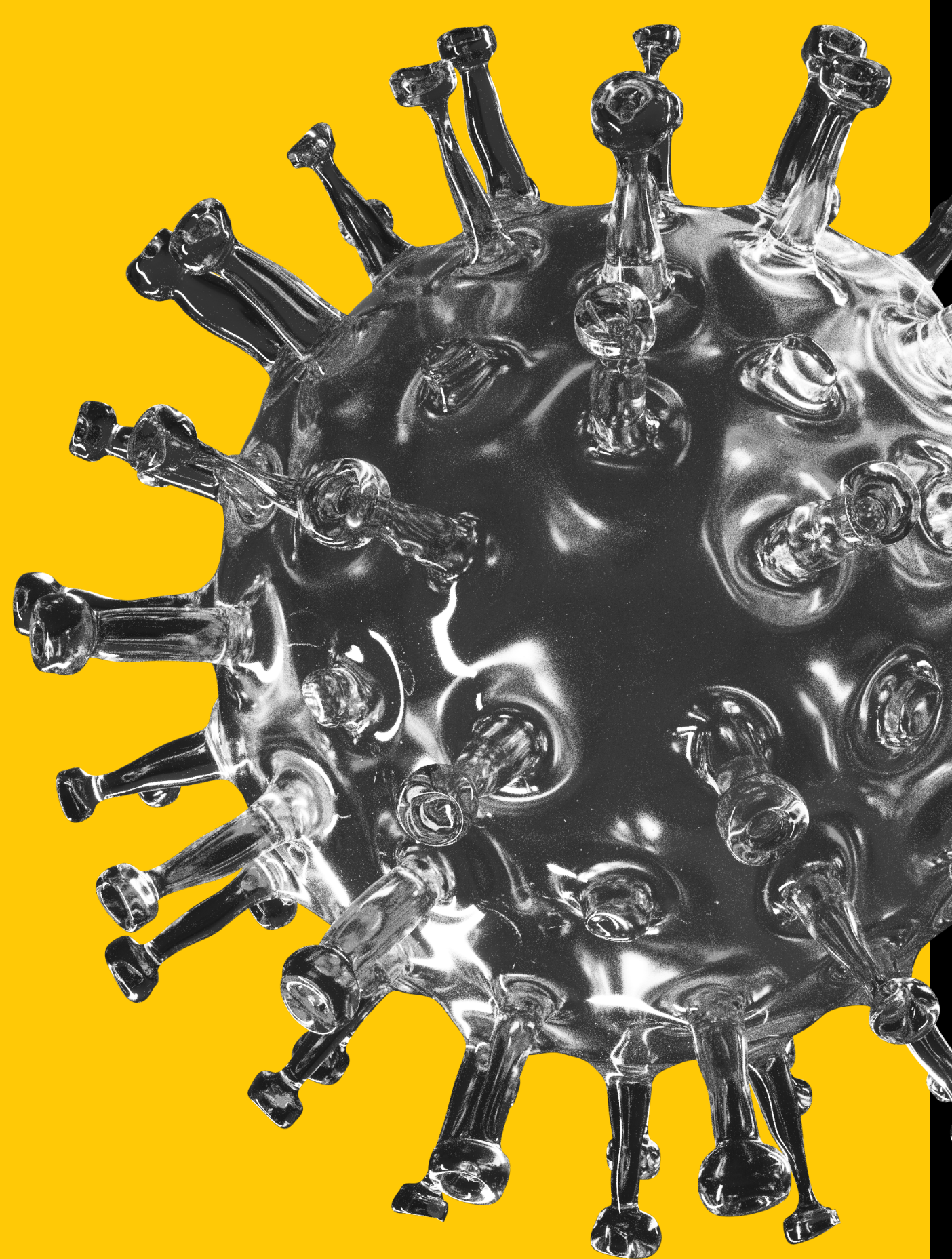


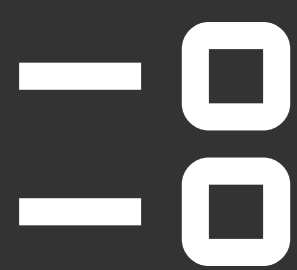


Основні правила кібергігієни

Поради для безпеки вашого
телефона



Міністерство
цифрової трансформації
України



Основні правила

Важливо дотримуватися основних правил кібергігієни для захисту персональних даних.

Ми зібрали основні базові поради, які допоможуть вам захистити свої пристрої від злому та від витоку персональних даних.

1. Встановити режим «Карантин» (Lockdown) →
2. Реєстрація SIM-карти мобільного оператора на контракт →
3. Двофакторна автентифікація →
4. Месенджери →
5. Встановіть надійні паролі для всіх акаунтів →
6. Придбайте YubiKey для пошти →
7. Своєчасно оновлюйте операційну систему та застосунки →
8. Регулярне резервне копіювання →
9. Аналізуйте застосунки, які встановлюєте →
10. VPN →
11. MacOS →
12. Windows →
13. Подивіться навчальний серіал на порталі Дія.Цифрова освіта →



