Мошенники взломали мой профиль на «Госуслугах». Что делать?

Евгения торопилась на родительское собрание, когда ей позвонил «специалист техподдержки «Госуслуг». Он сказал, что в ее учетной записи зафиксирована подозрительная активность и лучше временно заблокировать личный кабинет. Ей придет СМС с кодом от портала, и нужно будет продиктовать цифры. Евгения так и сделала и практически тут же поняла, что совершила ошибку. Как только собеседник простился с ней, она получила уведомление о смене номера телефона на «Госуслугах». Разбираемся, что делать в подобных ситуациях.

Не могу войти в аккаунт. Как восстановить доступ?

Для начала попробуйте сбросить старый пароль с помощью почты или по номеру телефона. Для этого на странице авторизации выберите «Восстановить». Затем введите телефон или e-mail и номер одного из документов: паспорта, ИНН или СНИЛС.

Не получилось войти с помощью номера телефона? Попробуйте вариант с адресом электронной почты. И наоборот.

Если вы устанавливали контрольный вопрос, система задаст его. После нужно будет либо ввести код из СМС, либо перейти по ссылке из письма. Потом создайте новый пароль.

Оба способа — и через телефон, и через почту — не срабатывают? Вероятно, злоумышленники уже успели поменять e-mail и номер телефона в вашем профиле.

В таком случае посмотрите список банков, в которых можно онлайн восстановить доступ к госпорталу. Если вы являетесь клиентом одного из них, зайдите в свой личный кабинет на сайте или в приложении, найдите сервис «Регистрация на «Госуслугах» и следуйте инструкциям. Не пугайтесь названия — у кого уже есть аккаунт на госпортале, здесь именно восстановят к нему доступ, а не заведут вторую учетную запись.

Новый пароль от аккаунта придет на номер телефона, который вы указали в банке как основной. Даже если мошенники успели заменить его в «Госуслугах» на свой, код для входа получите именно вы.

Но этот способ не сработает, если взломщики уже поменяли или установили контрольный вопрос. Тогда вернуть себе управление аккаунтом получится только оффлайн.

Восстановите доступ в одном из центров обслуживания клиентов «Госуслуг». Все они отмечены на карте госпортала. Но вам нужно выбрать с

помощью фильтра (значок, похожий на воронку) только те из них, которые проводят «Восстановление доступа». Найдите ближайший центр, проверьте режим его работы и быстрее отправляйтесь туда.

Возьмите с собой паспорт и СНИЛС — покажите их менеджеру. Попросите восстановить вам доступ к порталу и проверьте, какой номер телефона привязан к профилю. Если указан не ваш, сразу замените его. После этого сотрудник пришлет вам одноразовый пароль для входа в аккаунт в СМС или на электронную почту. В форме авторизации введите свой СНИЛС в поле «Логин» и вбейте пароль из СМС. После входа сразу поменяйте временный пароль на постоянный.

Иногда сообщение с одноразовым паролем не приходит с первого раза. Если оно не появится в течение пяти минут, попросите отправить его еще раз.

Доступ удалось восстановить. Что нужно проверить?

Когда аккаунт снова в ваших руках, важно перекрыть мошенникам доступ к вашему профилю, а также выяснить, какие именно данные их интересовали.

1. Первым делом зайдите в своем профиле в раздел «Безопасность». В подразделах «Мобильные приложения» и «Действия в системе» выйдите из аккаунта со всех устройств, кроме того, которым вы сейчас пользуетесь. Предварительно сделайте фото или скриншот — возможно, эта информация вам пригодится.

2. Проверьте, правильно ли указаны телефон и почта в графе «Учетная запись». Если там значатся неизвестные номер или адрес, скопируйте их или сделайте скриншот — эти данные тоже помогут в поиске преступников.

Поменяйте телефон на свой. Если у вас стандартная или упрощенная учетная запись, для смены номера потребуется ввести код подтверждения, который придет в СМС от портала.

Когда запись подтвержденная, нужно сразу обратиться в один из центров обслуживания «Госуслуг» или пройти процедуру восстановления доступа в своем онлайн-банке. Сменить номер по СМС не выйдет, поскольку требуется два кода подтверждения: один придет на ваш номер, а другой — на тот, что значится на портале.

После проверки номера телефона убедитесь, что в профиле указан верный e-mail. Если нет, введите свой адрес. Проверьте почту — там должно появиться письмо от портала. Нажмите в нем кнопку «Подтвердить». Затем на ваш номер придет СМС с кодом — введите его на портале.

