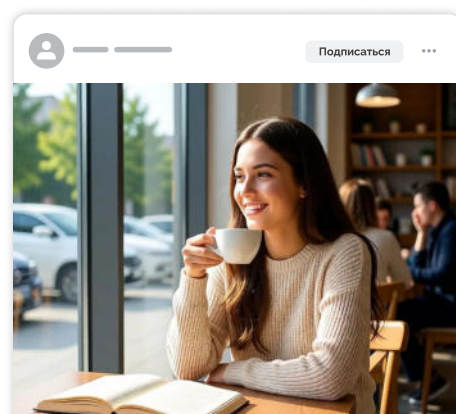
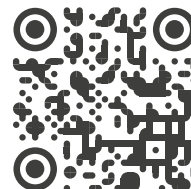


Х-банк мне заблокировал
карту из-за одного перевода



Алло, это служба
безопасности банка!
Видим, что у вас
возникли сложности,
назовите код для
снятия блокировки.

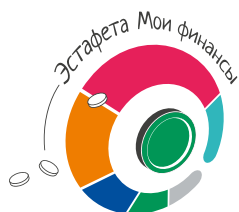
Подробнее
на портале
moifinansy.ru



Каждый вторник — завтрак
здесь, в кафе «Кошечка»!
Уже традиция так начинать
день ☕



Я знаю, где она
отдыхает, что любит,
что посещает.



ПАМЯТКА

Я ДРОППЕР?

Проверьте, не попали ли вы в ловушку
финансовых мошенников

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.

ВНИМАНИЕ!

Дроппером можно
стать случайно!



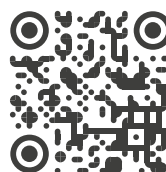
Дроппер —
это человек, которого
мошенники используют
для вывода и обналичивания
похищенных денег.

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.

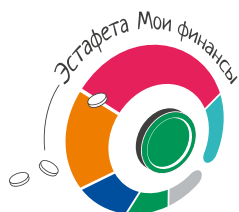
ВЫ ПОПАЛИ В БАЗУ ДРОППЕРОВ. ЧТО ДЕЛАТЬ, ЧТОБЫ ВЫЙТИ ИЗ НЕЕ И СНЯТЬ БЛОКИРОВКУ СО СВОИХ БАНКОВСКИХ КАРТ?

1. Обратитесь в интернет-приемную Банка России и запросите список спорных операций, из-за которых вы попали в базу дропперов.
2. Регулятор отправит список платежей и переводов, которые обжаловали пострадавшие. У каждой операции будет уникальный идентификатор — REQ.
3. Подайте заявление в свой банк об отказе от зачисления средств по этим операциям. В заявлении укажите REQ всех проблемных операций. Сделать это можно в отделении банка, приложении или личном кабинете на сайте банка.
4. После того как банк отправит платежи и переводы обратно жертвам, получите в отделении справку о возврате средств пострадавшим. В документе должны быть перечислены все операции с указанием их REQ.
5. Повторно подайте заявление в интернет-приемную Банка России об исключении из базы дропперов и приложите справку из банка. В течение 15 рабочих дней регулятор проведет проверку. Он уберет ваши данные из базы дропперов. Блокировки с банковских карт также будут сняты.



Подробнее
о дропперах
читайте
на moifinansy.rf

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.



ЧЕК-ЛИСТ

ОСТОРОЖНО: ЛЖЕБРОКЕР!

Проверьте, сможете ли вы распознать его

Представьте, что вы готовы начать инвестировать и вам надо открыть брокерский счет. В интернете вы нашли инвесткомпанию с подходящими вам условиями и предложениями. Какими будут ваши действия перед подписанием договора? Читайте ситуации, отмечайте «да» или «нет». В конце проверьте свой результат.

СИТУАЦИЯ 1

На сайте брокера нет информации о лицензии от Банка России. Вы откроете счет в этой компании?

ДА Брокер — это не банк и не обязан получать лицензию.

НЕТ Лицензия — это главное отличие легального брокера от мошенника.

СИТУАЦИЯ 2

Инвесткомпания обещает высокую фиксированную доходность за короткий срок. Для вас это хороший аргумент, чтобы заключить договор?

ДА Я ищу компанию, которая может гарантировать высокую доходность.

НЕТ Доходность в инвестициях гарантируют только мошенники.

Внимание! Если вы стали жертвой мошенников:

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



СИТУАЦИЯ 3

Вы нашли подходящего брокера, поговорили с его представителем, но еще в раздумьях, стоит ли открывать счет у него. Между тем представители компании начали активно звонить вам и подталкивать к решению. Это хороший знак?

ДА Это хороший клиентский сервис.

НЕТ Любые требования немедленно внести деньги настораживают.



СИТУАЦИЯ 4

На сайте компании все ссылки на контакты ведут на сторонние ресурсы или на главную страницу. Вы не можете найти ни юридический, ни фактический адрес. Менеджеры активно общаются с вами, но все общение идет через мессенджеры и по телефону. Это нормальная ситуация?