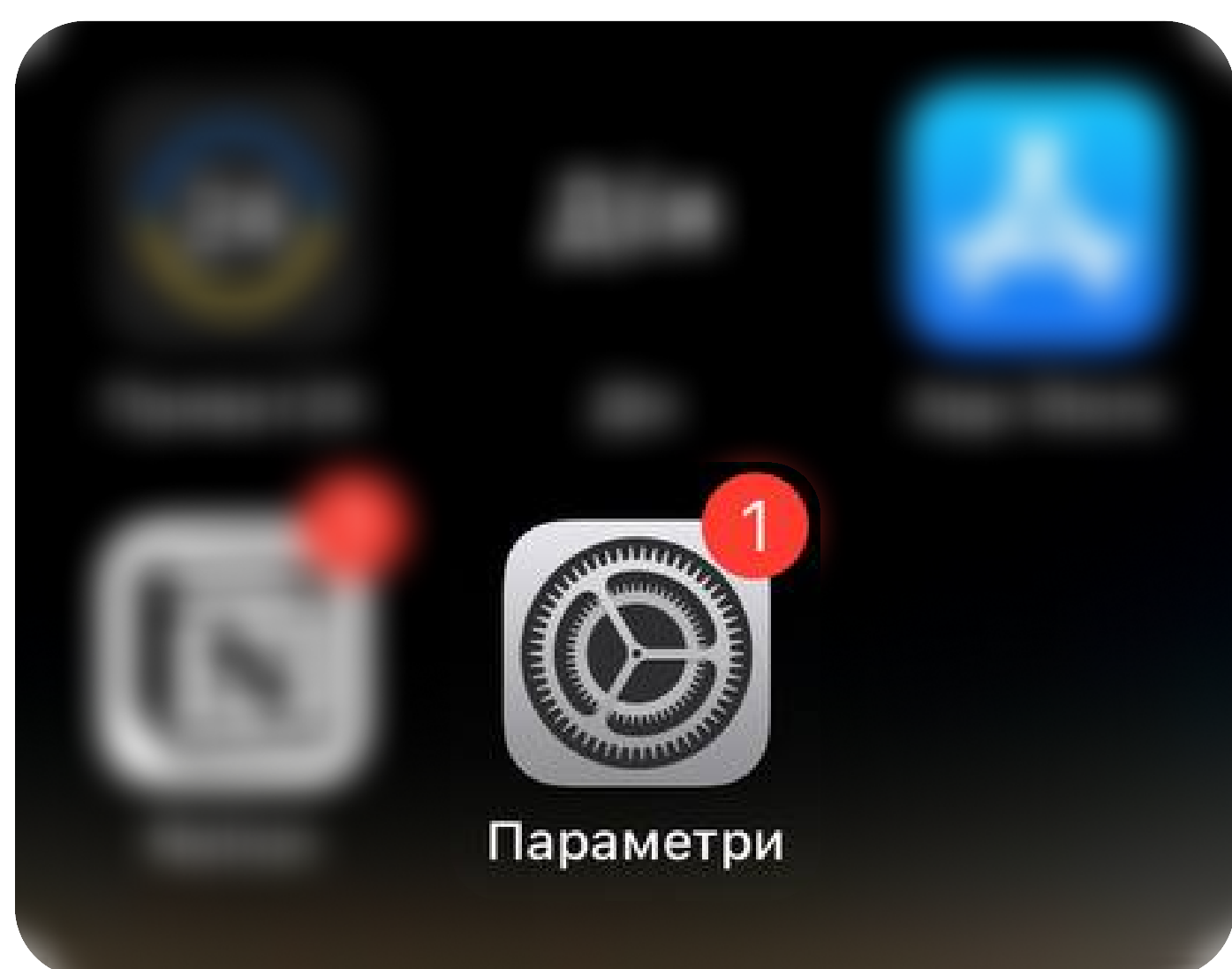
Встановити режим «Карантин» (Lockdown)

Тільки якщо у вас iPhone

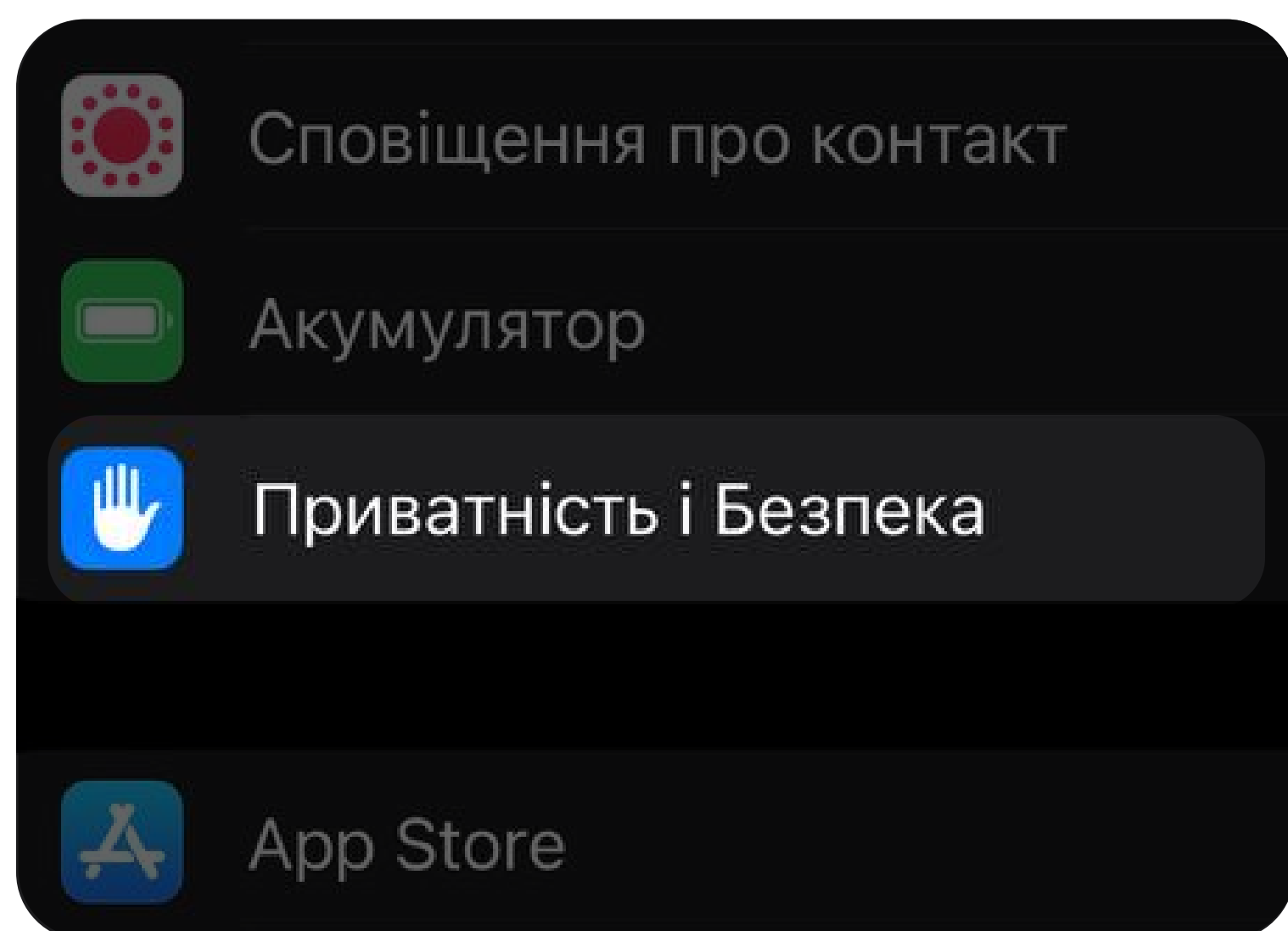
Карантин в iOS 16 — режим надбезпеки, який захищає від кібератак, спонсорованих урядом певних країн. Надає екстремальний рівень захисту, але деякі функції iPhone стають недоступними.

