

Цифровой профиль гражданина, способы защиты аккаунта «Госуслуг».

Под цифровым профилем гражданина понимается набор сведений о человеке в государственных информационных системах.

Цифровой профиль собирает актуальные данные о человеке из реестров государственных органов. Однако, это не означает, что любые организации могут получить сведения и использовать их по своему усмотрению.

Для того, чтобы коммерческие компании могли работать с такой информацией, гражданин должен дать согласие на предоставление персональных данных, а также у него должна быть подтвержденная учетная запись на «Госуслугах».

При запросе сведений из цифрового профиля гражданина компания должна указать, для чего и как будет использовать его данные.

Например, гражданин может дать согласие на оформление банковской карты, заключение кредитного договора или предоставление страховых услуг.

Учитывая широкий спектр возможностей не стоит пренебрегать защитой аккаунта на сайте «Госуслуг».

В случае, если злоумышленники получают доступ к аккаунту гражданина на «Госуслугах», они смогут совершать от его имени определенные действия, такие как оформление кредита, распоряжение собственностью, оформление юридического лица и другие.

Портал «Госуслуги» предлагает несколько инструментов для защиты аккаунта:

1. Используйте уникальный пароль, который не должен повторяться на других сервисах.
2. Включите оповещения о входе в ваш аккаунт «Госуслуг».

Если вы включите оповещения, то после каждого успешного входа вам придет письмо на электронную почту. Так вы узнаете, что кто-то получил доступ к Вашему аккаунту, и сможете своевременно поменять пароль.

3. Задайте контрольный вопрос.

Контрольный вопрос является дополнительной мерой защиты от попыток посторонних сменить пароль от вашего аккаунта. Злоумышленники могут взломать почтовый ящик, к которому привязан ваш аккаунт, а также узнать номера документов, которые сайт уточняет, чтобы подтвердить Вашу личность.

Стоит помнить, что контрольный вопрос не защитит вас, если ответ на него легко угадать или найти в Интернете.

4. Включите двухэтапную проверку входа.

После включения двухэтапной проверки, чтобы войти в вашу учетную запись, злоумышленнику потребуется ввести не только пароль, но и одноразовый SMS-код, который придет на ваш телефон.

Таким образом, вы будете в относительной безопасности и сможете оперативно сменить пароль.

5. Включите вход с помощью электронной подписи.

Если вы пользуетесь квалифицированной электронной подписью, можно применять ее и для входа в аккаунт.

Обозначенные способы защиты позволяют, с одной стороны, усложнить мошенникам работу, а с другой – помогут вовремя узнать о попытке взлома аккаунта.