



# Посібник користувача з особистої безпеки



Методи і рішення

# Зміст

<b>Огляд</b>	<b>4</b>
Основні відомості з особистої безпеки	4
Нові можливості персональної безпеки	7
<b>Методи і рішення</b>	<b>8</b>
Посібник з відновлення безпеки	8
Посібник з підтримання безпеки	15
Перевірка безпеки	17
Контрольні списки для пристроїв з iOS 15 або попередніми версіями	34
<b>Обмеження доступу до облікового запису та пристрою</b>	<b>40</b>
Доступ до облікового запису Apple	40
Доступ до пристрою	48
Паролі, ключі допуску, коли допуску	63
<b>Керування інформацією про геопозицію</b>	<b>71</b>
Використання функції «Супровід» у Повідомленнях	71
Виявлення небажаних трекерів	75
Локатор і поширення геопозиції	81
Керування параметрами Служби локації	86
Керування автоматичним доступом до ОЧП на Картах	89
Керування метаданими геопозиції у Фотографіях	91
<b>Керування вмістом</b>	<b>94</b>
Загальні відомості	94
Окремі програми та функції	111

<b>Додаткова інформація</b>	<b>154</b>
Міркування безпеки	154
Інші допоміжні ресурси	155
<b>Авторське право</b>	<b>156</b>

# Огляд

## Основні відомості з особистої безпеки



Якщо ви хочете переглядати, обмежувати, припиняти або унеможливити доступ інших осіб до своїх пристроїв Apple, облікового запису чи особистої інформації, цей посібник може стати в пригоді.



*Примітка.* Цей ресурс стосується насамперед пристроїв Apple з найновішими версіями операційних систем (iOS 18, iPadOS 18 та macOS 15), однак може застосовуватися також і до Apple Watch і HomePod.

## Не знаєте напевне, що вам потрібно?


- [Посібник з відновлення безпеки](#) може допомогти знайти негайні рішення.
- [Посібник з підтримання безпеки](#) може допомогти з плануванням наперед.

## Шукаєте конкретне рішення?

- Перегляньте й налаштуйте інформацію, яку ви поширюєте (і для кого), за допомогою функції «Перевірка безпеки» або контрольних списків (дивіться нижче).
- Отримайте доступ до десятків статей із практичними інструкціями, використовуючи поле пошуку або зміст (у верхньому лівому куті кожної сторінки посібника), або скористайтеся нашими тематичними покажчиками, щоб отримати додаткові вказівки щодо пошуку.

## Перевірка безпеки

Перевірка безпеки — це простий спосіб, що дає змогу швидко переглянути й налаштувати інформацію, яку ви поширюєте для програм та інших людей — і все це можна зробити на вашому iPhone з iOS 16 або новішою версією. Щоб знайти свою версію iOS, перейдіть у меню: Параметри > Загальні > Про цей пристрій. Щодо оновлення дивіться розділ [Оновлення ПЗ Apple](#) далі в цьому посібнику.

Для доступу до функції «Перевірка безпеки» перейдіть на iPhone у Параметри  > Приватність і безпека > Перевірка безпеки.

Докладніше про функцію «Перевірка безпеки» (вимоги, вказівки, поширені запитання) дивіться в розділі [Перевірка безпеки](#) далі в цьому посібнику.

## Контрольні списки

Хоча для багатьох користувачів простіше використовувати Перевірку безпеки, компанія Apple також пропонує контрольні списки, наведені далі в цьому посібнику, за допомогою яких можна вручну переглянути й налаштувати інформацію, яку ви поширюєте.

- [Контрольний список 1. Обмеження доступу до пристрою та облікового запису](#)
- [Контрольний список 2. Керування інформацією про геопозицію](#)
- [Контрольний список 3. Керування вмістом](#)

## Автономна довідка

Якщо ви хочете згодом звертатися до цієї інформації в режимі офлайн, ви можете зробити це таким чином:

- Викачайте повну версію цього посібника у форматі PDF за допомогою посилання *Викачати цей посібник* (у нижньому лівому куті кожної сторінки посібника).
- Надрукуйте окремі сторінки: скористайтесь комбінацією клавіш ⌘-P або клацніть, утримуючи клавішу Control > Друкувати сторінку. Щоб зберегти гіперпосилання у викачаній копії, виберіть «Зберегти як PDF» у нижньому лівому куті меню PDF у вікні принтера.

## Інші проблеми

- [Служба підтримки Apple](https://support.apple.com/uk-ua) (https://support.apple.com/uk-ua). Отримайте доступ до рішень для всіх продуктів і служб Apple, включно з посібниками користувача, допомогою з відновленням забутого пароля тощо.
- [Інші допоміжні ресурси](#) (далі в цьому посібнику). Якщо ви відчуваєте, що ваша безпека під загрозою, ці додаткові ресурси можуть стати в пригоді.

Цей посібник регулярно поповнюється інформацією, яка допоможе почуватися в безпеці під час використання продуктів Apple. Дивіться розділ [Що нового](#) далі в цьому посібнику.

# Нові можливості персональної безпеки

## Перейменування Apple ID

Apple ID відтепер має назву «обліковий запис Apple». Це глобальна зміна, що стосується всіх служб Apple.

## Оновлення Посібника користувача з особистої безпеки

Компанія Apple суттєво переробила вміст цього посібника; зокрема, внесено зазначені нижче зміни.

### Новий вміст

- [Посібник з відновлення безпеки](#): практичні методи, що враховують контекст і призначені для користувачів, яким потрібно вирішити поточну проблему, зокрема невідкладні заходи й альтернативні зручні способи пошуку статей з відповідних питань.
- [Посібник з підтримання безпеки](#): практичні методи, що враховують контекст і призначені для користувачів, які хочуть запобігти виникненню проблем у майбутньому.
- Розділ [Параметри сторонніх програм](#) допомагає користувачам зрозуміти, які додаткові кроки потрібні для роботи з програмами, розробником яких не є компанія Apple.
- Розділ [Міркування безпеки](#) спонукає користувачів заздалегідь обміркувати потенційні наслідки внесення змін.

### Покращення

- Оновлено [початкову](#) сторінку та зміст, щоб надати пріоритет шляхам до рішень.
- На переробленій сторінці [Перевірка безпеки](#) об'єднано й замінено розділи «Як функція "Перевірка безпеки" на iPhone працює задля вашої безпеки» й «Використання функції "Перевірка безпеки" на iPhone для припинення поширення інформації та захисту вашого облікового запису».
- Контрольні списки тепер містять додаткові кроки, більше посилань на докладну інформацію, яка допоможе користувачам персоналізувати налаштування, а також нові назви, які включають номери контрольних списків (1, 2, 3) для більшої зручності розпізнавання, пошуку та переходів за посиланнями.
- Розділ «Додаткові застереження щодо використання функції "Перевірка безпеки"» перейменовано на [Додаткові заходи безпеки](#), щоб відобразити його актуальність для всіх користувачів.

# Методи і рішення

## Посібник з відновлення безпеки


Якщо вас або ваших знайомих турбує можливість стати жертвою знуцання або цькування за допомогою технологій на виробі, пов'язаному з Apple, або існує потреба розірвати цифрові зв'язки з кимось, наведені нижче методи можуть стати в пригоді. Щоб зв'язатися з правозахисною організацією, яка надає підтримку у зв'язку зі знуцанням, домашнім насильством, переслідуванням або іншими проблемами, відвідайте [вебсторінку Here to Help](https://learn.appleservices.apple/here-to-help) (<https://learn.appleservices.apple/here-to-help>).

Якщо вас цікавлять превентивні заходи, яких можна вжити для захисту від проблем, пов'язаних з технологіями, перегляньте [Посібник з підтримання безпеки](#) далі в цьому посібнику.

## Методи забезпечення безпеки

Скористайтеся переліченими нижче кроками, щоб керувати спільним доступом до ваших даних, а також захистити свої пристрої та облікові записи.

### Крок 1. Безпека передусім

 **ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на вашу безпеку](#).

Ви можете викачати чи надрукувати цей Посібник з відновлення безпеки; для цього клацніть, утримуючи клавішу Control, і виберіть «Зберегти сторінку як» або «Друкувати сторінку».

### Крок 2. Оновлення ПЗ Apple

Щоб захистити свій пристрій, переконайтеся, що на всіх ваших пристроях Apple інстальовано найновішу версію операційної системи з останніми оновленнями системи безпеки та приватності. Інструкції дивіться в розділі [Оновлення ПЗ Apple](#).

*Примітка.* Виконання оновлень може зайняти певний час і потребувати живлення пристрою. Якщо у вас невідкладна чи екстрена ситуація, може бути доцільно перейти до наступного кроку.



### Крок 3. Скористайтеся інструкціями щодо рішень

Більшість проблем з особистою безпекою, пов'язаних з технологіями, стосуються поширення та доступу. Для отримання інструкцій для вирішення цих проблем, скористайтеся будь-яким із таких способів:

- *Перевірка безпеки.* Це найшвидший і найпростіший спосіб перегляду параметрів поширення й керування ними безпосередньо з iPhone. Інструкції дивіться в розділі [Перевірка безпеки](#) далі в цьому посібнику.

Для доступу використовуйте iPhone з iOS 16 або новішою версією. Перейдіть у Параметри > Приватність і безпека > Перевірка безпеки. (Може знадобитися прокрутити вниз.)

- *Контрольні списки.* Щодо iOS 15 і попередніх версій або інших пристроїв Apple дивіться далі в цьому посібнику:
  - [Обмеження доступу](#)
  - [Припинення спільного доступу](#)
  - [Керування геопозицією](#)

### Крок 4. Подальші дії

Деякі дані не можна перевірити чи змінити за допомогою інструкцій щодо рішень. Розгляньте ці важливі [додаткові кроки](#).

Цей посібник містить десятки статей про особисту безпеку, що стосуються пристроїв, функцій і параметрів. Якщо вам потрібна довідка щодо конкретної функції чи проблеми, використовуйте такі засоби:

- поле пошуку (угорі ліворуч);
- зміст цього посібника (угорі ліворуч);
- тематичний покажчик (унизу).

## Невідкладні заходи

🚩 **ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку](#) та приватність.

### Швидка допомога

- Швидке припинення всіх каналів поширення за допомогою функції [Екстрене скидання](#)
- [Екстрені виклики й текстові повідомлення на iPhone і Apple Watch](#)
- [Блокування викликів і повідомлень від певних осіб](#)
- [Відхилення невідомих спроб входу](#)
- [Отримання застережень щодо неприйнятних зображень і відео](#)
- [Надійне керування домашніми приладами](#)
- [Керування відбитками пальців для Touch ID](#)

### Збір доказів

- [Записування підозрілої активності](#)
- [Отримання доказів, пов'язаних з іншим обліковим записом Apple](#)

### Відновлення заводських параметрів пристрою

Якщо ви хочете стерти всі дані й параметри, включно усіма програмами, установленими без вашого відома, і скинути параметри приватності, щоб не поширювати геопозицію для жодних людей або програм, дивіться розділ [Відновлення заводських параметрів пристрою](#).

### Режим карантину

Якщо ви вважаєте, що могли стати мішенню складної кібератаки, наприклад з боку приватної компанії, яка розробляє шпигунське програмне забезпечення за сприяння держави, дивіться розділ [Посилення захисту пристроїв за допомогою режиму карантину](#).

## Допомога в конкретних ситуаціях

Рекомендовано почати з кроків 1–4 вище, але також можна скористатися розділами нижче, щоб швидко знайти статті, які можуть стати в пригоді у вашій ситуації.

### Іншій особі завжди відоме моє розташування

Це може бути пов'язано з тим, що хтось користується спільним доступом до вашого облікового запису Apple, групи сімейного доступу, геопозиції чи вмісту (як-от спільні календарі або фотографії, опубліковані в соціальних мережах чи спільних календарях).

Почніть із кроків 1–4 вище. Якщо ви використовуєте контрольні списки на кроці 3, почніть з [Обмеження доступу](#) та [Керування геопозицією](#).

### Мені не вдається отримати доступ до свого облікового запису Apple

Щоб відновити доступ до свого облікового запису Apple, ознайомтеся з такими статтями служби підтримки Apple:

- [Якщо ви вважаєте, що безпеку вашого облікового запису Apple порушено](#)
- [Якщо ваш обліковий запис Apple заблокований, неактивний або вимкнений](#)
- [Якщо ви забули пароль облікового запису Apple](#)
- [Як відновити обліковий запис, якщо не вдається скинути пароль облікового запису Apple](#)

Після відновлення доступу може бути доцільно вжити таких заходів:

- [Зміна облікового запису Apple — Стаття служби підтримки Apple](#)
- [Захист паролів для пристроїв, програм і вебсайтів](#)
- [Запобігання втраті доступу до облікового запису Apple і пристрою](#)
- [Превентивні заходи для захисту від потенційних проблем: Посібник з підтримання безпеки](#)

### Хтось замкнув мій пристрій, і я не можу його відімкнути

Щоб відновити доступ, дивіться статтю служби підтримки Apple [Якщо ви забули код допуску iPhone, скиньте його за допомогою Mac або пристрою Windows](#).

Після відновлення доступу може бути доцільно вжити таких заходів, щоб захистити пристрій на майбутнє:

- [Контрольний список 1. Обмеження доступу до пристрою та облікового запису](#)
- [Установлення унікального коду допуску пристрою або пароля](#)
- Використання [Touch ID](#) для захисту ваших пристроїв або видалення невідомих відбитків пальців
- [Захист пристроїв за допомогою Face ID \(iPhone або iPad\)](#)
- [Додавання контакту для відновлення облікового запису](#)
- Вжиття застережних заходів за допомогою [Посібника з підтримання безпеки](#).

## Я хочу втекти або розглядаю можливість розірвати стосунки, у яких не почуваюся в безпеці

Щоб зв'язатися з правозахисною організацією, яка надає жертвам підтримку у зв'язку зі знуцанням, домашнім насильством, переслідуванням або іншими проблемами, відвідайте [вебсторінку Here to Help](https://learn.apple.services.apple/here-to-help) (https://learn.apple.services.apple/here-to-help).

1. Скористайтеся інструкціями щодо рішень (вище), щоб переглянути параметри доступу й поширення, і внесіть зміни, якщо це безпечно для вас.
2. Щоб дізнатися більше про блокування, збір доказів тощо, перегляньте ці [невідкладні заходи](#).
3. Розгляньте ці [додаткові заходи безпеки](#), що включають оповістки про небажане відстеження, облікові записи, не пов'язані з Apple, стільникові тарифні плани тощо.

## Мені потрібно захистити іншу людину

### Доступ до ваших пристроїв

Перегляньте розділ: Контрольний список 1. [Обмеження доступу до пристрою та облікового запису](#).

Також розгляньте:

- [Установлення унікального коду допуску або пароля](#)
- [Заходи для запобігання втраті доступу до пристрою](#)
- [Використання режиму карантину](#)

Щоб переглянути інші статті про захист ваших пристроїв і облікових записів, дивіться зміст (у верхньому лівому куті) в розділі «Обмеження доступу до облікового запису та пристрою — статті».

### Ваша геопозиція

Перегляньте розділ: Контрольний список 2. [Керування інформацією про геопозицію](#).

Також розгляньте:

- [Забезпечення приватності історії перегляду в Safari і на Картах](#)

### Ваш вміст

Перегляньте розділ: Контрольний список 3. [Керування вмістом](#).

Також розгляньте:

- [Безпечне керування переспрямуванням вмісту — пошта, текстові повідомлення й виклики](#)
- [Попередження про неприйнятні фото й відео](#)
- [Керування параметрами спільного доступу до Фотографій](#)
- [Керування метаданими геопозиції у Фотографіях](#)

## Ваші програми та браузер

- [Безпека паролів](#)
- [Спільні паролі та ключі допуску](#)
- [Функції приватності програм](#)
- [Перегляд і видалення програм](#)
- [Параметри сторонніх програм](#)
- [Приватність історії перегляду Safari](#)
- [Повідомлення](#)
  - [Параметри безпеки](#)
  - [Блокування викликів і повідомлень від певних осіб](#)
  - [Використання функції «Супровід»](#)
- [Фотографії](#)
  - [Керування параметрами спільного доступу до Фотографій](#)
  - [Керування метаданими геопозиції](#)

## Ваші родина і дім

- [Сімейний доступ](#)
- [Домашні прилади](#)

## Які пристрої у вас є?

### iPhone, iPad і Mac

Майже весь вміст посібника користувача з особистої безпеки стосується iPhone, iPad і Mac.

- Щоб переглянути, обмежити або припинити доступ інших осіб до ваших пристроїв, облікового запису чи особистої інформації, дивіться розділ [Методи забезпечення безпеки](#) вище в цьому посібнику.
- Якщо ви плануєте заздалегідь запобігти доступу інших осіб, дивіться [Посібник з підтримання безпеки](#).
- Додаткові способи взаємодії із широким спектром вмісту в цьому посібнику користувача дивіться в [огляді](#).

Для отримання відомостей з інших тем, що стосуються цих пристроїв, дивіться [посібник користувача iPhone](#), [посібник користувача iPad](#) або [посібник користувача Mac](#).

### Apple Watch

Для отримання інформації з особистої безпеки, що стосується Apple Watch, дивіться розділи:

- [Керування поширенням даних про активність на Apple Watch](#)
- [Використання Локатора для керування поширенням геопозиції](#)
- [Надсилання текстового повідомлення екстреним службам](#)
- [Безпечне використання NameDrop \(превентивне\)](#)
- [Використання функції «Супровід» у Повідомленнях \(превентивне\)](#)

Для отримання відомостей з інших тем дивіться [посібник користувача Apple Watch](#).

### Домашні прилади

Для отримання інформації з особистої безпеки, що стосується Дому, дивіться розділ [Надійне керування домашніми приладами](#).

Для отримання відомостей з інших тем дивіться [посібник користувача програми «Дім»](#).

### AirTag

Для отримання інформації з особистої безпеки, що стосується AirTag, дивіться розділ [Виявлення небажаних трекерів](#).

Для отримання відомостей з інших тем виконайте пошук на сайті [служби підтримки Apple](#) за терміном «AirTag».

Дата опублікування: 28 жовтня 2024 року

# Посібник з підтримання безпеки

Ця сторінка призначена для всіх, хто прагне вжити превентивних заходів для захисту від потенційних випадків жорстокого поводження, переслідування або знуцання за допомогою технологій. Якщо у вас виникла пов'язана проблема, дивіться [Посібник з відновлення безпеки](#) вище в цьому документі. Якщо вам потрібні інші типи допомоги з продуктами чи службами Apple, дивіться розділ [Інші допоміжні ресурси](#) вище в цьому документі.

## Методи перебування в безпеці

В Apple передбачено багато функцій для підтримки особистої безпеки та приватності. Нижче описано деякі способи їх використання.

### Рівень 1. Мінімальний захист

Щоб забезпечити мінімальний захист своїх пристроїв і облікового запису Apple, кожен повинен вжити цих заходів.

- Оновіть програмне забезпечення Apple на всіх своїх пристроях Apple, щоб використовувати останні оновлення системи безпеки та приватності. Дивіться розділ «Оновлення ПЗ Apple». Інструкції дивіться в розділі [Оновлення ПЗ Apple](#).
- Захист доступу до ваших пристроїв:
  - [Установлення унікального коду допуску або пароля.](#)
  - [Захист iPhone або iPad за допомогою Face ID](#)
  - [Керування відбитками пальців для Touch ID.](#)
  - [Керування спільними паролями і ключами допуску.](#)

Захист облікового запису Apple:

- [Забезпечення захисту облікового запису Apple.](#)
- [Використання двофакторної автентифікації.](#)
- [Налаштування контакту для відновлення облікового запису.](#)

### Рівень 2. Кращий захист

Додатково до рівня 1 варто розглянути ваші програми, захист пов'язаних з ними паролів і керування даними, які ви їм поширюєте для них.

- [Використовуйте сильніші паролі для пристроїв, програм і вебсайтів.](#)
- Перевірка певних параметрів поширення:
  - Використовуйте параметр [Керування поширенням і доступом](#) у функції «Перевірка безпеки» на iPhone з iOS 16 або новішою версією.
  - [Контрольний список 3. Керування вмістом](#) (на інших пристроях, а також в iOS 15 і попередніх версіях).
  - [Безпечне використання AirDrop.](#)
  - [Безпечне використання NameDrop.](#)
  - [Керування спільними групами вкладок у Safari](#)
  - [Керування параметрами «Поширено для вас»](#)

- Керування приватністю програм:
  - [Функції приватності програм.](#)
  - [Перегляд і видалення програм.](#)
  - [Параметри сторонніх програм](#)
  - [Safari та Карти: Забезпечення приватності історії перегляду.](#)

### Рівень 3. Найкращий захист

Додатково до рівнів 1 і 2 дізнайтеся про засоби Apple для особистої безпеки й постійно дбайте про безпеку, щоб гарантувати найкращий захист.

- Підготовчі заходи
  - [Увімкнення сповіщень щодо стеження](#)
  - [Реагування на шахрайські запити на спільний доступ до інформації.](#)
  - [Відхилення невідомих спроб входу.](#)
  - [Дізнайтеся, як блокувати певних осіб.](#)
  - [Повідомлення, AirDrop, FaceTime: Налаштування застережень щодо неприйняттого вмісту.](#)
  - [Розгляньте можливість використання функції «Супровід» у Повідомленнях, щоб автоматично сповіщати друга, коли ви прибуваєте додому.](#)
  - [Дізнайтеся, як зателефонувати чи надіслати текстове повідомлення екстреним службам \(iPhone або Apple Watch; залежить від країни чи регіону\).](#)
- Постійні заходи безпеки
  - Вживіть [додаткових заходів](#) для захисту своїх облікових записів, відмінних від Apple, сторонніх програми, паролів і соціальних мереж, а також Дому, Гаманця Apple і Сімейного доступу.
  - Регулярно використовуйте [Перевірку безпеки](#) на iPhone з iOS 16 або новішою версією, щоб керувати тим, що ви поширюєте.

Додаткові заходи

- [Керування відбитками пальців для Touch ID.](#)
- [Посилення захисту пристроїв за допомогою режиму карантину.](#)
- [Керування параметрами безпеки в Повідомленнях.](#)
- [Отримання доказів, пов'язаних з іншим обліковим записом Apple.](#)

Дата опублікування: 28 жовтня 2024 року





# Перевірка безпеки

## Перевірка безпеки для iPhone з iOS 16 або новішою версією



Функція «Перевірка безпеки», доступна в програмі «Параметри» на iPhone з iOS 16 або новішою версією, дає змогу швидко переглянути, оновити або припинити поширення вашої інформації для окремих людей і програм. Перевірка безпеки передбачає дві опції:

- Керування параметрами поширення й доступу для перевірки та внесення окремих змін.
- Використання функції «Екстрене скидання» для негайного припинення поширення всієї інформації.

Для доступу до функції «Перевірка безпеки» перейдіть на iPhone у Параметри  > Приватність і безпека > Перевірка безпеки.

 **ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку](#) та приватність.

### Вимоги

- Наявність iPhone з iOS 16 або новішою версією.
  - Щоб знайти свою версію iOS, перейдіть у Параметри  > Загальні > Про цей пристрій.
  - Для оновлення з iOS 15.8.3 або попередньої версії: Параметри  > Загальні > Оновлення ПЗ. Відомості про додаткові варіанти дивіться в розділі [Оновлення ПЗ Apple](#).
- Наявність облікового запису Apple з увімкненою двофакторною автентифікацією.
- Має також бути виконано вхід у Параметри > [Ваше ім'я] на iPhone.

*Примітка.* Якщо на вашому iPhone увімкнено функцію «Захист украденого пристрою», процедура Перевірки безпеки може дещо відрізнятись. Докладніше дивіться в статті служби підтримки Apple [Відомості про Захист украдених пристроїв для iPhone](#).

### Альтернативний варіант: контрольні списки

Якщо у вас інший пристрій (iPad, Mac) або виникли проблеми з використанням Перевірки безпеки, ви можете налаштувати поширення і доступ вручну за допомогою таких контрольних списків:

- [Контрольний список 1. Обмеження доступу до пристрою та облікового запису](#)
- [Контрольний список 2. Керування інформацією про геопозицію](#)
- [Контрольний список 3. Керування вмістом](#)

## Огляд

Функція «Перевірка безпеки» на iPhone дає змогу швидко припинити поширення вашої інформації, а також переглянути й оновити параметри поширення для окремих людей і програм. Ви можете виконати такі дії:

- Перевірити, для кого ви поширюєте інформацію
- Переглянути і змінити перелік пристроїв, під'єднаних до вашого облікового запису Apple
- Скинути системні дозволи приватності для програм
- Змінити код допуску iPhone
- Змінити пароль облікового запису Apple
- Внести додаткові зміни



## Міркування безпеки, які слід врахувати перед початком роботи

▼ **ВАЖЛИВО.** Плануйте свої дії з урахуванням заходів безпеки.

- Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку](#) та приватність.
- Функція «Швидкий вихід» дає вам змогу швидко захистити свою приватність. Торкніть «Швидкий вихід», щоб негайно відкрити програму «Параметри» й повернутися на початковий екран (у правому верхньому куті на всіх екранах Перевірки безпеки). Будь-які зміни, внесені до застосування швидкого виходу, збережуться.
- Щоб відновити поширення для іншої особи після використання Перевірки безпеки, просто відкрийте програму чи службу, з яких потрібно поширити інформацію, і знову поширте цей вміст. Деякі програми та служби сповіщають вас про відновлення поширення інформації.


За допомогою функції «Перевірка безпеки» можна переглянути, для кого ви поширюєте інформацію, обмежити використання Повідомлень і FaceTime лише своїм iPhone, скинути системні дозволи приватності для програм, змінити код допуску, змінити пароль свого облікового запису Apple та багато іншого.


Якщо ви хочете відновити поширення для іншої особи після використання Перевірки безпеки, відкрийте програму чи службу, з яких потрібно поширити інформацію, і знову поширте цей вміст.

Якщо ви увімкнули функцію «Захист украденого пристрою», засіб перевірки безпеки може працювати дещо інакше. Щоб дізнатися більше про функцію «Захист украденого пристрою», перегляньте статтю служби підтримки Apple [Відомості про Захист украдених пристроїв для iPhone](https://support.apple.com/uk-ua/120340) (<https://support.apple.com/uk-ua/120340>).

*Примітка.* Якщо на вашому iPhone діють обмеження Екранного часу або якщо встановлено профіль керування мобільним пристроєм (MDM), ви так само можете користуватися функцією «Перевірка безпеки», однак певні опції можуть бути недоступні.


### Що потрібно, щоб користуватися функцією «Перевірка безпеки»?

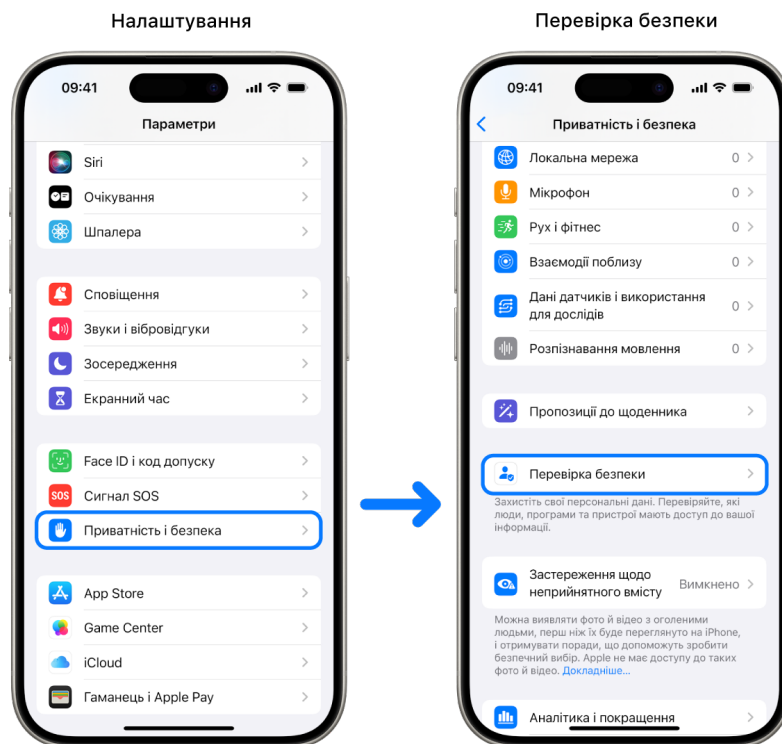
Функція «Перевірка безпеки» доступна лише на iPhone з iOS 16 або новішою версією. Для використання функції «Перевірка безпеки» вам потрібен обліковий запис Apple з увімкненою двофакторною автентифікацією. Ви повинні також виконати вхід у Параметри > [Ваше ім'я] на iPhone. (Щоб дізнатися версію програмного забезпечення, встановленого на вашому пристрої, перейдіть у Параметри  > Загальні, а потім торкніть «Про пристрій».)