Режим корисний міністрам та держслужбовцям, активістам, військовим або тим, хто проживає на окупованих територіях, у зонах бойових дій, всім, хто може зазнати шантажу та стеження через iPhone.

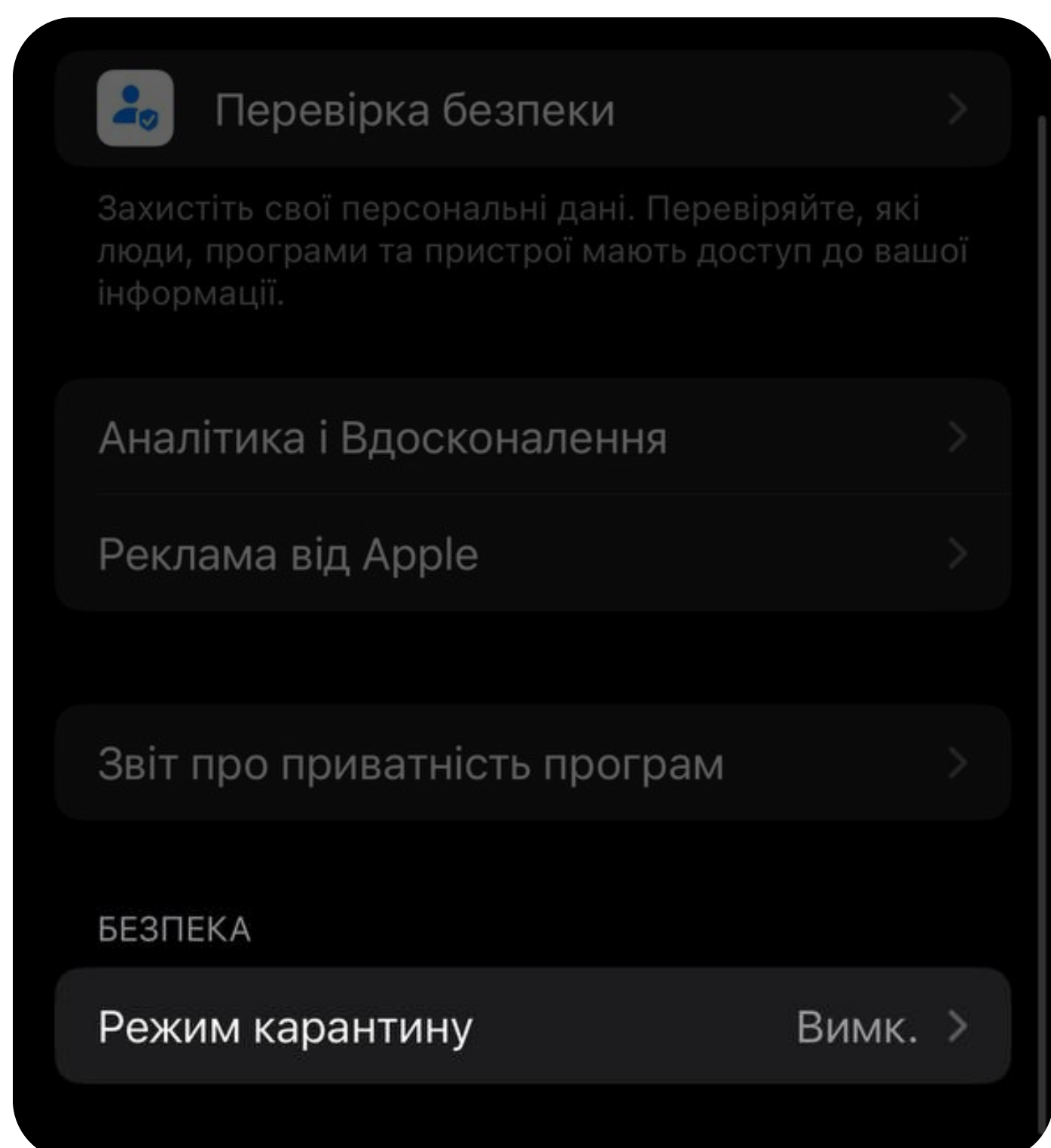
Як увімкнути режим карантину на iOS 16



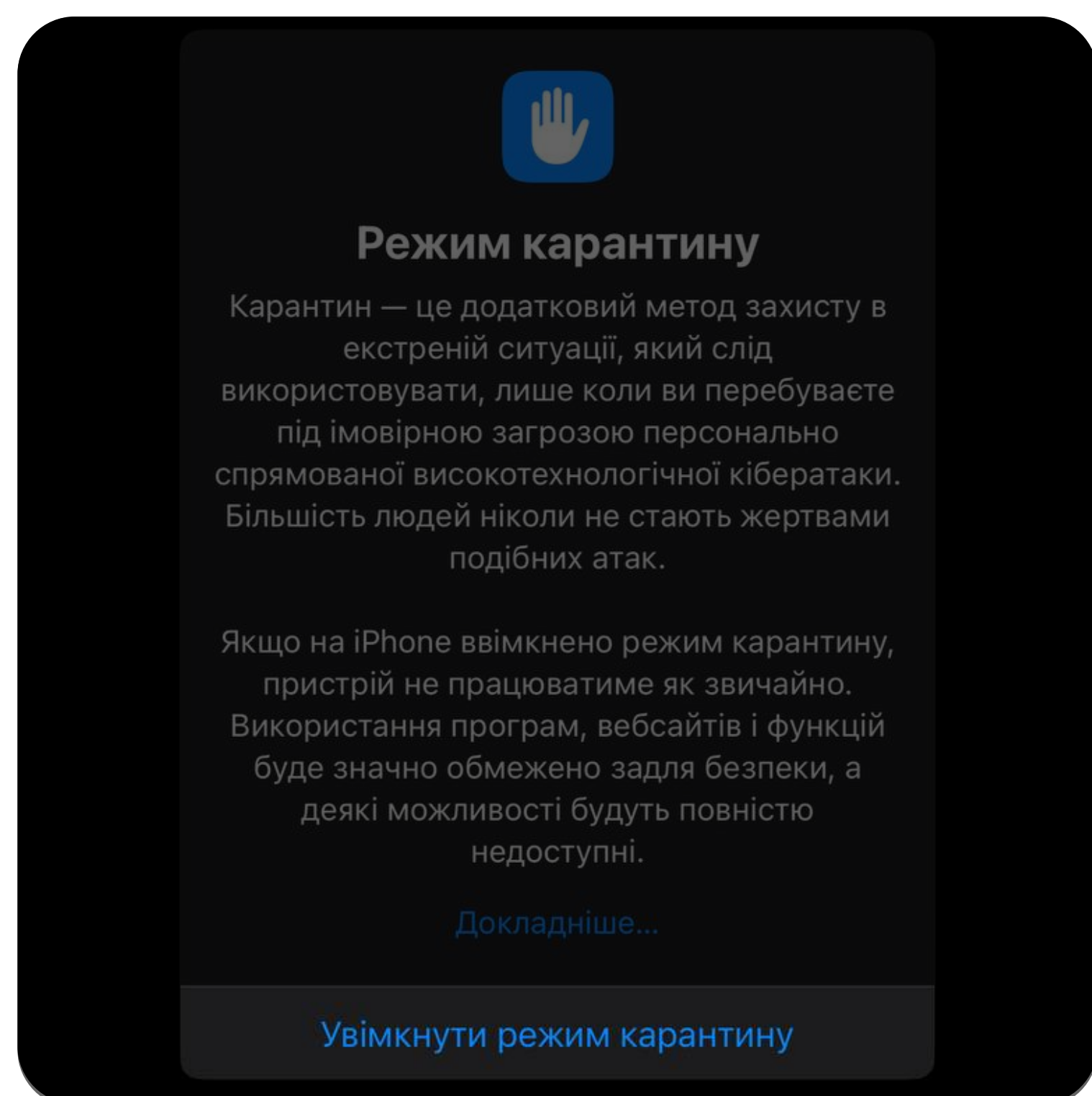
1. Перейдіть до «Параметрів»



