



Управление цифровым следом

Цифровой след — вся информация о пользователе в интернете, связанная с его сетевой активностью. Это, в частности, ваши сообщения в социальных сетях, чаты, тексты, история просмотров в браузере, электронные письма, а также данные о покупках в интернете и о местоположении. Ваш цифровой след может:

- **Повысить для вас риск стать жертвой мошенничества.** Разные мошенники могут воспользоваться вашим цифровым следом, чтобы сделать вас целью атаки, выдать себя за вас или похитить вашу информацию.
- **Сделать возможной слежку за вами со стороны государственных учреждений, а также злоумышленников или лиц, осуществляющих контроль.** Это получение информации о том, где вы находитесь, если на вашем устройстве включено отслеживание местоположения или если вы делаете отметку о своем местонахождении в социальных сетях.
- **Увеличить вероятность виктимизации.** Используя цифровой след другого человека, преступники могут сделать его целью атаки, связанной с принудительными формами труда. Экстремисты и прочие лица, выполняющие злонамеренные действия, также могут использовать цифровые следы людей для дискриминационных высказываний и преступлений на почве ненависти.
- **Негативно повлиять на ваше иммиграционное дело.** Учетные

записи в социальных сетях, имена пользователей и прочую цифровую информацию теперь необходимо сообщать при подаче многих стандартных иммиграционных заявок. Когда человек въезжает на территорию США или находится под стражей у представителей Министерства национальной

безопасности, содержимое его электронных устройств может быть проверено. На основе данных о сетевой активности лица могут приниматься решения о задержании, депортации, изменении статуса и натурализации, а также о предоставлении убежища или других форм иммиграционной помощи.

Управление цифровым следом является крайне важным для вашей безопасности, защиты и репутации!

12 советов по управлению цифровым следом

1. Обеспечьте защиту своих устройств и учетных записей.

Убедитесь, что на всех ваших устройствах установлен надежный пароль. В идеале следует дополнительно настроить двухфакторную аутентификацию. Двухфакторная аутентификация предполагает использование двух методов аутентификации, например пароля и кода, который приходит на ваш мобильный телефон.

2. Не делитесь личной информацией. Не размещайте свои Ф. И. О., адрес, номер телефона или другую личную информацию в интернете, включая социальные сети.

Не отмечайте свое местоположение в социальных

сетях.

Не публикуйте фотографии, с помощью которых можно определить, где вы находитесь, проживаете, работаете или учитесь, например номера домов, таблички с названиями улиц, номерные знаки автомобилей, логотипы на униформе и пр.

3. Сделайте свои учетные записи закрытыми. Если у вас есть учетные записи в социальных сетях, убедитесь, что они закрыты. Как правило, для этого необходимо войти в свою учетную запись, открыть раздел «Настройки» или «Конфиденциальность» и проверить, выбран ли параметр «Закрытая».

4. Удалите старые учетные записи.

Если вы больше не используете учетную запись, удалите ее. Аналогичным образом отключите облачные хранилища или учетные записи на всех старых устройствах, которыми вы редко пользуетесь.

5. Отключите функцию отслеживания местоположения.

Чтобы отключить функцию отслеживания местоположения на устройстве, откройте настройки раздела «Конфиденциальность», «Безопасность» или «Местоположение». Там отключите службы определения местоположения, чтобы приложения и сервисы не получали никакой информации о вашем местоположении.

6. Ограничьте объем размещаемых данных.

Размещайте в интернете минимальный объем данных.

Внимательно следите за тем, что вы размещаете. В противном случае информация может быть неправильно истолкована, а также для вас может увеличиться риск стать жертвой атаки. Например, речь идет о размещении фотографии, на которой человек распивает алкогольные напитки, держит в руках оружие и пр.

7. Не принимайте запросы на добавление в друзья от незнакомых людей.

Принимайте запросы на добавление в друзья только от людей, которых вы знаете. Профиль может принадлежать кому угодно, включая мошенников, торговцев людьми и тех, кто пытается следить за вами.

Удалите друзей из своих учетных записей, если вы не знаете их лично.

8. Удалите конфиденциальные материалы и приложения с телефонов и других устройств.

Если вы совершаете поездку в другую страну, работники Министерства национальной безопасности могут проверить содержимое ваших электронных устройств в пунктах пропуска при возвращении в США. Удалите всю текстовую информацию, фотографии, приложения и прочие материалы, которые могут быть неправильно истолкованы.

9. Общайтесь безопасно.

Используйте приложения для коммуникации со сквозным шифрованием, например WhatsApp, Signal и Telegram.

Примечание: ваш цифровой след может оставаться даже при использовании более безопасных платформ для обмена зашифрованными сообщениями,

поскольку сохраняются метаданные о том, с кем и когда вы общаетесь, а также совместно используемое содержимое, например видео, изображения и информация профиля. Внимательно следите за тем, что вы сообщаете.

- 10. Будьте осторожны при использовании веб-страниц.** Не переходите по подозрительным ссылкам от неизвестных отправителей и не открывайте ненадежные веб-сайты, которые могут содержать вирусы и средства слежки.

Предоставляйте только необходимую информацию и будьте крайне осторожны при использовании веб-сайтов или приложений, которые запрашивают слишком много персональных данных.

Регулярно удаляйте файлы cookie и очищайте кэш своего браузера. Как правило, для этого необходимо открыть в браузере раздел «Настройки», затем — «Настройки конфиденциальности», после чего

следует найти опцию «Очистить данные о просмотре» или аналогичный пункт.

- 11. Используйте временный или одноразовый мобильный телефон.** Тарифы для таких телефонов часто предоплаченные, а не контрактные, поэтому это более подходящие варианты для анонимной связи без риска отслеживания. Если же вы пользуетесь временным телефоном, обязательно убедитесь, что люди, которым необходимо выходить с вами на связь (социальный работник, адвокат и др.), знают ваш новый номер. Некоторым людям удобно пользоваться двумя телефонами: временным для сетевой активности и постоянным для важной и стабильной связи с определенными лицами.

- 12. Используйте наклейки для камер.** Используйте наклейки для камер на телефонах и ноутбуках, чтобы закрыть объектив, когда он не используется. Это позволяет избежать вмешательства в вашу частную жизнь.