

**О чем расскажет твой цифровой след
в Интернете и как его защитить**

Примеры цифрового профиля

Цифровой след может включать сотни составляющих. И это лишь некоторые действия, описывающие цифровой след.

Онлайн покупки

- Совершение покупок на сайтах электронной коммерции.
- Подписка на купоны или создание учетной записи.
- Загрузка и использование приложений для покупок.
- Подписка на рассылку новостей бренда.

Интернет-банкинг

- Использование мобильного банковского приложения.
- Покупка и продажа акций.
- Подписка на финансовые публикации и блоги.
- Открытие счета кредитной карты.

Здоровье и фитнес

- Использование фитнес-трекеров.
- Использование приложений для получения медицинской помощи.
- Регистрация адреса электронной почты в тренажерном зале.
- Подписка на блоги о здоровье и фитнесе.



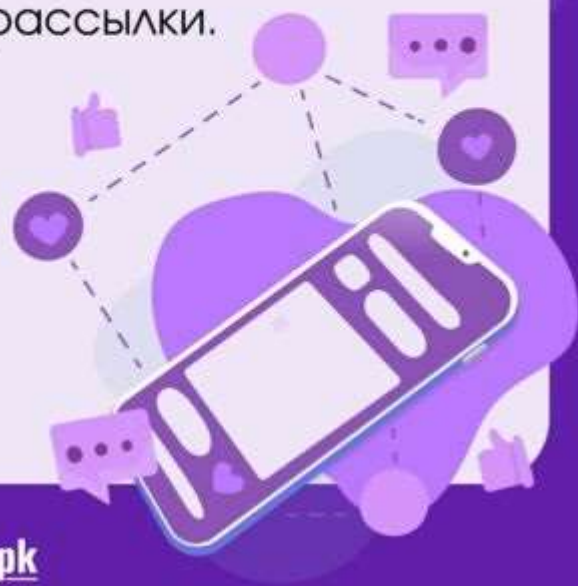
Социальные медиа

Использование социальных сетей на компьютере и устройствах.

- Вход на другие веб-сайты с использованием учетной записи социальной сети.
- Общение с друзьями и знакомыми.
- Обмен информацией, данными и фотографиями со знакомыми.
- Регистрация на сайте знакомств или в приложении.

Социальные медиа

- Чтение новостей.
- Подписка на новостные издания в интернете.
- Репосты прочитанных статей и информации.
- Просмотр статей в новостном приложении.
- Подписка на информационные рассылки.



Кто может воспользоваться твоим цифровым профилем?

Соцсети, поисковые сайты, Интернет-магазины и прочие крупные Интернет-ресурсы собирают данные для того, чтобы потом показывать своим пользователям рекламу.

Злоумышленники. Они могут использовать их для того, чтобы как можно больше узнать о жертве, выяснить, где человек работает, в каком банке у него открыт счет, как его зовут и так далее.

Соцсети собирают информацию буквально о каждой вашей активности. Под какими постами ты ставишь лайки, сколько времени ты читаешь новость, какие заголовки тебе нравятся больше, с какими людьми ты дружишь и общаешься, какую музыку ты слушаешь, какие видео тебе нравятся.

Как защитить цифровой след в Интернете?

Используйте поисковые системы для проверки своего цифрового следа.

Алгоритм:

- Введите свое имя в поисковую систему.
- Укажите имя и фамилию, используйте все варианты написания.
- Просмотр результатов поиска даст вам представление об общедоступной информации о вас.
- Если какой-либо из результатов поиска показывает вас не в лучшем свете, можно связаться с администраторами сайта и узнать, могут ли они удалить эту информацию.



Каждый раз при предоставлении личной информации вы расширяете свой цифровой след, а также увеличиваете вероятность того, что компания, хранящая ваши данные, воспользуется ими не по назначению или подвергнется взлому, в результате чего ваши данные могут попасть злоумышленникам. Поэтому прежде чем заполнять форму, **подумайте**, стоит ли это делать.

Есть ли другие способы получить информацию или услугу без предоставления личных данных?



Проверьте параметры конфиденциальности в социальных сетях.

Рекомендуется:

Настроить параметры конфиденциальности для просмотра вашего профиля и публикаций только для друзей.

Не рекомендуется:

Указывать номер телефона и адрес электронной почты в разделе «Информация» в социальных сетях. Ставить лайки вашему банку.

Не забывайте, что параметры конфиденциальности защищают вас только в конкретной социальной сети.



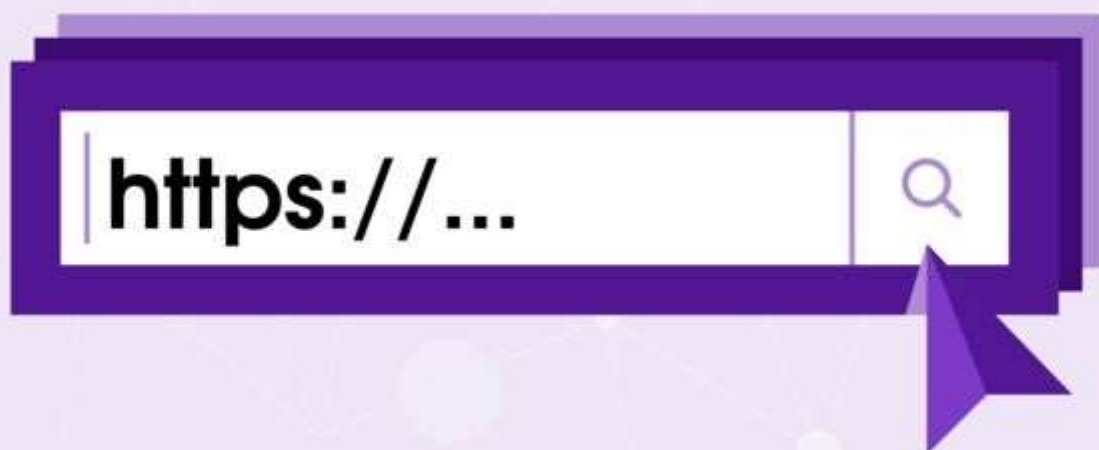
Избегайте незащищенных веб-сайтов.

Убедитесь, что вы совершаете транзакции на защищенном веб-сайте.

Его веб-адрес должен начинаться с **https://**, а не с **http://**; буква **s** означает «безопасный» и указывает на наличие у сайта **сертификата безопасности**.

Слева от адресной строки также должен отображаться значок замка.

Не разглашайте конфиденциальную информацию, особенно платежные данные, на незащищенных сайтах.



- **Не указывайте личные данные при использовании публичных сетей Wi-Fi.**
- **Удаляйте старые учетные записи.**

Один из способов уменьшить свой цифровой след - удалить старые учетные записи, например, неиспользуемые профили в социальных сетях и подписки на не интересующие вас информационные рассылки.



Создавайте надежные пароли и используйте менеджер паролей.

Надежный пароль является длинным состоит не менее чем из 12 символов, — а в идеале больше, и содержит сочетание заглавных и строчных букв, символов и цифр.

Чем сложнее ваш пароль, тем сложнее его взломать.

Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

