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 користуєтеся 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 піктограми

Параметри

Bluetooth

Wi-Fi

Перемикач

Карти

Три точки

Захист пристроїв

Перейменовуйте 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 посуньте **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

Безпечний зв’язок

У цьому ресурсі описано деякі перші практичні кроки для безпечного обміну повідомленнями й уникнення поширених форм стеження в Інтернеті. Також розглянуто певні дії, як-от вихід з облікових записів, вимкнення передачі інформації про місцезнаходження, перегляд параметрів приватності та зміна 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.

Виходьте з усіх облікових записів

Ви можете входити в деякі програми більш ніж на одному пристрої. Ось як вийти з *Facebook* на всіх пристроях: натисніть **три точки**, виберіть **«Параметри»**, потім «Пароль і безпека», далі «Центр облікових записів». Натисніть «Пароль і безпека», а потім «Де ви виконали вхід».

Після цього ви побачите всі свої облікові записи *Facebook*, *Instagram* або *WhatsApp*. Натисніть на кожен із них, щоб побачити, на яких пристроях ви ввійшли в систему, а потім натисніть «Вийти» для кожного пристрою, який не є вашим телефоном.

Ключ піктограми

Три точки

Параметри

Три точки, розташовані вертикально

Перемикач

Вимикайте передачу даних про місцезнаходження в соціальних мережах

Це важливо, якщо ви використовуєте додаток *Snapchat*, який показує ваше місцезнаходження на карті. Для цього відкрийте *Snapchat* і натисніть піктограму свого профілю. Потім натисніть **три точки, розташовані по вертикалі,** у правому верхньому куті й прокрутіть униз до розділу Who Can… (Хто може…). Якщо натиснути пункт See My Location (Подивитися моє розташування), з’явиться спливне вікно з написом Ghost Mode (Режим привиду). **Увімкніть** його, вибравши On (Увімк.).

У *Facebook* або *Instagram* можна вимкнути передавання даних про місцезнаходження. Для цього натисніть **«Параметри**> Конфіденційність > Служби розташування», а потім натисніть **перемикач** поруч із цим пунктом. У більшості соціальних мереж є подібні параметри в розділах «Конфіденційність» або «Безпека».

Ключ піктограми

Переглядайте параметри конфіденційності

В усіх облікових записах соціальних мереж є параметри конфіденційності. Зазвичай доступ до них можна отримати, натиснувши **«Параметри»**, а потім «Конфіденційність», «Конфіденційність і безпека», «Аудиторія» або аналогічний пункт. Простежте, щоб ваші публікації були видимі тільки вашим друзям.

Змінюйте паролі в хмарних сховищах

Якщо ви зберігаєте свої фотографії або відео в хмарному сховищі, як-от *iCloud* або *Google Диск*, обов’язково змінюйте пароль, щоб ніхто не міг отримати до них доступ.

MediaSmarts

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

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».

Ключ піктограми

Приватний режим або режим «Інкогніто»

Параметри

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**.

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.

MediaSmarts

Financial contribution from

Public Health Agency of Canada | Agence de la santé publique du Canada