Для доступу до функції «Перевірка безпеки» перейдіть у Параметри  > Приватність і безпека > Перевірка безпеки. (Може знадобитися прокрутити вниз.)

*Примітка.* Якщо у вас немає доступу до функції «Перевірка безпеки» або якщо вам складно користуватися нею, ви можете вручну відкоригувати параметри поширення й доступу до пристрою та облікових записів. Дивіться розділ [Контрольний список 3. Керування вмістом](#) далі в цьому посібнику.

## Крок 1. Відкрийте Перевірку безпеки

На iPhone перейдіть у Параметри  > Приватність і безпека > Перевірка безпеки.  
(Може знадобитися прокрутити вниз.)

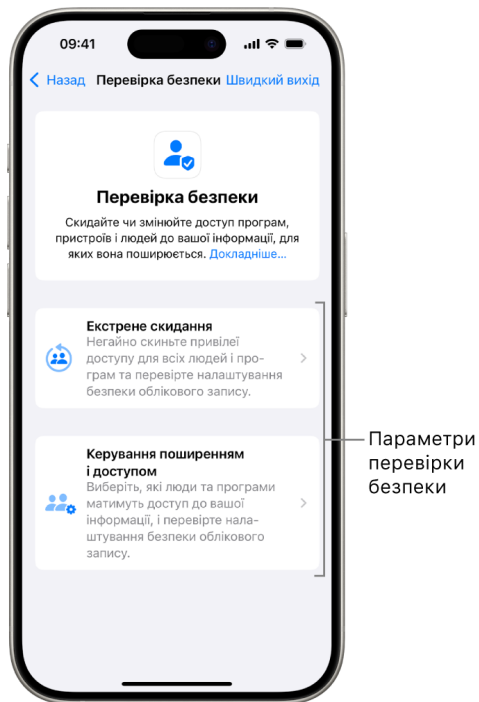


## Крок 2. Виберіть потрібний варіант

У функції «Перевірка безпеки» передбачено два способи керування поширенням, доступом і безпекою облікового запису:

- *Екстрене скидання.* Негайне й універсальне скидання поширення для всіх людей і програм.
- *Керування поширенням і доступом.* Перевірка й налаштування параметрів поширення і доступу для окремих людей і програм.

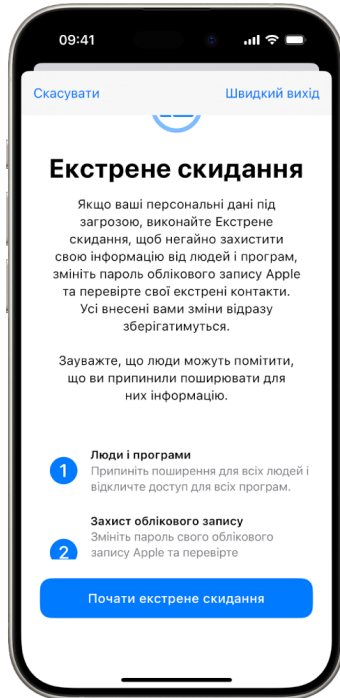
Докладніше про параметри, які можна змінити в Перевірці безпеки, дивіться в розділі [Запитання і відповіді щодо Перевірки безпеки](#) далі в цьому посібнику.



## Екстрене скидання

Використовуйте Екстрене скидання для таких завдань:

- Швидке припинення поширення для всіх людей і програм (докладніше дивіться в розділі «Запитання і відповіді щодо Перевірки безпеки»).
- Перегляд екстрених контактів.
- Перегляд пристроїв, під'єднаних до вашого облікового запису Apple.
- Перегляд номерів телефонів, які використовуються для перевірки вашої особи.
- Змінення пароля вашого облікового запису Apple й перегляд параметрів безпеки пристрою та облікового запису.



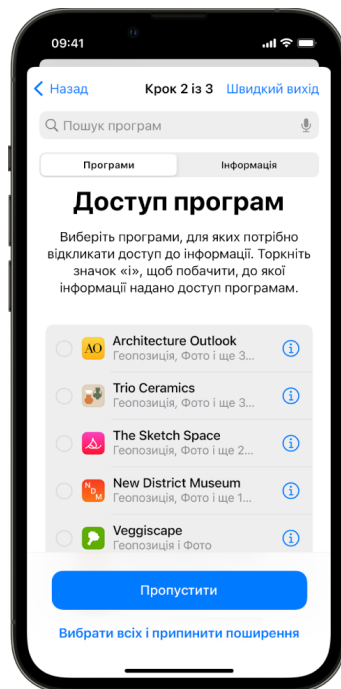
- Торкніть «Екстрене скидання», а потім виконайте екранні вказівки. Ваші зміни постійно зберігаються.

*Примітка.* Якщо ви ввімкнули функцію «Захист украденого пристрою», засіб перевірки безпеки може працювати дещо інакше. Щоб дізнатися більше про функцію «Захист украденого пристрою», перегляньте статтю служби підтримки Apple [Відомості про Захист украдених пристроїв для iPhone](https://support.apple.com/uk-ua/120340) (<https://support.apple.com/uk-ua/120340>).

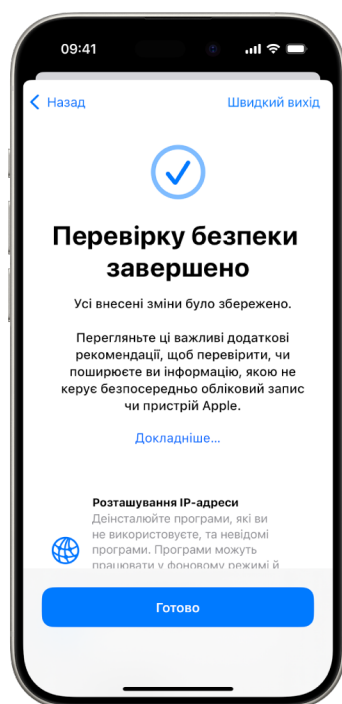
## Керування поширенням і доступом

Опція «Керування поширенням і доступом» дає змогу переглянути й налаштувати інформацію, яку ви поширюєте для інших людей, інформацію, до якої мають доступ програми, а також оновити параметри безпеки пристрою та облікового запису Apple. Виконайте ці п'ять кроків:

1. Торкніть «Керування поширенням і доступом». (Зміни зберігаються в міру того, як ви їх вносите.)
2. Щоб переглянути й припинити поширення інформації для інших людей, виконайте одну з таких дій:
  - Торкніть «Люди». Виберіть людей зі списку, перегляньте поширювану інформацію, а потім вирішіть, доступ до якої інформації потрібно припинити для вибраних людей.
  - Торкніть «Інформація». Виберіть програми зі списку, перегляньте поширювану інформацію, а потім вирішіть, доступ до якої інформації потрібно припинити для вибраних людей.
3. Щоб переглянути й припинити поширення інформації для інших програм, виконайте одну з таких дій:
  - Торкніть «Програми». Виберіть програми зі списку, перегляньте поширювану для них інформацію, а потім вирішіть, доступ до якої інформації потрібно припинити для вибраних програм.
  - Торкніть «Інформація». Виберіть поширювану інформацію зі списку, перегляньте поширювану для програм інформацію, а потім вирішіть, доступ до якої інформації потрібно припинити для вибраних програм.



4. Торкніть «Продовжити», а потім виконайте будь-які з таких дій:
  - Перегляньте перелік пристроїв, під'єднаних до вашого облікового запису Apple, і вилучіть непотрібні.
  - Перегляньте номери телефонів, які використовуються для підтвердження вашої особистості, і оновіть їх за потреби.
  - Оновіть пароль свого облікового запису Apple.
  - Додайте або оновіть свої екстрені контакти.
  - Оновіть код допуску пристрою або інформацію вашого Face ID чи Touch ID.
  - Перегляньте і вилучіть синхронізовані комп'ютери (лише iOS 17 і новіші версії).
  - Якщо у вас є підписка iCloud+, і ви ще не ввімкнули Приват-реле, це можна зробити зараз (лише iOS 17 і новіші версії).
5. Торкніть «Готово».



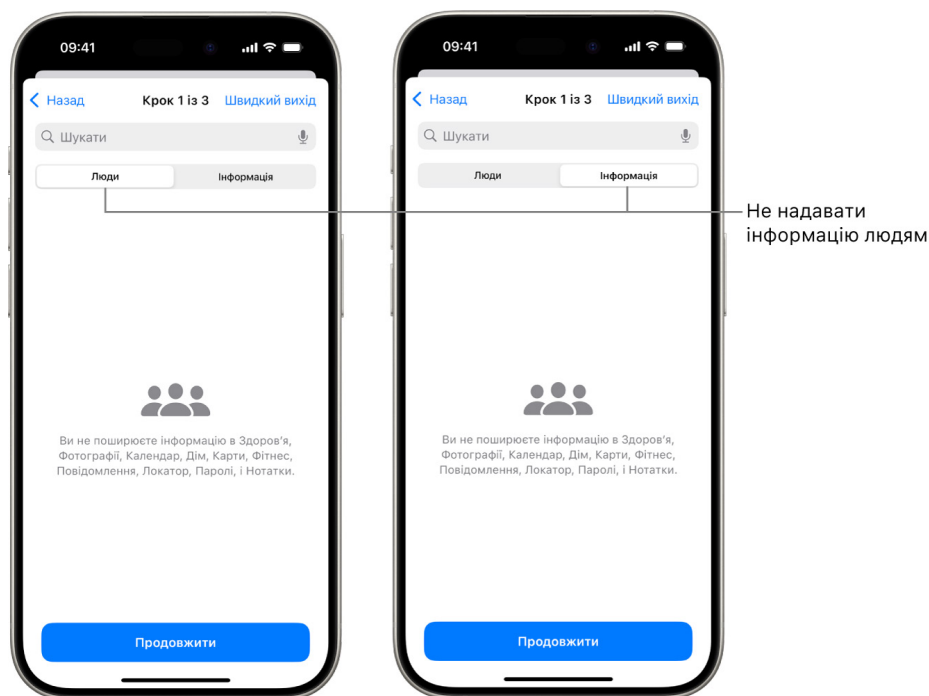
6. Завершивши, перейдіть до наступного завдання, щоб переконатися, що поширення зупинено.  
**▼ ВАЖЛИВО.** Перегляньте [додаткові заходи](#) далі в цьому посібнику, щоб ознайомитися з порадами щодо захисту приватної інформації, окрім Перевірки безпеки.



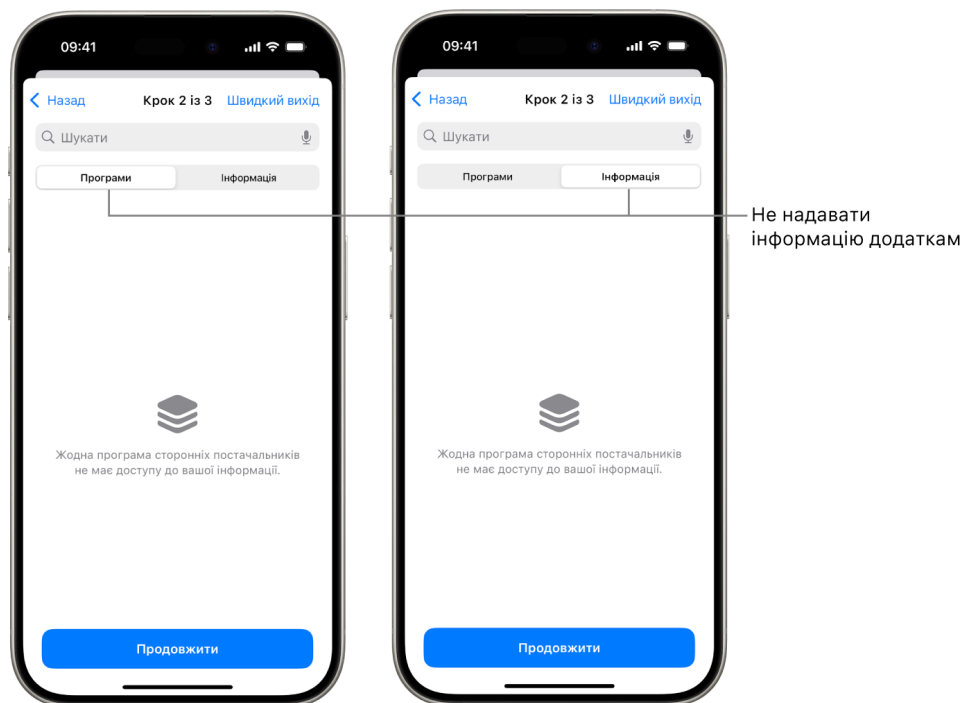
### Крок 3. Перевірте внесені вами зміни

Після використання функції «Перевірка безпеки» ви можете перевірити зміни, внесені вами до параметрів поширення за допомогою цих 4 кроків.

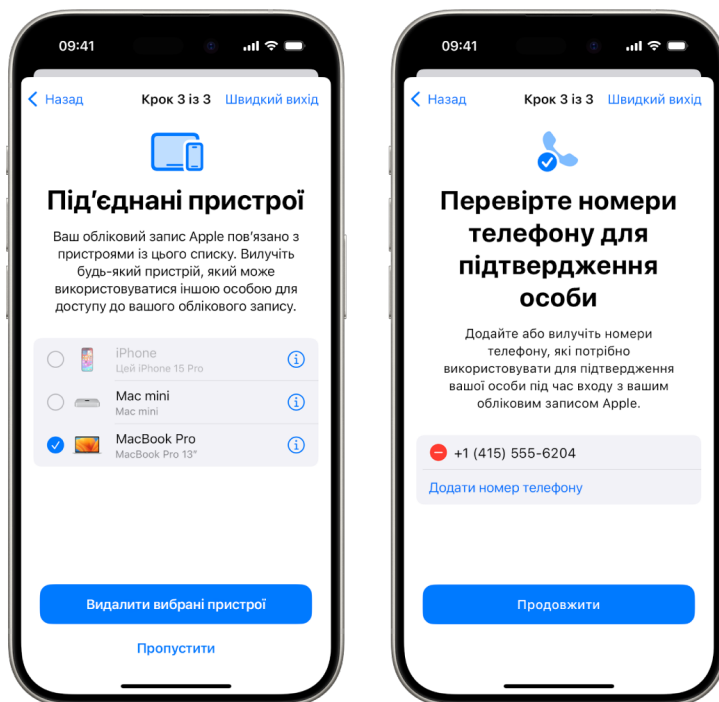
1. Торкніть кнопку «Назад» (ви також можете вийти й повторно відкрити Перевірку безпеки).
2. Перевірте, чи внесено потрібні зміни стосовно інформації, яку ви поширюєте для інших людей.



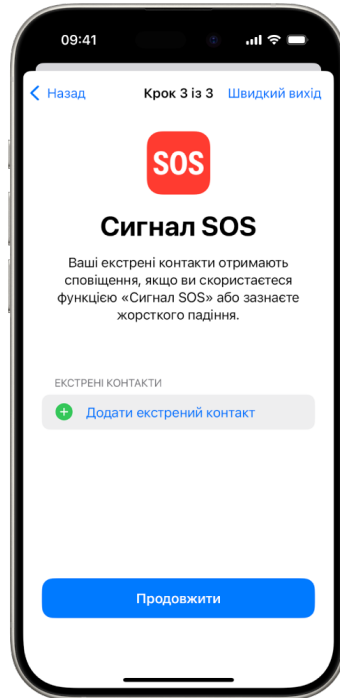
3. Перевірте, чи внесено потрібні зміни стосовно інформації, яку ви поширюєте для програм.



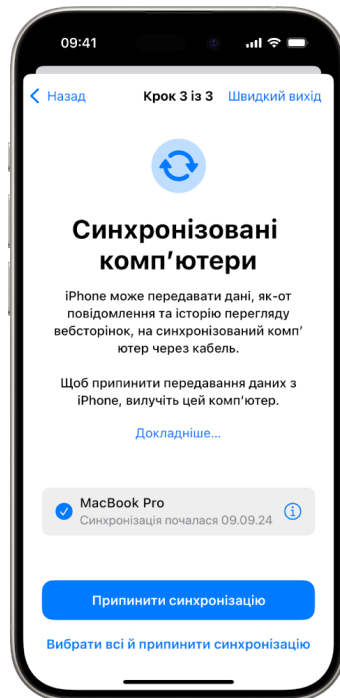
4. Перевірте всі зміни, внесені в обліковий запис, а саме:
- Пристрої, під'єднані до вашого облікового запису Apple.
  - Номери телефонів, які використовуються для перевірки вашої особи.



- Змінені або додані вами екстрені контакти.



- Вилучені вами синхронізовані комп'ютери.



## Відомості, на які не поширюється Перевірка безпеки












Деякі відомості не можна переглядати чи змінювати за допомогою функції «Перевірка безпеки», зокрема:

- облікові записи й паролі до них, не пов'язані з Apple;
- поширення в соціальних мережах;
- пристрої, на яких виконано вхід з використанням іншого облікового запису iCloud;
- iPad або Mac з параметрами поширення інформації, увімкненими для інших програм.

## Запитання і відповіді щодо Перевірки безпеки
















### Які програми та функції Apple можна переглядати й налаштовувати за допомогою Перевірки безпеки?

Функцію «Перевірка безпеки» можна використовувати для перегляду або припинення поширення інформації для інших людей з таких програм Apple:

Програма	Інформація, якою можна керувати
	Активність
	Дім
	Здоров'я
	Орієнтовний час прибуття на спільних картах
	Поширення геопозиції через Локатор
	Спільні календарі
	Спільні нотатки
	Спільні паролі
	Спільні речі в Локаторі
	Спільні фотографії (включно зі Спільною фототекою та спільними альбомами)
	Супровід

## Для яких сторонніх програм я можу переглядати й налаштовувати доступ за допомогою Перевірки безпеки?

За допомогою функції «Перевірка безпеки» можна вимкнути доступ сторонніх програм до перелічених нижче типів інформації.

	Bluetooth®
	Календарі
	Камера
	Контакти
	Файли та папки
	Здоров'я
	Локальна мережа
	Служби локації
	Медіа та Apple Music
	Мікрофон
	Рух і фітнес
	Фотографії
	Нагадування
	Дослідження
	Розпізнавання мовлення

## Які зміни можна внести до мого облікового запису Apple за допомогою функції «Перевірка безпеки»?

Функцію «Перевірка безпеки» можна використовувати для змінення інформації, пов'язаної з вашим обліковим записом Apple. Наприклад:

- Перегляд і вилучення пристроїв, на яких виконано вхід у ваш обліковий запис.
- Перегляд і оновлення довірених номерів телефонів.
- Змінення пароля облікового запису Apple.
- Оновлення екстрених контактів.
- Оновлення коду допуску пристрою та інформації щодо вашого Face ID чи Touch ID.

Якщо ви ввімкнули функцію «Захист украденого пристрою», засіб перевірки безпеки може працювати дещо інакше. Щоб дізнатися більше про функцію «Захист украденого пристрою», перегляньте статтю служби підтримки Apple [Відомості про Захист украдених пристроїв для iPhone](https://support.apple.com/uk-ua/120340) (<https://support.apple.com/uk-ua/120340>).

## Для чого призначена кнопка «Швидкий вихід»?


Особам, які зазнають жорстокого поводження, може бути потрібно швидко приховати, що вони використовують функцію «Перевірка безпеки». Це можна зробити за допомогою кнопки «Швидкий вихід».

## Додаткові заходи безпеки

Більшість проблем з особистою безпекою стосуються поширення та доступу. Для отримання інструкцій для вирішення цих проблем, скористайтеся будь-яким з таких способів:

- *Перевірка безпеки.* На iPhone з iOS 16 або новішою версією перейдіть у Параметри  > Приватність і безпека > Перевірка безпеки або перегляньте розділ [Перевірка безпеки](#).
- *Контрольні списки.* Для попередніх версій iOS або інших пристроїв дивіться такі контрольні списки: [Обмеження доступу](#), [Припинення поширення](#) або [Керування геопозицією](#).

Деякі дані не можна переглянути чи змінити за допомогою Перевірки безпеки або контрольних списків. Щоб далі обмежити поширення, можна вжити таких додаткових заходів:

 **ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку](#) та приватність.

## Заходи, не пов'язані з Apple

### Програми, не розроблені Apple

Програми, інстальовані на пристрій, можуть збирати інформацію про ваше загальне розташування. З урахуванням [потенційного впливу на безпеку та приватність](#) може бути доцільно переглянути інстальовані програми й видалити ті, які ви не використовуєте або не пам'ятаєте. Дивіться розділи [Перегляд і видалення програм](#) й [Параметри сторонніх програм](#).

### Облікові записи й паролі до них, не пов'язані з Apple

Захист конфіденційної особистої інформації в облікових записах у таких сферах, як банки, магазини, е-пошта, соціальні мережі, освіта:

- Змінення паролів облікових записів.
- Перегляд параметрів безпеки та приватності.
- Перегляд облікових записів зв'язку (е-пошта, телефон, обмін повідомленнями) для того, щоб гарантувати, що жодні відомості не пересилаються без вашого дозволу.

## Соціальні мережі, магазини й інші облікові записи

Публікування фотографій та іншої особистої інформації в соціальних мережах, магазинах чи на інших вебсайтах, може відкрити подробиці про ваше розташування й особисте життя. Обов'язково вживайте таких заходів:

- Перевірка параметрів приватності й безпеки в соціальних мережах, магазинах чи інших облікових записах в інтернеті
- Перевірка списків своїх контактів і читачів
- Уважне ставлення до вибору вмісту для публікації для забезпечення необхідного рівня приватності
- Керування метаданими геопозиції у Фотографіях

Дивіться розділ «[Керування метаданими геопозиції у Фотографіях](#)» далі в цьому посібнику.

## Інші пристрої, якими ви володієте чи користуєтеся

Перегляньте параметри поширення й доступу для інших пристроїв, якими ви користуєтеся, щоб захистити свою інформацію. Дивіться контрольний список [Обмеження доступу до пристрою і облікового запису](#). Якщо поруч із вами є ще хтось, як-от дитина чи друг, майте на увазі, що їхні пристрої також можуть поширювати інформацію.

## Стільниковий тарифний план

Якщо ви користуєтеся спільним стільниковим тарифним планом, інші члени плану можуть отримувати доступ до інформації про ваше розташування, виклики та обмін повідомленнями й відомості про виставлені рахунки. Зверніться до свого оператора, щоб дізнатися більше про свій тарифний план і додаткові заходи безпеки, які можна застосувати до вашого облікового запису, як-от PIN-код для доступу або введення коду безпеки перед внесенням змін.

Якщо у вас немає спільного тарифного плану, але хтось має онлайн-доступ до вашого облікового запису, ці особи можуть дізнатися ваше розташування, отримати інформацію про виклики та обмін повідомленнями або відомості про платежі. З урахуванням [потенційного впливу на безпеку та приватність](#) може бути доцільно оновити паролі, PIN-коди й інші функції безпеки, пов'язані з вашим стільниковим тарифним планом.



## Кроки, пов'язані з Apple

### Небажане відстеження

Може бути доцільно увімкнути сповіщення для виявлення небажаних пристроїв відстеження (як-от AirTag або інших приладів мережі Локатора). Щоб отримувати оповістки про те, що вони переміщуються з вами, увімкніть такі функції:

- Bluetooth
- Служби локації
- Сповіщення відстеження (відкрийте програму «Локатор», торкніть «Я», прокрутіть до пункту «Налаштувати сповіщення відстеження», а потім увімкніть «Дозволити сповіщення»)

Дивіться розділ [«Виявлення небажаних пристроїв відстеження»](#) далі в цьому посібнику.

### Дім і HomeKit

Якщо ви належите до дому Apple і хочете вилучити себе, пам'ятайте, що особа, яка керує домом, може й далі використовувати прилади HomeKit, як-от камери, що може мати вплив на вашу особисту безпеку.

Перегляньте розділ [«Надійне керування домашніми приладами»](#) далі в цьому посібнику.

### Гаманець Apple


Якщо ви надаєте комусь спільний доступ до карток чи ключів доступу в Гаманці Apple, ця особа може переглядати вашу історію покупок чи бачити, коли ви відмикаєте двері.

Деталі фінансових трансакцій можна також переглянути через спільні банківські рахунки та спільні кредитні картки або в разі онлайн-доступу до ваших фінансових рахунків. Щоб переглянути недавні трансакції та журнали, відкрийте Гаманець Apple. З урахуванням [потенційного впливу на безпеку та приватність](#) може бути доцільно оновити паролі, пов'язані з вашими банківськими рахунками та кредитними картками.

### Сімейний доступ

Якщо ви належите до групи Сімейного доступу Apple, організатор групи Сімейного доступу зможе побачити ваші покупки та вносити зміни до параметрів пристрою дитини. Щоб полишити сімейну групу, перейдіть у меню «Параметри», торкніть своє ім'я та відкрийте параметри сімейного доступу. Хоча ви не можете вилучити обліковий запис дитини з групи Сімейного доступу, ви можете перемістити його до іншої групи або просто видалити обліковий запис Apple дитини.

Перегляньте розділ [«Керування параметрами Сімейного доступу»](#) далі в цьому посібнику.

*Примітка.* Щоб перевірити, чи належите ви до групи Сімейного доступу, перейдіть у Параметри  > [ваше ім'я] > вкладка «Сімейний доступ». Якщо ви бачите імена членів родини, це означає, що ви належите до групи Сімейного доступу.

# Контрольні списки для пристроїв з iOS 15 або попередніми версіями

## Контрольний список 1. Обмеження доступу до пристрою та облікового запису


Безпечний доступ до ваших пристроїв і облікового запису Apple є критично важливим для особистої безпеки, пов'язаної з технологіями. У цьому контрольному списку пропонуються відповідні шляхи, які можна переглянути й оновити, щоб доступ до ваших пристроїв обмежувався лише тими, кому ви хочете це дозволити.

▼ **ВАЖЛИВО.** Якщо у вас iPhone з iOS 16 або новішою версією, ви можете скористатися функцією [Перевірка безпеки](#).

▼ **ВАЖЛИВО.** Якщо у вас iPhone з iOS 16 або новішою версією, ви можете скористатися функцією [Перевірка безпеки](#), описаною вище в цьому посібнику.



