

Взломали «Госуслуги»: что делать?



Для мошенников ключом к персональным данным может стать аккаунт на портале «Госуслуги». Его взлом грозит серьезными последствиями: от оформления кредитов на ваше имя до кражи налоговых вычетов. Расскажем, как распознать взлом, восстановить доступ, проверить наличие мошеннических действий и минимизировать риски в будущем.

Как понять, что профиль взломан?

Есть признаки, по которым можно заподозрить взлом личного аккаунта на портале «Госуслуги»:

1. Сработала двухфакторная аутентификация

Если вы не пытаетесь войти в аккаунт, но получили код из СМС, это тревожный сигнал. Он означает, что кто-то пытается войти в ваш профиль. Паниковать не нужно: без кода подтверждения злоумышленник не сможет авторизоваться.

Никому не передавайте коды из СМС-сообщений. Если звонящий представляется сотрудником службы поддержки, верить на слово ему нельзя. Это может быть мошенник.

2. Не получилось войти в аккаунт

Если пароль, который вы всегда использовали, внезапно перестал работать, высока вероятность, что мошенники изменили его. Это стандартная тактика: получив доступ к вашему аккаунту, злоумышленники сразу меняют учетные данные, чтобы заблокировать владельца аккаунта.

3. Пришло уведомление о подозрительной активности

Портал «Госуслуги» отслеживает подозрительные действия: входы в аккаунт с новых устройств, попытки смены пароля или редактирования персональных данных. Если вы получили такое оповещение:

- ✓ Проверьте историю входов в разделе «Безопасность» → «Действия в системе».

- ✓ Во вкладке «Мобильные приложения» нажмите «Выйти» из тех приложений, в которые вы не входили.
- ✓ Придумайте новый пароль.

Проверьте, не добавлены ли в аккаунт чужая почта, номера телефонов или паспортные данные. Мошенники часто подменяют контакты, чтобы перехватывать коды подтверждения.

Основные риски

Риски взлома аккаунта существенные. Хотя «Госуслуги» не выдают кредиты, через портал можно подтвердить личность для МФО и банков. Мошенники используют украденные личные данные и справки о доходах из кабинета налогоплательщика, чтобы оформить займы.

Через кабинет ФНС, доступный к входу через «Госуслуги», мошенники также могут подать заявление на возврат НДФЛ, указав реквизиты своего банковского счёта. Рекомендуется регулярно отслеживать статус налоговых деклараций и историю операций в личном кабинете налогоплательщика на сайте ФНС.

В профиле «Госуслуг» также хранится информация о месте жительства, банковских счетах, недвижимости, автомобилях и даже медицинских услугах. Эти данные злоумышленники могут продать в «даркнете» или использовать самостоятельно для обмана потенциальной жертвы – например, позвонить родственникам с просьбой о «срочной помощи».

Также личные данные могут быть использованы для шантажа или создания фэйковых документов. У мошенников в арсенале много схем обмана с использованием украденных персональных данных.

Встречаются также случаи, когда злоумышленники блокируют вход в «Госуслуги», а затем требуют деньги за восстановление пароля.

Восстанавливаем доступ к учетной записи

Заподозрив взлом аккаунта на портале «Госуслуги», паниковать не стоит, но и откладывать решение проблемы тоже нельзя. Есть несколько сценариев, как следует поступить.

Сценарий 1: Контактные данные (телефон, email) не изменены

Перейдите на страницу входа в аккаунт и нажмите «Восстановить доступ».

Выберите способ восстановления:

- по номеру телефона — введите цифры из СМС,
- по email — перейдите по ссылке из письма,
- подтвердите личность, указав данные паспорта, ИНН или СНИЛС,
- задайте новый сложный пароль.

Сценарий 2: Мошенники изменили телефон и email

Попробуйте зарегистрироваться заново онлайн через банк: СберБанк, Тинькофф, ВТБ и другие банки-партнеры позволяют создать учетную запись на «Госуслугах».

