

Захист пристроїв

У цьому ресурсі описано перші практичні кроки для захисту пристроїв від поширених форм відстеження. Також розглянуто певні дії, як-от вимкнення Bluetooth, Wi-Fi та надання даних про місцезнаходження; перейменування пристрою; перевірка на наявність шпигунських програм і дозволів додатків; а також скидання з відновленням заводських параметрів.



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.

Коли Bluetooth і Wi-Fi не використовуються, вимикайте їх

Через Bluetooth і Wi-Fi пристрій видимий для інших пристроїв. Вимикайте ці технології, коли не користуєтесь ними. Для цього відкрийте **«Параметри»** або натисніть піктограми **Bluetooth** і **Wi-Fi**.

Також можна відкрити параметри Bluetooth (**«Параметри > Bluetooth»**) і знайти будь-які пристрої, підключені до вашого телефона. Якщо ви побачите невідомі пристрої, відключіть їх.

Вимикайте передавання даних про місцезнаходження

Передача даних про місцезнаходження та додатки на зразок «Знайти мій телефон» продовжують працювати, навіть якщо телефон вимкнено, тому їх потрібно вимкнути в параметрах. На iPhone відкрийте **«Параметри > Приватність > Служби локації»** або знайдіть «Служби локації» та вимкніть передачу даних про місцезнаходження.

На пристрої Android відкрийте **«Карти»**, натисніть своє зображення профілю, а потім передачу даних про місцезнаходження. Натисніть зображення користувача, який *не повинен* бачити ваше місцезнаходження, а потім натисніть «Зупинити».

Ключ піктограм



Параметри



Bluetooth



Wi-Fi



Перемикач



Карти



Три точки

Захист пристроїв

Переименуйте свої пристрої

Навіть якщо ви ніколи не змінювали назву свого телефона, він усе одно її має, і за нею його можна ідентифікувати. На iPhone натисніть **«Параметри»** > Загальні > Про пристрій > Назва» або знайдіть параметр «Назва» й введіть нове ім'я, а потім натисніть «Готово».

На пристрої Android натисніть **«Параметри»** > Про телефон > Ім'я пристрою» або знайдіть параметр «Ім'я», а потім введіть нове ім'я та натисніть «ОК».

Перевіряйте пристрої на предмет шпигунських програм

«Шпигунськими» є програми, за допомогою яких хтось інший може шпигувати на вашому пристрої. Перевірте, чи є програми, які ви не впізнаєте. На iPhone проведіть по головному екрану праворуч, щоб відкрилася «Бібліотека програм».

Натисніть на поле пошуку у верхній частині екрана, а потім прокрутіть список програм і видаліть усі, які ви не впізнаєте.

На пристрої Android відкрийте **«Параметри»** > Програми й сповіщення > Усі програми» або знайдіть «Програми».

Також ви можете скористатися певними програмами, як-от *Certo* та *Incognito*, які скануватимуть ваші пристрої на предмет шпигунського ПЗ, але ви повинні знати, що завжди існує ймовірність, що шпигунське ПЗ є на телефоні.

Перевіряйте дозволи програм

Ви можете також заборонити будь-якій програмі збирати дані або надавати інформацію, наприклад про місцезнаходження. На iPhone натисніть **три точки** > «Приватність і безпека > Звіт про приватність програм», щоб подивитися, що передає кожна програма, або знайдіть параметр «Звіт про приватність». Щоб змінити параметри будь-якої програми, натисніть на неї.

Ключ піктограми



Параметри



Три точки



Перемикач

На пристрої Android завантажте програму *DuckDuckGo* з Google Play та відкрийте її. Натисніть **«Параметри»** > Захист від стеження програм», а потім посуňte **перемикач** праворуч.

Відновлення заводських параметрів

Якщо ви все зробили, але досі вважаєте, що хтось може стежити за вашим телефоном, можна відновити заводські параметри. Але це призведе до видалення всіх даних, у тому числі будь-яких доказів на вашому телефоні. Якщо ви скинете телефон, то не зможете відновити його зі збереженої резервної копії, оскільки в разі відновлення всі можливі програми стеження можуть бути знову завантажені: вам доведеться повністю починати з нуля.

Якщо ви дійсно хочете це зробити, на iPhone натисніть **«Параметри»** > Загальні > Перенести дані чи скинути iPhone», а потім «Стерти вміст і параметри». Також можна виконати пошук за словом «Скинути», щоб знайти цей параметр.

Якщо у вас iPhone, ви можете також увімкнути режим блокування, який захищає від більшості видів шпигунських програм. Він також обмежує використання певних програм, як-от FaceTime і Safari.

Див. <https://support.apple.com/en-ca/HT212650>, щоб більше дізнатися про режим блокування.

На пристрої Android спочатку відкрийте **«Параметри»**, а потім виконайте пошук за словом «Скинути». Пошукайте результат на зразок «Скинути до заводських параметрів» або «Стерті всі дані» й натисніть на нього.



Financial contribution from



Public Health
Agency of Canada

Agence de la santé
publique du Canada