## Обмеження доступу до ваших пристроїв

1. Перевірте, на яких пристроях здійснено вхід у ваш обліковий запис Apple, перейшовши в Параметри  > [ваше ім'я] > Пристрої. Щоб вилучити незнайомий пристрій, торкніть його назву й виберіть «Вилучити з облікового запису». Докладніше дивіться в розділі [Безпека облікового запису Apple](#) далі в цьому посібнику.
2. Перевірте пристрій на наявність неочікуваного вигляду [Face ID](#) чи [відбитка пальця Touch ID](#). Дивіться інформацію про Face ID й Touch ID далі в цьому посібнику.
3. Перевірте особисту й безпекову інформацію у вашому обліковому записі Apple, увійшовши на [вебсайт облікового запису Apple](#). Докладніше дивіться в розділі [Безпека облікового запису Apple](#) далі в цьому посібнику.
4. Якщо ви використовуєте [двофакторну автентифікацію](#), перевірте список довірених пристроїв на наявність незнайомих. Дивіться відомості про двофакторну автентифікацію далі в цьому посібнику.
5. Перевірте список програм, установлених на вашому пристрої, на наявність тих, які ви не впізнаєте або не пам'ятаєте, що ви їх установлювали. Інструкції дивіться в розділі [Перегляд і видалення програм](#) далі в цьому посібнику.
6. Перевірте, чи немає незнайомого профілю керування мобільними пристроями (MDM) або конфігураційного профілю. Профілі MDM зазвичай установлюються роботодавцями, навчальними закладами або іншими офіційними організаціями. Інструкції дивіться в розділі [Перегляд і видалення профілів конфігурації](#) далі в цьому посібнику.
7. Перегляньте і налаштуйте інформацію, яку ви поширюєте, використовуючи розділ [Контрольний список 3. Керування вмістом](#) далі в цьому посібнику.


## Контрольний список 2. Керування інформацією про геопозицію




Якщо у вас iPhone з iOS 15 або попередньою версією, скористайтеся цим контрольним списком, щоб обмежити коло тих, хто може бачити вашу геопозицію, або взагалі припинити поширення своєї геопозиції. Якщо у вас iPhone з iOS 16 або новішою версією, дивіться розділ [Перевірка безпеки](#).

1. Якщо у вас немає найновішої версії iOS, iPadOS або macOS і вас турбує, що хтось міг мати фізичний доступ до вашого пристрою, ви можете відновити його заводські параметри. Під час відновлення заводських параметрів буде стерто всю інформацію та параметри на вашому пристрої. Це включає видалення всіх програм, які було встановлено без вашого відома, і скидання параметрів приватності, щоб ви не поширювали геопозицію для жодних людей або програм. Під час відновлення заводських параметрів також буде встановлено найновішу версію операційної системи. Відомості про відновлення заводських параметрів дивіться в розділі [Відновлення заводських параметрів пристрою](#).
2. Щоб не поширювати свою геопозицію для жодних програм і служб навіть протягом короткого часу, перейдіть у Параметри  > Приватність > Служби локації та вимкніть поширення геопозиції. Після цього жодні програми на вашому пристрої, навіть «Карти», не зможуть використовувати вашу геопозицію. Ніхто не отримає сповіщення, якщо ви вимкнете Служби локації, але деякі функції можуть не працювати належним чином без доступу до вашої геопозиції.

*Примітка.* Окрім того, можна тимчасово вимкнути «Локатор» iPhone на тій самій вкладці, якщо ви вважаєте, що інша особа може мати доступ до вашого облікового запису iCloud. У списку програм, які використовують «Служби локації», торкніть «Локатор», а потім виберіть «Ніколи».

3. Щоб припинити поширення геопозиції для певних програм і служб, перейдіть у Параметри  > Приватність > Служби локації, а потім виберіть програми та служби, для яких потрібно припинити поширення. Торкніть назву програми, а потім у розділі «Дозволити доступ до геопозиції» виберіть «Ніколи».
4. Щоб зупинити поширення геопозиції для певної людини, відкрийте програму «Локатор» , торкніть пункт «Люди», виберіть людину, а потім торкніть пункт «Сховати мою геопозицію» внизу екрана.




Якщо ви почали, а пізніше припинили поширювати свою геопозицію в програмі «Локатор», ця особа не отримає сповіщення й не побачить вас у своєму списку друзів. Якщо ви знову ввімкнете спільний доступ, такі користувачі отримають сповіщення про те, що ви почали ділитися з ними своєю геопозицією.
5. Щоб зупинити поширення орієнтовного часу прибуття (ОЧП) на картах, відкрийте програму «Карты», виберіть «Улюблені», щоб відкрити вікно з усіма своїми улюбленими місцями. Торкніть  поряд із кожним місцем, для якого потрібно переглянути параметри поширення ОЧП, а потім прокрутіть униз до розділу «Поширення ОЧП» та вилучіть людину, для якої потрібно припинити поширення.
6. Щоб перевірити доступність пристроїв і приладів у Локаторі для людей, що мають доступ до вашого облікового запису Apple, перейдіть у Локатор, торкніть «Пристрої» та перегляньте список. Якщо ви помітили незнайомий пристрій і хочете вилучити його, торкніть його, а потім — «Вилучити цей пристрій».

*Примітка.* Якщо належите до групи Сімейного доступу, учасників вашої групи спільного доступу, які дозволили вам бачити геопозиції своїх пристроїв, буде перелічено з розділенням за іменем власника.
7. Коли фотографії та відео з метаданими геопозиції поширюються, люди з доступом до цих відомостей можуть отримати доступ до метаданих і дізнатися, де було зроблено зйомку. Якщо вас турбує те, що хтось має доступ до метаданих геопозиції для ваших фото чи відео, ви [можете вилучити поточні метадані](#) та припинити їх збір у майбутньому.

## Контрольний список 3. Керування вмістом

Якщо у вас iPhone з iOS 15 або попередньою версією, скористайтеся цим контрольним списком, щоб припинити спільний доступ для людини, якій ви раніше його надавали. Якщо у вас iPhone з iOS 16 або новішою версією, дивіться розділ [«Перевірка безпеки для iPhone з iOS 16 або новішою версією»](#) вище в цьому посібнику.



1. Перевірте, чи належите до групи Сімейного доступу, перейшовши в Параметри  > [ваше ім'я] та знайшовши вкладку «Сімейний доступ». Якщо ви належите до групи Сімейного доступу, відображаються імена членів родини.
2. Якщо ви належите до групи Сімейного доступу й більше не хочете ділитися інформацією, ви можете вилучити себе (якщо вам уже виповнилося 13 років). Якщо саме ви налаштували групу Сімейного доступу (під вашим іменем з'являється слово *Організатор*), ви можете вилучити із неї будь-кого, кому виповнилося 13 років.
3. У програмі «Локатор»  виберіть вкладку «Люди», щоб побачити, з ким ви ділитеся своєю геопозицією. Щоб припинити передавання даних певному користувачу, виберіть його й клацніть «Сховати мою геопозицію». Щоб припинити передавання даних усім, торкніть «Я», а потім вимкніть опцію «Поширювати мою геопозицію».
4. У програмі «Фотографії»  торкніть «Альбоми», після чого перейдіть до розділу «Спільні альбоми». Виберіть спільний альбом і натисніть вкладку «Люди», щоб побачити власника спільного альбому й людей, які мають спільний доступ до нього.
  - Якщо ви є власником альбому й хочете припинити його поширення, торкніть ім'я підписника, для якого потрібно припинити поширення, після чого виберіть відповідний варіант.
  - Якщо ви є підписником, можете торкнути «Відписатися» внизу екрана. Ви також можете видалити будь-які фотографії, до яких надали спільний доступ.

5. У програмі «Календар»  торкніть «Календарі». Виберіть спільний календар і торкніть , щоб побачити, хто має спільний доступ до календаря.
  - Якщо ви власник календаря й хочете припинити надавати спільний доступ до нього, торкніть ім'я підписника, для якого потрібно скасувати спільний доступ, після чого виберіть відповідний варіант.
  - Якщо ви є підписник, можете торкнути «Видалити календар» внизу екрана.
6. Якщо у вас є Apple Watch і ви поширили свої кільця активності для когось, ви можете припинити поширення. На iPhone перейдіть до програми «Активність» , а потім торкніть «Поширення». Виберіть користувача, якому ви надали спільний доступ, торкніть його ім'я, після чого торкніть «Вилучити друга» або «Сховати мою активність».
7. Ви також можете ділитися інформацією з іншими людьми за допомогою сторонніх програм. Перевірте програми, які ви встановили на своєму пристрої, щоб з'ясувати, чи надає будь-яка з них спільний доступ до інформації. Дивіться розділ [Керування параметрами спільного доступу до Фотографій](#)

# Обмеження доступу до облікового запису та пристрою

## Доступ до облікового запису Apple

### Безпека облікового запису Apple

Ваш обліковий запис Apple — це особистий обліковий запис, який ви використовуєте для входу на свої пристрої та доступу до служб Apple, як-от App Store, iCloud, «Повідомлення», FaceTime і «Локатор». Він також містить особисту інформацію, яку ви зберігаєте в Apple і поширюєте на різних пристроях, як-от контакти, платіжну інформацію, фотографії, резервні копії пристроїв тощо. Якщо хтось інший має доступ до вашого облікового запису Apple, він може переглядати інформацію, синхронізовану на різних пристроях, зокрема Повідомлення та геопозицію. Дізнайтеся, як захистити свій обліковий запис Apple на iPad, iPhone і Mac.



Нижче наведено кілька важливих заходів, яких ви можете взяти, щоб захистити свій обліковий запис Apple і свою приватність.



## Захист облікового запису Apple






1. Не надавайте доступ до свого облікового запису Apple нікому, навіть членам родини, партнерам і близьким друзям. Поділившись своїм обліковим записом Apple з іншою людиною, ви надаєте їй доступ до всіх своїх особистих даних і вмісту. Якщо хтось інший налаштував для вас обліковий запис Apple і пароль або мав доступ до вашого пароля, вам слід змінити пароль.
2. Використовуйте двофакторну автентифікацію для свого облікового запису Apple. Двофакторна автентифікація призначена для того, щоб ви були єдиною особою, яка може отримати доступ до вашого облікового запису, навіть якщо хтось інший знає ваш пароль. Під час використання двофакторної автентифікації вам потрібно буде надати свій пароль і шестизначний цифровий код перевірки, який автоматично з'являється на ваших довірених пристроях, коли ви хочете вперше увійти в систему нового пристрою.

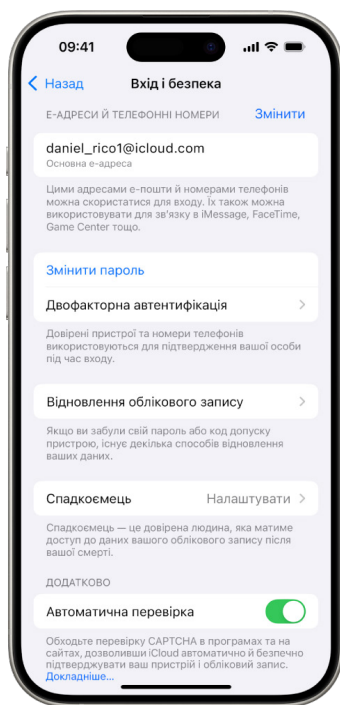
Щоб налаштувати двофакторну автентифікацію, потрібно підтвердити принаймні один довірений номер телефону — номер, на який можна отримувати коди підтвердження за допомогою текстових повідомлень або автоматичного телефонного виклику.

3. Звертайте увагу на сповіщення щодо свого облікового запису Apple. Компанія Apple сповіщає вас за допомогою е-пошти, текстових повідомлень або push-сповіщень, коли у ваш обліковому записі вносять зміни, наприклад у разі входу з нового пристрою або зміни пароля. Тому важливо підтримувати вашу контактну інформацію в актуальному стані.  
Перегляньте розділ [«Відхилення невідомих спроб входу»](#) вище в цьому посібнику.
4. Якщо ви отримуєте сповіщення про спробу входу або про те, що до облікового запису було внесено зміни без вашого дозволу, це може означати, що хтось отримав доступ або намагається отримати доступ до вашого облікового запису.

## Перевірка й оновлення безпекової інформації облікового запису Apple

Щоб переконатися, що особиста інформація, пов'язана з вашим обліковим записом Apple, є саме вашою:

1. Виконайте одну з таких дій:
  - На iPhone або iPad. Перейдіть у Параметри  > [ваше ім'я].
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть обліковий запис Apple .
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть обліковий запис Apple .
  - У браузері на Mac або пристрої з Windows. Перейдіть на [вебсайт облікового запису Apple](https://appleid.apple.com) (<https://appleid.apple.com>).
2. У розділі «Ім'я», «Номери телефонів», «Е-адреса» оновіть будь-яку інформацію, яка є неправильною або яку ви не впізнаєте, зокрема ваше ім'я, номери телефонів та адреси е-пошти, за якими з вами можна зв'язатися.



3. Виконайте одну з таких дій:
  - Якщо у вас увімкнено двофакторну автентифікацію, перегляньте свої довірені пристрої. Якщо ви бачите пристрої, які потрібно вилучити зі свого облікового запису, виконайте інструкції, наведені в наступному розділі.
  - Якщо ви ще не налаштували двофакторну автентифікацію, перегляньте статтю «[Використання двофакторної автентифікації](#)» далі в цьому посібнику.




## Захист вашого облікового запису та видалення невідомих пристроїв


Якщо до вашого облікового запису Apple під'єднано пристрої, які ви не впізнаєте або яким не надавали дозволу на використання свого облікового запису, ви можете захистити свій обліковий запис і вилучити їх, виконавши описані нижче дії. Видалення невідомого пристрою допомагає переконатися, що на ньому більше не будуть показуватися коди перевірки, а доступ до iCloud (та інших служб Apple на пристрої) буде заблоковано, доки ви знову не ввійдете в систему за допомогою двофакторної автентифікації.

Ви також можете зробити знімок екрана пристроїв для документування, перш ніж захистити свій обліковий запис.

Виконайте описані нижче дії, щоб переглянути інформацію свого облікового запису й захистити його.

1. Якщо ви хочете змінити свій пароль:

- *На iPhone або iPad.* Перейдіть у Параметри  > [ваше ім'я] > Вхід і безпека > Змінити пароль. Виберіть надійний пароль (він має містити вісім або більше символів і містити великі й малі літери та принаймні одну цифру).
- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть своє ім'я вгорі бічної панелі. Клацніть «Пароль і безпека», а потім — «Змінити пароль».
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть *ваше ім'я* > Пароль і безпека > Змінити пароль. Виберіть надійний пароль (він має містити вісім або більше символів і містити великі й малі літери та принаймні одну цифру).

2. Якщо ви хочете змінити адресу е-пошти, пов'язану з вашим обліковим записом Apple, щоб посилити безпеку, відкрийте Safari  й увійдіть у свій обліковий запис на [вебсайті облікового запису Apple](https://account.apple.com) (<https://account.apple.com>). Виберіть «Обліковий запис» і під своїм поточним обліковим записом Apple виберіть «Змінити обліковий запис Apple», а потім введіть нову е-адресу.

3. Якщо ви хочете видалити пристрої, які не потрібно підключати до свого облікового запису:


- *На iPhone або iPad.* Перейдіть у Параметри > [ваше ім'я], прокрутіть униз до списку пристроїв, торкніть пристрій, який потрібно вилучити, а потім торкніть «Вилучити з облікового запису».
- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть [ваше ім'я]. Прокрутіть униз до списку пристроїв, клацніть пристрій, який потрібно вилучити, а потім клацніть «Вилучити з облікового запису».
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть Apple ID , прокрутіть униз до списку пристроїв, торкніть пристрій, який потрібно видалити, а потім торкніть «Вилучити з облікового запису».

## Використання двофакторної автентифікації

Двофакторна автентифікація — це додатковий рівень безпеки для вашого облікового запису Apple, який гарантує, що ви є єдиною особою, яка може отримати доступ до вашого облікового запису, навіть якщо хтось знає ваш пароль. Ви можете налаштувати двофакторну автентифікацію на iPhone, iPad і Mac.



### Налаштування двофакторної автентифікації на iPhone та iPad

1. Перейдіть у Параметри  > [ваше ім'я] > Вхід і безпека.
2. Торкніть «Увімкнути двофакторну автентифікацію», а потім торкніть «Продовжити».
3. Введіть номер довіреного телефону, номер телефону, на який ви хочете отримувати коди перевірки для двофакторної автентифікації (це може бути номер вашого iPhone).

Ви можете отримувати коди за допомогою текстового повідомлення або автоматичного телефонного дзвінка.

4. Торкніть «Далі».
5. Введіть код перевірки, надісланий на номер довіреного телефону.




Щоб надіслати або повторно надіслати код перевірки, торкніть «Не отримали код підтвердження?»

Запит на введення коду перевірки більше не з'являтиметься на вашому iPhone, якщо ви не виконаєте одну з таких дій:

- Повний вихід з облікового запису
- Стирання даних iPhone
- Вхід у ваш обліковий запис Apple з вебсторінки облікового запису Apple
- Необхідність змінити обліковий запис Apple з міркувань безпеки

Після увімкнення двофакторної автентифікації у вас є двотижневий період, протягом якого її можна вимкнути. Після цього вимкнути двофакторну автентифікацію стане неможливо. Для вимкнення відкрийте е-лист із підтвердженням і натисніть посилання, щоб повернутися до попередніх параметрів безпеки. Пам'ятайте, що вимкнення двофакторної автентифікації робить ваш обліковий запис менш безпечним і означає, що ви не можете використовувати функції, які вимагають більш високого рівня безпеки.

## Налаштування двофакторної автентифікації на пристрої Mac

1. Виконайте одну з таких дій:
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть [ваше ім'я], а потім виберіть «Вхід і безпека» на бічній панелі.
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть Apple ID , а потім виберіть «Вхід і безпека».
2. Клацніть «Увімкнути двофакторну автентифікацію», а потім клацніть «Продовжити».
3. Дайте відповіді на питання перевірки, а потім клацніть «Перевірити».
4. Введіть свій номер телефону для перевірки, виберіть спосіб перевірки та натисніть «Продовжити».
5. На запит підтвердьте свою особу за допомогою шестизначного коду перевірки, надісланого на ваш довірений телефон. Запит на введення коду перевірки більше не з'являтиметься на вашому Mac, якщо тільки ви повністю не вийдете зі свого облікового запису Apple, не зітрете дані з Mac або не зміните пароль з міркувань безпеки.

### Ключі безпеки для облікового запису Apple

Ключ безпеки — це невеликий зовнішній пристрій, схожий на флеш-накопичувач або жетон, який можна використовувати для підтвердження під час входу з використанням облікового запису Apple та двофакторної автентифікації. Ключі безпеки для облікового запису Apple є додатковою функцією безпеки, призначеною для людей, яким потрібен підвищений захист від цілеспрямованих атак, як-от фішингу й шахрайства за допомогою соціальної інженерії. Оскільки замість шестизначного коду ви використовуватимете ключ безпеки, це посилить надійність процесу двофакторної автентифікації та перешкодить перехопленню чи запитуванню нападником вашого другого фактора автентифікації.

Щоб дізнатися більше про ключі безпеки, дивіться статтю служби підтримки Apple [Ключі безпеки для облікового запису Apple](https://support.apple.com/uk-ua/102637) (https://support.apple.com/uk-ua/102637).

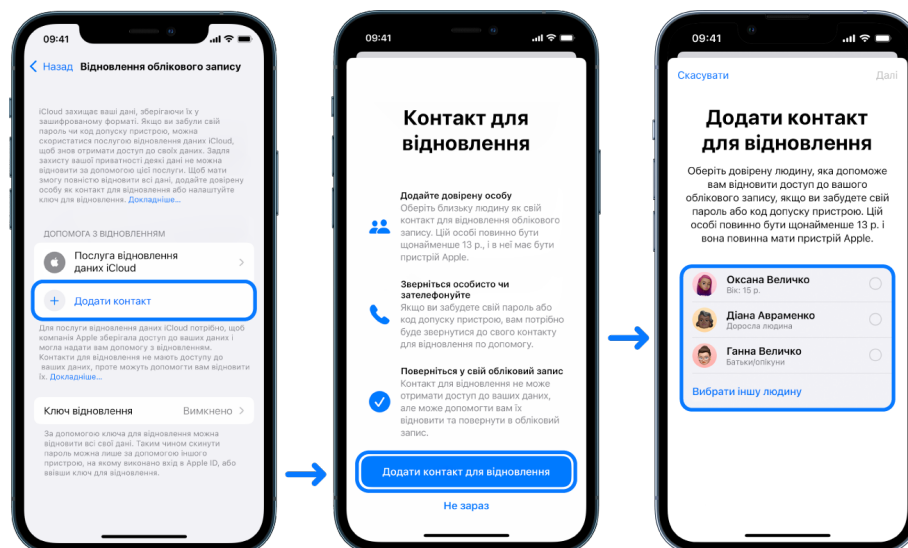
# Запобігання втраті доступу до облікового запису Apple і пристрою

Контакти для відновлення облікового запису — це довірені люди, які можуть допомогти вам відновити доступ до облікового запису, якщо ви забудете свій пароль чи код допуску до пристрою або якщо ваш пароль чи код допуску було змінено без вашого дозволу. Контакти для відновлення облікового запису не матимуть доступу до вашого облікового запису, вони зможуть лише в разі потреби надіслати вам код для відновлення облікового запису. Налаштуйте контакт для відновлення облікового запису на своєму iPhone, iPad чи Mac, щоб ви могли відновити доступ до своїх даних, якщо його буде втрачено.








**Примітка.** Крім контакту для відновлення можна визначити *спадкоємця*, що є найпростішим і найбезпечнішим способом передати дані, збережені у вашому обліковому записі Apple, довірній особі після вашої смерті. Дивіться статтю служби підтримки Apple [Як додати спадкоємця для облікового запису Apple](https://support.apple.com/102631) (<https://support.apple.com/102631>).

Щоб бути контактом для відновлення облікового запису, особа має бути старше 13 років, мати пристрій з iOS 15, iPadOS 15, macOS 12 або новішою версією, увімкнути двофакторну автентифікацію для свого облікового запису Apple та налаштувати пароль на своєму пристрої.








## Налаштування контакту для відновлення облікового запису

Якщо вас турбує, що ви можете втратити доступ до свого облікового запису через те, що хтось зможе отримати доступ до вашого облікового запису та змінити ваш пароль, ви можете встановити довірений контакт для відновлення облікового запису.

1. Виконайте одну з таких дій:
  - На iPhone або iPad. Перейдіть у Параметри  > [ваше ім'я], а потім торкніть «Вхід і безпека».
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , а потім виберіть «Вхід і безпека» на бічній панелі.
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , а потім виберіть «Вхід і безпека».
2. Виберіть «Відновлення облікового запису», додайте контакт для відновлення, а потім пройдіть автентифікацію за допомогою Face ID, Touch ID, коду допуску або пароля.
3. Якщо ви перебуваєте в групі «Сімейний доступ», рекомендовано додати членів групи. Або ви можете вибрати один зі своїх контактів.
4. Якщо ви виберете члена родини, він додається автоматично. Якщо ви виберете контакт, він повинен прийняти запит.
5. Після прийняття запиту ви побачите повідомлення про те, що цю особу додано як контакт для відновлення облікового запису.

## Перегляд і вилучення контакту для відновлення

Якщо ви хочете переглянути або вилучити свій контакт для відновлення.

1. Виконайте одну з таких дій:
  - На iPhone або iPad. Перейдіть у Параметри  > [ваше ім'я], а потім торкніть «Вхід і безпека».
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , а потім виберіть «Вхід і безпека» на бічній панелі.
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , а потім виберіть «Вхід і безпека».
2. У розділі «Допомога з відновленням» наведено ваші контакти для відновлення.
3. Виберіть контакт для відновлення, який потрібно вилучити, а потім вилучіть його.

# Доступ до пристрою

## Керування відбитками пальців для Touch ID

Використовуйте Touch ID, щоб безпечно та зручно відмикати iPhone або iPad, авторизувати покупки й платежі та входити в численні сторонні програми, натиснувши пальцем кнопку «Початок».

Щоб використовувати Touch ID, спочатку потрібно налаштувати код допуску на своєму iPhone, iPad або Mac.


⚠️**ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку та приватність.](#)



## Захист пристроїв за допомогою Touch ID

Щоб використовувати Touch ID, спочатку потрібно налаштувати код допуску на своєму iPhone або iPad.

### Налаштування Touch ID на iPhone або iPad

1. Якщо розпізнавання відбитків пальців не було ввімкнено під час першого налаштування пристрою iPhone чи iPad, перейдіть у Параметри  > Touch ID і код допуску.
2. Увімкніть будь-яку із цих опцій та виконуйте вказівки, які з'являться на екрані.  
Якщо ви бачите відбитки пальців, яких не додавали, дивіться розділ [Керування відбитками пальців для Touch ID](#) далі в цьому посібнику.





*Примітка.* Якщо ви не можете додати відбиток пальця або відімкнути свій iPhone чи iPad за допомогою Touch ID, перегляньте статтю служби підтримки Apple [Якщо Touch ID не працює на iPhone або iPad](https://support.apple.com/101612) (<https://support.apple.com/101612>).



## Налаштування Touch ID на Mac або Magic Keyboard

Щоб використовувати Touch ID, спочатку потрібно налаштувати пароль на Mac.

1. Виконайте одну з таких дій:

- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть Touch ID .
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть Touch ID .

2. Клацніть «Додати відбиток пальця», введіть пароль і дотримуйтесь інструкцій на екрані.


Якщо ваш Mac або Magic Keyboard має Touch ID, датчик розташований у верхньому правому куті клавіатури. Ви можете додати до трьох відбитків пальців у свій обліковий запис користувача (і ви можете зберегти до п'яти відбитків пальців на своєму пристрої Mac).

3. Установіть прапорці, щоб вибрати спосіб використання Touch ID:

- *Відмикання Mac.* Використовуйте Touch ID, щоб відімкнути Mac під час його виведення з режиму сну.
- *Apple Pay.* Використовуйте Touch ID для здійснення покупок на цьому Mac за допомогою Apple Pay.
- *iTunes Store, App Store і Apple Books.* Використовуйте Touch ID для здійснення покупок на цьому Mac в онлайн-магазинах Apple.
- *Автозаповнення паролів.* Використовуйте Touch ID, щоб автоматично заповнювати імена користувачів і паролі, а також автоматично заповнювати дані кредитної картки під час використання Safari та інших програм.
- Використання датчика Touch ID для швидкого перемикання між користувачами. Використовуйте Touch ID для перемикання між обліковими записами користувачів Mac.

## Видалення невідомих відбитків пальців для Touch ID з iPhone або iPad

Якщо на iPhone або iPad є кілька відбитків пальців для Touch ID, ви можете видалити їх, щоб забезпечити доступ до свого пристрою.





1. Перейдіть у Параметри  > Touch ID і код допуску.
2. Якщо є кілька відбитків пальця і вони не мають імені, прикладіть палець до кнопки «Початок», щоб визначити його відбиток. Варто дати ім'я відбитку пальця, щоб було легше ідентифікувати його згодом.
3. За необхідності торкніть відбиток пальця, а потім торкніть «Видалити відбиток».

*Примітка.* Якщо ви не можете додати відбиток пальця або відімкнути свій iPhone чи iPad за допомогою Touch ID, дивіться статтю служби підтримки Apple [Якщо Touch ID не працює на iPhone або iPad](#).

## Видалення невідомих відбитків пальців для Touch ID з Mac або Magic Keyboard

Якщо на Mac або Magic Keyboard є кілька відбитків пальців для Touch ID, ви можете видалити їх, щоб забезпечити доступ до свого пристрою.

### 1. Відкрийте Touch ID.

- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», потім клацніть «Touch ID та пароль» .
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть Touch ID .

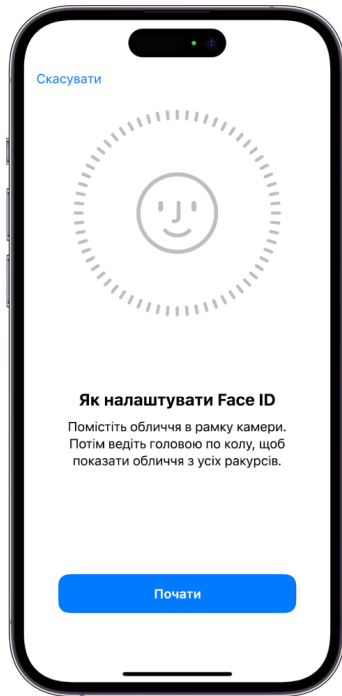
### 2. Виконайте будь-які з таких дій:

- *Видалити відбиток.* Клацніть відбиток пальця, введіть свій пароль, клацніть ОК, потім клацніть «Видалити».
- *Додати відбиток.* Клацніть «Додати відбиток пальця», щоб додати новий відбиток пальця, а потім виберіть опції, які ви хочете використовувати з Touch ID.


## Захист iPhone або iPad за допомогою Face ID

Функція Face ID призначена для тих, кому потрібен додатковий рівень захисту iPhone або iPad. Вона гарантує, що більше ніхто не зможе отримати доступ до інформації, яка зберігається на вашому пристрої. Щоб використовувати Face ID, спочатку потрібно налаштувати код допуску на своєму iPhone або iPad.

Щоб переглянути список підтримуваних пристроїв, дивіться статтю служби підтримки Apple [Моделі iPhone та iPad з підтримкою Face ID](https://support.apple.com/102854) (<https://support.apple.com/102854>).

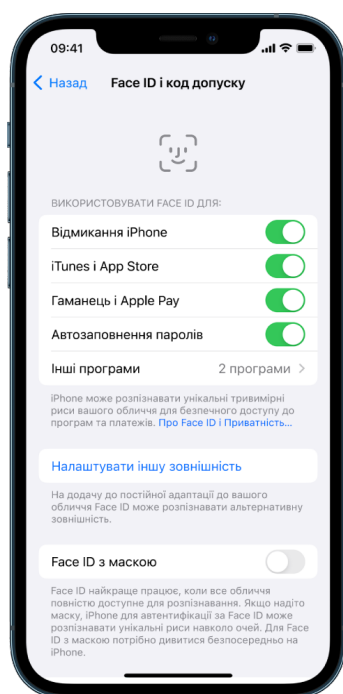


## Захист iPhone або iPad за допомогою Face ID

- Якщо ви не встановили Face ID під час першого налаштування iPhone або iPad, перейдіть у Параметри  > Face ID і код допуску > Налаштувати Face ID, а потім виконайте інструкції на екрані.

Якщо у вас є фізичні обмеження, ви можете торкнутися «Опції доступності» під час налаштування Face ID. Після виконання цієї дії налаштування розпізнавання обличчя не вимагає повного діапазону рухів голови. Використання Face ID все одно є безпечним, але вимагає, щоб ви виглядали на iPhone або iPad більш однотипно.


Face ID також має функцію доступності, яку можна використовувати, якщо ви незрячі або погано бачите. Якщо ви не хочете, щоб Face ID вимагав від вас дивитися на iPhone або iPad із відкритими очима, перейдіть у Параметри > Доступність, а потім вимкніть параметр «Вимагати уваги для Face ID». Ця функція автоматично вимикається, якщо функція VoiceOver увімкнута під час першого налаштування iPhone або iPad.



Дивіться розділи [Змінення параметрів Face ID та уваги на iPhone](https://support.apple.com/guide/iphone/iph646624222) (<https://support.apple.com/guide/iphone/iph646624222>) у Посібнику користувача iPhone або [Змінення параметрів Face ID та уваги на iPad](https://support.apple.com/guide/ipad/ipad058b4a31) (<https://support.apple.com/guide/ipad/ipad058b4a31>) у Посібнику користувача iPad.

## Скидання Face ID для видалення альтернативних варіантів зовнішнього вигляду

Якщо є альтернативний зовнішній вигляд для Face ID, який ви не хочете зберігати, або якщо ви вважаєте, що хтось міг додати альтернативний варіант вигляду на вашому пристрої без вашого дозволу, ви можете скинути Face ID, а потім налаштувати цю функцію знову.

1. Перейдіть у Параметри  > Face ID і код допуску, а потім торкніть «Скинути Face ID».
2. Для повторного налаштування Face ID дивіться процедуру вище.

## Відхилення невідомих спроб входу

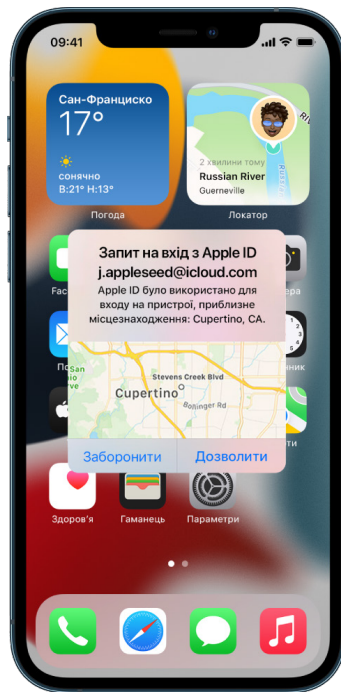
Якщо ввімкнено двофакторну автентифікацію і спроба входу здійснюється з нового пристрою, ви отримаєте сповіщення на інших довірених пристроях. Сповіщення містить карту, на якій показано розташування нового пристрою. Це сповіщення може з'явитися на будь-якому довіреному iPhone, iPad чи Mac.

Це приблизне розташування місця входу, визначене на основі IP-адреси або мережі, яку зараз використовує пристрій, а не точного розташування пристрою.



Якщо ви бачите сповіщення про те, що ваш обліковий запис Apple використовується для входу на новому пристрої, але ви цього не робите, виберіть «Не дозволяти», щоб заблокувати спробу входу.

▼ **ВАЖЛИВО.** Ви можете зробити знімок екрана сповіщення, перш ніж закрити його. Дивіться розділ [Записування підозрілої активності](#) далі в цьому посібнику.



Якщо ви вважаєте, що безпеку вашого облікового запису Apple могло бути порушено, дивіться розділ [Захист вашого облікового запису Apple](#) (далі в цьому посібнику) і вилучіть невідомі пристрої.

## Оновлення ПЗ Apple

Щоб захистити свій пристрій і керувати доступом до своєї особистої інформації, переконайтеся, що ви інсталиювали останню версію операційної системи з останніми оновленнями безпеки та приватності. Коли ваші пристрої буде оновлено, ви зможете дізнатися, як керувати своїм обліковим записом Apple. Усі пристрої Apple отримують переваги від оновлень програмного забезпечення.




Оновлення програмного забезпечення операційної системи є однією з найважливіших речей, які ви можете зробити, щоб захистити свій пристрій і свою інформацію. Apple спрощує завантаження та встановлення цих оновлень.

Щоб ознайомитися зі списком оновлень безпеки для пристроїв Apple, дивіться статтю служби підтримки Apple [Випуски безпеки Apple](https://support.apple.com/uk-ua/100100#update) (<https://support.apple.com/uk-ua/100100#update>).

### Автоматичне оновлення iPhone та iPad

Якщо ви не вмикали автоматичні оновлення під час першого налаштування пристрою, ви можете зробити це зараз.

1. Перейдіть у Параметри  > Загальні > Оновлення ПЗ > Автоматичні оновлення.
2. Увімкніть усі три опції: «Автоматично інсталиювати оновлення [iOS або iPadOS]», «Безпечкові оновлення й системні файли» та «Автоматично викачувати оновлення [iOS або iPadOS]».

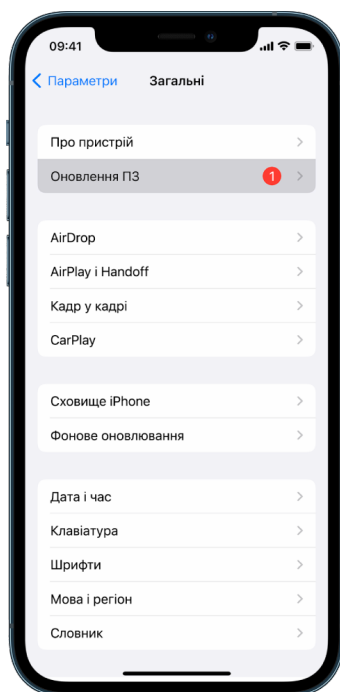
Коли оновлення доступне, пристрій завантажує та встановлює оновлення протягом ночі, поки він заряджається та під'єднується до Wi-Fi. Ви отримаєте сповіщення перед установленням оновлення.

Щоб вимкнути автоматичні оновлення, перейдіть у Параметри > Загальні > Оновлення ПЗ > Автоматичні оновлення, а потім вимкніть параметри «Автоматично інсталиювати оновлення [iOS або iPadOS]» і «Безпечкові оновлення й системні файли».

## Оновлення iPhone або iPad вручну

Перевірити наявність оновлень програмного забезпечення та встановити їх вручну можна в будь-який час.

- Перейдіть у Параметри  > Загальні > Оновлення ПЗ.



На екрані відображається поточна встановлена версія iOS і сповіщення, якщо доступне оновлення.

## Оновлення iPhone або iPad за допомогою комп'ютера

1. Переконайтеся, що у вас є один із таких пристроїв:
  - Mac із портом USB та OS X 10.9 або новішої версії
  - Пристрій з Windows із портом USB та Windows 7 або новішою версією
2. Виконайте одну з таких дій:
  - Підключіть пристрій до комп'ютера за допомогою кабелю Lightning — USB, що входить у комплект. Якщо на вашому комп'ютері є порт USB-C, використовуйте адаптер USB-C — USB або кабель USB-C — Lightning (кожен продається окремо).
  - Якщо ваш пристрій постачається з кабелем USB-C — Lightning, а комп'ютер має порт USB, використовуйте кабель Lightning — USB (продається окремо).
  - Якщо у вашому iPad був зарядний кабель USB-C, а на комп'ютері є порт USB, використовуйте адаптер USB-C — USB і кабель USB-A (кожен продається окремо).
  - Якщо у вашому iPad був зарядний кабель Thunderbolt 4/USB-4, а комп'ютер має порт USB, використовуйте адаптер USB-C — USB і кабель USB-A (кожен продається окремо). Ви можете використовувати кабелі Thunderbolt або USB з пристроями Thunderbolt, такими як 12,9-дюймовий iPad Pro (5-го покоління) і 11-дюймовий iPad Pro (3-го покоління).

3. Після успішного підключення пристрою до комп'ютера виконайте одну з таких дій:
  - *На бічній панелі Finder на вашому Mac.* Виберіть свій пристрій, а потім натисніть «Загальні» у верхній частині вікна.

Щоб використовувати Finder для оновлення пристрою до iOS 15 або iPadOS 15, необхідна macOS 10.15 або новіша версія. У попередніх версіях macOS **використовуйте iTunes для оновлення пристрою**. Перегляньте розділ «Оновлення програмного забезпечення на пристроях iOS в iTunes» (<https://support.apple.com/guide/itunes/itns3235/12.9/mac/10.14>).
  - *У програмі iTunes на пристрої з Windows.* Натисніть кнопку iPhone у верхньому лівому куті вікна iTunes, а потім натисніть «Підсумок».
4. Клацніть «Шукати оновлення».
5. Щоб установити доступне оновлення, натисніть «Оновити».

### **Автоматичне оновлення Mac**

1. Виконайте одну з таких дій:
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Загальні», а потім клацніть «Оновлення ПЗ».
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Оновлення ПЗ» .
2. Щоб автоматично встановлювати оновлення macOS, виберіть «Автоматично оновлювати мій Mac».
3. Щоб налаштувати розширені параметри оновлення, клацніть «Експертні», а потім виконайте будь-які з таких дій:
  - *Щоб ваш Mac автоматично перевіряв наявність оновлень.* Виберіть «Пошук оновлень».
  - *Щоб ваш Mac автоматично викачував оновлення без запиту.* Виберіть «Викачувати нові оновлення, якщо доступно».
  - *Щоб ваш Mac автоматично інстальював оновлення macOS.* Виберіть «Інстальювати оновлення macOS».
  - *Щоб ваш Mac інстальював оновлення з App Store автоматично.* Виберіть «Інстальювати оновлення програм із App Store».
  - *Щоб ваш Mac автоматично інстальював системні файли та безпекові оновлення.* Виберіть «Інстальювати безпекові оновлення й системні файли».
4. Клацніть ОК.





Для автоматичного отримання останніх оновлень рекомендується вибрати опції «Шукати оновлення», «Викачувати нові оновлення, якщо доступно» та «Інстальювати системні файли та оновлення безпеки».

*Примітка.* Для автоматичного завантаження оновлень для MacBook, MacBook Pro і MacBook Air необхідно підключити адаптер живлення.



## Оновлення Mac вручну

Ви можете вручну оновити операційну систему свого Mac і будь-яке програмне забезпечення, отримане з App Store.

- Виконайте одну з таких дій:
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Загальні», а потім клацніть «Оновлення ПЗ».
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Оновлення ПЗ» .
- Щоб оновити програмне забезпечення, завантажене з App Store, натисніть меню Apple. Кількість доступних оновлень за їх наявності відображається поруч з App Store. Виберіть App Store, щоб продовжити в програмі App Store .

## Перегляд і видалення профілів конфігурації

Профілі конфігурації пристроїв, інструменти керування мобільними пристроями (MDM) і спеціальні програми можуть використовуватися організаціями (зокрема, навчальними закладами й підприємствами) для керування пристроями або нагляду за ними, водночас ці інструменти можуть надавати доступ до даних або геопозиції на пристрої.

Профіль конфігурації може керувати різноманітними параметрами облікових записів користувачів, а також іншими функціональними можливостями пристрою. Профілі конфігурації можуть працювати на iPhone, iPad, Mac, Apple TV і Apple Watch.

Якщо ви знайдете на своєму пристрої профіль конфігурації, якого там не повинно бути, можливо, вам вдасться його видалити. Можливість видалення залежить від того, ким був установлений профіль. При цьому видаляються всі налаштування, програми та дані, пов'язані із цим профілем конфігурації.

⚠️**ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку](#) та приватність.

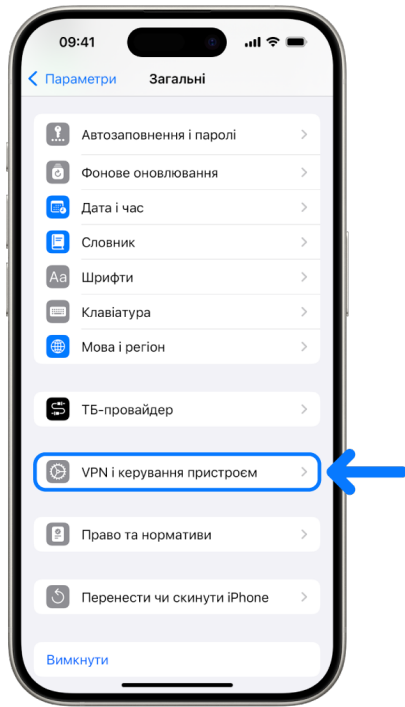



### Перегляд профілів конфігурації

**Важливо!** Якщо ваш пристрій належить навчальному закладу чи компанії, зверніться до свого системного адміністратора, перш ніж видаляти будь-які програми чи профілі.

## Видалення невідомих профілів конфігурації на iPhone та iPad





Коли ви видаляєте профіль, усі його налаштування та інформація видаляються. Зокрема, якщо за допомогою профілю надавалися дозволи для використання віртуальної приватної мережі (VPN) під час доступу до мережі навчального закладу, VPN надалі не зможе під'єднатися до цієї мережі.




1. Перейдіть у Параметри  > Загальні > VPN і керування пристроєм.  
Якщо ви не бачите жодних профілів, то на вашому пристрої не встановлено профілі керування пристроєм.
2. Виберіть профіль, торкніть «Видалити профіль» і дотримуйтесь інструкцій, які з'являться на екрані.
3. Перезапустіть свій пристрій.

## Видалення невідомих профілів конфігурації на Mac

Коли ви видаляєте профіль, усі його налаштування та інформація видаляються. Наприклад, якщо профіль налаштував ваш обліковий запис е-пошти, видалення профілю призведе до видалення інформації облікового запису е-пошти з вашого Mac.

1. Виконайте одну з таких дій:
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», виберіть «Приватність і безпека», а потім клацніть «Профілі» .
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть «Профілі» .

Якщо ви не бачите панель параметрів «Профілі», то на вашому пристрої не встановлено профілі керування пристроєм.

2. Виберіть профіль у списку «Профілі», а потім клацніть .
3. Перезапустіть Mac.

## Посилення захисту пристроїв за допомогою режиму карантину

Режим карантину — додатковий засіб захисту iPhone, iPad і Mac з iOS 16, iPadOS 16.1, macOS 13 або новішою версією для екстремальних випадків, яким слід користуватися, лише якщо ви вважаєте, що можете стати ціллю висококваліфікованої кібератаки, наприклад, з боку приватних компаній, які розробляють шпигунські програми за державним замовленням.

*Примітка.* Більшість людей не зазнають подібних атак.






У режимі карантину пристрій не працює як зазвичай. Використання програм, вебсайтів і функцій суворо обмежується, а деякі можливості недоступні. У режимі карантину діють такі захисні механізми:

- *Повідомлення.* Більшість типів вкладень, крім зображень, блокуються. Деякі функції, як-от попередній перегляд посилань, вимикаються.
- *Вебперегляд.* Певні складні вебтехнології, як-от компіювання just-in-time (JIT) JavaScript, вимикаються, якщо користувач не виключить довірений сайт із режиму карантину.
- *Служби Apple.* Вхідні запрошення та запити на обслуговування, включно з викликами FaceTime, блокуються, якщо користувач раніше не надіслав ініціатору виклик чи запит.
- *Зв'язані з'єднання.* З'єднання з комп'ютером чи приладдям блокуються, коли пристрій замкнено.
- *Конфігураційні профілі.* Коли ввімкнуто режим карантину, конфігураційні профілі не можна інсталювати, і пристрій не можна зареєструвати в рішенні керування мобільними пристроями (MDM). Однак будь-які профілі MDM, які було ввімкнуто до застосування режиму карантину, залишаться на пристрої.

## Увімкнення або вимкнення режиму карантину

Режим карантину потрібно вмикати окремо на пристроях iPhone, iPad і Mac. Коли ви вмикаєте режим карантину на iPhone, цей режим автоматично вмикається на всіх спарених Apple Watch з watchOS 10 або новішою версією. Режим карантину не можна вмикати чи вимикати безпосередньо на Apple Watch.


- Виконайте одну з таких дій:
  - *На iPhone або iPad.* Перейдіть у Параметри  > Приватність і безпека > Режим карантину, торкніть «Увімкнути режим карантину», торкніть «Увімкнути й перезапустити», а потім введіть код допуску пристрою.
  - *На Mac.* Виберіть меню Apple , виберіть «Системні параметри», виберіть «Приватність і безпека» , а потім — «Режим карантину». Торкніть «Увімкнути», введіть пароль, якщо з'явиться відповідний запит, і торкніть «Увімкнути й перезапустити».

## Надійне керування домашніми приладами

Якщо наразі ви є учасником групи «Дім», то можете легко й безпечно переглядати домашні прилади та керувати ними за допомогою програми «Дім» на своєму iPhone, iPad чи Mac або за допомогою HomePod.


*Примітка.* Домашніми приладами можуть бути вироби Apple чи інших компаній. Список доступних домашніх приладів, сумісних із програмою «Дім» і вашими пристроями Apple, наведено на сторінці «[Домашні прилади](https://www.apple.com/home-app/accessories/)» (<https://www.apple.com/home-app/accessories/>).

## Припинення спільного доступу до дому для інших користувачів

1. Виберіть програму «Дім» , а потім виберіть «Налаштування Дому». Якщо показано декілька домів, виберіть дім, з якого ви хочете вийти, потім виберіть «Налаштування дому».
2. У розділі «Люди» виберіть користувача, якого потрібно вилучити з вашого дому, а потім виберіть «Вилучити особу».

## **Вихід із дому, до спільного користування яким вас запросили**


Після виходу з дому ви більше не зможете переглядати прилади, розташовані в цьому домі.

1. У програмі «Дім»  виберіть іконку «Дім», а потім — «Налаштування Дому». Якщо показано декілька домів, виберіть той, з якого ви хочете вийти, потім виберіть «Налаштування Дому».
2. Прокрутіть униз і виберіть «Вихід із дому». Виберіть «Покинути».

## **Скидання стану дому**

В iOS 16, iPadOS 16.1 і macOS 13 або новіших версіях, коли ви вилучаєте дім із програми «Дім», усі пристрої HomeKit необхідно знову додати до нового дому. Перш ніж вилучити дім, переконайтеся, що ви оновили програмне забезпечення на всьому приладді вдома до найновіших версій.

Якщо ви не оновлювали свої операційні системи, обов'язково виконайте крок 4.

1. У програмі «Дім»  виберіть іконку «Дім», а потім — «Налаштування Дому».
2. У нижній частині діалогового вікна виберіть «Вилучити дім», а потім — «Вилучити».
3. Закрийте програму «Дім».
4. Знайдіть усі домашні прилади, потім відновіть для кожного приладу заводські налаштування.
5. Знову відкрийте програму «Дім» та створіть новий дім.
6. Додайте кожний прилад до нового дому.

# Паролі, ключі допуску, коли допуску


## Захист паролів для пристроїв, програм і вебсайтів

На iPhone чи iPad з iOS 17, iPadOS 17 або попередньою версією можна керувати паролями в Параметрах, у пошуку Spotlight або за допомогою Siri. Також за допомогою функції «Рекомендації щодо безпеки паролів» можна виявляти слабкі або вразливі паролі. Збережені паролі відображаються в алфавітному порядку, упорядковані за вебсайтом чи платформою, на яких вони збережені.

На iPhone чи iPad з iOS 18, iPadOS 18, або новішою версією можна керувати паролями в програмі «Паролі», де можна тримати всі паролі, ключі допуску й коди перевірки разом. Ви можете використовувати їх на всіх своїх пристроях, якщо ви ввійшли в iCloud з використанням одного облікового запису Apple і ввімкнули функцію «Паролі та В'язка» в параметрах iCloud. А якщо ви використовуєте функцію «Автозаповнення» під час входу в програми й на вебсайти, ваші паролі автоматично з'являтимуться у відповідній програмі.




### Керування паролями в iOS 18, iPadOS 18 або новішій версії

1. Відкрийте програму «Паролі»  на iPhone.
2. Торкніть «Усі», а потім — обліковий запис, паролем для якого потрібно керувати.
3. Торкніть «Змінити».
4. Змініть або видаліть пароль, а потім торкніть, щоб підтвердити.

## Керування паролями в iOS 17, iPadOS 17 або попередній версії

Ви можете керувати своїми паролями в меню «Параметри», у пошуку Spotlight або за допомогою Siri.

1. Перейдіть у Параметри  > Паролі, а потім виконайте будь-які з таких дій:
  - Щоб вручну додати новий пароль, торкніть «Додати» у верхньому правому куті.
  - Щоб змінити або видалити пароль, торкніть «Редагувати» у верхньому правому куті, торкніть «Вибрати збережені паролі», а потім торкніть «Редагувати» або «Видалити».

**Важливо!** Видаливши пароль, ви не зможете його відновити.
2. Якщо ви додали новий пароль, перевірте, що ви правильно його ввели.

## Використання рекомендацій щодо безпеки паролів в iOS 17, iPadOS 17 або попередніх версіях




Якщо ви створюєте та зберігаєте власні паролі для вебсайтів і програм, за допомогою функції «Рекомендації щодо безпеки паролів» ви можете виявляти слабкі та вразливі паролі (наприклад, які легко вгадати або які використано багато разів). Також за допомогою цієї функції можна безпечно стежити за паролями й отримувати оповістки, якщо якийсь із них потрапив до відомого витоку даних.

1. Перейдіть у Параметри  > Паролі > Рекомендації з безпеки.
2. Увімкніть функцію «Виявляти скомпрометовані паролі», щоб дозволити своєму iPhone безпечно відстежувати ваші паролі й сповіщати, якщо якийсь із них буде виявлено у відомому витоці даних.
3. Перегляньте наведені нижче рекомендації для створених паролів.
  - Паролі, позначені як *використані повторно*, використовуються в різних доменах. Використанням одного пароля для кількох служб, можна зробити обліковий запис вразливим до атак нападника, який заволодів вашими обліковими даними.
  - Паролі, позначені як *слабкі*, нападник може легко вгадати.
  - Паролі позначаються *скомпрометованими*, якщо функція моніторингу паролів виявила їх у відомому витоці даних.
4. Щоб оновити повторно використаний, слабкий чи скомпрометований пароль, торкніть елемент і дотримуйтеся екранних указівок.



## Автоматичне видалення одноразових кодів перевірки

В iOS 17, iPadOS 17 і macOS 14 або новіших версіях одноразові коди перевірки заповнюються автоматично, тож вам не потрібно виходити з програми чи вебсайту, де ви здійснюєте вхід. Можна налаштувати автоматичне видалення кодів перевірки після того, як функція автозаповнення їх ввела.

- Виконайте одну з таких дій:
  - На iPhone чи iPad з iOS 18, iPadOS 18 або новішою версією. Перейдіть у Параметри  > Загальні > Автозаповнення й паролі. У розділі «Коди перевірки» торкніть «Видаляти після використання», а потім увімкніть цю опцію.
  - На iPhone чи iPad з iOS 17, iPadOS 17 або попередньою версією. Перейдіть у Параметри  > Пароль, виберіть «Параметри паролів», а тоді увімкніть опцію «Автоматичне очищення».
  - На Mac з macOS 15. Виберіть меню Apple , виберіть «Системні параметри», потім — «Загальні», а тоді — «Автозаповнення і паролі». У розділі «Коди перевірки» торкніть «Видаляти після використання», а потім увімкніть цю опцію.
  - На Mac з macOS 14 або macOS 13. Виберіть меню Apple , виберіть «Системні параметри», виберіть «Пароль» на бічній панелі, потім — «Параметри паролів», а тоді увімкніть параметр «Автоматичне очищення».

## Установлення унікального коду допуску пристрою або пароля


Щоб ніхто, крім вас, не міг використовувати ваші пристрої та отримувати доступ до вашої інформації, установіть унікальний код допуску або пароль, відомий лише вам. Якщо ви користуєтеся пристроєм спільно з іншими людьми або якщо вони знають ваш код допуску чи пароль, вони мають змогу переглядати інформацію на вашому пристрої та пов'язаному обліковому записі Apple і вносити до неї зміни. Якщо ви вважаєте, що ще хтось знає ваш код допуску або пароль вашого пристрою, і хочете встановити пароль або код допуску, які буде відомо тільки вам, ви можете скинути пароль або код допуску в системних параметрах (дивіться інструкції нижче).



### Налаштування коду допуску на iPhone або iPad

Для посилення безпеки налаштуйте код допуску, який потрібно буде вводити для відмикання iPhone чи iPad після ввімкнення пристрою чи виведення його з режиму сну. Установлення коду допуску також вмикає функцію захисту даних, яка шифрує дані вашого iPhone або iPad, щоб доступ до них мали лише ті, хто знає код допуску.


*Примітка.* Код допуску вашого пристрою не ідентичний паролю облікового запису Apple, який надає доступ до iTunes Store, App Store, Apple Books, iCloud та інших служб Apple.

- Перейдіть у Параметри , а потім виконайте будь-яку з таких дій:
  - На iPhone або iPad з Face ID. Торкніть «Face ID і код допуску», а потім торкніть «Увімкнути код допуску» або «Змінити код допуску».
  - На iPhone або iPad з кнопкою «Початок». Торкніть «Touch ID і код допуску», а потім торкніть «Увімкнути код допуску» або «Змінити код допуску».

Щоб переглянути параметри створення пароля, торкніть «Параметри коду допуску». За замовчуванням коди допуску містять шість цифр, але варіанти варіюються від найменш безпечного, чотиризначного, до найбільш безпечного (літерно-цифрового).

## Змінення коду допуску і позначення попереднього коду допуску недійсним на iPhone або iPad

Якщо ви остерігаєтеся, що хтось може мати доступ до вашого коду допуску і хочете захистити свій iPhone, можна змінити код допуску для захисту приватності і зробити попередній код недійсним. Щоб змінити свій код допуску, виконайте наведені нижче дії.


1. Перейдіть у Параметри , а потім виконайте будь-яку з таких дій:
  - На iPhone або iPad з Face ID. Торкніть «Face ID і код допуску», а тоді введіть свій код допуску.
  - На iPhone або iPad з кнопкою «Початок». Торкніть «Touch ID і код допуску», а тоді введіть свій код допуску.

2. Торкніть «Змінити код допуску» і введіть поточний код допуску.

3. Для додаткового захисту торкніть «Опції коду допуску», щоб вибрати формат наступного коду допуску.

Серед доступних форматів: чотиризначний цифровий, шестизначний цифровий, власний буквено-числовий або власний числовий код.

4. Введіть новий код допуску двічі.






 **ВАЖЛИВО.** Після зміни коду допуску в iOS 17 або iPadOS 17 його можна скинути впродовж 72 годин за допомогою старого коду допуску. Це зроблено з метою захисту у разі, якщо ви випадково забудете новий код. Щоб повністю деактивувати старий код допуску після його зміни, торкніть «Анулювати попередній код допуску» на сторінці «[Face ID][Touch ID] і код допуску» в Параметрах.

## Зміна паролю для входу на Mac

Якщо ви остерігаєтеся, що хтось може мати доступ до вашого паролю і хочете захистити свій Mac, можна змінити пароль для захисту приватності.

*Примітка.* Ваш пароль для входу — це пароль, який ви вводите, щоб розблокувати пристрій Mac під час увімкнення або виведення зі сну. Оскільки ви створили його, він може бути таким самим, як і пароль облікового запису Apple, який надає доступ до iTunes Store, App Store, Apple Books, iCloud та інших служб Apple.


1. Виконайте одну з таких дій:

- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Загальні», клацніть «Користувачі та групи» , а потім клацніть .
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Користувачі та групи» , а потім клацніть «Змінити пароль».

2. Клацніть «Змінити пароль».

3. Введіть поточний пароль у поле «Старий пароль».

4. Введіть новий пароль у поле «Новий пароль», а потім знову введіть його в поле «Підтвердити».

Щоб отримати допомогу у виборі надійного пароля, клацніть  поряд із полем «Новий пароль».


5. Введіть підказку, яка допоможе запам'ятати пароль.

Підказка з'явиться, якщо ви введете неправильний пароль три рази поспіль або клацнете знак питання в полі для пароля у вікні входу.

6. Клацніть «Змінити пароль».

## Автоматичне замикання пристроїв

Щоб додатково захистити свою приватність, можна налаштувати пристрій, щоб він автоматично замикався за певних умов.

- *iPhone, iPad.* Перейдіть у Параметри > Дисплей і яскравість > Автозамикання, а потім установіть період часу.
- *Mac.* Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть «Замкнути екран» на бічній панелі (може бути потрібно прокрутити вниз).

Докладніше дивіться в розділі [Змінення налаштувань замкненого екрана на Mac](https://support.apple.com/guide/mac-help/mh11784) у Посібнику користувача Mac. (<https://support.apple.com/guide/mac-help/mh11784>)

- *Apple Watch.* Відкрийте програму «Параметри», торкніть «Код допуску», а потім увімкніть або вимкніть параметр «Виявлення руки».

Докладніше дивіться в розділі [Автоматичне замкнення](https://support.apple.com/guide/watch/apd0e1e73b6f#apd6771615db) в Посібнику користувача Apple Watch. (<https://support.apple.com/guide/watch/apd0e1e73b6f#apd6771615db>)

## Керування спільними паролями і ключами допуску




В iOS 17, iPadOS 17 і macOS 14 або новіших версіях можна створювати групи довірених контактів або приєднуватися до них для спільного доступу до паролів і ключів допуску з різних пристроїв. Є дві різні ролі користувача у групах спільних паролів: власник групи і учасник групи. Кожна з цих ролей визначає завдання, які ви можете виконувати.

- **Власник групи.** Власник групи — це учасник групи, який її створив. Тільки власник може додавати або вилучати інших учасників.
- **Учасник групи.** Кожна особа, яка отримала і прийняла запрошення від власника, є учасником групи. Всі учасники групи можуть додавати, переглядати, редагувати і видаляти паролі в будь-який момент. Учасник групи може покинути її в будь-який момент.







*Примітка.* Якщо ви видалите пароль або ключ допуску, який ви поширили в групі, у вас є 30 днів на його відновлення. Якщо ви видалите пароль або ключ допуску, який інший учасник поширив у групі, він отримає сповіщення про те, що у нього є 30 днів на відновлення. Дивіться розділ [Відновлення недавно видаленого пароля або ключа доступу на Mac](https://support.apple.com/guide/mac-help/mchlee73013a) (<https://support.apple.com/guide/mac-help/mchlee73013a>) у Посібнику користувача macOS.

### Визначення вашої ролі у групі спільних паролів

- Виконайте одну з таких дій:
  - *На iPhone або iPad.* Перейдіть до Параметри  > Паролі, знайдіть групи спільних паролів , виберіть групу, а тоді подивіться, чи ви власник, чи учасник.
  - *На Mac з macOS 14 або попередньою версією.* Виберіть меню Apple , виберіть «Системні параметри», виберіть «Паролі» на бічній панелі, знайдіть групу спільних паролів , виберіть групу, клацніть «Керувати», а потім подивіться, є ви *власником* чи *учасником*.





## Вилучення учасника з групи спільних паролів, у якій ви є власником

Якщо ви вилучаєте учасника з групи спільних паролів, він все ще може мати доступ до облікових записів і паролів, які ви поширювали, коли він був учасником. Після вилучення учасника слід змінити паролі для облікових записів, які ви поширювали, і більше не хочете, щоб цей учасник мав до них доступ.

- Виконайте одну з таких дій:
  - *На iPhone або iPad.* Перейдіть до Параметри  > Паролі, знайдіть групи спільних паролів , виберіть групу, а тоді вилучіть учасника.
  - *На Mac з macOS 14 або попередньою версією.* Виберіть меню Apple , виберіть «Системні параметри», виберіть «Паролі» на бічній панелі, знайдіть групу спільних паролів , виберіть групу, клацніть «Керувати», а тоді вилучіть учасника.

## Вихід із групи спільних паролів, учасником якої ви є






Якщо ви вилучаєте себе з групи спільних паролів, інші учасники групи все ще можуть мати доступ до облікових записів, паролів і ключів допуску, які ви поширювали, коли були в групі. Покинувши групу, слід змінити паролі і ключі допуску для своїх облікових записів, якщо ви не хочете, щоб учасники групи мали до них доступ.

- Виконайте одну з таких дій:
  - *На iPhone або iPad.* Перейдіть у Параметри  > Паролі, знайдіть групу спільних паролів , виберіть групу, а тоді вилучіть себе з неї.
  - *На Mac з macOS 14 або попередньою версією.* Виберіть меню Apple , виберіть «Системні параметри», виберіть «Паролі» на бічній панелі, знайдіть групу спільних паролів , виберіть групу, клацніть «Керувати», а тоді вилучіть себе з групи.

## Вилучення паролю або ключа допуску з групи спільних паролів

Якщо ви видаляєте паролі або ключі допуску з групи спільних паролів, учасники групи все ще можуть мати доступ до облікових записів, паролів і ключів допуску, які ви поширювали в групі. Після видалення слід також змінити паролі і ключі допуску для своїх облікових записів, якщо ви не хочете, щоб учасники групи мали до них доступ.

*Примітка.* Якщо ви видалите пароль або ключ допуску, який ви поширили в групі, у вас є 30 днів на його відновлення. Якщо ви видалите пароль або ключ допуску, який інший учасник поширив у групі, він отримає сповіщення про те, що у нього є 30 днів на відновлення. Дивіться розділ [Відновлення недавно видаленого пароля або ключа доступу на Mac](https://support.apple.com/guide/mac-help/mchlee73013a) (<https://support.apple.com/guide/mac-help/mchlee73013a>) у Посібнику користувача Mac.

- Виконайте одну з таких дій:
  - *На iPhone або iPad.* Перейдіть до Параметри  > Паролі на бічній панелі, знайдіть групи спільних паролів , виберіть групу, а тоді подивіться, чи ви власник, чи учасник.
  - *На Mac з macOS 14 або попередньою версією.* Виберіть меню Apple , виберіть «Системні параметри», клацніть «Паролі»  на бічній панелі, клацніть  поряд із обліковим записом з паролем або ключем допуску, який ви хочете видалити, клацніть «Видалити пароль» або «Видалити ключ допуску», а тоді клацніть «Видалити пароль» або «Видалити ключ допуску» (ще раз).

# Керування інформацією про геопозицію

## Використання функції «Супровід» у Повідомленнях

Ви можете використовувати функцію «Супровід» на iPhone, щоб автоматично сповіщати друга про прибуття свого iPhone, а також обирати інформацію, яка відобразиться за неуспішного завершення супроводу.

У подібній ситуації, коли друг надсилає вам запит на супровід, але їхній iPhone не прибуває, вони можуть переглядати ваше розташування, рівень заряду батареї, рівень стільникового сигналу тощо.

*Примітка.* Функція «Супровід» потребує iOS 17 або новішої у відправника та отримувача. Поширення геопозиції не підтримується в Північній Кореї, а також може бути обмежене місцевими законами в інших регіонах.

Коли ви починаєте супровід *на основі подорожі*, ваш контакт отримує таку інформацію:

- ваше місце призначення та приблизний час прибуття;
- що робити, якщо ви не відповідаєте на запити, якщо ви активували сигнал SOS під час супроводу, або якщо ваш телефон не прибуває вчасно у визначене місце.

Коли ви починаєте супровід *на основі таймера*, ваш контакт отримує таку інформацію:

- час, коли ви запустили таймер;
- час, коли таймер закінчується;
- що робити, якщо ви не відповідаєте на запити про таймер або якщо ви активували сигнал SOS під час супроводу.

## Яка інформація поширюється та коли?

Під час налаштування функції «Супровід» ви можете вибрати обсяг інформації, яку отримуватиме ваш контакт, коли Супровід не завершуватиметься очікуваним чином. Після налаштування функції «Супровід» можна змінити тип даних, які ви надсилаєте, у меню Параметри > Повідомлення > Супровід > Дані.

Ви можете вибрати один з наведених нижче рівнів інформування:

- *Обмежений обсяг даних.* Містить дані про вашу поточну геопозицію та відомості про рівень заряду батареї й сигналу мережі на iPhone і Apple Watch.
- *Усі дані.* Містить усі дані з обмеженого рівня, а також пройдений вами маршрут і місце останнього розблокування вашого iPhone та зняття Apple Watch.

Вашому контакту буде автоматично надіслано посилання на перегляд інформації, вибраної вами для поширення, за таких умов:

- ваш телефон не прибув у визначене місце;
- ви значно затримуєтеся та не відповідаєте на запит збільшення часу подорожі;
- ви розпочали екстрений виклик і не відповідаєте на наступний запит на супровід;
- ви не відповідаєте на запит наприкінці супроводу на основі таймера.

**Важливо!** Якщо ваш телефон загубився з активним режимом супроводу, контакт отримуватиме сповіщення як ніби ви не відповідаєте.

## Коли діє супровід

Під час активного супроводу на основі подорожі на екрані блокування з'являється таке повідомлення: «Супровід: розблокуйте, щоб переглянути деталі». Якщо торкнутися це повідомлення та розблокувати пристрій, ви побачите місце призначення, поточний час до прибуття, який оновлюється на основі інформації про затори та дорожні умови, а також тип даних (повний або обмежений обсяг), які надсилаються вашому контакту, якщо супровід не завершується успішно. Ви також можете скасувати супровід.

### Як розпочати супровід на основі таймера


Якщо ви не почуваетесь безпечно там, де ви зараз перебуваєте, і прагнете підтримки довіреної контактної особи через функцію «Супровід», ви можете почати супровід на основі таймера. Супровід на основі таймера сповістить довірену контактну особу, якщо ви не відповісте на запит наприкінці цього таймера.

Під час активного супроводу на основі таймера на екрані блокування з'являється таке повідомлення: «Супровід: розблокуйте, щоб переглянути деталі». Якщо торкнутися це повідомлення та відімкнути пристрій, відобразиться така інформація:

- Час, що залишився на супровід
- Вибрана вами контактна особа, яка отримує ваш запит на супровід
- Тип даних, які отримує ваша контактна особа:
  - Обмежений чи повний обсяг



Щоб розпочати супровід на основі а таймера:


1. Відкрийте програму «Повідомлення» , а потім виберіть людину, яку хочете сповістити.
2. Торкніть «Новий лист» вгорі екрана й виберіть отримувача або виберіть наявне обговорення.
3. Торкніть **+**, торкніть «Супровід», а потім торкніть «Редагувати».  
Можливо, потрібно буде торкнути елемент «Більше», щоб знайти функцію «Супровід».
4. Виберіть «Після таймера».
5. Виберіть кількість часу для таймера.

Коли супровід на основі таймера завершиться, ви отримаєте запит на завершення супроводу або додання часу. Коли супровід завершується, ваш контакт отримує сповіщення про успішне завершення. Ви також можете додати часу до свого супроводу: 15, 30 або 60 хвилин додатково. Час завершення оновиться для вашої контактної особи.

### **Як розпочати супровід на основі подорожі**

Якщо ви подорожуєте автомобілем, громадським транспортом або пішки, ви можете почати супровід з автоматичним сповіщенням друга про прибуття в заплановане місце.

Під час активного супроводу на основі подорожі на екрані блокування з'являється таке повідомлення: «Супровід: розблокуйте, щоб переглянути деталі». Якщо торкнути це повідомлення та розблокувати пристрій, ви побачите місце призначення, поточний час до прибуття, який оновлюється на основі інформації про затори та дорожні умови, а також тип даних, які надсилаються вашому контакту, якщо супровід не завершується успішно. Ви також можете скасувати супровід.

1. Відкрийте програму «Повідомлення» , а потім виберіть людину, яку хочете сповістити.
2. Торкніть «Новий лист» вгорі екрана й виберіть отримувача або виберіть наявне обговорення.
3. Торкніть **+**, торкніть «Супровід», а потім торкніть «Редагувати».  
Можливо, потрібно буде торкнути елемент «Більше», щоб знайти функцію «Супровід».
4. Виберіть «Коли я буду на місці».
5. Торкніть «Змінити» і введіть заплановане місце в полі пошуку.
6. Щоб визначити радіус місця прибуття, торкніть «Малий», «Середній» або «Великий» унизу екрана. Ваш друг отримає сповіщення про прибуття, щойно ви введете радіус.

7. Торкніть «Готово».
8. Торкніть «Автомобілем», «Громадським транспортом» або «Пішки», а потім за потреби торкніть «Додати час».

Якщо ваш пристрій не рухається до визначеного місця, ви отримаєте запит і матимете 15 хвилин на відповідь на цей запит. Якщо відповіді не буде, ваша близька людина автоматично отримає сповіщення.

Коли ваш iPhone прибуває до місця призначення під час супроводу на основі подорожі, супровід завершується й ваша контактна особа отримує оповістку про ваше прибуття.

## Виявлення небажаних трекерів

Компанія Apple розробила пристрої AirTag і мережу Локатора, щоб користувачі могли відстежувати свої речі, а також водночас могли уникати небажаного відстеження. Щоб унеможливити відстеження користувачів пристроями без їхнього відома, компанії Apple і Google створили галузевий стандарт. Завдяки цьому стандарту користувачів (iPhone, iPad, Android) можна сповіщати про відстеження.



Якщо ви відчуваєте, що ваша безпека під загрозою, зверніться до місцевої правоохоронної установи. Якщо річ є продуктом Apple, правоохоронний орган [може звернутися до Apple по інформацію, пов'язану із цією річчю](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>). Можливо, вам потрібно буде надати пристрій AirTag, AirPods, прилади з мережі Локатора, а також серійний номер пристрою.

### Сповіщення про небажане відстеження

Доступність програм для сповіщення про небажане відстеження.

- Сповіщення про небажане відстеження для пристроїв AirTag та інших приладів мережі Локатора доступні на iPhone або iPad з iOS 14.5, iPadOS 14.5 або новішими версіями.
- Сповіщення про небажане відстеження для невідомих Bluetooth-пристроїв відстеження, які сумісні з вимогами стандарту [виявлення небажаних трекерів геопозиції](#), доступні на пристроях iPhone з iOS 17.5 або новішою версією.
- Google забезпечує функцію [виявлення небажаного відстеження](#) на пристроях з Android 6.0 або новішою версією. Пристрої з попередніми версіями операційної системи можуть оновитися або використовувати [програму Tracker Detect](#).

## Увімкнення сповіщень про небажане відстеження

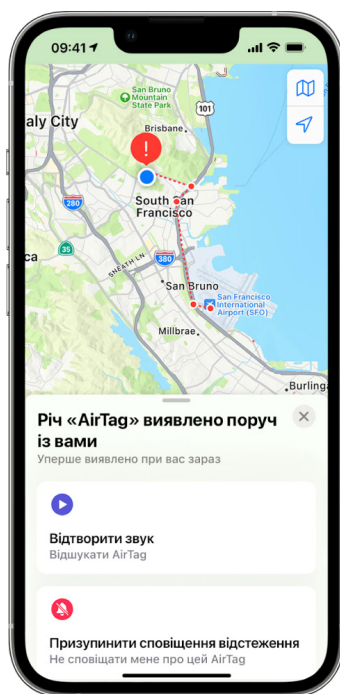
Щоб отримувати сповіщення про небажане відстеження на iPhone чи iPad з iOS 14.5, iPadOS 14.5 або новішою версією, необхідно виконати такі дії:

- Перейдіть у Параметри > Приватність і безпека > Служби локації та увімкніть параметр «Служби локації».
- Перейдіть у Параметри > Приватність і безпека > Служби локації > Системні сервіси й увімкніть параметр «Де iPhone».
- Перейдіть у Параметри > Bluetooth і увімкніть Bluetooth.
- Перейдіть у Параметри > Сповіщення, прокрутіть униз до пункту «Сповіщення відстеження», а потім увімкніть параметр «Дозволити сповіщення».
- Вимкніть режим польоту. Якщо ваш пристрій перебуває в режимі польоту, ви не отримуватимете сповіщення про відстеження.

## Якщо ви отримали сповіщення про небажане відстеження



Щоб знайти річ, скористайтеся цими порадами:

1. Торкніть сповіщення.
2. Торкніть «Продовжити», а потім торкніть «Відтворити звук» або, якщо ви поруч, торкніть «Пошук неподалік», щоб скористатися функцією «Точний пошук» для виявлення невідомої речі.



Якщо функція відтворення звуку недоступна або якщо вам не вдається знайти річ за допомогою функції «Точний пошук», можливо, цієї речі вже немає поблизу. Якщо ви вважаєте, що цей предмет усе ще поруч, пошукайте його серед своїх речей. Огляньте свій одяг, а також свої речі, де може бути цей пристрій. Пристрій може лежати там, куди ви рідко зазираєте, як-от кишеня піджака, зовнішній відділ сумки чи автомобіль. Якщо вам не вдається знайти пристрій і ви вважаєте, що ваша безпека під загрозою, знайдіть безпечне публічне місце та зверніться до правоохоронних органів.

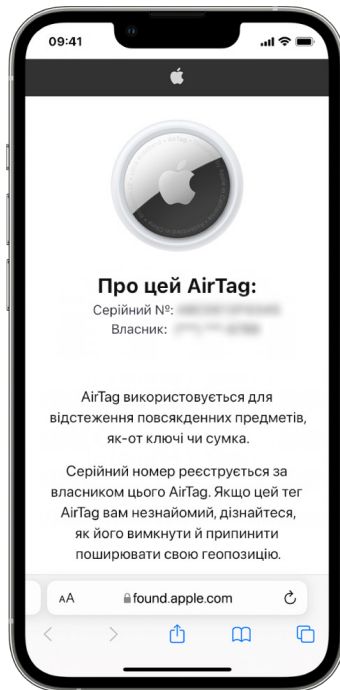
**Якщо ви раніше отримали сповіщення про небажане відстеження і хочете знову перевірити цю інформацію, виконайте одну з таких дій:**

- *На iPhone або iPad.* Відкрийте програму «Локатор» , торкніть «Речі», а потім торкніть «Невідомі речі, виявлені при вас».
- *На Mac.* Відкрийте програму «Локатор» , клацніть «Речі», а потім — «Невідомі речі, виявлені при вас».

### **Якщо ви знайшли мітку AirTag, приладдя мережі Локатора або сумісний Bluetooth-пристрій відстеження**

Щоб отримати про нього інформацію, дотримуйтеся цих указівок:

1. Піднесіть пристрій до свого iPhone, щоб з'явилося сповіщення.
2. Торкніть сповіщення. Відтак відкриється вебсайт, який надасть вам інформацію про предмет, зокрема:
  - серійний номер або ідентифікатор пристрою;
  - останні чотири цифри номера телефону або замасковану е-адресу людини, яка його зареєструвала. Це допоможе вам ідентифікувати власника, якщо він вам відомий.
3. Якщо власник позначив пристрій як загублений, можливо, ви побачите інформацію з його контактними даними.



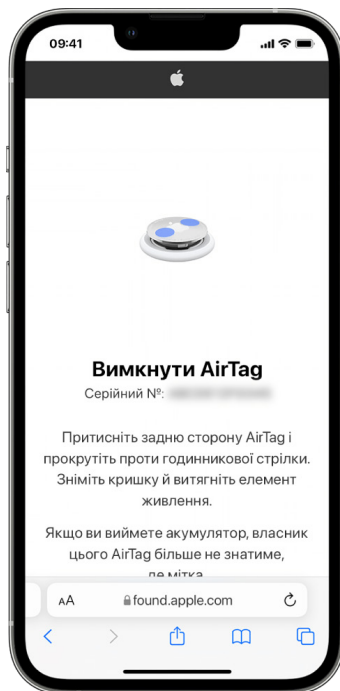
## Якщо ви переймаєтеся через імовірність відстеження вас пристроєм

▼ **ВАЖЛИВО.** Перед тим як вносити зміни, [врахуйте потенційний вплив на безпеку та приватність](#). Якщо ви відчуваєте, що ваша безпека під загрозою, зверніться до місцевої правоохоронної установи. Якщо річ є продуктом Apple, правоохоронний орган [може звернутися до Apple по інформацію, пов'язану із цією річчю](#) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>). Можливо, вам потрібно буде надати пристрій AirTag, AirPods, прилади з мережі Локатора, а також серійний номер пристрою.

1. [Зробіть знімок екрана](#) з інформацією про пристрій і його власника.
2. Вимкніть пристрій і припиніть поширення його геопозиції, торкнувшись елемент «Інструкції з вимкнення» й виконавши вказівки на екрані.
3. Якщо ви відчуваєте, що ваша безпека під загрозою, зверніться до місцевої правоохоронної установи. Якщо річ є продуктом Apple, правоохоронний орган [може звернутися до Apple по інформацію, пов'язану із цією річчю](#). Можливо, вам потрібно буде надати пристрій AirTag, AirPods, прилади з мережі Локатора, а також серійний номер пристрою.

Більше інформації в документі за адресою <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>.

Після вимкнення пристрою його власник більше не зможе дізнаватися про його поточне розташування. Ви також більше не отримуватимете жодних сповіщень про небажане відстеження для цієї речі.



## Пошук міток AirTag або приладдя мережі Локатора за допомогою пристрою Android

Дивіться [сторінку служби підтримки «Як знаходити невідомі трекери»](https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&), щоб отримати більше інформації про перевірку на небажане стеження на пристроях Android. ([https://support.google.com/android/answer/13658562?visit\\_id=638525910154486952-839086324&](https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&))

### Якщо ви чуєте, як мітка AirTag подає звук

Під час переміщення будь-яка мітка AirTag, відокремлена на певний час від її власника, подає звуковий сигнал, щоб сповістити людей поблизу. Якщо ви знайшли мітку AirTag, почувши її звуковий сигнал, можете скористатися будь-яким пристроєм, який підтримує технологію комунікації ближнього поля (NFC), наприклад iPhone або телефоном Android, щоб перевірити, чи власник позначив її як втрачену, і допомогти повернути її.

**⚠️ ВАЖЛИВО.** Якщо ви відчуваєте, що ваша безпека під загрозою, ви можете звернутися до місцевих правоохоронних органів, [які можуть співпрацювати з Apple](https://www.apple.com/legal/transparency/government-information.html) (<https://www.apple.com/legal/transparency/government-information.html>). Можливо, вам потрібно буде надати мітку AirTag або її серійний номер.

### Пристрої, під'єднані до вашого облікового запису Apple

Якщо ви намагаєтеся налаштувати AirPods, AirTag чи інший прилад мережі Локатора й відображається повідомлення про те, що цей пристрій чи річ сполучено з іншим обліковим записом Apple, необхідно спершу вилучити їх з того облікового запису Apple. Докладніше про вилучення чи відлучення речі або пристрою, а також про налаштування їх з іншим обліковим записом Apple, дивіться в статті служби підтримки Apple [«Якщо аксесуар або пристрій пов'язано з іншим Обліковим записом Apple»](https://support.apple.com/102620) (<https://support.apple.com/102620>).

### Спільний доступ до AirTag

Функція «Спільний доступ до речі» дає змогу власникам міток AirTag спільно використовувати річ одночасно з п'ятьма іншими людьми. Позичальники можуть:

- Бачити розташування AirTag у Локаторі.
- Використовувати «Точний пошук» для пошуку AirTag.
- Відтворювати звук, якщо AirTag загубиться.
- Отримувати сповіщення про приєднання інших людей до групи спільного користування.
- Бачити облікові записи Apple інших учасників або контактну інформацію, якщо інший учасник належить до їхніх контактів.

*Примітка.* Позичальники не можуть бачити, у кого зараз AirTag.


Оскільки всі учасники групи спільного доступу можуть бачити розташування AirTag, сповіщення про небажане стеження для цього AirTag приглушуються для всіх учасників групи. Коли хтось полишає групу спільного доступу або коли власник речі вилучає їх із групи, вони не можуть бачити розташування AirTag, а сповіщення про небажане відстеження відновлюються.

Докладніше дивіться в розділі [Спільний доступ до AirTag або іншого елемента в Локаторі на iPhone](https://support.apple.com/guide/iphone/iph419cc5f28) у посібнику користувача iPhone. (<https://support.apple.com/guide/iphone/iph419cc5f28>)

## Як вилучити себе з групи спільного доступу


Якщо ви хочете вилучити себе з групи спільного доступу, можете скористатися Локатором або функцією «Перевірка безпеки».

**ПОПЕРЕДЖЕННЯ.** Вилучивши себе, ви не зможете бачити розташування AirTag, а сповіщення про небажане відстеження відновляться. Перш ніж вилучити себе з групи спільного доступу, може бути потрібно перевірити, чи AirTag поблизу.

1. Перейдіть у Параметри  > Приватність і безпека > Перевірка безпеки.
2. Торкніть «Керування поширенням і доступом».
3. Торкніть Речі > Припинити спільне користування.


## Використання Локатора

Щоб вилучити себе за допомогою Локатора, виконайте такі дії:

1. Відкрийте програму «Локатор» .
2. Торкніть «Речі», а потім торкніть пристрій, від якого ви хочете себе відлучити.
3. Торкніть «Вилучити».


## Використання функції «Перевірка безпеки»

Щоб вилучити себе за допомогою функції «Перевірка безпеки», виконайте такі дії:

1. Торкніть Параметри  > Приватність і безпека > Перевірка безпеки.
2. Торкніть «Керування поширенням і доступом».
3. Торкніть Речі > Припинити спільне користування.

## Вилучення інших учасників із групи спільного доступу за допомогою Локатора

Якщо ви є власником, ви можете вилучити інших учасників із групи спільного доступу за допомогою Локатора.

1. Відкрийте програму «Локатор» .
2. Торкніть елемент «Речі», а потім торкніть назву предмета.
3. Торкніть ім'я учасника, якого потрібно вилучити.
4. Торкніть Вилучити > Припинити спільне користування.

## Вилучення інших учасників із групи спільного доступу за допомогою функції «Перевірка безпеки»

Якщо ви є власником, ви можете вилучити інших учасників із групи спільного доступу за допомогою функції «Перевірка безпеки».

1. Торкніть Параметри > Приватність і безпека > Перевірка безпеки.
2. Торкніть Керування поширенням і доступом > Продовжити.
3. Торкніть ім'я людини, для якої потрібно припинити спільний доступ, а потім — «Перевірити, що поширюється».
4. Торкніть «Речі», а потім торкніть «Припинити спільне користування».



## Локатор і поширення геопозиції

Програма Локатор для iPhone, iPad, Mac і Apple Watch дає вам змогу стежити за пристроями й поширювати для інших свою геопозицію.





Якщо ви налаштували «Сімейний доступ» і поширюєте свою геопозицію, члени вашої родини автоматично з'являться на вкладці «Люди», хоча вони все одно мають явним чином поділитися своєю геопозицією з вами. Перегляньте розділ [«Керування параметрами Сімейного доступу»](#) далі в цьому посібнику.





## Подобиці поширеної геопозиції та де їх можна переглянути

Коли ви ділитеся своєю геопозицією з іншими людьми через програму «Локатор», вони можуть переглядати цю інформацію у своїх програмах, список яких наведено нижче.

Якщо і у вас, і в людини, для якої ви поширюєте геопозицію, є iPhone з iOS 15 або новішою версією, також поширюється геопозиція наживо в усіх програмах, список яких наведено нижче. Якщо ви рухаєтеся, інші люди знатимуть ваш приблизний напрямок руху та швидкість.






Програма	Опис
 Локатор	У програмі «Локатор» інші люди можуть бачити ваше розташування, перейшовши на вкладку «Люди» й торкнувши ваше ім'я.
 Локатор	Якщо і у вас, і в людини, для якої ви поширюєте геопозицію, є iPhone 15 і ви перебуваєте поблизу, ви можете за допомогою функції «Точний пошук» дізнатися точну геопозицію одне одного. Коли ви будете поблизу цієї людини, функція «Точний пошук» допомагатиме їй знайти вас із точністю в кілька метрів. Якщо хтось намагатиметься знайти вас за допомогою функції «Точний пошук», ви отримаєте відповідне сповіщення.  Докладніше дивіться в розділі <a href="#">Використання функції «Точний пошук» на iPhone 15 для зустрічі з другом</a> в посібнику користувача iPhone. ( <a href="https://support.apple.com/guide/iphone/iph3effd0ed6">https://support.apple.com/guide/iphone/iph3effd0ed6</a> )

Програма	Опис
 Локатор	Якщо ви налаштували Сімейний доступ і поширюєте свою геопозицію, члени вашої родини автоматично з'являться на вкладці «Люди», однак поширення геопозиції не почнеться, доки ви не надасте доступ до геопозиції одне одному. Дивіться розділ <a href="#">Керування параметрами «Сімейного доступу»</a> далі в цьому посібнику.
 Повідомлення	Коли інші люди, для яких ви поширили свою геопозицію, торкають вашу іконку контакту в Повідомленнях, вони переходять у подання «Деталі», де можна побачити вашу поточну геопозицію, яка поширюється через Локатор.
 Повідомлення	У Повідомленнях в iOS 17 та iPadOS 17 або новіших версіях інші люди, для яких ви поширили свою геопозицію, можуть також бачити ваше приблизне розташування вгорі гілки в Повідомленнях.
 Карти	Коли інші люди, для яких ви поширили свою геопозицію, шукають вас за іменем у Картах, на своїй карті вони бачитимуть вашу поточну геопозицію, яка поширюється через Локатор.

## Сповіщення про зміну геопозиції

Програму «Локатор» можна використовувати, [щоб повідомити друга про зміну свого місця](https://support.apple.com/guide/iphone/iph9bfec93b1) (https://support.apple.com/guide/iphone/iph9bfec93b1). Люди, з якими ви ділитесь своєю геопозицією, також можуть налаштувати сповіщення про зміну вашої геопозиції.


Ви можете вимкнути будь-які сповіщення про зміну вашої геопозиції. Це стосується як налаштованих вами сповіщень, так і сповіщень, створених вашими друзями.


- Щоб переглянути всі сповіщення, що стосуються вас, виконайте одну з таких дій:
  - На iPhone або iPad.* Відкрийте програму «Локатор» , потім торкніть «Я».
  - На Mac.* Відкрийте програму «Локатор» , клацніть «Я», а потім натисніть .
- Знайдіть розділ «Сповіщення про вас».
  - Якщо ви *бачите* розділ «Сповіщення про вас», виберіть ім'я, щоб переглянути докладнішу інформацію.
  - Якщо ви *не бачите* розділ «Сповіщення про вас», ви не сповіщаєте коли ваша геопозиція змінюється.
- Якщо ви бачите сповіщення, яке потрібно видалити, виберіть ім'я, а потім виберіть сповіщення.
- Видаліть сповіщення, а потім підтвердьте цю дію.

## Як припинити поширення геопозиції в Локаторі на iPhone або iPad

Коли ви припиняєте поширення за допомогою одного з наведених нижче способів, відомості про вашу геопозицію зникають у програмах «Локатор», «Карти», «Контакти» й «Повідомлення» на пристроях інших людей.



**ВАЖЛИВО.** Коли ви припиняєте поширення геопозиції, люди, для яких ви раніше її поширювали, можуть це помітити. У попередніх версіях операційних систем вони можуть отримати сповіщення в Повідомленнях про те, що ви припинили поширення.

1. Відкрийте програму «Локатор» .
2. Виконайте одну з таких дій:
  - *Припинення поширення для однієї людини.* Виберіть вкладку «Люди», знайдіть людину, для якої потрібно зупинити поширення, і торкніть її ім'я, а потім прокрутіть сторінку вниз і торкніть «Сховати мою геопозицію».
  - *Припинення поширення для всіх.* Виберіть вкладку «Я», а потім вимкніть «Поширити мою геопозицію».

*Примітка.* Якщо програму «Локатор» видалено з вашого пристрою, ви можете вимкнути служби локації (перейдіть у меню Параметри  > Приватність і безпека > Служби локації), щоб упевнитися в тому, що геопозиція не поширюється. Відтак викачайте програму «Локатор» знову з App Store.


## Як припинити поширення геопозиції в Повідомленнях на iPhone або iPad

Коли ви зупиняєте поширення за допомогою одного з наведених нижче способів, відомості про вашу геопозицію зникають у програмі «Повідомлення» на пристроях інших людей.


1. Відкрийте програму «Повідомлення» .
2. Виконайте одну з таких дій:
  - *Припинення поширення повідомлень в обговоренні.* Виберіть обговорення з людиною, для якої потрібно припинити поширення, торкніть її ім'я вгорі обговорення, а потім торкніть «Вимкнути поширення».
  - *Припинення поширення шляхом видалення обговорення.* У списку обговорень програми «Повідомлення» проведіть ліворуч по обговоренню, торкніть , а потім торкніть «Так», щоб підтвердити припинення поширення геопозиції для учасників обговорення.

## Як припинити поширення геопозиції в Контактах на iPhone або iPad

Коли ви зупиняєте поширення за допомогою одного з наведених нижче способів, відомості про вашу геопозицію зникають у програмі «Контакти» на пристроях інших людей.

1. Відкрийте програму «Контакти» .
2. Торкніть ім'я людини.
3. Торкніть «Сховати мою адресу».


## Коли вимикати функцію «Де iPhone» для втраченого чи вкраденого пристрою

Функція «Де iPhone» (у меню Параметри  > Локатор) допомагає вам знайти телефон, якщо його втрачено чи вкрадено.



Коли ввімкнено функцію «Де iPhone», ваш пристрій може відобразитися в мережі Локатора протягом щонайбільше 24 годин після вимкнення живлення або від'єднання від інтернету. Відомості про місцезоположення вашого пристрою доступні в розділі «Локатор» на вкладці «Пристрої» на ваших інших пристроях, а також усім учасникам групи сімейного доступу, яким ви надали доступ до своєї геопозиції.

Якщо вам потрібно дістатися до безпечного місця й ви хочете вимкнути свій пристрій, але вас турбує, що хтось інший може використовувати цю функцію для визначення вашої геопозиції, ви можете тимчасово вимкнути функцію «Мережа Локатора», коли вимикаєте живлення пристрою. Для цього торкніть «iPhone можна знайти навіть після вимкнення» (у розділі «Вимкнути») і дотримуйтесь інструкцій на екрані. Скористайтеся наведеною нижче процедурою, якщо необхідно вимкнути цю функцію.

**ПОПЕРЕДЖЕННЯ.** Якщо ви вимкнете функцію «Де [пристрій]» та мережу Локатора, ви не зможете знайти й заблокувати пристрій та стерти з нього дані в разі його крадіжки або втрати.

- На iPhone або iPad. Перейдіть у Параметри  > [ваше ім'я] > Локатор > Де iPhone > Мережа Локатора.


У разі вимкнення цієї функції ви не зможете використовувати її, якщо ваш пристрій буде втрачено або вкрадено й вимкнено.

- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , клацніть iCloud, а потім клацніть «Опції» біля пункту «Де Mac».
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , клацніть iCloud, потім клацніть «Опції» біля пункту «Де Mac».

## Керування параметрами Служби локації

Служби локації дають вам змогу вибирати програми (як-от Карти, Камера, Погода й інші) та вебсайти, для яких ви хочете поширювати свою геопозицію. Коли їх увімкнено, Служби локації використовують інформацію з різноманітних мереж для визначення вашої приблизної або точної геопозиції. Служби локації є на iPhone, iPad, Mac і Apple Watch.



Коли програма використовує Служби локації, іконка Служб локації  з'являється на iPhone та iPad (на смужці статусу вгорі екрана) та на Mac (на смужці меню).

Навіть якщо вимкнути Служби локації, сторонні програми й вебсайти все одно зможуть визначати ваше розташування в інші способи. Однак із міркувань безпеки дані про геопозицію вашого пристрою можуть бути використані для екстрених викликів, щоб сприяти рятувальним заходам незалежно від того, чи увімкнено Служби локації.

### Увімкнення або вимкнення Служб локації



Під час налаштування пристрою відобразиться запит на увімкнення Служб локації. Після налаштування Служб локації їх можна увімкнути або вимкнути в будь-який момент.

- *На iPhone або iPad.* Перейдіть у Параметри  > Приватність і безпека > Служби локації, а потім увімкніть або вимкніть поширення геопозиції.
- *На Mac з macOS 13 або новішою версією.* Виберіть меню Apple , виберіть «Системні параметри», клацніть «Приватність і безпека» , клацніть «Служби локації», увімкніть або вимкніть параметр «Служби локації», введіть свій пароль, а потім клацніть «Відімкнути».
- *На Mac з macOS 12 або попередньою версією.* Виберіть меню Apple , виберіть «Системні параметри», клацніть «Безпека та приватність» , а потім клацніть «Приватність». Клацніть «Служби локації». Якщо внизу ліворуч відображається значок замкненого замка , клацніть його, щоб відкрити панель параметрів. Увімкніть або вимкніть параметр «Служби локації».
- *На Apple Watch.* Перейдіть у Параметри  > Приватність і безпека > Служби локації.

## Увімкнення Служб локації

Під час налаштування пристрою відобразиться запит на увімкнення Служб локації. Після налаштування Служб локації їх можна увімкнути або вимкнути в будь-який момент.

Якщо під час налаштування ви не увімкнули Служби локації:


- *На iPhone або iPad.* Перейдіть у Параметри  > Приватність і безпека > Служби локації та увімкніть параметр «Служби локації».
- *На Mac з macOS 13 або новішою версією.* Виберіть меню Apple , виберіть «Системні параметри», клацніть «Приватність і безпека» , клацніть «Служби локації», увімкніть параметр «Служби локації», введіть свій пароль, а потім клацніть «Відімкнути».
- *На Mac з macOS 12 або попередньою версією.* Виберіть меню Apple , виберіть «Системні параметри», клацніть «Безпека та приватність» , а потім клацніть «Приватність». Клацніть «Служби локації». Якщо внизу ліворуч відображається значок замкненого замка , клацніть його, щоб відкрити панель параметрів, а потім виберіть «Увімкнути Служби локації».

## Визначення програм, які можуть використовувати Служби локації, на iPhone та iPad

Деякі програми можуть не працювати, якщо не увімкнути Служби локації. Коли програма вперше потребуватиме доступу до інформації зі служб локації, ви отримаєте відповідний запит. Виберіть одну з опцій:

- Дозволити один раз
- Дозволяти за використання
- Не дозволяти






Ви також можете переглянути або змінити доступ до своєї геопозиції для окремих програм і зазначити, як часто вони можуть використовувати вашу геопозицію. Далі наведено інструкції для iPhone або iPad.

1. Перейдіть у Параметри  > Приватність і безпека > Служби локації, а потім перегляньте або змініть параметри доступу для програми.  
Щоб побачити пояснення щодо запитів на місцеперебування, торкніть програму.
2. Визначте, наскільки інші програми повинні мати до доступу до інформації про ваше місцезнаходження.
  - Щоб дозволити програмі використовувати вашу точну геопозицію, залиште параметр «Точна геопозиція» увімкненим.
  - Щоб поширити лише свою приблизну геопозицію (цього може бути достатньо для програми, якій не потрібне ваше точне місцезнаходження), можна вимкнути опцію «Точна геопозиція».

*Примітка.* Якщо ви налаштуєте доступ для програми на «Питати наступного разу», вам буде запропоновано знову увімкнути Служби локації, коли наступного разу програма спробує ними скористатися.

## Укажіть, які програми можуть використовувати Служби локації на Mac

1. Виконайте одну з таких дій:


- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , клацніть Системні параметри, клацніть «Приватність і безпека» , клацніть «Служби локації», вимкніть «Служби локації», введіть свій пароль, а потім клацніть «Відімкнути».
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple  > Системні параметри > Безпека та приватність  > Служби локації, а потім скасуйте вибір параметра «Увімкнути Служби локації». Для внесення змін може бути потрібно спочатку розблокувати Системні параметри. Для цього натисніть  в нижньому лівому куті, а потім введіть свій пароль.

2. Установіть прапорець біля програми, щоб дозволити їй використовувати Служби локації. Зніміть прапорець, щоб вимкнути Служби локації для цієї програми.

Якщо Служби локації вимкнено для певної програми, вам буде запропоновано увімкнути їх знову, коли ця програма спробує скористатися даними про ваше розташування.

3. Прокрутіть до низу списку програм, щоб відкрити системні служби, а потім натисніть кнопку «Деталі», щоб побачити конкретні системні служби, які використовують вашу геопозицію.

Щоб дозволити програмам «Пропозиції Siri» та «Пропозиції Safari» використовувати геопозицію вашого Mac, виберіть «Пропозиції за місцем».

Щоб дозволити вашому Mac визначати важливі для вас місця та надавати корисну пов'язану інформацію в «Картах», «Календарі», «Нагадуваннях» тощо, виберіть «Важливі місця». Важливі геопозиції зашифровані та не можуть бути прочитані Apple. Натисніть «Деталі», щоб переглянути список визначених геопозицій. Щоб вилучити геопозицію зі списку, виберіть її та натисніть —. Щоб вилучити всі геопозиції, натисніть , а потім клацніть «Очистити історію».





# Керування автоматичним доступом до ОЧП на Картах

У Картах на iPhone та iPad (Wi-Fi + стільникові моделі) ви можете автоматично поширювати орієнтовний час прибуття (ОЧП) до улюбленого місця для будь-кого з ваших Контактів. Налаштувавши цю функцію пам'ятайте, що під час кожного відвідування улюблених місць ваш очікуваний час прибуття поширюється для ваших контактів. Вирушивши в дорогу, унизу екрана буде зазначено, що ви ділитесь очікуваним часом прибуття з іншими людьми.





## Керування поширенням ОЧП на iPhone або iPad

1. У програмі «Карти»  на своєму iPhone або iPad (Wi-Fi + стільникові моделі) торкніть свій профіль праворуч від поля пошуку.
2. Виберіть «Улюблені», щоб відкрити вікно з усіма своїми улюбленими місцями.
3. Торкніть  поряд з улюбленим цікавим місцем.
4. Прокрутіть униз до розділу «Поширити ОЧП», щоб переглянути імена людей, для яких автоматично поширюється ОЧП.
5. Щоб вилучити когось, торкніть кнопку «Зупинити поширення ОЧП» поряд з іменем людини, яку ви хочете вилучити.
6. Щоб додати когось, торкніть «Додати людину», а потім у Kontakтах виберіть людину, для якої ви хочете автоматично поширювати ОЧП до цього цікавого місця.
7. Повторіть кроки 3–6 для всіх додаткових цікавих місць з розділу «Улюблені».

## Як зупинити автоматичне поширення ОЧП після початку навігації

Ви можете зупинити автоматичне поширення ОЧП навіть після переходу до розділу «Улюблені». Якщо так зупинити поширення свого ОЧП, людина отримує сповіщення на своєму пристрої про ваш рух до вибраного улюбленого місця, однак вона більше не матиме доступу до інформації про ваш ОЧП або маршрут.

 **ВАЖЛИВО.** Цей метод не вимикає назавжди автоматичне поширення для цієї людини. Коли ви знову вирушите до того самого улюбленого місця, автоматичне поширення ОЧП почнеться знову. Щоб запобігти цьому, ви повинні вилучити контакт у розділі «Ширити ОЧП» в улюблених.

1. У програмі «Карти»  на своєму iPhone чи iPad (Wi-Fi + стільникові моделі), торкніть «Поширення для [ім'я контакту]» внизу екрана.
2. Знайдіть у списку людину, з якою ви більше не хочете ділитися своїм ОЧП.
3. Виберіть «Торкніть, щоб зупинити» під іменем людини.

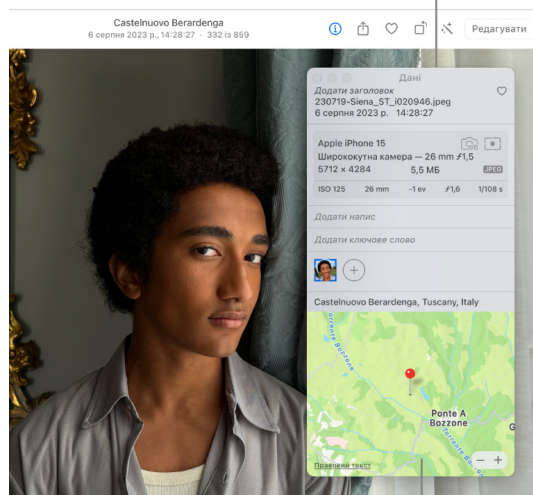
# Керування метаданими геопозиції у Фотографіях

Якщо для програми «Камера» ввімкнено Служби локації, вони використовують інформацію, відому як метадані, зібрану з мереж стільникового зв'язку, Wi-Fi, GPS та Bluetooth, для визначення координат місця зйомки фото або відео. Ці координати додаються до кожного фото і відео, то ж згодом ви можете виконувати пошук у програмі «Фотографії» за місцем зйомки або переглядати колекції в альбомі «Місця» на основі геопозиції.

Коли фотографії та відео з метаданими геопозиції поширюються, люди з доступом до цих відомостей можуть отримати доступ до метаданих і дізнатися, де було зроблено зйомку. Якщо вас турбує те, що хтось має доступ до метаданих геопозиції для ваших фото чи відео, ви можете вилучити поточні метадані та припинити їх збір у майбутньому.


## Перегляд фото, які містять метадані геопозиції, на iPhone або iPad

Використовуйте вікно «Досьє» для перегляду або змінення інформації про фотографію.





Якщо фотографія містить інформацію GPS, місце зйомки фотографії відображається у вікні «Досьє».

Можна скористатися альбомом «Місця» у програмі «Фотографії», щоб легко переглянути, які фото у вашій фототеці мають вбудовані метадані геопозиції.

1. Відкрийте програму «Фотографії» , а потім торкніть «Альбоми».
2. Торкніть альбом «Місця», а потім виконайте будь-які з таких дій:
  - Щоб переглянути фотографії за певний період, торкніть «Сітка», щоб відобразити їх у хронологічному порядку.
  - Щоб переглянути фото за місцем зйомки, торкніть «Карта», щоб переглянути за геопозицією.



## Перегляд фото, які містять метадані геопозиції, на Mac

Можна скористатися альбомом «Місця» у програмі «Фотографії», щоб легко переглянути, які фото у вашій фототеці мають вбудовані метадані геопозиції.

1. У програмі «Фотографії»  на Mac виберіть фото, які ви хочете переглянути.
2. Клацніть , а потім перегляньте інформацію про геопозицію.

## Вилучення метаданих геопозиції у Фотографіях на iPhone або iPad


Щоб вилучити метадані геопозиції з певного фото.

1. Відкрийте програму «Фотографії» , а потім торкніть «Альбоми».
2. Торкніть альбом «Місця», а потім виконайте одну з наведених нижче дій:
  - Щоб переглянути фотографії за певний період, торкніть «Сітка», щоб відобразити їх у хронологічному порядку.
  - Щоб переглянути фото за місцем зйомки, торкніть «Карта», щоб переглянути за геопозицією.
3. Відкрийте фото, з якого потрібно вилучити метадані геопозиції, а тоді торкніть  або проведіть угору.

У програмі «Карти» з'явиться зображення, що показує місце зйомки.
4. Щоб вилучити метадані геопозиції, торкніть «Змінити», а тоді торкніть «Вилучити геопозицію».


## Вилучення метаданих геопозиції у Фотографіях на Mac

Щоб вилучити метадані геопозиції з фотографій:

1. У програмі «Фотографії»  на Mac виберіть фото, які ви хочете змінити.
2. Виберіть Зображення > Геопозиція, а потім виберіть «Сховати місце» або «Назад до вихідного місця».

## Припинення збору метаданих геопозиції у Камері на iPhone або iPad




Метадані геопозиції для фото і відео можуть збиратися, лише якщо програма «Камера» має доступ до Служб локації.

- Перейдіть у «Параметри» , торкніть Приватність і Безпека > Служби локації > Камера, а тоді торкніть «Ніколи».

Якщо ви не хочете повністю припинити збір метаданих геопозиції, можна натомість вимкнути опцію «Точна геопозиція». Це дозволить програмі «Камера» збирати дані про ваше приблизне розташування замість точної геопозиції.

## Поширення фото у програмі «Фотографії» на iPhone або iPad без поширення метаданих геопозиції

Ви можете поширювати фото, не поширюючи при цьому інформацію про місце його зйомки.

1. Виконайте будь-які з таких дій:
  - Відкрийте програму «Камера» , виберіть фотоплівку, а тоді виберіть одне або декілька фото для поширення.
  - Відкрийте програму «Фотографії» , а тоді виберіть одне або декілька фото для поширення.
2. Торкніть , а потім торкніть «Опції».
3. Вимкніть опцію «Геопозиція», а потім торкніть «Готово».
4. Поширте фото за допомогою одного із способів у меню поширення.

# Керування вмістом

## Загальні відомості

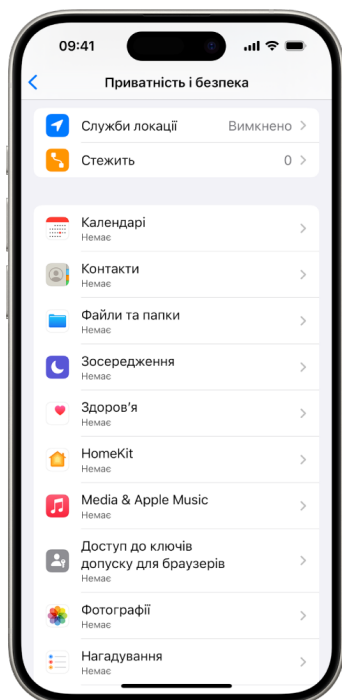
### Функції приватності програм у продуктах Apple



Apple надає параметри, функції й елементи керування, які допомагають переглядати й керувати даними, які ви поширюєте в програмах.



## Перегляд і оновлення параметрів приватності програм на пристроях Apple

Параметри приватності на вашому пристрої були ретельно розроблені, щоб ви могли контролювати свої дані. Наприклад, ви можете дозволити програмі соціальної мережі використовувати вашу камеру, щоб можна було робити та завантажувати фотографії в цю програму. Однією із ситуацій, коли слід переглянути ці налаштування, є ситуація, коли хтось інший налаштував ваш пристрій або мав до нього доступ і знає ваш пароль. У такій ситуації слід переконаватися, що інша людина не змінила ваші налаштування.



1. Виконайте одну з таких дій:
  - На iPhone або iPad. Перейдіть у Параметри  > Приватність і безпека .
  - На Mac з macOS 13 або новішою версією. Виберіть меню Apple , клацніть «Системні параметри», а потім виберіть «Приватність і безпека» на бічній панелі.
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , клацніть «Системні параметри», клацніть «Вхід і безпека», а тоді — «Приватність».
2. Перегляньте перелік типів даних (наприклад, Календарі, Контакти, Фотографії, Нагадування тощо).


3. Виберіть тип даних зі списку, щоб побачити, які програми на пристрої мають доступ до них.

Програма не з'явиться в списку, доки не відобразиться запит на дозвіл, водночас ви можете надати або видалити дозвіл для будь-якої програми, що вимагала доступу. Для фотографій також можна змінити доступ, наданий програмам. Програма може використовувати тип даних у налаштуваннях, лише якщо ви надали їй дозвіл.

*Примітка.* Зміна параметрів приватності на пристрої Apple змінить лише спосіб доступу цих програм до ваших даних. Якщо треба змінити параметри «Приватність і безпека» для сторонньої програми, створеної не компанією Apple, увійдіть до облікового запису третьої сторони (через відповідну програму або браузер) та оновіть параметри звітти.

### **Використання функції «Відстеження в програмах»**


Функція «Відстеження в програмах» дозволяє визначити, чи дозволяти програмі відстежувати ваші дії в програмах і на вебсайтах сторонніх розробників. Ви можете відкликати дозволи відстежувати ваші дії в будь-який момент. Якщо вимкнути параметр «Запити на відстеження», ви не отримуватимете запитів від програм, які намагаються відстежувати вашу активність. Програма, яка запитує дозвіл на відстеження, коли ця опція вимкнена, отримує відповідь «Просити програму не стежити».

- Виконайте одну з таких дій:
  - На iPhone або iPad. Перейдіть у Параметри  > Приватність і безпека > Відстеження, а тоді вимкніть параметр «Запити на відстеження».
  - На Apple TV. Перейдіть у Параметри > Загальні > Приватність і безпека > Відстеження, а потім вимкніть параметр «Запити на відстеження».

### **Перегляд доступу програм до ваших даних у Звіті про приватність програм**

Якщо ви стурбовані тим, що хтось із ваших близьких інстальював програми або змінив параметри програм на вашому iPhone або iPad без вашого дозволу, ви можете увімкнути «Звіт про приватність програм».

Ви знайдете детальну інформацію про те, як часто кожна програма отримує доступ до ваших даних (наприклад вашого місцезнаходження, камери та мікрофона).

1. Перейдіть у Параметри  > Приватність і безпека.
2. Прокрутіть униз і торкніть «Звіт про приватність програм».
3. Увімкніть «Звіт про приватність програм».

Звіт про приватність програм можна вимкнути будь-коли в меню Параметри > Приватність і безпека > Звіт про приватність програм. При цьому дані звіту будуть видалені з вашого пристрою.

*Примітка.* «Звіт про приватність програм» починає збирати інформацію лише після ввімкнення, тому може знадобитися деякий час, перш ніж з'являться відомості. У процесі користування програмами на своєму пристрої ви побачите більше даних. Дані у «Звіті про приватність програм» шифруються та зберігаються лише на вашому пристрої. У звіті зазначається, скільки разів і коли програма отримувала доступ до конфіденційних даних або датчиків пристрою за останні 7 днів. Ви можете торкнути кожен програму та тип даних, щоб дізнатися більше.



## Перегляд і видалення програм

Якщо вас турбує те, що хтось міг установити програму на ваш пристрій без вашого дозволу, ви можете переглянути список своїх програм, щоб упевнитися, що серед них немає нічого небажаного (інструкції починаються в наступному розділі нижче).

Якщо ви не знаєте напевне, для чого призначена якась програма, ви можете знайти її в App Store.

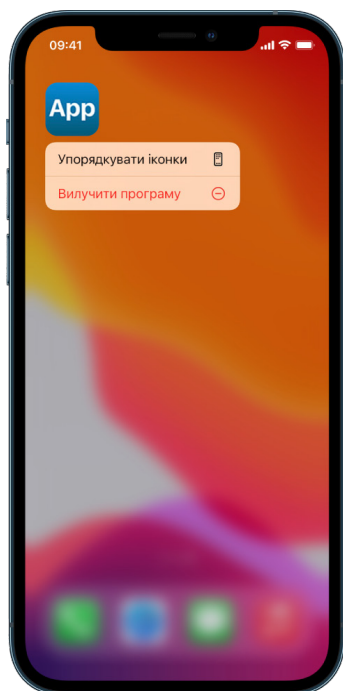
Ви можете переглянути і змінити тип даних, до яких кожна програма має доступ (наприклад, геопозиція, фотографії тощо). Це можна зробити за допомогою функції [«Перевірка безпеки»](#) в iOS 16 і новіших версіях.

Ви також можете переглянути [параметри сторонніх програм](#), які доступні лише в програмах, якими не можна керувати через Apple.

**⚠️ ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, [врахуйте потенційний вплив на безпеку](#) та приватність.



## Як видалити програму з бібліотеки програм на iPhone чи iPad



1. Перейдіть на головний екран, змахом прогорніть всі сторінки до бібліотеки програм.
2. Торкніть у полі пошуку. Буде відображено список усіх програм на пристрої в алфавітному порядку.
3. Якщо ви побачите програму, яку хотіли б вилучити, торкніть і утримуйте її іконку, доки не з'явиться меню.
4. Торкніть «Видалити програму», щоб видалити її.

Докладніше дивіться в розділі [Вилучення або видалення програм з iPhone](https://support.apple.com/guide/iphone/iph248b543ca) у посібнику користувача iPhone. (<https://support.apple.com/guide/iphone/iph248b543ca>)


### Як видалити програму з початкового екрана

1. Торкніть і утримуйте програму на початковому екрані.
2. Торкніть «Вилучити програму», а потім — «Видалити програму», щоб видалити її.

Докладніше дивіться в розділі [Вилучення або видалення програм з iPhone](https://support.apple.com/guide/iphone/iph248b543ca) у посібнику користувача iPhone (<https://support.apple.com/guide/iphone/iph248b543ca>)

## Видалення програми з Mac

Ви можете видалити програми, які, можливо, було викачано й встановлено з інтернету або із зовнішнього пристрою, наприклад USB-пристрою.

1. Клацніть іконку Finder  у Dock, потім клацніть «Програми» на бічній панелі Finder.
2. Виконайте одну з таких дій:
  - *Якщо програма в папці.* Відкрийте папку програми, щоб перевірити наявність деінсталлятора. Якщо відображається «Видалити [програму]» або «Деінсталлятор [програми]», двічі клацніть цей пункт, а потім дотримуйтесь інструкцій на екрані.
  - *Якщо програми немає в папці або немає деінсталлятора.* Якщо програми немає в папці або немає деінсталлятора. Перетягніть програму з папки «Програми» в «Смітник» (в кінці Dock).

**ЗАСТЕРЕЖЕННЯ.** Програму буде остаточно видалено з вашого Mac наступного разу, коли ви або Finder очистите Смітник. Якщо у вас є файли, створені за допомогою цієї програми, можливо, ви не зможете відкрити їх знову. Якщо ви вирішите зберегти програму, поверніть її, перш ніж очищати Смітник. Виберіть програму в Смітнику, потім виберіть Файл > Повернути назад.

Щоб видалити програми, завантажені з App Store, скористайтеся Launchpad.

## Параметри сторонніх програм

### Основні відомості про сторонні програми


В екосистемі Apple усі програми належать до двох категорій:

- *Власні програми.* Розроблені компанією Apple, як-от «Повідомлення», «Календар», Safari або FaceTime.
- *Сторонні програми.* Розроблені компаніями й організаціями, відмінними від Apple, як-от Instagram, YouTube, Threads чи Google.

Сторонні програми доступні в App Store або альтернативних магазинах програм. Параметри облікових записів та елементи керування в них можуть відрізнятися порівняно з програмами, розробленими Apple, а деякі із цих елементів керування можуть бути доступні лише в програмі або на вебсайті розробника сторонньої програми. Ця відмінність є важливою, оскільки для керування параметрами поширення та приватності сторонніх програм зазвичай потрібні додаткові дії.

### Параметри Apple для сторонніх програм

Деякими параметрами сторонніх програм можна керувати в програмі «Параметри». До них, зокрема, належать функціональні можливості пристрою Apple, до яких така програма може мати доступ і які може використовувати. Це може бути доступ до геопозиції, контактів і фотографій або здатність надсилати сповіщення.

Щоб керувати цими параметрами, відкрийте Параметри , прокрутіть униз, а потім торкніть відповідну програму.

### Параметри сторонніх програм, доступні лише в програмі

Параметрами деяких сторонніх програм не можна керувати через Apple — це можна робити лише безпосередньо в програмі. Щоб керувати параметрами сторонньої програми, що визначають те, як вона надає доступ до інформації іншим особам, відкрийте цю програму й перейдіть до параметрів облікового запису. Ці параметри можуть бути в розділі з назвою на кшталт «Параметри» чи «Налаштування», а деякі з них можуть бути в інших розділах параметрів облікового запису. Важливо перевірити будь-які параметри, що стосуються безпеки, захисту, приватності, поширення даних і можливості виявлення. Для деяких програм, щоб знайти всі доступні для керування параметри, буде необхідно виконати пошук статей служби підтримки чи відповідей на поширені запитання.

*Примітка.* У деяких випадках певні параметри, як-от видалення облікового запису або надсилання запиту на копію ваших даних, можуть бути доступні лише на вебсайті розробника сторонньої програми. Якщо ви хочете змінити параметри облікового запису, вам необхідно увійти на вебсайт сторонньої програми й оновити їх там.

### Блокування, вимкнення сповіщень і видалення з друзів

Керування взаємодіями в екосистемі Apple не поширюється на окремих осіб і комунікації в сторонній програмі. Наприклад, коли ви блокуєте когось у Повідомленнях, Телефоні чи FaceTime, це не призводить до блокування цієї особи в Instagram. Такими взаємодіями необхідно керувати із самої сторонньої програми. Для отримання докладної інформації про тимчасове чи постійне блокування користувача, вимкнення сповіщень від нього чи видалення з друзів, перегляньте сайт служби підтримки сторонньої програми.

## Перегляд параметрів переадресації

Ви можете переглядати параметри переадресації вмісту й керувати ними.

⚠️**ВАЖЛИВО.** Перед тим як вносити зміни чи видаляти інформацію, **врахуйте потенційний вплив на безпеку та приватність.**



### Керування переадресацією Пошти iCloud

Ви можете переглянути, чи здійснюється автоматична переадресація ваших повідомлень у Пошті iCloud на іншу е-адресу, а також легко вимкнути переадресацію.

1. Увійдіть до iCloud за адресою <https://www.icloud.com> за допомогою імені користувача й пароля свого облікового запису Apple. У разі потреби введіть код двофакторної автентифікації.
2. Клацніть «Пошта», а потім натисніть ⚙️ вгорі списку «Скриньки» й виберіть «Параметри».
3. У вкладці «Загальні» перевірте, чи вибрано параметр «Пересилати», а також на які адреси має пересилатися ваша е-пошта. У разі потреби видаліть адресу пересилання й припиніть пересилання поштових повідомлень.
4. На вкладці «Правила» перегляньте всі правила, що мають параметр «Потім» з установленим значенням «Переслати до» або «Переслати на е-адресу та позначити прочитаним», і в разі потреби змініть правило відповідним чином.
5. Вихід з iCloud.


### Керування пересиланням текстових повідомлень на пристрої iPhone

Якщо ви надсилаєте повідомлення особі, яка користується телефоном, відмінним від iPhone, воно надсилається як текстове повідомлення. Можна налаштувати iPhone, так щоб текстове повідомлення, яке ви надсилаєте чи отримуєте, відображалось на інших пристроях, на яких виконано вхід у ваш обліковий запис Apple. Із цих пристроїв також можна надсилати нові текстові повідомлення. Якщо вас турбує, що ваші повідомлення пересилаються на інші пристрої, ви можете переглянути список цих пристроїв і вимкнути переадресацію текстових повідомлень.

1. На iPhone перейдіть у Параметри ⚙️ > Програми > Повідомлення.
2. Торкніть «Переадресація», щоб переглянути пристрої, які можуть надсилати текстові повідомлення й отримувати їх з вашого пристрою.
3. Вимкніть будь-які пристрої, які ви не хочете використовувати для отримання чи надсилання текстових повідомлень.

## Керування переадресацією викликів на інші пристрої на iPhone

Залежно від оператора мобільного зв'язку пристрій iPhone може переадресовувати отримувані виклики на інший номер телефону. Можна перевірити, чи переадресовуються отримувані виклики на інший номер телефону, а також вимкнути цю функцію.

1. На iPhone перейдіть у Параметри  > Програми > Телефон > Виклики > Переадресація викликів.

Якщо повзунок зелений, переадресація викликів увімкнена, тобто ви можете побачити номер телефону, на який переадресовуються ваші виклики.

*Примітка.* Якщо ця опція не відображається, переадресація викликів недоступна на вашому пристрої iPhone. Щоб отримати додаткову інформацію, зверніться до оператора мобільного зв'язку.

2. У разі потреби вимкніть переадресацію викликів.


Вимкнення переадресації викликів не супроводжується надсиланням відповідного сповіщення на телефонний номер, на який переадресовувалися виклики.

## Приховування фотографій і відео на пристроях Apple


У Фотографіях на Mac можна приховати фото і відео, які ви не хочете відображати. Приховані фотографії залишаються у вашій фототеці, і за бажанням їх можна згодом знову відобразити.

[Відкрити програму «Фотографії»](#)

### Як тимчасово приховати фотографії

1. Перейдіть у програму «Фотографії»  на Mac.
2. Клацніть «Фототека» на бічній панелі, а потім виберіть фотографії, які потрібно приховати.
3. Виберіть Зображення > Сховати [кількість] фото, а потім клацніть «Сховати». Вибрані фотографії більше не відобразатимуться, але їх не буде видалено.

### Як відобразити приховані фото

1. Перейдіть у програму «Фотографії»  на Mac.
2. Клацніть «Фототека» на бічній панелі, а потім виберіть Перегляд > Показати фотоальбом «Приховані». Альбом «Приховані» з'явиться на бічній панелі в категорії «Інше». Якщо альбом «Приховані» замкнено, його можна відімкнути за допомогою Touch ID або пароля. Щоб приховати альбом «Приховані», виберіть Перегляд > Сховати фотоальбом «Приховані».
3. Виберіть фотографії, які потрібно показати, а потім виберіть Зображення > Не ховати [кількість] фото.

## Як відобразити або приховати альбом «Приховані»

Типово альбом «Приховані» замкнено та приховано. Ви можете дозволити його показ у категорії «Інше», а також будь-коли приховати.

1. Перейдіть у програму «Фотографії» 📷 на Mac.
2. Клацніть «Фототека» на бічній панелі, а потім виконайте будь-які з таких дій:
  - *Показ альбому «Приховані» в категорії «Інші».* Виберіть Перегляд > Показати фотоальбом «Приховані».
  - *Приховування альбому «Приховані».* Виберіть Перегляд > Сховати фотоальбом «Приховані».

Щоб відімкнути колекцію «Приховані» потрібен пароль або Touch ID. Щоб змінити це, перегляньте параметри Фотографій.

## Попередження про неприйнятні фото й відео

Застереження щодо неприйнятного вмісту дають дорослим користувачам можливість уникати перегляду небажаних фото і відео, отриманих через Повідомлення, AirDrop, відеоповідомлення FaceTime і постер контакту в програмі «Телефон», за допомогою тієї ж технології захисту приватності, яка лежить в основі функції «Безпека спілкування». Функція є додатковою, її може ввімкнути користувач у параметрах «Приватність і безпека».







Ви (або член вашої родини) побачите застереження, перш ніж отримати чи надіслати фотографії відвертого сексуального характеру. У програмі «Екранний час» можна також блокувати неприйнятний вміст і налаштувати обмеження на покупки.

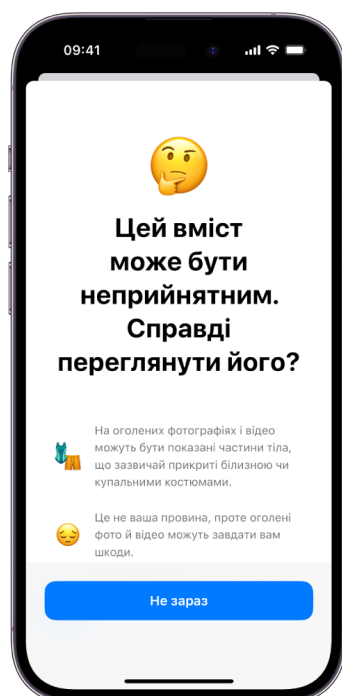
Перегляньте розділ [Як дозволяти чи блокувати комунікацію на пристрої члена родини](#) в посібнику користувача iPhone.



## Налаштування функції «Застереження щодо неприйняттого вмісту» на iPhone, iPad або Mac

1. Виконайте одну з таких дій:

- На iPhone або iPad. Перейдіть у Параметри  > Приватність і безпека , а потім торкніть «Застереження щодо неприйняттого вмісту».
- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , клацніть «Системні параметри», клацніть «Приватність і безпека» , а потім клацніть «Застереження щодо неприйняттого вмісту».
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple  > Системні параметри > Безпека та приватність , а потім клацніть «Застереження щодо неприйняттого вмісту».



2. Прокрутіть донизу і торкніть «Застереження щодо неприйняттого вмісту», а тоді ввімкніть опцію «Застереження щодо неприйняттого вмісту».
3. Виберіть, щоб вимкнути або ввімкнути дозвіл на виявлення чутливого вмісту, перш ніж його буде переглянуто, а також щоб отримувати поради щодо безпечного вибору.



## Отримання доказів, пов'язаних з іншим обліковим записом Apple

Компанія Apple прагне забезпечувати безпеку та приватність своїх користувачів. Якщо ви зазнаєте жорстокого поведіння, переслідування або знущання, здійснюваних за допомогою технологій, і хочете подати запит на докази, пов'язані з обліковим записом іншої людини, ви маєте звернутися місцевої правоохоронної установи або суду. Для задоволення потреб правоохоронних установ у цифрових доказах ми маємо окрему команду професіоналів у нашому юридичному відділі, які керують усіма юридичними запитами, що надходять від правоохоронних установ по всьому світу, і відповідають на них.

Усі інші запити на інформацію про клієнтів Apple, включно із запитаннями клієнтів про розкриття інформації, слід спрямовувати на адресу <https://www.apple.com/privacy/contact/>.

### Настанови Apple щодо запитів для правоохоронних установ

Перегляньте наведені нижче вказівки щодо запитів для правоохоронних установ, які розташовані як на території США, так і за їх межами.

- *Установи на території США:* [Настанови щодо юридичних процедур](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf) (https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf)
- *Установи за межами США:* [Настанови щодо юридичних процедур](https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf) (https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf)

## Записування підозрілої активності

Якщо ви зазнаєте знуцання або вас непокоїть підозріла активність у вашому обліковому записі чи пристрої, ви можете зробити знімок або запис екрана з відповідним вмістом. Знімок екрана — це зображення того, що відображається на екрані вашого пристрою. Запис екрана — це відео, яке фіксує те, що відображається на екрані вашого пристрою, зі звуком, який відтворювався на пристрої під час записування. Ви можете зберегти ці матеріали як файли зображення чи відео на своєму iPhone, iPad або Mac.

Якщо ви хочете надіслати Apple запит на інформацію про обліковий запис іншої особи, пов'язаний з випадком переслідування чи знуцання, дивіться розділ [Отримання доказів, пов'язаних з іншим обліковим записом Apple](#) далі в цьому посібнику.



### Знімки екрана або запис відео екрана на iPhone або iPad

1. Виконайте одну з таких дій:

- На iPhone або iPad з Face ID. Одночасно натисніть, а потім відпустіть бічну кнопку та кнопку збільшення гучності.
- *На iPhone або iPad з кнопкою «Початок».* Одночасно натисніть, а потім відпустіть кнопку «Початок» та бічну кнопку або кнопку «Спати/Будити» (залежно від моделі).

2. Торкніть знімок екрана в лівому нижньому куті, а потім торкніть «Готово».

3. Виберіть «Зберегти до Фотографій», «Зберегти до Файлів» або «Видалити знімок екрана».

Якщо ви вибрали «Зберегти до Фотографій», ви можете переглянути знімок в альбомі «Знімки екрана» в програмі «Фотографії» або в альбомі «Усі фотографії», якщо ввімкнено параметр «Фотографії iCloud» у меню Параметри > Фотографії.

## Створення знімків або записів екрана на Mac

1. Натисніть Shift+Command+5 (або скористайтеся Launchpad), щоб відкрити програму «Знімок екрана» та відобразити інструменти.



2. Клацніть інструмент, який потрібно використовувати, щоб вибрати те, що ви хочете зняти або записати.

Для частини екрана перетягніть рамку, щоб змінити її положення, або перетягніть її краї, щоб налаштувати розмір області, яку потрібно зняти або записати.


Дія	Інструмент
Знімок усього екрана	
Знімок вікна	
Знімок частини екрана	
Запис усього екрана	
Запис частини екрана	

3. Виберіть потрібний варіант.

Доступні варіанти залежать від того, що ви робите: знімок екрана чи запис відео екрана. Наприклад, можна встановити тимчасову затримку або показати вказівник миші чи клацання, а також вказати, де зберегти файл.

Опція «Показати плаваючу мініатюру» полегшить подальшу роботу із виконаним знімком або записом. Вона «плаває» в нижньому правому куті екрана протягом кількох секунд, щоб у вас був час перетягнути знімок у документ, позначити або поділитися ним, перш ніж він буде збережений у вказаному вами місці.

4. Зробіть знімок екрана або запис відео екрана:

- Для всього екрана або його частини. Клацніть «Знімок».
- Для вікна. Перемістіть вказівник на вікно, а потім клацніть вікно.
- Для запису. Клацніть «Запис». Щоб зупинити запис, натисніть  на смузі меню.

Коли встановлено прапорець «Показувати плавучу мініатюру», можна зробити будь-які з таких дій, поки мініатюра на короткий час відображається в нижньому правому куті екрана:

- Проведіть пальцем вправо, щоб негайно зберегти файл, після чого мініатюра припинить відображатися.
- Перетягніть мініатюру в документ, е-лист, нотатку або вікно Finder.
- Натисніть мініатюру, щоб відкрити вікно; у ньому ви можете розмітити знімок екрана — або обрізати запис — і поділитися результатом.

Залежно від того, де ви вирішили зберегти знімок екрана або запис, може відкритися відповідна програма.

## Відновлення заводських параметрів пристрою

Якщо вас турбує те, що хтось міг мати фізичний доступ до вашого пристрою, порушити його вбудовані засоби захисту й установити шкідливе програмне забезпечення на кшталт програм для стеження, ви можете відновити заводські параметри пристрою. Це гарантує, що ніхто, крім вас, не матиме доступу до вашого пристрою.

### ⚠️ ВАЖЛИВО.

- У результаті скидання пристрою до заводських параметрів буде стерто весь вміст і всі параметри. Перед тим як відновлювати заводські параметри пристрою, запустіть інструмент [Керування поширенням і доступом](#) функції «Перевірка безпеки». Проблеми, які вас турбують, можуть бути пов'язані з поширенням параметрів або доступом програм, про які вам не було відомо.
- Якщо ви зітрете весь вміст і параметри через побоювання, що ваш пристрій зламали й установили на ньому шкідливе програмне забезпечення, не відновлюйте його дані з резервної копії. Відновлення з резервної копії може призвести до повторного встановлення шкідливого програмного забезпечення, якого ви намагаєтеся позбутися.

Відновлення заводських параметрів призводить до таких наслідків:

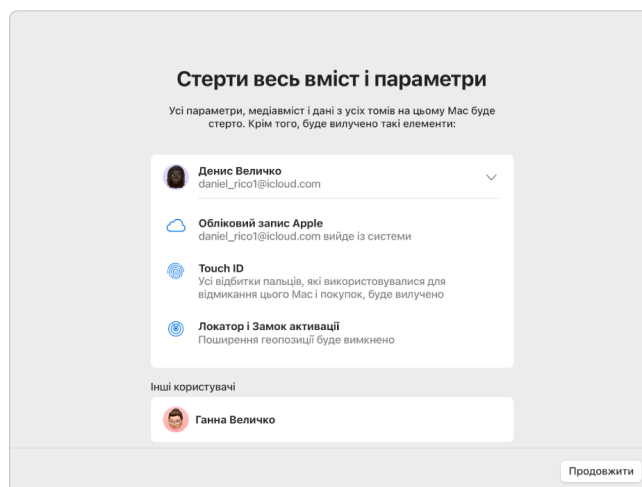
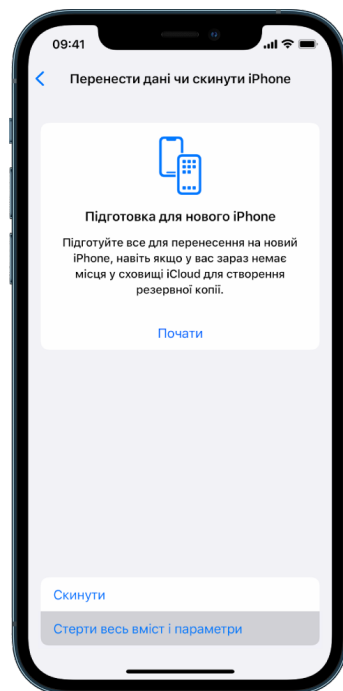
- Буде стерто всі дані, збережені на пристрої, включно з даними Face ID й Touch ID, кодом допуску та паролями, повідомленнями, е-листами, фотографіями, файлами, медіавмістом тощо.
- Буде вилучено всі програми, включно з установленими без вашого відома.
- Буде скинуто всі параметри приватності, тому ви не зможете надавати доступ до своєї геопозиції жодним людям чи програмам.
- Буде встановлено найновішу версію операційної системи (незалежно від того, яку версію було встановлено до цього).



Вимоги:

- доступ до інтернету;
- код допуску пристрою або пароль;
- пароль облікового запису Apple;
- час.

Якщо ви хочете скористуватися функцією «Стерти весь вміст і налаштування» на Mac, має бути встановлено macOS 12.0.1 або новішу версію. Як варіант, можна стерти всі дані на Mac. Перегляньте статті служби підтримки Apple про [використання дискової утиліти для стирання Mac із процесором Apple](https://support.apple.com/102506) (https://support.apple.com/102506) та [використання дискової утиліти для стирання Mac із процесором Intel](https://support.apple.com/HT208496) (https://support.apple.com/HT208496).



## Для iPhone та iPad

- [Як відновити заводські параметри на iPhone, iPad чи iPod за допомогою комп'ютера](https://support.apple.com/108931) (https://support.apple.com/108931) — стаття служби підтримки Apple

## Стирання всього вмісту й параметрів на Mac

- Зітріть Mac (macOS 12.0.1 або новіша версія) — видаліть вміст, параметри й усі встановлені програми без перевстановлення macOS, щоб відновити заводські параметри.
  - [Стирання Mac](https://support.apple.com/guide/mac-help/mchl7676b710) для видалення вмісту (програм, даних) і параметрів (наприклад, перед тим як продати, обміняти чи віддати пристрій) (https://support.apple.com/guide/mac-help/mchl7676b710).
  - [Стирання та повторне інсталиювання macOS](https://support.apple.com/guide/mac-help/mh27903) для Mac із Apple silicon або Mac із процесором Intel. (https://support.apple.com/guide/mac-help/mh27903)
- [Як стерти дані з комп'ютера Mac із процесором Apple за допомогою «Дискової утиліти»](https://support.apple.com/102506) — стаття служби підтримки Apple (https://support.apple.com/102506)
- [Як стерти дані з комп'ютера Mac із процесором Intel за допомогою програми «Дискова утиліта»](https://support.apple.com/102639) — стаття служби підтримки Apple (https://support.apple.com/102639)

## Окремі програми та функції

### Екстрені виклики й текстові повідомлення на iPhone і Apple Watch

У надзвичайних ситуаціях ви можете використовувати iPhone або Apple Watch, щоб швидко викликати допомогу.




Якщо ви вирішите поділитися своїм медичним ID, пристрій iPhone може надіслати вашу медичну інформацію до служб екстреної допомоги, коли ви зателефонуєте чи напишете 911 або скористаєтесь сигналом SOS (лише в США). Для отримання подальшої інформації про медичний ID перегляньте розділ «[Створення медичного ID](https://support.apple.com/guide/iphone/iph08022b194/#iphbcea12902)» (<https://support.apple.com/guide/iphone/iph08022b194/#iphbcea12902>) у Посібнику користувача iPhone.

*Примітка.* Щоб отримати невідкладну допомогу в деяких районах, ви також можете надіслати текстове повідомлення на номер 911. У місцях, де цього не передбачено, ви можете отримати зворотне повідомлення про те, що ваше текстове повідомлення не було прийняте. Дивіться статтю служби підтримки Apple [Як надіслати повідомлення до служби екстреної допомоги 911 на iPhone або Apple Watch](https://support.apple.com/101996) (<https://support.apple.com/101996>).

З функцією «Сигнал SOS» можна легко й швидко викликати допомогу та сповіщати екстрені контакти. У зв'язку із цим важливо переконатися, що особа або особи, призначені як екстрені контакти випадків, є людьми, яким ви довіряєте.




## Змінення параметрів функції «Сигнал SOS» на iPhone

1. Перейдіть у Параметри  > Сигнал SOS.
2. Виконайте будь-які з таких дій:
  - *Щоб увімкнути або вимкнути виклик утриманням*, натисніть і утримуйте бокову кнопку та кнопки гучності, аби запустити відлік до виклику екстрених служб.
  - *Щоб увімкнути або вимкнути виклик п'ятьма натисканнями*, швидко натисніть бокову кнопку п'ять разів, аби запустити відлік до виклику екстрених служб.
  - *Щоб керувати своїми екстреними контактами*, у програмі «Здоров'я» торкніть «Налаштувати екстрені контакти» або «Редагувати екстрені контакти». Перегляньте розділ [Налаштування та перегляд свого медичного ID](https://support.apple.com/guide/iphone/iph08022b192) (<https://support.apple.com/guide/iphone/iph08022b192>) у Посібнику користувача iPhone.


## Налаштування або зміна екстрених контактів на iPhone

Екстрені контакти можна налаштувати так, що якщо ви зателефонуєте за номером екстреної допомоги, iPhone надішле цим контактам сповіщення про те, що ви зателефонували за допомогою, поділиться вашою геопозицією із цими контактами та сповістить їх, якщо ваше місцезнаходження зміниться. Якщо раніше ви додали когось як екстрений контакт і зараз ви хочете вилучити їх, ви можете видалити відомості про цю особу.

