

Безпечний перегляд вебсайтів

У цьому ресурсі описано деякі перші практичні кроки для безпечного перегляду вебсайтів і уникнення поширених форм стеження в Інтернеті. Також розглянуто певні дії, як-от використання браузерів підвищеної конфіденційності, перегляд у приватному режимі/ режимі «Інкогніто», очищення історії та вхід за допомогою анонімних адрес електронної пошти й надійних паролів.



Нижче наведено загальні поради щодо захисту пристроїв.

Фактичні кроки можуть відрізнятися, вони залежать від конкретного пристрою і можуть змінюватися з плином часу.



На iPhone та iPad зазвичай можна знайти потрібний параметр, натиснувши «Параметри» на головному екрані, а потім провівши по екрану вниз, щоб відкрити рядок пошуку. (Довідка: <http://tiny.cc/iphonesearch.>)



На пристроях Android потрібно провести вгору на головному екрані: з'явиться рядок пошуку з написом «Пошук на телефоні та інше». Введіть потрібний параметр у рядку пошуку.

Використовуйте браузер із підвищеною конфіденційністю

Деякі браузери, як-от *Firefox* і *DuckDuckGo*, забезпечують високу конфіденційність користувачів, тому стеження в них мінімально можливе. Спробуйте використовувати їх, а не браузери, установлені на пристрої на момент продажу.

Перегляд у приватному режимі або режимі «Інкогніто»

У більшості браузерів є **приватний** режим або режим **«Інкогніто»**. У такому режимі браузер не записує, які вебсайти ви відвідали, але не заважає цим вебсайтам (або вашому Інтернет-провайдеру чи іншим програмам, установленим на вашому пристрої) записувати ваші дії.

Ключ піктограми



Приватний режим або режим «Інкогніто»



Параметри

Безпечний перегляд вебсайтів

Видаляйте історію

Знайдіть розділ «Історія». Якщо у вас є обліковий запис *Google*, ви можете також очистити свою історію *Google* і *YouTube*. Перейдіть на сторінку myactivity.google.com і вимкніть «Історію додатків і вебпошуку», «Хронологію» та «Історію YouTube».

Щоб очистити історію браузера Safari, натисніть **«Параметри»** потім виберіть Safari > «Очистити історію та дані вебсайтів» або знайдіть «Дані вебсайтів».

Виконуйте вхід за допомогою анонімної адреси електронної пошти

Багато вебсайтів і сервісів запитують у користувачів адресу електронної пошти для входу. Якщо не потрібно переходити за посиланням для перевірки, ви можете використовувати несправжню адресу електронної пошти, створену на вебсайті [Sharklasers.com](https://sharklasers.com).

Ви також можете безкоштовно створити приватну й надійну адресу *Protonmail*, щоб не використовувати іншу, яку хтось може впізнати.

Використовуйте надійні паролі

Ви можете створити надійний пароль, розпочавши з фрази, яку легко запам'ятати, наприклад «я їм банани», а потім замінити деякі літери на цифри або інші символи (зірочки чи знаки оклику), наприклад: Ya!mB@n@ny.

Але не використовуйте той самий пароль для різних облікових записів. Важливо використовувати інший надійний пароль для основної адреси електронної пошти, оскільки повідомлення для відновлення доступу до облікових записів будуть надсилати на неї. Також можна користуватися диспетчером паролів, як-от *1Password*. У такому разі обов'язково створіть для нього надійний пароль, який відрізнятиметься від усіх інших паролів.

Ключ піктограми



Приватний режим або режим «Інкогіто»



Параметри



Financial contribution from



Public Health
Agency of Canada

Agence de la santé
publique du Canada