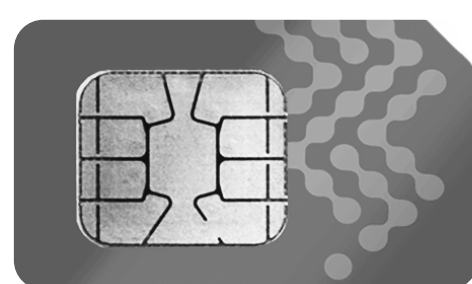
2. Відкрийте «Приватність і Безпека»



3. Прогортайте донизу та виберіть «Режим карантину»



4. Активуйте його



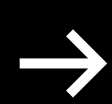
Реєстрація SIM-карти мобільного оператора на контракт

Зловмисники відновлюють SIM-карту з вашим номером телефону, легко імітуючи, що вона належить саме їм. **Якщо номер прив'язаний до паспорта, цього зробити не вдасться.** Адже для перевипуску SIM-карти людина має прийти до відділення з документами.

Прив'язка номера до паспорта допоможе зменшити кількість шахрайських схем, викрадення номерів для злому акаунтів у соцмережах та банківських акаунтів, спаму, небажаних дзвінків від колекторів і з невідомих номерів.

Як це зробити

Онлайн

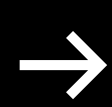


У мобільному застосунку чи на сайті мобільного оператора.

Для цього необхідно мати електронний цифровий підпис. Щоб зареєструвати номер, виберіть оператора та натисніть на потрібну кнопку:



Офлайн



У відділенні оператора.

Із собою потрібно мати Дію або паспорт та ідентифікаційний номер (ІПН), SIM-карту.





Двофакторна автентифікація

Це посилення захисту облікових записів різних онлайн-сервісів від несанкціонованого доступу.

Найчастіше використовують додаткові SMS-повідомлення або окрему програму, яка генерує код доступу. Користувач вводить стандартний пароль, який він установив сам, а потім додатковий код, який приходить у SMS-повідомленні або ж у спеціальному застосунку.

