Как защитить учётную запись на Госуслугах?

1. Настройте вход с дополнительным способом подтверждения. Он обязателен - такой вход позволяет защитить ваши данные на всех сайтах, куда можно войти по логину и паролю от Госуслуг. Это означает, что помимо пароля вам нужно дополнительно подтвердить вход ещё одним способом:
- кодом из смс
- одноразовым кодом (ТОТР)
- с помощью биометрии
2. Подключите уведомления о входе на электронную почту. Вы будете получать письмо каждый раз, когда кто-то входит в вашу учётную запись, в том числе вы сами. Это позволит быстро узнать о взломе, если он произошёл без вашего участия
3. Установите контрольный вопрос. Ответ на контрольный вопрос усложнит доступ мошенников к вашей учётной записи, если они попытаются восстановить пароль от неё

<u>Дополнительные меры безопасности</u>

- Используйте уникальные логин и пароль, которые не встречаются на других сайтах
- Никому не сообщайте ответ на контрольный вопрос и коды из смс, которые приходят от отправителя gosuslugi и с номера 0919
- Внимательно проверяйте адрес сайта. Единственно верный адрес Госуслуг - gosuslugi.ru. Проверяйте, чтобы в адресной строке не было похожих написаний вроде gossuslugi, gos.uslugi, gosuclugi и других.
- Не переходите по подозрительным ссылкам. Ссылки от Госуслуг ведут в личный кабинет, на конкретную услугу, другие разделы портала, сайты ведомств, правовые системы и формы заявлений
- Не открывайте присланные файлы, если не уверены в отправителе. Письма от Госуслуг
приходятс адресов no-reply@gosuslugi.ru, no-reply@pos.gosuslugi.ru, no-reply@dom.gosuslugi.ru
Устанавливайте официальные приложения. Приложение «Госуслуги» можно скачать в RuStore, Google Play, App Store и AppGallery

Если учётную запись взломали

Шаг 1: восстановите доступ к учётной записи
Восстановите пароль. Это можно сделать:
- на Госуслугах - если телефон или электронная почта указаны в личном кабинете и есть доступ к одному из контактов
- онлайн через банк - если нет доступа к телефону или почте из личного кабинета
- лично в Многофункциональном центре - во всех случаях
- Проверьте, ваш ли номер телефона указан в личном кабинете

Шаг 2: защитите учётную запись
- Подключите контрольный вопрос и другие возможности для защиты учётной записи

Шаг 3: выйдите из учётной записи со всех устройств, кроме текущего
- Перейдите в личный кабинет → Профиль → Безопасность
- Во вкладке «Действия в системе» нажмите «Выйти»
- Во вкладке «Моб. приложения» нажмите «Выйти» из тех приложений, в которые вы не входили

Шаг 4: посмотрите, где использовалась учётная запись
- Перейдите в личный кабинет → Профиль → Безопасность → Действия в системе
- Проверьте, не было ли подозрительных действий в учётной записи, чтобы понять, в каких организациях мошенники хотели взять кредиты. Обращайте особое внимание на упоминания банков и микрофинансовых организаций (МФО)
- Свяжитесь с этими организациями. Уточните, есть ли заявления от вас, и сообщите, что их подавали не вы
- Проверьте и отзовите разрешения и согласия. Для этого перейдите в личный кабинет → Профиль → Согласия и доверенности:
во вкладке «Разрешения» откройте каждое из них и нажмите «Отозвать разрешение»
во вкладке «Согласия» откройте каждое из них и нажмите «Отозвать согласие»
Если отзовёте нужные разрешения, их можно будет выдать повторно

Шаг 5: проверьте заявления и уведомления
- Проверьте список поданных заявлений и ленту уведомлений за то время, пока у мошенников был доступ к вашей учётной записи
- Обычно они запрашивают обновление данных электронной трудовой книжки (ЭТК), индивидуального лицевого счёта (ИЛС), 2-НДФЛ, чтобы узнать больше финансовой информации о вас

Шаг 6: убедитесь, что на вас не взяли кредит
- Запросите на Госуслугах список бюро кредитных историй (БКИ), в которых хранится ваша кредитная история
- Закажите в БКИ отчёты. Это можно делать бесплатно 2 раза в год, дальше — платно. У каждого бюро свои тарифы и условия
- Посмотрите, какие заявки на кредиты подавались от вашего имени
- Если на вас взяли кредит - срочно обратитесь в банк или МФО и сообщите, что заявку на кредит подали мошенники

Шаг 7: подайте заявление в МВД

- Это нужно сделать, даже если в кредитной истории нет неизвестных вам заявок на кредит. Мошенники могут использовать ваши данные позже, если у них останется доступ к учётной записи на Госуслугах. Поданное заявление поможет доказать, например, что кредит или заём оформляли не вы
- Подать заявление можно лично или онлайн. Чтобы обратиться онлайн, выберите свой регион на сайте МВД и подайте обращение через интернет-приёмную на сайте вашего территориального органа.

Схемы мошеннических действий

Как мошенники воруют доступ к аккаунтам на Госуслугах?

В результате утечки данных и беспечности самих пользователей. Вот несколько популярных схем:

1.Человеку поступает звонок от «специалиста техподдержки Госуслуг».
Он сообщает, что в учётной записи замечена подозрительная активность и лучше на время заблокировать личный кабинет. Это очень просто: пользователь сейчас получит SMS и должен продиктовать из него код. Если жертва так и делает, мошенник получает доступ к аккаунту. Ну и вместе с ним — данные владельца. В последнее время всё больше людей становятся жертвами такой схемы мошенничества.

