

Базова безпека вашого мобільного пристрою

Нині безпека даних на мобільних пристроях — одна з найбільш актуальних тем. І це не дивно, адже наші смартфони містять величезну кількість особистої інформації — від паролів і контактів до фінансових даних та особистих повідомлень. У цій статті ми розглянемо основні засоби захисту мобільного пристрою. Однак пам'ятайте: найкраще свій пристрій можна захистити, одночасно використовуючи різні методи.

Пароль та/або відбиток пальця

Один із найбільш очевидних методів захисту мобільного пристрою полягає в налаштуванні пароля або використанні відбитка пальця для його розблокування. Це допоможе захистити дані на пристрої від несанкціонованого доступу. Не використовуйте легко вгадуванні комбінації, як-от 123456.

Ще один важливий рівень захисту — використання *Touch ID* або *Face ID*. Вони дають змогу легко та швидко розблокувати пристрій, не вводючи щоразу пароль.

Оновлення програмного забезпечення та встановлення додатків

Відколи було випущено ваш пристрій, цілком імовірно, з'явилося безліч програм і додатків для роботи з ним. Проте з появою нових програм і версій ОС з'являються нові проблеми з безпекою.

Одним із найважливіших кроків для убезпечення мобільних пристроїв є оновлення програмного забезпечення, зокрема операційної системи, програм і додатків. Такі оновлення можуть містити важливі патчі та виправлення вразливостей і покращують безпеку пристрою та даних на ньому.

- **Оновлення операційної системи**

Виробники пристроїв періодично випускають нові версії операційних систем, у яких додають нові функції, виправляють помилки та загалом покращують їх продуктивність і безпечність. Щоб оновити ОС на мобільному пристрої, перевірте наявність нових версій у налаштуваннях пристрою та встановіть їх. Сам процес оновлення може зайняти деякий час, тому радимо запланувати його заздалегідь.

- **Оновлення програм і додатків**

Якщо програма міститиме вразливості, зловмисник зможе скористатися ними, щоб отримати доступ до вашого пристрою та даних. Зазвичай програми автоматично перевіряють наявність оновлень і попереджають про необхідність їх завантаження та встановлення. Однак якщо вимкнути автоматичне оновлення, вам доведеться самостійно стежити за оновленнями та встановлювати їх.

Деякі власники мобільних пристроїв можуть не оновлювати програми або операційну систему через небажання втратити налаштування або особисті дані. Проте якщо цього не робити, ваш пристрій і дані на ньому опиняться під загрозою.

- **Як вибрати безпечний додаток**

Перед встановленням додатків слід звертати увагу на рейтинг і відгуки користувачів, а також перевіряти, чи є додаток відомим та чи має він сертифікат безпеки.

Додатки можна завантажити з офіційного магазину додатків на вашому пристрої (наприклад, *Google Play* для *Android* або *App Store* для *iOS*) або з інших джерел, зокрема сторонніх сайтів. Радимо завжди встановлювати додатки з офіційного магазину додатків, оскільки перед публікацією в магазині вони підлягають перевірці. Не встановлюйте додатки з підозрілих джерел, як-от неофіційних магазинів, адже це може призвести до появи шкідливого програмного забезпечення на вашому пристрої.

Після встановлення додатка зверніть увагу, які дозволи на доступ до пристрою він запитує. Наприклад, якщо додаток для читання новин запитує доступ до камери та мікрофона, варто задуматися, для чого це йому потрібно. Якщо додаток запитує конфіденційну інформацію, як-от пароль або номер телефону, ретельно перевірте його рейтинг і відгуки користувачів, знайдіть інформацію про розробника. Ось декілька порад:

1. Перевірте інформацію про розробника в магазині додатків. Більшість магазинів надають інформацію про розробника під час завантаження додатку. Наприклад, у *Google Play* ви можете натиснути на ім'я розробника, щоби переглянути його профіль. Там міститься інформація про компанію, яка створила додаток, а також про інші додатки, які вона розробляла.
2. Перевірте веб-сайт розробника. Переважна більшість розробників має веб-сайти, де надають додаткову інформацію про свої продукти та компанію.
3. Перевірте рейтинг і відгуки. Рейтинг і відгуки про додаток можуть дати уявлення про те, наскільки популярним і якісним є цей додаток. Пам'ятайте: деякі рейтинги можуть бути підробленими, тому ретельно перегляньте відгуки, щоби переконатися в їх достовірності.
4. Перевірте соціальні мережі. Розробники часто мають сторінки в соціальних мережах, наприклад, у *Facebook*, *X (Twitter)* і *LinkedIn*.

Крім того, важливо слідкувати за налаштуваннями безпеки мобільного пристрою. Наприклад, можна ввімкнути двофакторну автентифікацію для входу в обліковий запис. Також варто встановити антивірусні програми. Багато безкоштовних варіантів можна завантажити з *Google Play* чи *App Store*. Ці додатки дозволяють виявляти шкідливе програмне забезпечення, а також дають змогу віддалено видаляти дані з пристрою, якщо він був викрадений або загублений. Ось кілька антивірусів для мобільних пристроїв:

- *Norton Mobile Security*. Це один із найкращих антивірусних додатків для мобільних пристроїв, який захищає від вірусів, шпигунського програмного забезпечення та інших загроз. Він також має вбудований блокувальник реклами та функцію відстеження пристрою в разі втрати. *Norton* перестала обслуговувати користувачів із Росії та Білорусії з 15.03.2022 ([Link](#))
- *Bitdefender Mobile Security*. Цей антивірусний додаток має добру репутацію й забезпечує повний захист від вірусів, троянських програм та інших загроз. Він також має вбудований блокувальник викликів і повідомлень. Компанія підтримує Україну й надає безкоштовний доступ до своїх продуктів і консультації для кіберзахисту українського бізнесу з 18.03.2022 ([Link](#))
- *McAfee Mobile Security*. Цей антивірусний додаток є одним із найбільш популярних серед користувачів мобільних пристроїв. Він має вбудований блокувальник реклами, функцію відстеження пристрою та захист від шкідливих

програм. *McAfee* призупинила розвиток свого бізнесу в Росії та Білорусі з 23.03.2022 ([Link](#))

- *Avast Mobile Security*. Цей антивірусний додаток має широкий спектр функцій, зокрема захист від вірусів, троянських програм і шпигунського програмного забезпечення. Він також має функцію блокування дзвінків і повідомлень від небажаних контактів. *Avast* перестала постачати послуги в Росії та Білорусії з 10.03.2022 ([Link](#))

Резервне копіювання

Віруси, помилкове видалення файлів або крадіжка телефону можуть призвести до втрати даних. Тому надійне резервне копіювання є запорукою інформаційної безпеки мобільних пристроїв.

Резервне копіювання — це процес створення копії важливих даних із метою їх збереження в разі втрати оригіналу. Копії можуть зберігатися як на самому телефоні або інших зовнішніх носіях, так і в хмарному сховищі.

- **Використання хмарного сховища**

Багато хмарних сервісів, як-от *Google Drive*, *iCloud*, *OneDrive* і *Dropbox*, пропонують можливість зберігання даних на серверах в Інтернеті. Це дає змогу отримати доступ до цих даних із будь-якого мобільного пристрою або комп'ютера з підключенням до мережі. Більшість хмарних сервісів мають додатки для мобільних пристроїв, за допомогою яких можна автоматично робити резервні копії даних із вашого телефона.

- **Використання зовнішнього жорсткого диска**

Іншим варіантом є збереження резервних копій на зовнішньому жорсткому диску. Він стане в пригоді, якщо у вас обмежений доступ до Інтернету або ви не хочете постійно сплачувати за хмарне сховище. Для збереження даних на зовнішньому жорсткому диску необхідно використовувати спеціальне програмне забезпечення, наприклад, *iTunes* для *iPhone* або *Samsung Smart Switch* для *Samsung Galaxy*. Ці програми дозволяють створювати резервну копію даних на комп'ютері або зовнішньому жорсткому диску.