Если восстановить аккаунт не получилось, обратитесь в ближайший центр «Мои документы» (МФЦ):

- ✓ Возьмите с собой паспорт и СНИЛС
- ✓ Сообщите о взломе
- ✓ После проверки документов вам выдадут временный пароль для входа в аккаунт и при необходимости

Сценарий 3: Аккаунт полностью заблокирован

Обратитесь в службу поддержки «Госуслуг». Для этого позвоните на горячую линию 8 800 100 70 10 либо напишите в онлайн-чат через Telegram или мобильное приложение. Для восстановления понадобится:

- ✓ скан паспорта,
- ✓ СНИЛС,
- ✓ доказательства взлома (скрины уведомлений, заявление в полицию).

Рекомендуется также подать заявление в МВД – это можно сделать как лично, так и онлайн. На сайте МВД нужно выбрать свой регион и подать обращение через интернет-приёмную 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. Они могут пригодиться для оспаривания мошеннических сделок – например, если мошенники оформили на вас кредит или заем.

Как проверить, не оформили ли на вас кредит

Если удалось восстановить доступ к вашему аккаунту, хорошо. Однако не лишним будет проверить, не получили ли злоумышленники на ваше имя кредит или заем. Это можно сделать самостоятельно. Для этого закажите кредитную историю через «Госуслуги». Нужно зайти в раздел «Штрафы и налоги», а затем нажать «Поиск бюро с вашей кредитной историей». Закажите в кредитных бюро отчёты.

Проанализируйте полученный отчет. В разделе «Текущие обязательства» ищите незнакомые кредиты или займы. Если вы обнаружили кредит, который не брали, действуйте:

- ✓ Свяжитесь с кредитором: позвоните в банк или МФО, объясните ситуацию, запросите копию договора и документы, которые предоставил «заемщик».
- ✓ Напишите заявление об оспаривании: укажите, что не подавали заявку и не получали деньги, приложите справку из полиции, требуйте провести экспертизу подписи в договоре.
- ✓ Обратитесь в суд, если кредитор отказывается списывать долг. Используйте доказательства: данные о взломе аккаунта, геолокацию (если заявку подавали из другого города).

Также проверить запросы на кредитование и займы можно через вкладку «Безопасность» → «Действия в системе». Проверьте разрешения и согласия. Для этого в личном кабинете нужно зайти в «Профиль» → «Согласия и доверенности».

Отзовите согласия и разрешения, которые вы не давали. Если случайно отзовете нужные, их можно будет потом выдать повторно.

Профилактика взломов: 7 правил безопасности

Взлом аккаунта на «Госуслугах» — это не только угроза финансовым ресурсам, но и риск потери репутации, времени и нервов. Соблюдая правила цифровой гигиены, вы минимизируете вероятность компрометации данных. Помните, что профилактика всегда проще, чем устранение последствий.

- ✓ Создайте надежный пароль. Старайтесь использовать комбинацию из различных символов: латиница + кириллица + цифры + знаки (Пример: **«М0йП@р0ль_2024!»**). Не применяйте одинаковые пароли для разных сервисов.
- ✓ Включите двухфакторную аутентификацию. В настройках «Госуслуг» активируйте «Вход с подтверждением по СМС».
- ✓ Настройте уведомления о входах. В разделе «Безопасность» включите опции: «Присылать оповещения о новых входах» и «Требовать подтверждение для смены пароля».
- ✓ Регулярно обновляйте данные: если сменили телефон или email, сразу внесите изменения в профиль.
- ✓ Используйте функцию «Самозапрет на кредиты» – так можно запретить онлайн-оформление займов без личного визита в банк.
- ✓ Установите контрольный вопрос (Профиль → Безопасность → Вход в систему) – это усложнит доступ мошенников к вашей учётной записи
- ✓ Никогда не сообщайте коды/пароли доступа к «Госуслугам» посторонним, не входите на портал по присланным ссылкам.