

З його допомогою ви також можете просканувати смартфон на наявність шпигунського програмного забезпечення. Цей застосунок платний. Але зверніть увагу, що подібні продукти інші розробники часто пропонують у пакетах разом із антивірусом та VPN.

6. **Ігноруйте невідомі посилання** й уникайте перегляду файлів невідомого походження чи нетипового для відправника змісту (навіть якщо їх надіслали родичі чи друзі).
7. У випадку загрози користуйтеся функцією **скидання даних до заводських налаштувань** (перед цим обов'язково зробіть резервну копію даних).
8. Встановлюйте застосунки й програми **лише з офіційних магазинів**.
9. **Дбайте про фізичну безпеку вашого телефона:** не залишайте без нагляду, користуйтеся блокуванням екрану.
10. Використовуйте **надійні паролі та періодично їх змінюйте**. Для кожного акаунта слід вигадати інший пароль, а для зберігання паролів використовуйте менеджер паролів - програми, що допомагають безпечно зберегти всі паролі.
11. **Налаштуйте двоетапну перевірку**, щоб захистити свою електронну пошту та інші важливі акаунти (Налаштування акаунту → Безпека → Двофакторна аутентифікація → виконайте дії за запропонованою інструкцією).
12. Пам'ятайте, що шпигунські застосунки також **можуть бути в смартфоні** або іншій техніці, що прив'язана до телефона (наприклад, через Bluetooth).
13. Якщо у вашому пристрої з'явилися **невідомі застосунки**, обов'язково їх видаліть. За можливості проскануйте телефон або скиньте налаштування до заводських.

6 ЯК ДОБРЕ, ЩО ТИ Є У FACEBOOK!

Facebook – невичерпне джерело персональних даних користувача. Окрім того, користувачі охоче проходять різні тести (наприклад, «Ваш психологічний вік», «На яку зірку ти схожий?» і т. п.), надаючи сумнівним програмам доступ до акаунта.

ЯК УБЕЗПЕЧИТИ СЕБЕ У FACEBOOK?

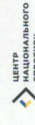
1. Використовуйте двофакторну авторизацію.
2. Налаштуйте параметри конфіденційності профілю: найкраще зробити його закритим.
3. Приховуйте свій номер телефона та адресу електронної пошти. Це зменшить ризик отримання небажаних повідомлень і спаму.
4. Видаляйте геотеги з фотографій перед публікацією. Це допоможе зберегти місце вашого перебування в таємниці.
5. Додавайте в список друзів тільки тих людей, яких знаєте.
6. Ігноруйте заклики проходити тести у Facebook, наприклад, психологічні або жартівливі.
7. Налаштуйте профіль так, щоб Facebook не знаходив вас у соцмережі та в інтернеті за номером телефону або адресою електронної пошти. Ці опції потрібно вимкнути в налаштуваннях конфіденційності вашої сторінки у Facebook.

НАОСТАНОК ПРО WI-FI:

- довіряйте лише мережам із паролем, особливо, якщо вони публічні;
- вимкніть функцію автоматичного підключення до Wi-Fi;
- передавайте інтернет-сервісам логіни, паролі та інші важливі дані лише за умови користування знайомою вам мережею Wi-Fi.



Усе про безпеку вашого пристрою читайте на dovidka.info



DOVIDKA.INFO



ЦЕНТР ЦИБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОЇ ЗАХИСТИ



Міністерство культури і спадщини України

ВОРОГ МОЖЕ ШПИГУВАТИ ЗА ВАМИ ЧЕРЕЗ ТЕЛЕФОН. ЯК УБЕРЕГТИСЯ?

Що ближче ви перебуваєте до лінії фронту, то більша ймовірність, що ворог може шпигувати за вами. Особливо, якщо ви допомагаєте руху спротиву. Саме тому слід уважно ставитися до безпеки свого смартфона, адже ворог може зламати його й отримати доступ до фото, аудіо, текстових заміток, телефонних номерів, геоданих, а також стежити за вами в режимі реального часу.

ЧЕРЕЗ ШПИГУНСЬКІ ПРОГРАМИ ВОРОГ МОЖЕ:

- бачити вашу геопозицію в реальному часі;
- «читати» все, що ви пишете, та дізнатися всі ваші паролі;
- відстежити ваш маршрут та історію переміщень;
- побачити вас та все, що довкола, за допомогою камери вашого смартфона;
- прослухати все, про що ви говорите, навіть тоді, коли телефон не працює, за допомогою доступу до мікрофона у вашому смартфоні.

1 Я ЗНАЮ, ДЕ ТИ СЬОГОДНІ БУВ!

Ворог може стежити за вашим пересуванням у режимі реального часу. Щоб такого не трапилося, варто **вимкнути геолокацію на вашому смартфоні**.

Для iOS: Налаштування / Параметри → Конфіденційність / Приватність і безпека → Служби локації.