2.Телефонный мошенник представляется сотрудником мобильного оператора.
Он сообщает, что срок действия SIM-карты клиента заканчивается. Если человек по-прежнему хочет пользоваться номером, нужно продлить договор. Для этого нужно сообщить код. Прямо во время разговора на телефон действительно поступает SMS от Госуслуг с кодом. Жертва теряет бдительность и делится доступом.

3.Злоумышленники могут притворяться сотрудниками государственных органов, банков, налоговой инспекции.
Повод для связи может быть любым: уточнить данные для декларации на налоговый вычет, оплатить штраф, отменить заявку на заём в МФО и так далее. И во всех случаях мошенники пытаются выманить код из SMS. Как правило, жертву торопят, а для убедительности обращаются по имени и называют адрес регистрации. Важно помнить: все эти данные легко отыскать в интернете, а цель мошенника — втереться в доверие и получить от вас нужную информацию.

4. Преступники используют фальшивые сайты-двойники, фишинговые ссылки в электронных письмах и звонки на мобильные телефоны для мошенничеств, связанных с порталом «Госуслуг».

*Фишинговые ссылки - это вредоносные ссылки, которые злоумышленники отправляют в фишинговых электронных письмах и текстовых сообщениях. В текст письма или сообщения они добавляют ссылку, которая вместо обещанных викторин и видео ведет на фишинговый сайт. Его создают специально для этой аферы, чтобы собирать личные и платежные данные пользователей. В некоторых случаях при переходе по ссылке загружается вирус, который ворует данные с вашего устройства.

По словам эксперта, ссылки на поддельные сайты могут появляться в виде рекламы на сторонних сайтах, например, в период самоизоляции мошенники создавали сайты, где публиковали сообщения о выплатах семьям с детьми, с помощью которых похищались данные банковских карт.

Некоторые уловки преступников, на которые стоит обратить внимание:

Похожие символы в адресе могут быть заменены (например, g0suslugi.ru или gosulugl.ru). Если предварительно был осуществлен вход на портал в соседней вкладке браузера, то переход по официальной ссылке на сайт «Госуслуг» не должен требовать повторной авторизации. В противном случае это свидетельствует о том, что вы имеете дело с поддельной страницей. Эксперты советуют самостоятельно заходить на официальный сайт портала «Госуслуг», не переходить по каким-либо ссылкам якобы ведущим на портал.

Перечень услуг, предоставляемых порталом gosuslugi.ru, обширен: обратиться в какое-либо ведомство, подать заявление, оплатить налоги, госпошлины, например, с помощью банковской карты.

Вы, наверно, догадались, что мимо ресурса, аккумулирующего личные данные граждан, информацию об их налоговых долгах и платежах, мошенники пройти не могли.

Как сообщает телеграмм-канал «Защитник закона», жулики извлекают интересующие их данные старым добрым способом - рассылая СМС и письма на электронную почту от лица ресурса, вызывающего доверие.

Выглядит все очень правдоподобно: в строке отправителя указан актуальный адрес портала, логотипы и оформление, характерные для Госуслуг присутствуют. В содержании послания — информация о наличии небольшой задолженности перед бюджетом в 10 или 20 рублей, которую можно сразу погасить, перейдя по ссылке в письме.

Воспользовавшись ссылкой и введя данные карты, гражданин допускает ошибку, которая будет стоить ему всех денег на счету.

Но это еще не все. На портал Госуслуги россияне вносят персональные данные и загружают копии различных документов. Заменив оригинал сайта подставной копией, аферисты узнают логин и пароль пользователя, и получают доступ к личным данным гражданина, которые можно будет применить в своих преступных схемах.

Поэтому, получив письмо от портала Госуслуги о задолженности, не нужно бежать по ссылке оплачивать долги. Проверка на настоящем сайте (не по ссылке) поможет сохранить деньги и уберечь свои данные.

Зачем мошенникам Госуслуги?

Главная добыча мошенников — это ваши данные. Вот в каких целях они могут их использовать:

1. Взять кредит. У вас подтверждённая учётная запись на Госуслугах? Значит, при оформлении кредитов и займов на сайтах банков или МФО вам легко подтвердить свою личность — достаточно нажать на кнопку. Кажется, что это очень удобно. Но удобство сыграет злую шутку с владельцем аккаунта, если его взломают мошенники. Злоумышленники авторизуются на сайтах финансовых организаций через профиль жертвы, а после получат займы на её имя. Кроме того, в профиле на Госуслугах есть реквизиты паспорта. Их тоже можно использовать для подачи заявки на онлайн-кредит.

2. Получить чужой налоговый вычет. Для этого злоумышленники сначала авторизуются через портал на сайте федеральной налоговой службы (ФНС). Получив доступ к личному кабинету налогоплательщика, они просматривают суммы отчислений по налогам и подают заявление на вычет. К нему прикладывают липовые документы — справку об оплате образования, лечения, лицензии и так далее. В обращении указывают банковский счёт, на который нужно перечислить деньги. Если во время проверки декларации сотрудник налоговой ничего не заподозрит, положенный вам по закону вычет достанется мошенникам.
3. Обмануть других людей. К мошеннику будет больше доверия, если он предоставит паспортные данные, реквизиты документов на машину или квартиру и т. п. Например, на сайтах объявлений мошенники демонстрируют чужие фото паспорта. Так они пытаются убедить жертв, что переводить оплату или вносить залог абсолютно безопасно. Конечно, после получения денег мошенник бесследно пропадает. А у человека, чьими данными он воспользовался, возникают проблемы.
4. Продать данные другим мошенникам. Многие взломщики не охотятся за вашими деньгами и не планируют получать на ваше имя кредиты. Им достаточно скопировать ваши данные из профиля на портале и продать их в даркнете.

Источник информации Портал Госуслуг:
https://www.gosuslugi.ru/help/faq/personal_data/100465