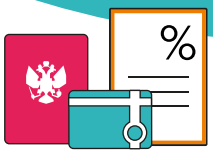
Эстафета Мои финансы

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.

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.

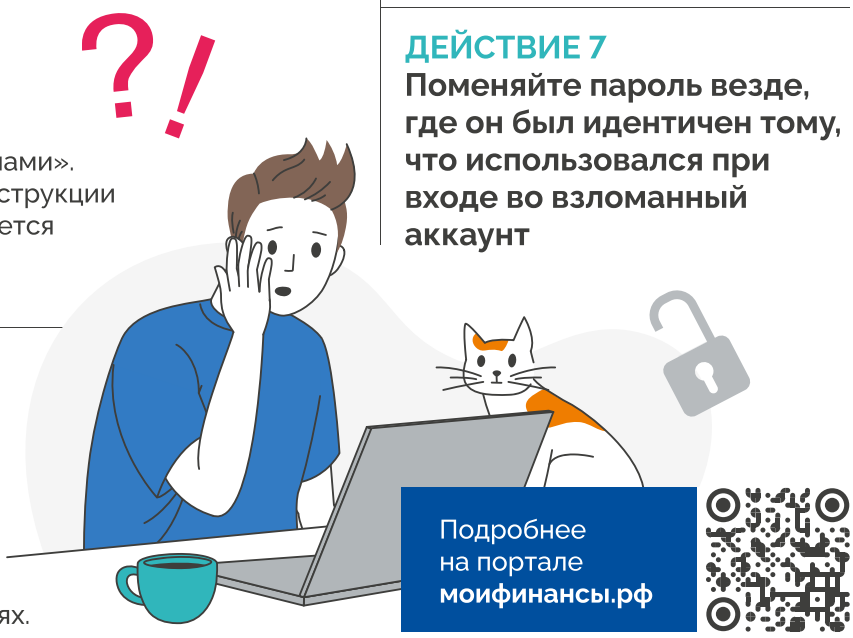
ДЕЙСТВИЕ 5
Обратитесь в банк или платежный сервис, если к учетной записи была привязана карта

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!

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.

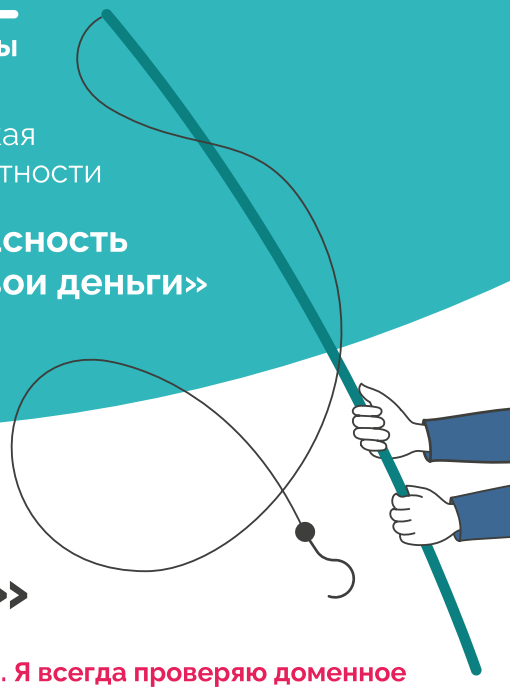
ФИНИШ

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**