Правила кибергигиены:

7 шагов для улучшения защиты данных

С каждым днем информационные технологии все больше проникают в жизнь современного человека. Сегодня почти каждый имеет смартфон с доступом к сети Интернет, что позволяет пользователям всегда быть онлайн. В частности, в любой момент вы можете проверить почту или мессенджер, купить билет в кино или забронировать жилье для отпуска и даже осуществлять платежи, не обращаясь в отделения банка. Все эти действия в Интернете предусматривают обмен определенной личной информацией или конфиденциальными данными, которые в случае вашей невнимательности могут оказаться в руках злоумышленников.

Для обеспечения защиты персональных данных при работе в Интернет-сети специалисты рекомендуют придерживаться основных правил кибергигиены. В свою очередь **кибергигиена** — это меры безопасности, разработанные для защиты устройств пользователя от заражения вредоносным программным обеспечением и возможного похищения конфиденциальной информации.

Правила кибергигиены: 7 шагов для улучшения защиты данных

1. **Проверка безопасности активных аккаунтов.**

Первым правилом кибергигиены является проверка безопасности уже существующих учетных записей электронной почты и аккаунтов в соцсетях. В частности, такие сайты как haveibeenpwned.com и breachalarm.com помогут выяснить, был ли пароль к электронной почте похищен злоумышленниками.

2. **Анализ программ.**

Сегодня у каждого сайта, магазина и даже банка есть специальное мобильное приложение. Однако это не значит, что все они должны быть на вашем устройстве. Загружайте только необходимые для работы программы. Специалисты советуют проанализировать уже загруженные приложения, удалить ненужные и в дальнейшем контролировать установку каждой программы. Также во время загрузки каждого приложения стоит обращать внимание на разрешения, которые вы предоставляете. Часто вредоносные программы запрашивают множество разрешений, которые не соответствуют их функционалу. Это позволяет собирать большое количество информации о пользователе с целью получения прибыли.

3. **Регулярное обновление.**

Для предотвращения заражения вредоносными программами следует осуществлять своевременное обновление операционной системы и отдельных приложений, которое предусматривает исправление уязвимостей и ошибок в программном обеспечении.

4. **Надежный пароль.**

С целью предотвращения несанкционированного доступа к устройствам убедитесь в надежности ваших паролей. Важно создать сложную комбинацию, которая содержит не менее 12 символов, большие и малые буквы, цифры и символы. Кроме этого, для каждого аккаунта стоит использовать уникальный пароль. Таким образом кража одной из комбинаций не поставит под угрозу другие учетные записи. Дополнительный уровень защиты.

5. **Дополнительный уровень защиты**

Для улучшения безопасности учетных записей используйте двухфакторную аутентификацию, которая предусматривает подтверждение личности при входе в определенный аккаунт. Чаще всего для этого используются SMS-сообщения или отдельная программа. Таким образом в случае кражи пароля злоумышленники не смогут получить доступ к вашим данным.

6. **Регулярное резервное копирование.**

Необходимым шагом для предотвращения потери важных данных является регулярное резервное копирование информации на внешний жесткий диск или в облако. Это поможет восстановить нужные данные в случае их шифрования программой-вымогателем или удаления вредоносным программным обеспечением.

7. **Надежная защита.**

Последним, но не менее важным, правилом кибергигиены является использование надежного решения для защиты вашего компьютера или смартфона от различных угроз, в том числе программ-вымогателей, шпионских программ, вирусов, троянов и фишинг-атак.

Эти семь основных правил кибергигиены помогут вам своевременно обнаружить подозрительную деятельность злоумышленников и предотвратить потерю персональных данных и другой личной информации.

Источник: https://eset.ua/ru/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya