



Керування цифровим слідом

Цифровий слід — уся інформація про користувача в інтернеті, пов'язана з його мережевою активністю. Зокрема, це ваші повідомлення в соціальних мережах, чати, тексти, історія переглядів у браузері, електронні листи, а також дані щодо купівель в інтернеті й щодо розташування. Ваш цифровий слід може:

- **Підвищити для вас ризик стати жертвою шахрайства.** Різні шахраї можуть скористатися вашим цифровим слідом, щоб зробити вас ціллю атаки, видати себе за вас або викрасти вашу інформацію.
- **Уможливити стеження за вами з боку державних установ, а також зловмисників або осіб, які здійснюють контроль.** Це отримання інформації про те, де ви перебуваєте, якщо на вашому пристрої ввімкнене відстеження розташування або якщо ви робите позначку про своє місцезнаходження в соціальних мережах.
- **Збільшити ймовірність віктимізації.** Використовуючи цифровий слід іншої людини, злочинці можуть зробити її ціллю атаки, пов'язаної з примусовими формами праці. Екстремісти та інші особи, які вчиняють зловмисні дії, також можуть використовувати цифрові сліди людей для дискримінаційних висловлювань і злочинів на ґрунті ненависті.
- **Негативно вплинути на вашу імміграційну справу.** Облікові записи в соціальних мережах, імена користувачів та іншу цифрову інформацію тепер потрібно повідомляти під час подання багатьох

стандартних імміграційних заявок. Коли особа в'їжджає на територію США або перебуває під вартою у представників Міністерства національної безпеки, уміст її електронних пристроїв може бути перевірено. Зважаючи на дані про

мережеву активність особи можуть ухвалюватися рішення щодо затримання, депортації, зміни статусу й натуралізації, а також щодо надання притулку або інших форм імміграційної допомоги.

Керування цифровим слідом є вкрай важливим для вашої безпеки, захисту й репутації!

12 порад щодо керування цифровим слідом

1. Забезпечте захист своїх пристроїв та облікових записів.

Переконайтеся, що на всіх ваших пристроях встановлено надійний пароль. Найліпше рішення — додатково налаштувати двофакторну автентифікацію. Двофакторна автентифікація означає, що застосовуються два методи автентифікації, наприклад пароль і код, що надсилається на ваш мобільний телефон.

2. Не поширюйте приватну інформацію. Не розміщуйте свої ПІБ, адресу, номер телефону або іншу приватну інформацію в інтернеті, включно із соціальними мережами.

Не ставте жодних позначок про своє місцезнаходження в соціальних мережах.

Не публікуйте жодних фотографій, за допомогою яких можна

визначити, де ви перебуваєте, мешкаєте, працюєте або навчаєтеся, наприклад номери будинків, таблички з назвами вулиць, номерні знаки автомобілів, логотипи на уніформі тощо.

3. Зробіть свої облікові записи закритими. Якщо у вас є облікові записи в соціальних мережах, переконайтеся, що вони закриті. Зазвичай для цього потрібно увійти до свого облікового запису, відкрити розділ «Налаштування» або «Конфіденційність» і перевірити, чи встановлено параметр «Закритий».

4. Видаліть старі облікові записи. Якщо ви вже не використовуєте обліковий запис, видаліть його. В аналогічний спосіб вимкніть хмарні сховища або облікові записи на всіх старих пристроях, якими ви рідко користуєтеся.

5. Вимкніть функцію відстеження розташування. Щоб вимкнути функцію відстеження розташування на пристрої, відкрийте налаштування розділу «Конфіденційність», «Безпека» або «Розташування». Там вимкніть служби визначення розташування, щоб застосунки й сервіси не отримували жодної інформації про ваше місцезнаходження.

6. Обмежте обсяг даних, які розміщуєте. Розміщуйте в інтернеті мінімальний обсяг даних.

Уважно стежте за тим, що ви розміщуєте. Інакше інформацію може бути неправильно витлумачено, а також для вас може збільшитися ризик стати жертвою атаки. Наприклад, ідеться про розміщення фотографії, на якій людина п'є алкогольні напої, тримає в руках зброю тощо.

7. Не приймайте запитів на додавання в друзі від незнайомих людей. Приймайте запити на додавання в друзі тільки від людей, яких ви знаєте. Профіль може належати будь-кому, зокрема шахраям, торговцям людьми й особам, які намагаються стежити за вами. Видаліть друзів зі своїх облікових записів, якщо ви не знаєте їх особисто.

8. Видаліть конфіденційні матеріали й застосунки з телефонів та інших пристроїв. Якщо ви здійснюєте поїздку в іншу країну, фахівці Міністерства національної безпеки можуть перевірити вміст ваших електронних пристроїв у пунктах пропуску під час повернення до США. Видаліть усю текстову інформацію, фотографії, застосунки та інші матеріали, які може бути неправильно витлумачено.

9. Спілкуйтеся безпечно. Використовуйте застосунки для комунікації з наскрізним шифруванням, наприклад WhatsApp, Signal і Telegram.

Примітка: ваш цифровий слід може залишатися навіть під час використання безпечніших платформ для обміну зашифрованими повідомленнями, оскільки зберігаються метадані про те, з ким і коли ви спілкуєтеся, а також спільно використовуваний уміст, наприклад відео, зображення та інформація профілю. Уважно стежте за тим, що ви повідомляєте.

10. Будьте обережні під час використання вебсторінок. Не переходьте за підозрілими посиланнями від невідомих відправників і не відкривайте ненадійні вебсайти, що можуть

містити віруси й засоби стеження.

Надавайте лише потрібну інформацію та будьте вкрай обережними під час використання вебсайтів або застосунків, які відображають запити щодо надто великої кількості персональних даних.

Регулярно видаляйте файли cookie й очищуйте кеш свого браузера. Зазвичай для цього потрібно відкрити в браузері розділ «Налаштування», потім — «Налаштування конфіденційності», після чого потрібно знайти опцію «Очистити дані щодо перегляду» або аналогічний пункт.

11. Використовуйте тимчасовий або одноразовий мобільний телефон. Тарифи для цих

телефонів часто передплачені, а не контрактні, тому це ліпші варіанти для анонімного зв'язку без ризику відстеження. Якщо ж ви користуєтеся тимчасовим телефоном, обов'язково переконайтеся, що люди, яким потрібно встановлювати зв'язок із вами (соціальний працівник, адвокат тощо), знають ваш новий номер. Деяким людям зручно користуватися двома телефонами: тимчасовим для мережевої активності й постійним для важливого й стабільного зв'язку з певними особами.

12. Використовуйте накладки для камер. Використовуйте накладки для камер на телефонах і ноутбуках, щоб закрити об'єктив, коли він не використовується. Це дає змогу уникнути втручання у ваше приватне життя.