**Взлом Госуслуг в 2025 году: чем грозит**

Почему опасно, если к госуслугам получит доступ посторонний человек, в [интервью Банки.ру](https://www.banki.ru/news/daytheme/?id=11015171) рассказала эксперта проекта Минфина России «Мои финансы» Ольга Дайнеко.

В личном кабинете портала Госуслуги содержится значимый массив основной личной информации, а учетная запись – ключ от многих дверей для идентификации личности. Злоумышленник, завладевший госуслугами своей жертвы, получает доступ к паспортным данным, сведениям о детях, оформленным соцвыплатам, номеру СНИЛС, перечню банковских счетов и недвижимости, автотранспорту в собственности.

С помощью доступа к аккаунту Госуслуг можно:

- заменить учетные данные (например, номер телефона, на который будут приходить коды подтверждения действий на портале). Однако, без помощи владельца аккаунта и его телефона сделать это нельзя, но мошенники активно используют социальную инженерию и убеждают своих жертв передавать необходимые коды из смс;

-использовать идентификацию личности на портале и подать заявку на кредитование/оформить микрозайм;

- с помощью идентификации личности на Госуслугах войти в личный кабинет налогоплательщика и оформить полагающийся налоговый вычет (например, по предзаполненным заявлениям), указав свои банковские данные для получения денег;

- оформить eSIM (цифровой аналог пластиковой сим-карты) и далее использовать их в своих схемах обмана;

- подать заявление на снятие наложенного ранее самозапрета на кредитование;

-самое очевидное- получить доступ к персональным/личным данным, которые потом можно использовать для мошеннических действий далее (обладание расширенными личными данными жертвы, а также сведениями о детях, поданных заявлениях на соцвыплаты, об имущественном и семейном положении позволяют создавать правдоподобные сценарии обмана). Кроме того, все похищенные данные объединяют в базы, которые потом продаются. Чем больше в базе сведений, тем дороже «товар».

**Как защититься?**

«Госуслуги» - простой, удобный и надежно защищенный сервис. Взломать личный кабинет извне без участия владельца учетной записи невозможно, поэтому все способы защиты своего аккаунта на Госуслугах нацелены на сохранение конфиденциальности данных для входа на портал:

- использовать надежный пароль для входа и регулярно его обновлять, не использовать один и тот же пароль для нескольких цифровых сервисов;

- использовать дополнительное подтверждение для входа в систему: в настоящее время двухфакторная аутентификация при входе в Госуслуги встроена по умолчанию (вход нужно подтверждать одноразовым кодом из СМС или ТОТР), а задача пользователя-никому не передавать данные с полученным кодом;

- заходить в Госуслуги только на официальном сайте платформы или через официальное приложение. Не проходить авторизацию по ссылкам, прикрепленных к присланным сообщениям или письмам. Мошенники создают поддельные сайты, визуально похожие на портал Госуслуг, чтобы похищать логины/пароли и коды из смс для входа в личный кабинет;

- создать контрольный вопрос для восстановления доступа к учетной записи (при восстановлении система сначала запросит дополнительную информацию (например, дату выдачи паспорта) и следом- контрольный вопрос). Это усложнит доступ к учетной записи посторонним.

Также необходимо соблюдать общую цифровую гигиену: не использовать для входа в Госуслуги публичный доступ в интернет, не скачивать файлы и приложения из неизвестных источников, не переходить по присланным ссылкам, не сохранять логины и пароли доступа в браузере (не использовать автосохранение) и не входить в аккаунт с чужих устройств.

Для дополнительной защиты аккаунта (контролирования входа и его действий на портале) слишком доверчивого родственника можно использовать для Госуслуг отдельную сим-карту, вставленную в телефон другого близкого родственника. Однако основные данные для входа (логин/пароль) все-таки передаваться не должны: отношения даже между членами семьи могут испортиться и это не должно отражаться на возможности использования платформы. Кроме того, физическое отсутствие телефона, на который приходит СМС и уведомления о действиях-не панацея. Мошенники умело обрабатывают своих жертв, в том числе, могут убедить лично обратиться в МФЦ для смены телефонного номера. Важнее быть в контакте с пожилым родственником, регулярно проговаривать правила цифровой и финансовой безопасности, убеждать советоваться с близкими родственниками при принятии значимых решений и рассказывать о своих контактах с незнакомцами (кем бы они не представлялись). Вместо или вместе с сим-картой в удаленном доступе владельца можно использовать присоединение к аккаунту Госуслуг электронной почты близкого родственника, на который будут дублироваться уведомления обо всех действиях на портале.