ДА Персонал постоянно на связи. Это главное.

НЕТ На сайте должны быть указаны полные контактные данные юрлица.

СИТУАЦИЯ 5

По условиям брокера на счет можно внести любую сумму, чтобы начать инвестировать. Менеджер говорит: «Кладите хоть 100 рублей». Это подозрительно?

ДА Какие инвестиции со 100 рублями? Явно что-то не то.

НЕТ Брокера не должно волновать, сколько у меня денег.



СИТУАЦИЯ 6

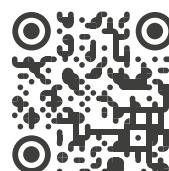
Вы изучили условия брокерского обслуживания и обратили внимание на то, что брокер взимает ощутимые комиссии за вывод средств и проценты по займам. Это мошенник?

ДА Проценты по займам берет только банк.

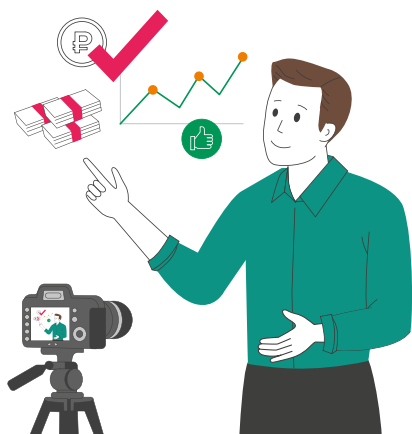
НЕТ Это стандартные условия договора легального брокера.

РЕЗУЛЬТАТЫ

Если на все вопросы вы ответили «НЕТ», поздравляем, вы точно можете отличить лицензированного брокера от мошенника и избежать потери денег. Если хотя бы на один вопрос вы ответили «ДА», ваши инвестиции в зоне риска.



Подробнее
на портале
moi-finansy.ru



ГАЙД

ШАРЛАТАН VS ФИНАНСОВЫЙ БЛОГЕР: КАК РАСПОЗНАТЬ

Семь важных признаков псевдо-экспертов. Задумайтесь, прежде чем отдавать свои деньги финансовому эксперту, у которого есть хотя бы один признак.

ПРИЗНАК 1

НЕ ПОДТВЕРЖДАЕТ СВОЕ ОБРАЗОВАНИЕ И ОПЫТ

Проверьте, есть ли у блогера профильное образование, сертификаты или подтвержденный опыт работы в финансах. Часто курсы от условного ноунейма оказываются содержательнее и полезнее, чем от раскрученного блогера.

ПРИЗНАК 2

НЕТ КОНКРЕТИКИ И ПРИМЕРОВ

Эксперт не говорит открыто о своей квалификации и источниках знаний. В публикациях нет реальных кейсов, расчетов, ссылок на официальные источники. Финансовый управляющий не показывает свой портфель и достижения на фондовом рынке.

ПРИЗНАК 3

ОБЕЩАЕТ «ЗОЛОТЫЕ ГОРЫ»*

Гарантирует прибыль от своих проектов, «уникальные продукты» и быстрое улучшение финансового состояния, стоит только пройти его платные курсы.

ПРИЗНАК 4

О КУРСАХ ЭКСПЕРТА НЕТ ОТЗЫВОВ ИЛИ ОНИ ТОЛЬКО ПОЗИТИВНЫЕ

Комментарии под постами закрыты. Оставить свою реакцию невозможно.

ПРИЗНАК 5

АКЦЕНТ НА РОСКОШНЫЙ ОБРАЗ ЖИЗНИ

Навязчиво демонстрируют финансовый достаток: дорогие машины, рестораны, квартиры, отдых. Основной посыл: «Делай как я, и станешь миллионером». Помните, что роскошь — это маркетинг, а никак не доказательство компетенции.

ПРИЗНАК 6

АГРЕССИВНЫЕ ПРОДАЖИ И ИСКУССТВЕННЫЙ АЖИОТАЖ

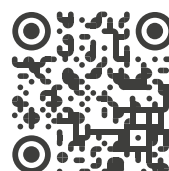
«Остались последние места на интенсив», «Цена взлетит уже завтра, нужно купить сейчас». Если блогер постоянно навязывает платные курсы, марафоны или консультации, давит и манипулирует, это тревожный знак.

ПРИЗНАК 7

ТОРГУЕТ «ГОТОВОЙ СТРАТЕГИЕЙ» И «ДОСТУПОМ В ЗАКРЫТЫЙ КЛУБ»

Продаются не знания, а готовые указания, логика которых не ясна. Вы не учитесь инвестировать, а следуете за финансовым гуру. Это уязвимая позиция, когда не ясно, что делать, если ситуация на рынке пойдет не так, как говорит стратегия.

*Сразу закрывайте предложения, если вы видите гарантированную доходность существенно выше ключевой ставки Банка России.



Подробнее
на портале
moi-finansy.ru