Незалежно від того, який метод ви оберете для збереження резервних копій даних, важливо регулярно ним користуватися. Ідеальним є щотижневе створення резервної копії, що «застрахує» від непередбачуваних утрат даних.

Використання VPN

Віртуальна приватна мережа (VPN) — це інструмент, який забезпечить вашу конфіденційність в Інтернеті. Використання VPN дозволяє захистити особисті дані від зловмисників, які можуть перехопити ваш трафік, а також отримати доступ до контенту, недоступного у вашій країні. Використання VPN — хороша ідея при підключенні до Wi-Fi у громадських місцях. Вибираючи провайдера VPN, зверніть увагу на такі характеристики:

- **Протоколи шифрування**

Найважливішою характеристикою безпечного VPN є наявність надійних протоколів шифрування. Деякі з найпоширеніших протоколів: *OpenVPN*, *L2TP/IPSec* і *IKEv2*. Щоби

гарантувати достатній рівень захисту VPN, перевірте наявність цих протоколів у його налаштуваннях.

- **Логування**

Іншою важливою характеристикою безпечного VPN є його політика логування. Ідеальний VPN не зберігає жодних логів, адже тільки так можна забезпечити максимальний рівень приватності для користувачів. Якщо ваш VPN зберігає логи, це потенційно може призвести до витоку особистих даних.

- **Репутація провайдера**

При виборі VPN важливо перевірити репутацію його провайдера. Зверніть увагу на відгуки користувачів і дослідження, що були проведені спеціалізованими порталами з вивчення безпеки в Інтернеті. Якщо провайдер має добру репутацію, це збільшує шанси на те, що ваші дані будуть надійно захищені.

- **Сервери**

Безпечний VPN має мати велику кількість серверів у різних країнах. Це гарантуватиме високу швидкість підключення та доступ до контенту з різних країн. Крім того, що більше серверів використовується, то менша ймовірність перевантаження та пов'язаних із цим проблем.

- **Kill switch**

Функція *kill switch* — важлива характеристика безпечного VPN, оскільки вона забезпечує максимальний рівень приватності для користувачів у разі втрати підключення. Якщо підключення до VPN втрачається, функція *kill switch* автоматично вимикає ваш доступ до Інтернету, щоб уникнути можливого витоку інформації про ваші дії.

- **Захист від реклами та шкідливих програм**

Деякі VPN мають додаткові функції, як-от захист від реклами та шкідливих програм.

Залежно від доступних функцій, кількості серверів і їх продуктивності, сервіси VPN можуть суттєво різнитися за ціною, тож важливо знайти баланс між вашими потребами та можливостями сервісу. Ось кілька сервісів VPN для мобільних пристроїв: *CyberGhost*, *Surfshark*, *ProtonVPN*. Втім, пам'ятайте: жоден VPN не може гарантувати 100-відсоткову безпеку й анонімність в Інтернеті.

Висновок

Варто пам'ятати, що безпека — це процес, а не одноразова дія. В обмін на певні затрати часу та зусилля ви отримаєте більшу захищеність і спокій. Щоби ваші дані були завжди в безпеці, потрібно постійно здійснювати заходи щодо їх захисту, регулярно перевіряти й оновлювати встановлені програми та використовувати додаткові засоби захисту, коли це потрібно. Складіть власний план захисту, поєднавши кілька методів, щоб забезпечити максимальний захист вашого пристрою.

Ефективність вибраних засобів захисту залежатиме від багатьох факторів, зокрема вашого стилю користування мобільним пристроєм. Встановлення надійного пароля,

використання *Touch ID* або *Face ID*, вчасні оновлення ОС і програм, резервне копіювання даних і вихід у мережу через *VPN* — усе це важливі кроки до забезпечення вашої інформації.