



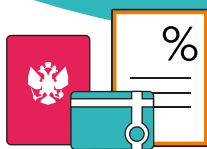
Минфин
России

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

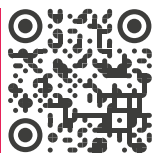
Злоумышленники рассылают сообщения от имени государственных и финансовых организаций, интернет-магазинов, организаторов лотерей и даже родственников и близких. Их цель — заманить жертву на фишинговый сайт, чтобы украсть ее личные данные, информацию о банковской карте и деньги.

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



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»

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.

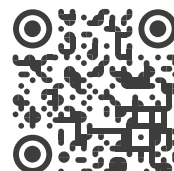
☐ ДА ☐ НЕТ

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





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

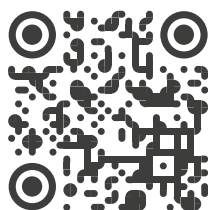


СХЕМА 4. Заканчивается договор сотовой связи

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 предложения, чтобы выманить его. Этот код дает доступ к вашим персональным данным и банковским счетам.



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

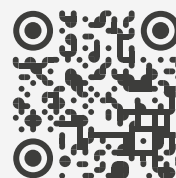
Преступникам важно, чтобы вы действовали импульсивно.

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!**