Інструкції, як встановити двофакторну автентифікацію для онлайн-сервісів



Акаунт Gmail



Facebook



Instagram



Twitter



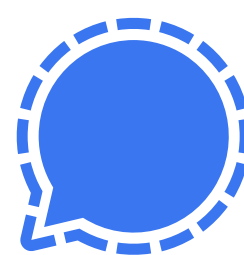
Viber



WhatsApp

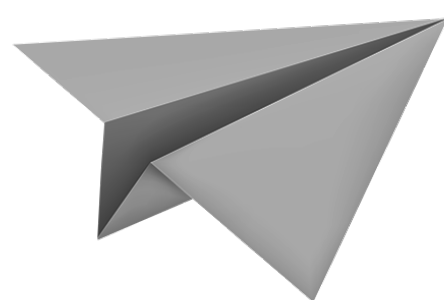


Telegram



Signal



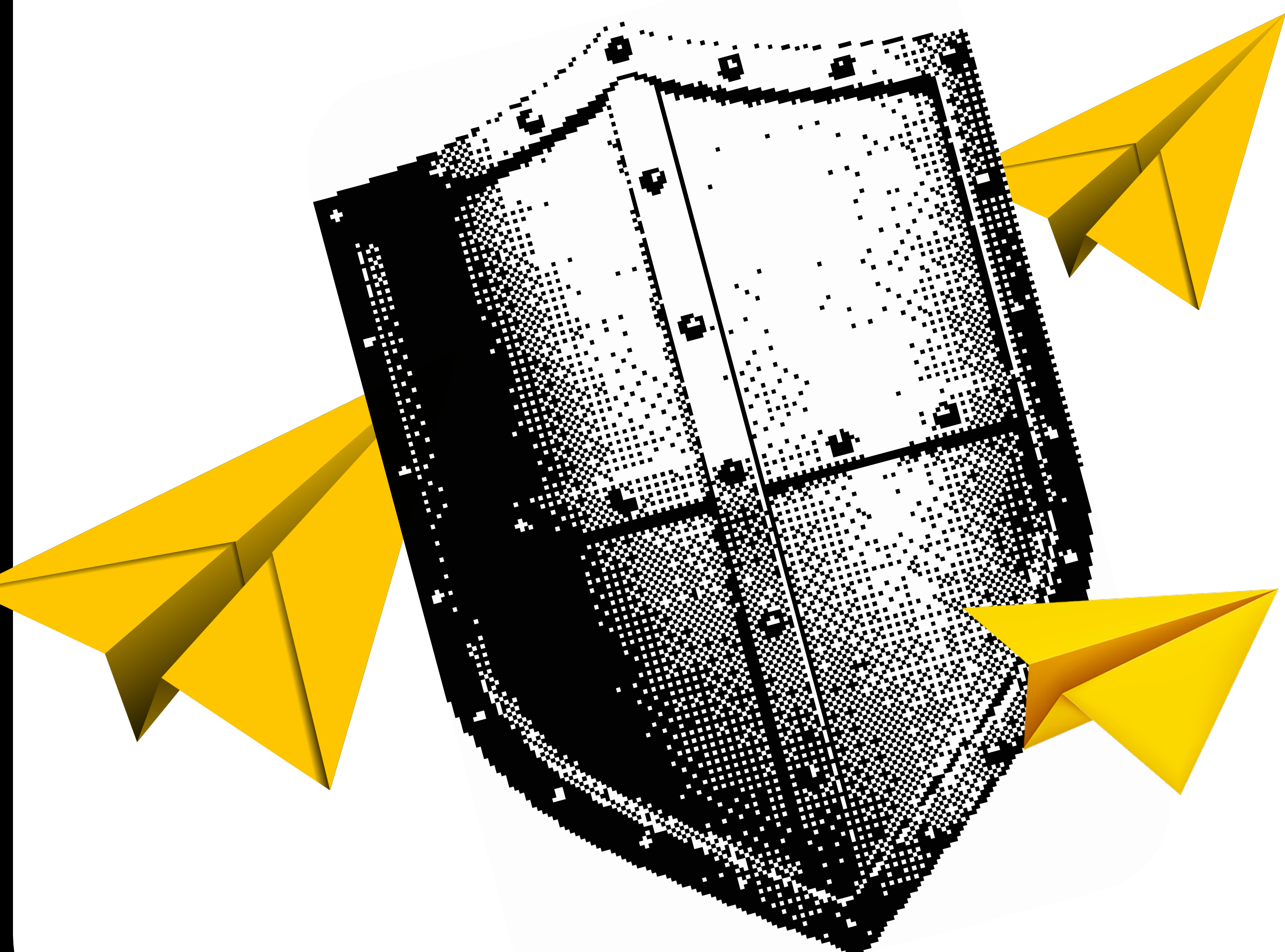


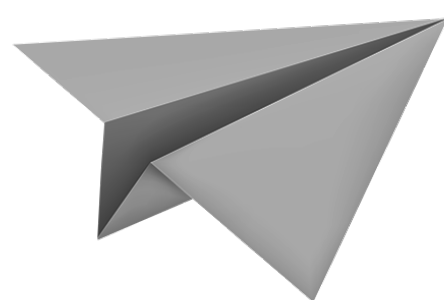
Месенджери

Який месенджер найбезпечніший?

Безпечних на 100% немає. Є популярні, якими користується більшість. Серед них – WhatsApp, Telegram, Viber та Signal. Пріоритет слід надати месенджерам, які використовують наскрізне шифрування. Це коли повідомлення надійно зашифровуються при надсиланні з вашого пристрою і розшифровуються лише на пристрої співрозмовника, а сервери розробників месенджера лише транспортують зашифроване повідомлення чи голосовий дзвінок. Як-от Signal або WhatsApp.

Надійність – це якість шифрування при передаванні повідомлень. Якщо хтось перехопить розмову, то не зможе розшифрувати повідомлення і прочитати його. Але месенджери не забезпечують анонімності. Якщо у вас відібрали чи вкрали телефон – усі повідомлення залишаються на пристрої.





Месенджери

WhatsApp

Найпопулярніший месенджер, використовується у більш ніж 180 країнах світу. У 2016 році запровадив наскрізне шифрування.

Telegram

За замовчуванням не має наскрізного шифрування як для повідомлень, так і для груп або метаданих. Дані зберігаються у хмарі, на серверах Telegram. За словами розробників, інформація звичайних чатів зберігається на кількох серверах по всьому світу і контролюється різними законами з надання доступу до неї. Ключі для розшифровки також зберігаються окремими блоками на різних серверах.

Однак лише секретні чати підтримують наскрізне шифрування, тому чутливу інформацію рекомендується передавати через них.

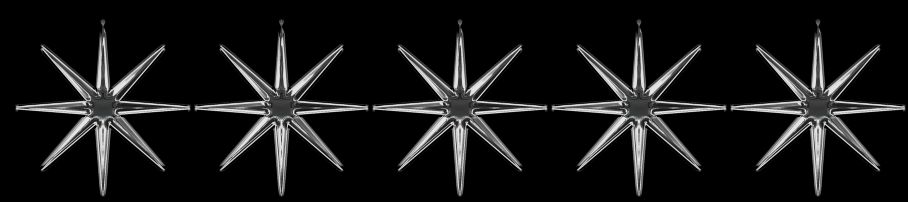
Signal

Безкоштовний месенджер, вважається одним із найбезпечніших. Розробники впровадили свою систему шифрування повідомлень, дзвінків та файлів. Вона настільки надійна, що доступ до цих даних не можуть отримати навіть сервери, які їх передають. Повідомлення зберігаються на пристрої і локально шифруються за допомогою парольної фрази перед відправкою на сервер. Signal – єдиний месенджер, який відкрив свої протоколи даних. Їх вивчили фахівці і підтвердили його безпеку.

Threema

Платний месенджер, який приділяє багато уваги безпеці. Уперше відвідуючи застосунок, користувач проводить пальцем по екрану, щоб згенерувати свій унікальний ідентифікатор.

Застосунок гарантує, що всі повідомлення шифруються одразу на пристрої й прочитати їх зможе тільки одержувач.



Встановіть надійні паролі для всіх акаунтів

Надійний пароль — комбінація мінімум з 12 символів, містить великі та малі літери, цифри та символи. Для кожного акаунту використовуйте унікальний пароль. Змінюйте їх регулярно — раз на 6 місяців. Щоб створити унікальний складний пароль, скористайтеся будь-яким генератором паролів, наприклад [ось цим ↗](#).

Перевірте наявні облікові записи електронної пошти та акаунти в соцмережах. Сайти haveibeenpwned.com та breachalarm.com допоможуть з'ясувати, чи був пароль до електронної пошти викрадений зловмисниками.

Не зберігайте паролі в легкодоступних місцях, наприклад у нотатках. Використовуйте для їх зберігання спеціальні програмні засоби (наприклад, KeePass). В iPhone можете використовувати вбудований застосунок «Паролі», який генерує безпечні паролі та надійно зберігає їх.





Придбайте YubiKey для пошти

YubiKey – це фізичний ключ безпеки, флешка, яка забезпечує надійну автентифікацію одним дотиком і працює з обліковими записами Google. Захистіть акаунт на gmail, увімкнувши двоетапну перевірку Google і зареєструвавши YubiKey у своєму обліковому записі.

Фізичний ключ для входу захищає обліковий запис від віддаленого та несанкціонованого доступу.

Тож ви зможете безпечно зберігати у хмарі акаунту Google усі особисті документи, фото та дані.





New tab



Тричі подумайте перед відкриттям вкладень

1. **Не відкривайте підозрілі посилання (URL), які ви отримали поштою, у SMS чи повідомлені у месенджері від незнайомих осіб чи пабліків. Особливо ті, що вказують на сайти, якими ви зазвичай не користуєтесь.**

2. **Найпоширеніший засіб — фішинг.**

Фішинг — це спроба отримати особисту інформацію, зламати облікові записи або зламати пристрій через електронні листи, повідомлення, оголошення або сайти, схожі на ті, яким ви вже довіряєте. Наприклад, ви можете отримати електронний лист, який оформлений так, неначе його відправили із соцмережі, і який містить посилання. Переходячи за посиланням, ви надаєте доступ зловмиснику до вашого пристрою та усієї інформації.

Звертайте увагу на доменне ім'я сайту або застосунку, що запитує персональні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим, як-от `facebook.com`, `google.com` тощо. В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самотійно «віддати» власні дані та паролі.

- У разі необхідності введення особистих даних упевніться в тому, що використовується захищене з'єднання HTTPS. Відкрийте вебсторінку в браузері.
- Перевірте, який значок статусу безпеки сайту відображається ліворуч від вебадреси. Якщо є символ замочка або напис З'єднання безпечне — все добре. Щоб переглянути інформацію про дозволи й захист конфіденційності для сайту, натисніть на значок безпеки.



website.domain



Своєчасно оновлюйте операційну систему та застосунки

Регулярне оновлення сприятиме виправленню вразливостей та помилок у програмному забезпеченні. Допомогає не потрапити на «вразливість першого дня» (0-day) — це неусунені вразливості, шкідливі програми, проти яких ще не розроблено захисні механізми.

Тож налаштуйте автоматичне оновлення застосунків у телефоні та завжди перевіряйте доступність оновлення програмного забезпечення.

Для iOS

Перейдіть у меню «Параметри» > «Загальні» > «Оновлення ПЗ». Виберіть «Автоматичні оновлення», а потім увімкніть параметр «Викачати оновлення iOS». Увімкніть параметр «Інсталювати оновлення iOS». Пристрій автоматично оновиться до останньої версії iOS або iPadOS. Деякі оновлення може знадобитися інсталювати вручну.

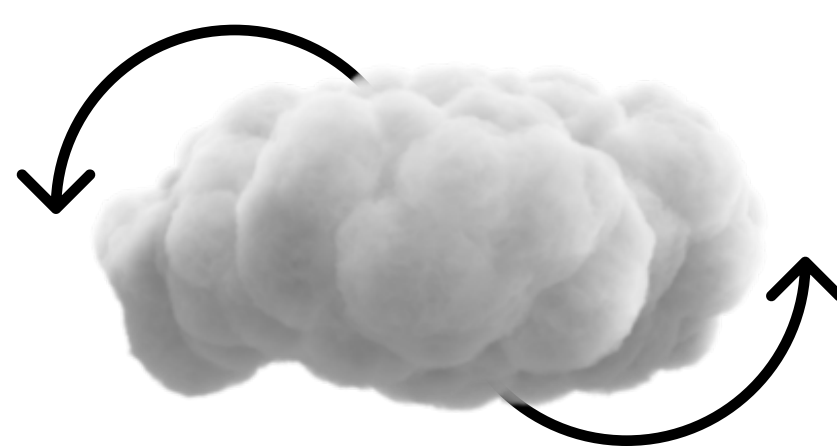
Для Android

Відкрийте магазин Google Play. Торкніться трьох горизонтальних ліній у верхньому лівому куті екрана, щоб відкрити меню Play Store. У меню виберіть «Налаштування». У розділі «Загальні» натисніть на «Автоматичне оновлення програм». Ви можете дозволити автоматичне оновлення в будь-який час або лише через Wi-Fi.



UPD 4.2





Регулярне резервне копіювання

Резервне копіювання інформації слід виконувати на зовнішній жорсткий диск або у хмару. Це допоможе відновити потрібні дані у разі пошкодження або видалення шкідливим програмним забезпеченням.

Як налаштувати регулярне резервне копіювання

Для iOS

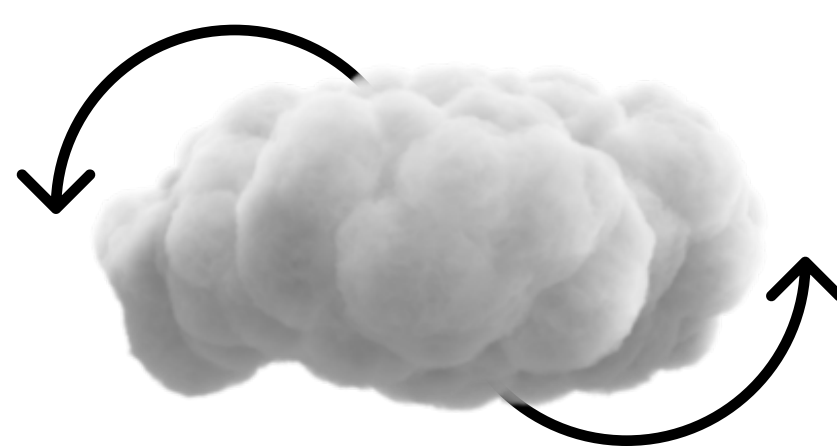
Резервне копіювання iPhone за допомогою iCloud

1. Перейдіть до **Параметрів**
2. > [ім'я пристрою] > iCloud > Архівація в iCloud.
3. Увімкніть **«Архівація в iCloud»**. iCloud автоматично створюватиме резервну копію iPhone щодня, коли iPhone підключено до джерела живлення, замкнено та під'єднано до Wi-Fi.
4. Щоб створити резервну копію вручну, торкніть **«Виконати зараз»**.