3. В разделе «Безопасность» в подразделе «Действия в системе» посмотрите, на каких ресурсах проходили авторизации через ваш профиль. Например, злоумышленники могли использовать ваш аккаунт для входа в личный кабинет банка или микрофинансовой организации МФО. В таком случае срочно свяжитесь с финансовой организацией. Скажите, что ваш профиль взломали. Выясните, что происходило с вашими счетами за последнее время и не появилось ли у вас новых кредитов и займов.

Если мошенникам удалось украсть ваши накопления или набрать долгов на ваше имя, подайте в банк или МФО заявление о том, что это сделали не вы.

Никакого финансового ущерба не обнаружилось? На всякий случай все равно напишите заявление о том, что доступ к онлайн-банку был у посторонних, и перевыпустите свои карты.

В разделе «Заявления» посмотрите, какую информацию о вас запрашивали взломщики.

Если мошенники заказали справку из налоговой, выписку о состоянии вашего пенсионного счета и сведения из трудовой книжки, вероятно, они попытаются оформить заем на ваше имя. Обязательно выполните следующие действия.

4. Сообщите о случившемся в техподдержку «Госуслуг» и в полицию.

Передайте все известные вам подробности: время взлома, чужие контактные данные, которые появились в аккаунте вместо ваших. Сохраните копию заявления в полицию и талон-уведомление о его приеме. Если мошенники наберут долгов на ваше имя, будет проще доказать, что займы брали не вы.

5. Периодически проверяйте свою кредитную историю – данные обо всех ссудах на ваше имя. Так вы быстро узнаете, если мошенникам все-таки удастся взять займы на ваше имя, и сможете их оспорить.

Чтобы предотвратить взлом профиля в дальнейшем, задайте сложный пароль и не забывайте время от времени обновлять его.

Как еще защитить свой аккаунт?

Зайдите в раздел «Безопасность». На вкладке «Вход в систему» перечислены разные способы защиты. Чтобы включить любой из них, передвиньте ползунок в нужной графе.

Выберите один или несколько вариантов:

Установите вход с подтверждением по СМС. При каждой авторизации на ваш мобильный будет приходить новый код для входа. Перед тем как подключать услугу, убедитесь, что в профиле записан актуальный телефон.

Если меняете номер, сразу же обновите его в учетной записи на «Госуслугах». Иначе коды от портала будут приходить другому человеку, а он может оказаться мошенником.

Настройте уведомление о входе на «Госуслуги» по электронной почте. Вы будете получать письмо каждый раз, когда вы или кто-то другой будет заходить в ваш аккаунт. Заранее проверьте, верно ли указан ваш e-mail.

Создайте контрольный вопрос – он защитит вас, если мошенники попытаются сменить пароль от вашего кабинета и под каким-то предлогом выманят у вас код из СМС или почты. Даже зная секретные цифры, они не смогут войти в ваш профиль без правильного ответа на контрольный вопрос. Главное держать его в тайне.

Вы сами выбираете тему, но не устанавливайте слишком простые вопросы, ответы на которые легко найти в ваших соцсетях — например, про даты рождения близких или клички животных.

Не раскрывайте никому свои логин и пароль, паспортные данные, не называйте коды из СМС. Помните, что сотрудники «Госуслуг» не обратятся к вам сами, если вы не подавали им никаких заявок. Если кто-то без вашей инициативы звонит и общается с вами от имени портала, лучше всего повесить трубку.

Когда в почте вы видите письмо от «Госуслуг» о выплатах, штрафах или с информацией, которую вы не запрашивали, не торопитесь кликать по ссылке. Посмотрите адрес отправителя. Настоящие письма от портала приходят только с почты no-reply@gosuslugi.ru. Зайдите на сайт или в приложение «Госуслуг» и проверьте, есть ли такое же уведомление в личном кабинете.

Помните, что мошенники часто создают поддельные сайты. Поэтому внимательно сверяйте символы в адресной строке страницы, на которой находитесь. Введете логин и пароль от «Госуслуг» на фальшивом портале — злоумышленники смогут взломать ваш аккаунт и набрать кучу займов на ваше имя. А если оставите на поддельной странице свои платежные данные (например, для оплаты штрафа или оформления субсидии), с вашей карты украдут все деньги.