



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

### 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

### 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

### 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.

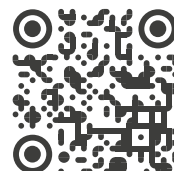
☐ ДА ☐ НЕТ

### 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](http://моифинансы.рф)





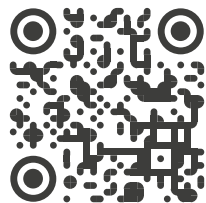
Минфин  
России

мои финансы

Всероссийская просветительская Эстафета  
по финансовой грамотности

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

Подробнее  
на портале  
[моифинансы.рф](http://моифинансы.рф)



СТАРТ

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

НЕТ

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

ДА

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

НЕТ

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

ДА

Вы прочитали отзывы перед покупкой и проанализировали стоимость товара

НЕТ

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

ДА

ФИНИШ

Вы подключили уведомления банка об операциях по вашей карте.

НЕТ

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

ДА

## 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.

Вы не подключаетесь к публичному WiFi при оплате товара.

НЕТ

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

ДА

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

ДА

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

НЕТ

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

ДА

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

НЕТ



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 нужно назвать 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.

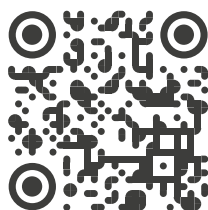
**Курьерские службы не просят** коды из смс для подтверждения доставки. Свяжитесь с отправителем подарка и уточните детали. Если это сделать не удастся — не принимайте презент.

### 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  
[moifinansy.rf](http://moifinansy.rf)



### 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.



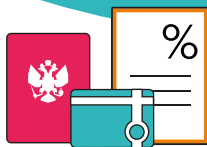
Минфин  
России

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

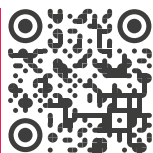
Злоумышленники рассылают сообщения от имени государственных и финансовых организаций, интернет-магазинов, организаторов лотерей и даже родственников и близких. Их цель — заманить жертву на фишинговый сайт, чтобы украсть ее личные данные, информацию о банковской карте и деньги.

### 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  
[моифinanсы.рф](http://моифinanсы.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 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 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 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.



«lLoveYou2025»



«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.

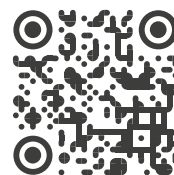


Запоминать пароль в уме. Придумайте ассоциацию, которая позволит легко воспроизвести код. Например, «Mountain!TriP2019#» может ассоциироваться с походом в горы.

## 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](http://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

# 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

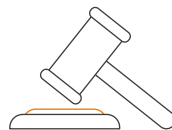
Напишите заявление  
в полицию. Предоставьте  
доказательства: записи  
разговоров, сообщения,  
данные о переводах.



### 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.



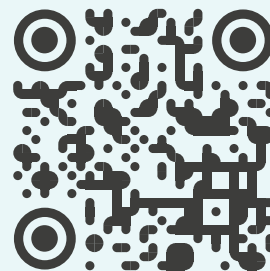
### ШАГ 7

#### 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  
[moifinansy.rf](https://moifinansy.rf)



**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 открытом 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

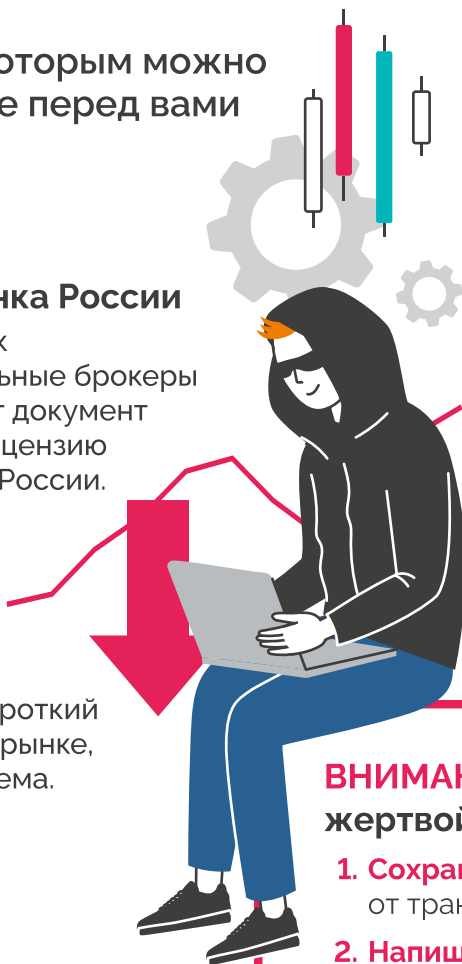
**Требуется перевести  
деньги на карту физлица**

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**

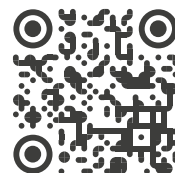
Брокеры-мошенники  
в большинстве случаев строят  
все общение через соцсети  
и телефон. А на сайте  
компании все ссылки  
на контакты ведут  
на сторонние ресурсы или  
на главную страницу.

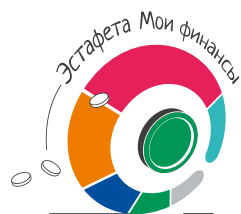


**ВНИМАНИЕ! Если вы стали  
жертвой мошенников на бирже**

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](http://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.



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

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



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

Незнакомцы могут предлагать схемы, направленные на кражу ваших денег.



**Не возвращайте деньги, присланные по ошибке неизвестными**

Такие переводы могут быть связаны с мошенническими схемами.



**Остерегайтесь фишинга**

Будьте внимательны к сайтам, которые требуют вводить личные данные.



**Не спешите реагировать на тревожные звонки и сообщения**

Мошенники манипулируют эмоциями, которые притупляют бдительность.



**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](http://моифинансы.рф) рассказываем больше про финансово-цифровую безопасность →