Резервне копіювання iPhone за допомогою Mac

1. Під'єднання до комп'ютера за допомогою кабелю.
2. На бічній панелі Finder на Mac виберіть **iPhone**. Щоб використовувати Finder для резервного копіювання iPhone, потрібна macOS 10.15 або пізнішої версії. З попередніми версіями macOS **використовуйте iTunes** для резервного копіювання iPhone.
3. Угорі вікна Finder клацніть **«Загальні»**.
4. Виберіть **«Створити резервну копію всіх даних з вашого iPhone на цьому Mac»**.
5. Щоб зашифрувати дані резервної копії та захистити їх за допомогою пароля, виберіть **«Шифрувати локальну резервну копію»**.
6. Клацніть **«Створити резервну копію зараз»**.





Регулярне резервне копіювання

Резервне копіювання iPhone за допомогою ПК з Windows

1. Під'єднання до комп'ютера за допомогою кабелю.
2. У програмі iTunes на ПК клацніть кнопку iPhone угорі зліва вікна iTunes.
3. Клацніть **«Підсумок»**.
4. Клацніть **«Створити резервну копію зараз»** (у розділі **«Резервні копії»**).
5. Щоб зашифрувати резервні копії, виберіть **«Шифрувати локальну резервну копію»**, введіть пароль, а потім клацніть **«Задати пароль»**.

Для Android

1. Відкрийте додаток **«Налаштування»**,
2. Торкніться параметра **«Облікові записи»**,
3. Виберіть свій обліковий запис Google і переконайтеся, що всі програми і служби в цей обліковий запис були недавно синхронізовані.
4. Якщо деякі служби не були синхронізовані недавно, натисніть кнопку **«Синхронізувати зараз»**.





Аналізуйте застосунки, які встановлюєте

Завантажуйте тільки необхідні для роботи програми. Коли встановлюєте застосунок, звертайте увагу на дозволи, які надаєте. Часто шкідливі програми надсилають запит на отримання більшої кількості дозволів, ніж вимагає їх функціонал. Це сприяє поглибленню збору інформації про користувача з метою отримання прибутку. Переконайтеся в безпеці програм та дозволів, яких вони потребують.

Для iOS

Використовуйте функцію **«Перевірка безпеки»**. Перевіряйте й оновлюйте інформацію, до якої надаєте доступ людям і програмам. Якщо ваша особиста безпека під загрозою, скористайтесь функцією **«Перевірка безпеки»**, щоб негайно закрити доступ до інформації.

Усі програми обов'язково мають запитувати ваш дозвіл, перш ніж починати відстежувати iPhone на вебсайтах і в програмах, що належать іншим компаніям, для показу реклами чи передавання вашої інформації брокеру даних. Ви можете заборонити всім програмам запитувати такий дозвіл.

Ви можете переглянути й налаштувати дані, якими обмінюєтеся з програмами, інформацію про розташування й апаратне забезпечення, які ви поширюєте, та параметри того, як Apple надсилає вам рекламу в App Store, Apple News і Біржах.

Для Android

Після встановлення програми ви самостійно надаєте їй доступ до камери, сповіщень, контактів, сховища та інших складників системи.

Шкідлива програма зазвичай маскується під звичайні додатки, як-от браузер, плеєри, ігри, навігатори, книги і навіть антивіруси. Такі програми можуть витягати інформацію з вашого пристрою, тому будьте обережні з наданням дозволів. Наприклад, звичайній грі не потрібен доступ до контактів та SMS-повідомлень.

Однак вам не варто перейматися, якщо всі додатки ви встановлюєте виключно з Play Маркету. Додатки, що там розміщені, ретельно перевіряються.





VPN

VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером.

Дані в ньому надійно зашифровані: інтернет-провайдер не дізнається вашої локації та вебресурсів, які відвідали.

Оновлена IP-адреса зазвичай створюється з іншого міста або країни. Наприклад, ви можете увійти в систему з Києва, перебуваючи в Україні, але ваша IP-адреса буде вказувати, що ви, наприклад, у Лондоні, Великій Британії.

Коли варто користуватись VPN

- Під час користування незахищеними загальнодоступними мережами Wi-Fi, щоб захистити свої дані. Це відкриті Wi-Fi точки доступу в громадських місцях, кафе, ресторанах парках тощо.
- Коли необхідний захищений доступ до інтернет-мережі та систем під час організації віддаленої роботи.
- Щоб захистити себе від вебсайтів, програм і сервісів, які хочуть відстежувати ваші дії.
- Щоб оператор або провайдер не міг відслідковувати ваших дій в інтернеті.





VPN

Як вибрати VPN

Вибираючи VPN, зверніть увагу на такі критерії:

- **Захист.** Краще вибрати VPN, в якому є шифрування військового класу (наприклад, AES-256), асортимент протоколів безпеки (OpenVPN, L2TP, IKEv2, WireGuard та інші), захист від витоків через DNS, технологія TrustedServer, яка видаляє всі ваші дані під час кожного перезапуску, та функція автоматичного аварійного відключення (kill switch).
- **Підтримка операційних систем.** Переконайтесь, що VPN підтримує операційні системи, якими ви користуєтесь: Android, iOS, Windows та інші потрібного покоління.
- **Кількість одночасних активних пристроїв.** Головне, щоб вам вистачило.
- **Вартість.** VPN бувають платні та безоплатні. Платні можуть мати кращий рівень захисту, вищу швидкість з'єднання, підтримку більшої кількості операційних систем.
- **Перевірте репутацію сервісу** в пошуковику – чи не було фактів витоку або продажу даних користувача.
- **Не використовуйте російських VPN**, вони, ймовірно, можуть надсилати дані російським спецслужбам.

Кілька варіантів VPN-сервісів, які рекомендують фахівці



ClearVPN



Безкоштовний для українців



ExpressVPN



Surfshark



PrivateInternetAccess



CyberGhostVPN



NordVPN



ProtonVPN



MacOS

Для MacOS працюють ті самі правила, що й для айфонів:

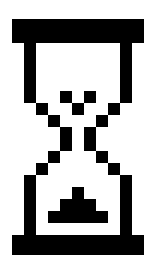
- встановіть режим «Карантин»
- своєчасно оновлюйте систему та застосунки
- створюйте резервну копію системи та файлів
- не переходьте за незнайомими посиланнями

Ще декілька корисних порад

Захист комп'ютера від шкідливих програм: Один із найпоширеніших способів розповсюдження шкідливих програм — це вбудовування їх в інші програми, що видаються безпечними.

Можна зменшити цей ризик, використовуючи тільки програми, що походять із надійних джерел. Параметри «Захист і безпека» дають змогу визначити джерела, з яких програми встановлюватимуться на комп'ютер Mac.

1. На Mac виберіть **меню Apple**
2. **> Системні параметри**, а потім клацніть **«Захист і безпека»**
3. На боковій панелі (імовірно, потрібно буде прокрутити вниз) перейдіть у розділ **«Безпека»**, клацніть спливне меню поруч із **«Дозволити програми, які викачано з»**, а потім виберіть джерела, з яких ви дозволите інсталювати програмне забезпечення:
 - a. **App Store:** дозволити програми тільки з Mac App Store. Цей параметр гарантує найбільшу безпеку. Усі розробники програм, що доступні в Mac App Store, перевіряються Apple, і кожна програма оцінюється, перш ніж стає доступною. Система macOS перевіряє програму перед першим запуском, щоб пересвідчитися, що програму не було змінено після випуску від розробника. У разі виникнення будь-яких проблем Apple видаляє такі програми з Mac App Store.
 - b. **З App Store і від довірених розробників:** дозволити програми з Mac App Store і від довірених розробників. Ідентифіковані розробники реєструються компанією Apple і можуть за потреби закачувати свої програми в Apple для перевірки безпеки. У разі виникнення проблем з програмою Apple може відкликати її. Система macOS перевіряє програму перед першим запуском, щоб пересвідчитися, що її не було змінено після випуску від розробника.



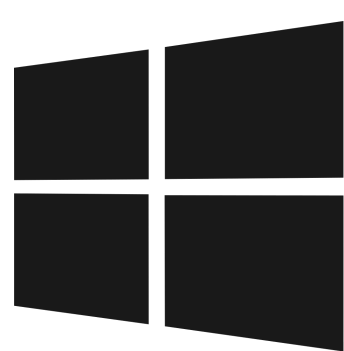


MacOS

Встановіть програму clean my mac. Вона видаляє шкідливе ПО з пристрою, зупиняє специфічні для macOS віруси, захищає від троянських коней, видобувачів даних та зламувачів браузера в режимі реального часу.

hello





Windows

Встановіть програму для захисту від зловмисних програм – антивірус

Інсталяція програми і підтримання її в актуальному стані може допомогти захистити комп'ютер від вірусів та інших зловмисних програм.

Не відкривайте повідомлення електронної пошти від незнайомих відправників

Або нерозпізнані вкладення електронної пошти – багато вірусів додаються до повідомлень електронної пошти та поширюються, щойно ви відкриєте вкладення. Не відкривайте жодні вкладення, якщо ви їх не очікуєте. [Детальніше ↗](#)

Використовуйте блокувальник спливних елементів у браузері

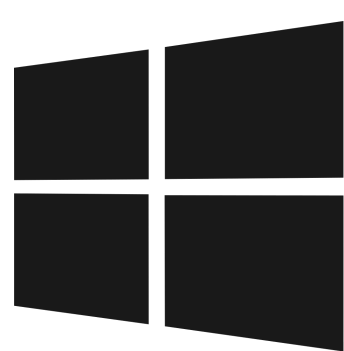
Спливні вікна – це невеликі вікна браузера, що відображаються поверх вебсайту, який ви переглядаєте. Хоча більшість із них створено рекламодавцями, вони можуть містити зловмисний або небезпечний код. Блокувальник спливних елементів може заблокувати відображення деяких або всіх спливних вікон. Блокувальник спливних параметрів у Microsoft Edge увімкнено за замовчуванням.

Зверніть увагу на Windows сповіщень SmartScreen

Будьте обережні із запуском нерозпізнаних програм, завантажених з інтернету. Є висока ймовірність того, що нерозпізнані програми є небезпечними. Коли ви завантажуєте та запускаєте програму з інтернету, фільтр SmartScreen використовує відомості про репутацію програми, щоб попередити вас, якщо програма не відома та може бути зловмисною. [Детальніше ↗](#)

Оновлюйте Windows

Періодично корпорація Майкрософт випускає спеціальні оновлення системи безпеки, які можуть допомогти захистити ваш комп'ютер. Ці оновлення допомагають захистити комп'ютер від вірусів та інших атак зловмисних програм, закриваючи можливі прогалини в системі безпеки. Windows Update допомагає переконатися, що ПК отримує ці оновлення автоматично, але, можливо, доведеться час від часу перезавантажувати комп'ютер, щоб оновлення повністю інсталювалися.



Windows

Використання параметрів конфіденційності браузера

Деякі вебсайти можуть намагатися використовувати ваші особисті відомості для цільової реклами, шахрайства та викрадення особистих даних. Усі сучасні браузери мають параметри конфіденційності, які дають змогу керувати відображенням і виконанням сайтів. [Детальніше ↗](#)

Переконайтеся, що службу захисту користувачів (UAC) увімкнено

Коли на ПК буде внесено зміни, для яких потрібен дозвіл на рівні адміністратора, служба захисту користувачів сповіщає вас про це та дає змогу їх затвердити. UAC може заборонити вірусам вносити небажані зміни. Щоб відкрити UAC, проведіть від правого краю екрана та торкніться кнопки «Пошук». (Якщо ви використовуєте мишу, наведіть її вказівник на правий верхній кут екрана, перемістіть його вниз і натисніть кнопку «Пошук»). У поле пошуку введіть uac, а потім виберіть пункт «Змінити параметри служби захисту користувачів».

Переконайтеся, що захист від підробок увімкнено

У Windows 10 та 11 у нас є функція «Захист від підробок», яка перешкоджає неавторизованим програмам змінювати налаштування безпеки. Багато вірусів і зловмисних програм намагаються вимкнути антивірусне програмне забезпечення або інші параметри безпеки, коли їх інстальовано, щоб уникнути виявлення вірусів. [Детальніше ↗](#)





Подивіться навчальний серіал «Основи кібергігієни» на порталі Дія.Цифрова освіта

Про що цей освітній серіал

Високий рівень комп'ютеризації вимагає дотримання певних правил поведінки для забезпечення себе та оточення від загроз в інформаційній сфері. Цей курс покликаний допомогти засвоїти базові принципи кібергігієни та типові алгоритми дій у разі виявлення ознак інформаційних атак. Протягом навчання ви дізнаєтеся за допомогою реальних прикладів, як не стати жертвами зловмисників. Участь у курсі рекомендується державним службовцям та посадовим особам органів місцевого самоврядування. Отримайте сертифікат, що засвідчує успішне проходження базового курсу з цифрової грамотності обсягом 0,33 кредиту ЄКТС.

Тисніть, щоб подивитися
серіал

