

Что значит мошенничество на Госуслугах

Сценариев мошенничества много. Злоумышленники представляются специалистами Госуслуг, операторами сотовой связи, сотрудниками Роскомнадзора. Говорят уверенно и правдоподобно, ссылаются на законы. Но задача у них одна — получить доступ к данным человека.

ВАЖНО: Служба поддержки Госуслуг никогда не звонит и не запрашивает пароли, коды доступа или ответы на контрольные вопросы.

Если вам пришло письмо, СМС или сообщение в мессенджере о взломе или блокировке Госуслуг — это мошенники. Удалите сообщение и не переходите по ссылкам из письма. Сервис не блокирует учётные записи без запроса пользователя.

Официальные уведомления приходят только через личный кабинет или приложение.

Последствия взлома аккаунта

Если злоумышленники всё-таки получают доступ к Госуслугам, они используют личные данные для телефонных атак или обмана родственников жертвы.

Злоумышленники получают возможность заказать электронную SIM-карту и использовать её для других схем. Например, для регистрации на поддельных сайтах или рассылки спама.

Через аккаунт также оформляют кредиты, займы или налоговый вычет. В последнем случае деньги уходят на счёт аферистов, если вовремя не отменить заявку на сайте налоговой.

С 1 марта 2025 года можно оформить самозапрет на кредит через Госуслуги. Запрет будет действовать бессрочно — пока вы его не отмените. Количество установок и отмен неограниченно.

Какие признаки взлома аккаунта

- Не получается войти. При вводе логина и пароля система не пускает в личный кабинет.
- Появились подозрительные уведомления и записи. Например, неожиданно приходит сообщение о смене пароля, привязке нового номера телефона или оформлении услуг.
- Пришло уведомление о подозрительной активности. Если система сама сообщает о возможном взломе, это повод проверить безопасность аккаунта.

Как защитить от мошенников аккаунт на Госуслугах

Чтобы личный кабинет не взломали, соблюдайте несколько правил безопасности. Эти меры помогут избежать неприятных ситуаций.

1. Настройте двухфакторную аутентификацию. Это дополнительная защита: для входа потребуется не только пароль, но и код, который придёт на телефон. Как это сделать: зайдите в настройки личного кабинета, выберите раздел «Безопасность», «Вход в систему». Затем выберите способ аутентификации.

2. Выберите дополнительный способ входа в систему. Можно выбрать несколько вариантов входа в систему, в том числе по биометрии, по ответу на контрольный вопрос. Также пользователю доступно получение уведомлений на электронную почту каждый раз при входе в учётную запись. Это поможет узнать, если кто-то попытается попасть в аккаунт.

3. Подберите сложный надёжный пароль, который нельзя угадать. Он должен содержать буквы (в верхнем и нижнем регистре), цифры и специальные символы, например `**~!@#$%^&***`. Избегайте простых комбинаций, таких как `qwerty` или `123456`. Не берите за основу имя, дату рождения.

4. Регулярно обновляйте данные. При изменении номера телефона или электронной почты обновите их в настройках. Мошенники могут воспользоваться, например, предыдущим номером, чтобы зайти в профиль. Также это упростит восстановление доступа, если что-то пойдет не так.

Советы по безопасности в интернете

Будьте внимательны всегда: аферисты могут атаковать не только Госуслуги, но и другие сервисы, соцсети, интернет-банки, почту. Если вам пришло письмо с просьбой подтвердить данные, не спешите вводить пароль. Не открывайте письма о сомнительных выигрышах и выгодных предложениях, новых выплатах от государства или голосованиях о ремонте дома.

Информационный материал подготовлен Прокуратурой Кытмановского района