Рекомендуємо скасувати дозволи на доступ до геолокації для всіх програм.

Вибірково ви можете надати в налаштуваннях дозвіл «За використання програми» у тих застосунках, для яких важливо знати місце вашого перебування (служба виклику таксі чи мапа). Завдяки таким обмеженням геолокація буде вмикатися лише тоді, коли ви використовуєте програму.

Для Android: Налаштування → У пошуку введіть Місцезнаходження / Розташування / Геолокація (у різних смартфонах різні назви) → Відкрийте відповідний пункт і вимкніть геолокацію.

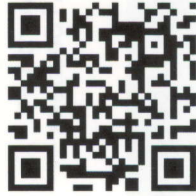
Також можна налаштувати геолокацію для кожного застосунку окремо. Для цього зайдіть у **Налаштування → у пошуку введіть Геодані**. Система покаже всі застосунки, які є на телефоні. Натисніть на потрібний застосунок і відрегулюйте його доступ до місця перебування:

- дозволяти, лише коли застосунок використовується;
- запитувати щоразу;
- не дозволяти.

2 Я ТЕБЕ ЧУЮ!

Ще одним із поширених способів шпигунства є **прослуховування вашого телефону**. Запідозрити це можливо, якщо:

- на екрані **раптово з'являються підозрілі крапки або емблема мікрофона** (зловмисники можуть дистанційно вмикати мікрофон та прослуховувати навіть розмову через захищений месенджер);
- **телефон швидко нагрівається**;
- **й розряджається**;
- **інтернет-трафік різко збільшився** (це може вказувати на передавання записаних розмов);
- на пристрої з'явилися **невідомі застосунки**.



Детальніше про
прослуховування
читайте на dovidka.info

3 Я ТЕБЕ БАЧУ!

Доступ до камери для ворожих програм більш складний: стежити за вами через камеру зможуть лише ті програми, яким ви самі надали такий дозвіл при встановленні. Тож звертайте увагу: якщо Zoom просить доступу до камери девайсу, це нормально, коли ж це робить мобільна гра, варто замислитися.

Те саме стосується й доступу до запису екрану вашого смартфона. Жодна програма (крім тих, яким він справді потрібен, як-от Zoom) не повинна мати такого дозволу.

4 Я ЧИТАЮ ВСЕ, ЩО ТИ ДРУКУЄШІ!

Особливо небезпечним видом шкідливого програмного забезпечення є кейлогери. Це програми, що записують, які кнопки ви натискаєте на клавіатурі. Завдяки цьому хакери можуть дізнатися зміст усіх повідомлень, отримати ваші паролі та іншу особисту інформацію.

5 Я ЗНАЮ ПРО ТЕБЕ ВСЕ!

Вірусні пости на кшталт «Дивися, хто загинув у ДТП», «Це ти на фото?», що спонукують перейти за лінком, чи повідомлення з проханням позичити грошей від знайомих вам людей, а насправді – від шахраїв, які зламали акаунт, – усе це фішинг. За допомогою фішинг-атак зловмисники можуть украсти логін і пароль вашої електронної пошти й отримати доступ до банківської картки, конфіденційної інформації, а також інших ресурсів, де ви реєструвалися.



Більше про
фішинг читай
на dovidka.info

ЯК «ШПИГУН» ОПИНЯЄТЬСЯ НА ТЕЛЕФОНІ?

«Шпигуни» та інші шкідливі програми можуть потрапити на ваш пристрій через:

- відкритий Wi-Fi;
- Bluetooth;
- небезпечну розсилку (посилання чи файли);
- фізичний доступ до пристрою.

ЯК ЗАХИСТИТИ СВІЙ ТЕЛЕФОН ВІД ШПИГУНСТВА?

1. Перевіряйте, які застосунки мають дозвіл для використання мікрофона, камери, запису екрана, геолокації (**Налаштування / Параметри → Конфіденційність / Приватність → Дозволи → далі виберіть необхідний розділ**). Обмежуйте зайві дозволи.
2. Використовуйте **надійні месенджери**, наприклад, **Signal** або **WhatsApp**, користуйтеся секретними чатами.
3. Регулярно **оновлюйте програмне забезпечення** смартфона загалом і застосунків зокрема. Також радимо налаштувати автоматичне оновлення й періодично перевіряти їх завантаження.
4. Встановіть антивірус та VPN.
Зверніть увагу: категорично заборонено використовувати програми російського та китайського походження! Вони неодноразово були помічені на збиранні та продажу даних. А ще через ці програми росіяни легко можуть зламати ваш пристрій.
5. **Регулярно скануйте систему на наявність шкідливих програм**. Для цього скористайтеся **спеціальним програмом**. Ми радимо застосунок iVeriFu, що пропонує покроковий алгоритм для захисту ваших гаджетів.