Додавання або вилучення екстрених контактів:

1. Відкрийте програму «Здоров'я» , потім торкніть зображення свого профілю.
2. Торкніть пункт «Медичний ID».
3. Торкніть «Змінити», потім прокрутіть до пункту «Екстрені контакти».
4. Додайте або видаліть контакт.
  - *Додати контакт.* Торкніть , щоб додати екстрений контакт (не можна вказувати екстрені служби як екстрені контакти).
  - *Видалити контакт.* Торкніть  поряд із контактом, який потрібно видалити, а потім торкніть «Видалити».
5. Торкніть «Готово», щоб зберегти зміни.

## Здійснення екстреного виклику із замкненого пристрою iPhone

1. На екрані «Код допуску» торкніть пункт «Екстрена ситуація».
2. Наберіть номер екстреної служби (наприклад, 911 у США), а потім торкніть .




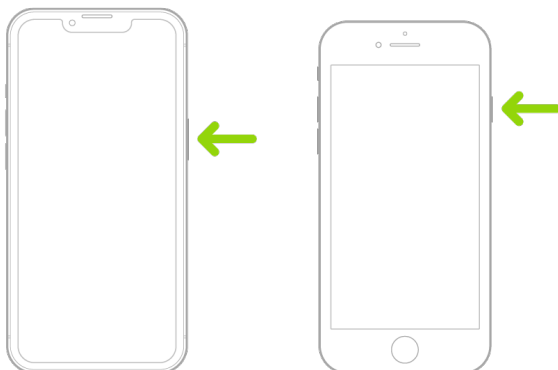
## Використання сигналу SOS на iPhone (усі країни чи регіони, окрім Індії)

У разі екстреної ситуації використовуйте свій iPhone, щоб швидко подзвонити і сповістити свої екстрені контакти (якщо доступна стільникова служба). Після завершення екстреного дзвінка iPhone попереджає ваші екстрені контакти текстовим повідомленням, якщо ви не скасуєте цю дію. Ваш iPhone надсилає ваше поточне місцеположення (якщо доступно), а потім протягом певного періоду часу після активації режиму SOS ваші екстрені контакти отримують звістки, коли ваше місцеположення змінюється.

*Примітка.* Якщо у вас iPhone 14 або новіший (будь-яка модель), можливо, вам вдасться зв'язатися з екстреними службами через супутниковий зв'язок, якщо стільникові мережі недоступні. Дивіться розділ «[Використання сигналу SOS через супутник на iPhone](#)» далі в цьому посібнику.

- Одночасно натисніть та утримуйте бічну кнопку разом із будь-якою з кнопок гучності, поки з'являться повзунки і завершиться зворотний відлік Сигналу SOS, а тоді відпустіть кнопки.

Або можна налаштувати iPhone, щоб він надсилав Сигнал SOS, коли бічну кнопку буде швидко натиснуто п'ять разів. Перейдіть у Параметри  > Сигнал SOS, а потім увімкніть «Виклик 5-ма натисненнями».



## Використання сигналу SOS на iPhone (Індія)

- Швидко натисніть бокову кнопку тричі, поки з'являться повзунки і завершиться зворотний відлік Сигналу SOS.
- Якщо ви ввімкнули Скорочення доступності, одночасно натисніть та утримуйте бічну кнопку разом із будь-якою з кнопок гучності, поки з'являться повзунки і завершиться зворотний відлік Сигналу SOS, а тоді відпустіть кнопки.

Стандартно iPhone відтворює звук застереження, починає відлік, а потім викликає екстрені служби.

Після завершення екстреного дзвінка iPhone попереджає ваші екстрені контакти текстовим повідомленням, якщо ви не скасуєте цю дію. Ваш iPhone надсилає ваше поточне місцеположення (якщо доступно), а потім протягом певного періоду часу після активації режиму SOS ваші екстрені контакти отримують звістки, коли ваше місцеположення змінюється.

## Зв'язок з екстреними службами за допомогою Apple Watch

Виконайте одну з таких дій:

- Натисніть і утримуйте бокову кнопку, поки з'являться повзунки, а тоді перетягніть повзунок «Екстрений виклик» вправо.



Apple Watch здійснює виклик на номер екстреної служби у вашому регіоні, наприклад 911. (У деяких регіонах може знадобитися натиснути номер на клавіатурі, щоб здійснити виклик).

- Натисніть і утримуйте бічну кнопку, поки Apple Watch не подасть попереджувальний звуковий сигнал і не почне зворотний відлік. Коли зворотний відлік закінчиться, Apple Watch викличе екстрені служби. Apple Watch подає попереджувальний звуковий сигнал, навіть якщо він перебуває в режимі тиші. То ж якщо ви опинилися в надзвичайній ситуації, коли не хочете видавати шум, використовуйте повзунок екстреного виклику без зворотного відліку.

Якщо ви не хочете, щоб ваш Apple Watch автоматично розпочинав екстрений зворотний відлік, коли ви натискаєте й утримуєте бічну кнопку, вимкніть автоматичний набір. Відкрийте програму «Параметри» на Apple Watch, торкніть SOS, торкніть «Утримування бічної кнопки», а тоді вимкніть опцію «Утримування бічної кнопки». (Або відкрийте програму Apple Watch на iPhone, торкніть «Мій годинник», торкніть «Сигнал SOS», а тоді вимкніть опцію «Затисніть бічну кнопку, щоб набрати номер».) Ви все ще зможете здійснювати екстрені виклики за допомогою повзунка «Екстрений виклик».




- Промовте «Hey Siri, call 911».

### Текстове повідомлення до екстрених служб з iPhone (доступно не в усіх країнах і регіонах)

1. Відкрийте програму «Повідомлення» , а тоді введіть 911 або номер місцевої екстреної служби у полі «Кому».
2. У полі тексту повідомлення вкажіть характер невідкладної ситуації.
3. Торкніть .

**Важливо!** Після повідомлення до служби 911, iPhone переходить в екстрений режим на 30 хв. Щоб вийти з екстреного режиму, перезапустіть iPhone.

### Текстове повідомлення до екстрених служб з Apple Watch (доступно не в усіх країнах і регіонах)

1. Відкрийте програму «Повідомлення» , а потім торкніть «Нове повідомлення».
2. Торкніть «Додати контакт».
3. Торкніть , введіть 911, а тоді торкніть ОК.
4. Торкніть «Створити повідомлення», а тоді торкніть SMS.
5. Напишіть текст повідомлення пальцем, торкніть , щоб продиктувати повідомлення, або введіть повідомлення з клавіатури.
6. Торкніть «Готово», а тоді торкніть «Надіслати».

**Важливо!** Після повідомлення до служби 911, Apple Watch переходить в екстрений режим на 30 хвилин. Щоб вийти з екстреного режиму, перезапустіть свій Apple Watch.

## Використання сигналу SOS через супутник на iPhone

На iPhone 14 та новіших моделях (будь-яких) з iOS 16.1 або новішою версією можна використовувати функцію «Сигнал SOS через супутник», щоб надсилати текстові повідомлення екстреним службам, коли ви перебуваєте за межами покриття стільникових мереж і Wi-Fi. Докладніше дивіться в статті служби підтримки Apple [Як використовувати функцію «Сигнал SOS через супутник» на iPhone 14](https://support.apple.com/HT213426) (https://support.apple.com/HT213426).

Ви також можете використовувати програму Локатор, щоб через супутник ділитися своїм місцезнаходженням із людьми. Перегляньте розділ [Надсилання своєї геопозиції через супутник у Локаторі на iPhone](https://support.apple.com/guide/iphone/iph2aac8ae20) (https://support.apple.com/guide/iphone/iph2aac8ae20) у посібнику користувача iPhone.

Докладніше дивіться в розділі [Важлива інформація про екстрені виклики на iPhone](#) у посібнику користувача iPhone.

## Керування поширенням даних про активність на Apple Watch


Якщо у вас є Apple Watch і ви раніше поділилися кільцями активності з іншими користувачами, вони зможуть побачити інформацію про рівень вашої активності та тренування. Але вони не отримують жодної інформації про ваше місцезнаходження.



### Припинення поширення на Apple Watch

Ви можете приховати свої досягнення чи зупинити поширення даних про свою активність для певної особи у вкладці «Спільний доступ» у програмі «Активність».

Як припинити поширення кільця активності для певної особи на Apple Watch:

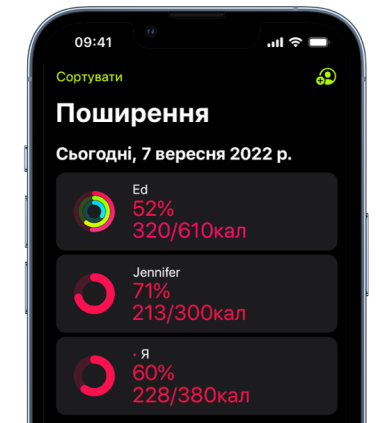
1. Відкрийте програму «Активність»  на своєму Apple Watch.
2. Проведіть вліво, потім поверніть Digital Crown, щоб прокрутити до нижньої частини екрана.
3. Щоб вилучити користувача зі спільного доступу, торкніть їх ім'я, а потім торкніть «Вилучити».


Докладніше дивіться в розділі:

- [Поширення даних активності за допомогою Apple Watch](https://support.apple.com/guide/watch/apd68a69f5c7) у Посібнику користувача Apple Watch (<https://support.apple.com/guide/watch/apd68a69f5c7>)

## Припинення поширення на iPhone

Ви можете припинити поширення кілець активності для певної особи на iPhone.




1. Відкрийте програму «Фітнес»  на iPhone, а потім торкніть «Поширення».
2. Торкніть особу, для якої ви поширюєте дані.
3. Торкніть кнопку «Поширити» у верхньому правому куті екрана.
4. Торкніть «Вилучити друга» або «Сховати мою активність».

Докладніше дивіться в розділі:

- [Поширення даних активності за допомогою Apple Watch](https://support.apple.com/guide/watch/apd68a69f5c7) у Посібнику користувача Apple Watch (<https://support.apple.com/guide/watch/apd68a69f5c7>)


## Безпечне використання AirDrop

### Що таке AirDrop?

AirDrop  — це простий спосіб обміну зображеннями, документами чи іншими файлами між пристроями Apple, розташованими поруч. Ви можете за допомогою свого пристрою поширювати дані для кожного, хто перебуває поряд з вами, обмежити поширення вашими контактами або взагалі заборонити поширення.

*Примітка.* Варіант «Тільки контакти» доступний на пристроях з iOS 10, iPadOS 13.1 та macOS 10.12 або новішими версіями. Якщо на вашому пристрої використовується попередня версія програмного забезпечення і ви хочете обмежити тих, хто може надсилати вам файли через AirDrop, можете ввімкнути цю функцію, коли вам це потрібно, а потім вимкнути, коли вона не використовується.

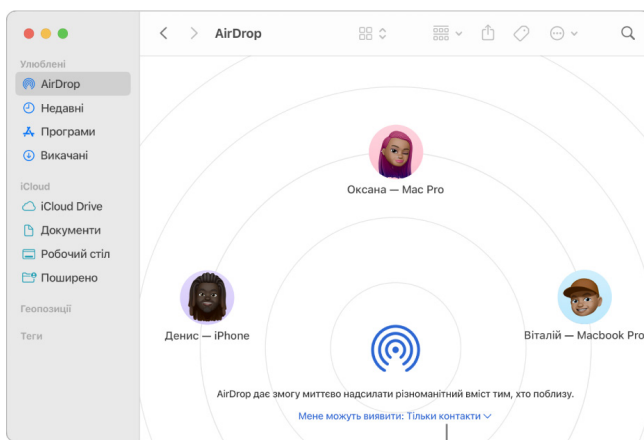
## iPhone або iPad

- На своєму iPhone чи iPad перейдіть у Параметри  > Загальні, торкніть AirDrop, а потім виберіть варіант, який вам найкраще підходить.


Докладніше дивіться в розділі:

- [Використання AirDrop на iPhone для надсилання елементів на розташовані поблизу пристрої](https://support.apple.com/guide/iphone/iphcd8b9f0af) у Посібнику користувача iPhone (<https://support.apple.com/guide/iphone/iphcd8b9f0af>)
- [Використання AirDrop на iPad для надсилання елементів на розташовані поблизу пристрої](https://support.apple.com/guide/ipad/ipadf0a1530e) у Посібнику користувача iPad (<https://support.apple.com/guide/ipad/ipadf0a1530e>)

## На Mac за допомогою Finder



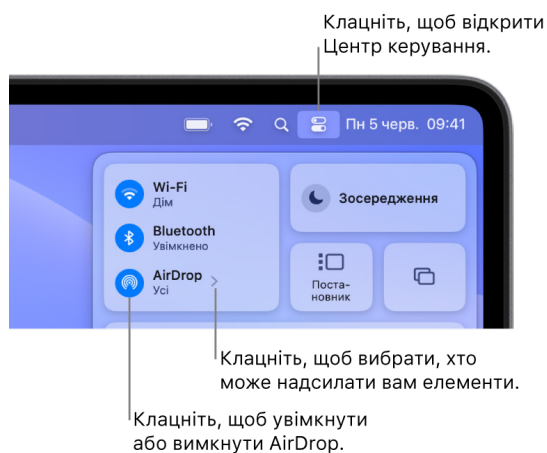
Контролюйте, хто може надсилати вам елементи.




1. Клацніть іконку Finder  у Dock, щоб відкрити вікно Finder.
2. На бічній панелі Finder клацніть AirDrop.
3. У вікні AirDrop клацніть спливне меню «Мене можуть виявити» та виберіть варіант, який найкраще вас влаштовує.

Докладніше дивіться в розділі:

- [Використання AirDrop для надсилання елементів на сусідні пристрої Apple](https://support.apple.com/guide/mac-help/mh35868) у Посібнику користувача Mac (<https://support.apple.com/guide/mac-help/mh35868>)

## На Mac за допомогою Центру керування



1. На Mac клацніть  на смузі меню, а потім — . Якщо іконка синя, функцію ввімкнено.
2. Клацніть  поряд з AirDrop, а потім виберіть варіант, який найкраще підходить для вас.

Докладніше дивіться в розділі:

- [Використання AirDrop для надсилання елементів на сусідні пристрої Apple у Посібнику користувача Mac \(https://support.apple.com/guide/mac-help/mh35868\)](https://support.apple.com/guide/mac-help/mh35868)


## Керування параметрами спільного доступу до Календаря на пристроях Apple

Якщо ви раніше запросили іншу людину, щоб надати їй спільний доступ до свого календаря, ви можете керувати її можливістю вносити зміни до календаря або припинити її спільний доступ до календаря.

▼ **ВАЖЛИВО.** Коли ви видаляєте або припиняєте спільний доступ до календаря, інших учасників може бути сповіщено про ці зміни.




### Керування параметрами спільного доступу до календаря на iPhone або iPad

1. Торкніть «Календар»  на своєму iPhone або iPad, а потім торкніть  поряд зі спільним календарем, який потрібно змінити.
2. Торкніть людину, а потім виконайте будь-які з таких дій:
  - Увімкніть або вимкніть параметр «Дозволити редагування».
  - Торкніть «Припинити поширення».

### Видалення календаря на Mac

Деякі календарі не можна видалити.

- Делеговані календарі не можна видалити, але можна більше не відображати їх у головному вікні Календаря. Дивіться розділ [Скасування публікації календаря на Mac](#).
- Якщо ви не можете видалити календар для певного облікового запису календаря, спробуйте зробити це на вебсайті постачальника облікового запису. Наприклад, видалити календар Google можна на вебсайті [google.com](https://www.google.com).
- Якщо в обліковому записі календаря є лише один календар (не враховуючи календарі інших осіб, до яких ви маєте спільний доступ), його не можна видалити.

1. Відкрийте програму «Календар»  на Mac і клацніть назву календаря в списку календарів.

Якщо список календарів не відображається ліворуч, виберіть Перегляд > Показати список календарів.

2. Виберіть Редагувати > Видалити.


Докладніше дивіться в розділі:

- [Додавання і видалення календарів на Mac](https://support.apple.com/guide/calendar/icl1005) у Посібнику користувача Календаря (<https://support.apple.com/guide/calendar/icl1005>)



## Скасування підписки на календар на Mac

Якщо вам більше не потрібна підписка на чийсь календар, її можна скасувати.

- Відкрийте програму «Календар»  на Mac, утримуючи клавішу Control, клацніть назву календаря в списку календарів, а потім виберіть «Відписатися».

Якщо список календарів не відображається ліворуч, виберіть Перегляд > Показати список календарів.

*Примітка.* Відписуючись від календаря, можна також повідомити про спам.

Повідомлення про спам допомагає програмі Календар краще виявляти спам-підписки.


Докладніше дивіться в розділі:


- [Підписка на календарі на Mac](https://support.apple.com/guide/calendar/icl1022) у Посібнику користувача Календаря (<https://support.apple.com/guide/calendar/icl1022>)

## Скасування публікації календаря на Mac

Якщо в списку календарів є розділ «На моєму Mac», ви можете опублікувати календар у цьому розділі на сервері WebDAV, до якого у вас є доступ. Інші люди можуть підписуватися на ваші опубліковані календарі або переглядати їх у веббраузері. Публікування календаря можна припинити будь-коли, не видаляючи його з Mac.

*Примітка.* Неопубліковані календарі не видаляються з Mac.

1. Відкрийте програму «Календар»  на Mac, а потім клацніть назву календаря чи групи календарів у списку календарів.

Якщо список календарів не відображається ліворуч, виберіть Перегляд > Показати список календарів. Якщо календар опубліковано, поряд з його назвою є кнопка .

2. Виберіть Редагувати > Припинити публікацію.

Після скасування публікації календаря нові користувачі не зможуть підписатися на нього. Користувачі, які вже підписані на нього, бачитимуть останню опубліковану копію, доки не видалять її.


Докладніше дивіться в розділі:

- [Публікування та скасування публікації календарів на Mac](https://support.apple.com/guide/calendar/icl1017) у Посібнику користувача Календаря (<https://support.apple.com/guide/calendar/icl1017>)

## Припинення поширення календаря iCloud на Mac


Якщо ви [налаштували iCloud на Mac](#), ви можете використовувати Календар, щоб керувати спільними календарями iCloud. Якщо ви надаєте спільний доступ до календаря iCloud або приєднуєтесь до спільного календаря iCloud іншої особи, ви можете отримувати е-листи після кожного оновлення спільного календаря. Ви можете припинити надходження цих е-листів у параметрах Календаря на iCloud.com.

Якщо ви отримали запрошення приєднатися до спільного календаря iCloud, ви можете прийняти його на пристрої iPhone, iPad або Mac, на якому виконано вхід у той самий обліковий запис Apple, у Календарі iCloud або на сайті iCloud.com.

1. Відкрийте програму «Календар»  на своєму Mac.

Якщо список календарів не відображається ліворуч, виберіть Перегляд > Показати список календарів.

2. Виконайте будь-які з таких дій:


- *Припинення спільного доступу до календаря для певних людей.* Наведіть вказівник на назву календаря в списку календарів, а потім натисніть . Клацніть ім'я людини, а потім натисніть «Видалити».
  - *Припинення спільного доступу до календаря для всіх.* Утримуючи клавішу Control, клацніть назву календаря в списку календарів, а потім виберіть «Припинити поширення».
  - *Припинення підписки на календар іншої особи.* Утримуючи клавішу Control, клацніть назву календаря в списку календарів, а потім виберіть «Відписатися».
- Відписуючись від календаря, можна також повідомити про спам. Повідомлення про спам допомагає програмі Календар краще виявляти спам-підписки.

Докладніше дивіться в розділі:

- [Отримання оновлень щодо календарів на сайті iCloud.com](https://support.apple.com/guide/icloud/mm8074582205) у Посібнику користувача Календаря (<https://support.apple.com/guide/icloud/mm8074582205>)

## Керування параметрами «Сімейного доступу»

Сімейним доступом можуть користуватися до п'яти членів родини, щоб ділитися підписками, покупками, фотографіями, фотоальбомами, календарем тощо, і все це без спільного доступу до облікових записів Apple один одного. Якщо ви використовуєте родинний тарифний план iCloud для зберігання даних, усі файли та документи кожного учасника залишаються приватними, водночас займане кожним користувачем місце в сховищі видиме для всіх.

Щоб перевірити, чи належите ви до групи Сімейного доступу, перейдіть у Параметри  > [ваше ім'я] > вкладка «Сімейний доступ». Якщо ви бачите пункт «Налаштуйте Сімейний доступ», це означає, що ви не використовуєте Сімейний доступ із цим обліковим записом Apple. Якщо ви бачите іконку «Сімейний доступ», ви можете торкнутися її, щоб побачити членів родини та ролі.

Поради:

- Щоб перевірити, чи належите ви до групи Сімейного доступу, перейдіть у Параметри  й пошукайте слово «Сімейний» під своїм іменем.
- Щоб дізнатися, як припинити Сімейний доступ, дивіться розділ [Припинення «Сімейного доступу» на iPhone або iPad з iOS 17, iPadOS 17 або попередньою версією](#) та [Припинення Сімейного доступу на Mac](#).
- Щоб дізнатися, як вийти з групи Сімейного доступу, перегляньте вказівки в розділах [Вихід із групи Сімейного доступу на iPhone та iPad з iOS 17, iPadOS 17 або попередньою версією](#) і [Вихід із групи Сімейного доступу на Mac](#).
- Щоб дізнатися, як вилучити членів родини, перегляньте вказівки в розділах [Вилучення учасників із сімейної групи на iPhone та iPad з iOS 17, iPadOS 17 або попередньою версією](#) і [Вилучення учасників із сімейної групи на Mac](#).



## Хто може вийти з групи Сімейного доступу?

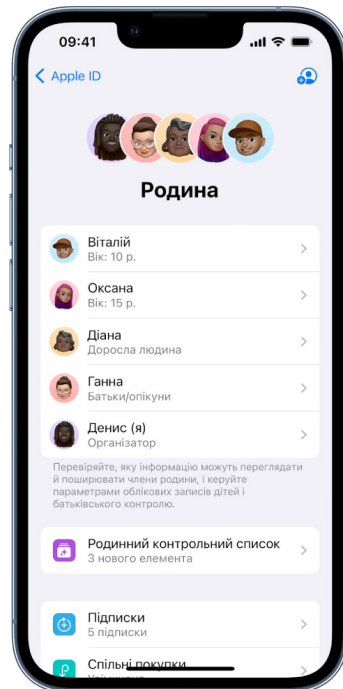
Можливість внесення змін до групи Сімейного доступу чи виходу з неї залежить від статусу учасника.

- Організатор може вийти з групи Сімейного доступу, вимкнувши Сімейний доступ. Після вимкнення Сімейного доступу всі члени родини вилучаються із сімейної групи одночасно. Якщо в сімейній групі є діти віком до 13 років, організатор повинен перемістити їх до іншої групи Сімейного доступу. Члени родини більше не матимуть спільного доступу до підписок, покупок та інших служб, доступних через Сімейний доступ.
- Будь-які члени родини, яким виповнилося 13 років, можуть будь-коли вийти із сімейної групи. Просто виберіть своє ім'я, а потім виберіть «Припинити використання Сімейного доступу». Ви також можете ввійти на вебсайт облікового запису Apple або вибрати «Вилучити обліковий запис» у розділі Сімейного доступу.
- З міркувань безпеки дитина (до 13 років) не може самостійно вилучити свій обліковий запис із сім'ї та не може припинити ділитися такими деталями, як екранний час, без коду допуску до екранного часу. Організатор сім'ї має доступу до спільного вмісту на вашому пристрої, такого як спільні фотоальбоми та спільні календарі, а також може переглядати активність екранного часу.

## Типи учасників «Сімейного доступу»

Учасники групи «Сімейного доступу» можуть виконувати різні ролі залежно від віку.

*Примітка.* Вік, у якому хтось вважається дорослим або дитиною, залежить від країни чи регіону.



Щоб змінити свій статус у «Сімейному доступі», корисно знати, як працюють різні ролі в групах «Сімейного доступу».

- **Організатор:** Доросла людина, яка створює групу Сімейного доступу. Організатор може запрошувати й вилучати членів родини, а також розпустити групу.
- **Дорослий:** Учасник групи Сімейного доступу, якому виповнилося 18 років.
- **Батьки/опікуни:** Дорослий учасник групи Сімейного доступу, який може допомогти керувати батьківським контролем для дітей у групі. Коли організатор додає дорослого до групи Сімейного доступу, він може призначити його як одного з батьків або опікуна.
- **Дитина або підліток:** Учасник групи Сімейного доступу у віці до 18 років. Організатор, один з батьків чи опікун можуть створити обліковий запис Apple для дитини, яка замала, щоб створити свій власний.

У вашій родині один дорослий — *організатор родини* — вибирає функції, якими буде користуватися родина, і запрошує приєднатися до групи щонайбільше п'ять додаткових осіб. Після того як запрошення будуть прийняті, функція «Сімейний доступ» налаштовується автоматично на всіх пристроях, включаючи спільний календар і спільний фотоальбом. Організатор родини може додати до сімейної групи будь-кого, хто має обліковий запис Apple, і вилучити будь-кого, кому виповнилося 13 років.


## Що відбувається після виходу з групи Сімейного доступу

Якщо учасника вилучають із групи Сімейного доступу або він її залишає, то він зберігає покупки, оплачені за допомогою спільної кредитної картки, але відразу втрачає доступ до інших речей, які спільно використовують члени родини:

- Геопозиції пристроїв колишніх членів родини не відображаються в програмі Локатор на iCloud.com, а також на iPhone, iPad чи Mac.
- Покупки колишніх членів родини більше не відображаються в розділі «Придбано» в iTunes Store, App Store і Apple Books.
- Музику, фільми, телешоу, книги та програми, які було раніше викачано, більше не можна використовувати, якщо початкову покупку здійснив хтось інший. Колишні члени родини більше не можуть використовувати цей вміст, викачаний із вашої колекції.
- Покупки в програмах стають недоступними, якщо їх було здійснено за допомогою програми, яку спочатку придбав хтось інший. Ви можете відновити доступ до покупок у програмі, купивши цю програму.


### Вихід із групи Сімейного доступу на iPhone чи iPad з iOS 18, iPadOS 18 або новішою версією

Якщо вам більше 13 років і ви є учасником групи Сімейного доступу:

1. Перейдіть у Параметри  > Родина під пунктом [ваше ім'я].
2. Торкніться [ваше ім'я], потім торкніться «Припинити використання Сімейного доступу».






### Вихід із групи Сімейного доступу на iPhone чи iPad з iOS 17, iPadOS 17 або попередньою версією

Якщо вам більше 13 років і ви є учасником групи Сімейного доступу:

1. Перейдіть у Параметри  > [ваше ім'я] > Сімейний доступ.
2. Торкніться [ваше ім'я], потім торкніться «Припинити використання Сімейного доступу».

### Вихід із групи Сімейного доступу на Mac


Якщо вам більше 13 років і ви є учасником групи Сімейного доступу:

1. Виконайте одну з таких дій:
  - На Mac з macOS 15 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть «Родина» під пунктом [ваше ім'я].
  - На Mac з macOS 13 або macOS 14. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Сімейний доступ» , а потім виберіть «Сімейний доступ» на бічній панелі.
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Сімейний доступ» , а потім виберіть «Сімейний доступ».

2. У списку членів родини клацніть своє ім'я або «Деталі» поряд зі своїм іменем, клацніть «Припинити використання Сімейного доступу», а потім виконайте інструкції на екрані.
3. Клацніть «Готово».


### **Припинення Сімейного доступу на iPhone чи iPad з iOS 18, iPadOS 18 або новішою версією**

Вимкнути «Сімейний доступ» може тільки організатор родини.

1. Перейдіть у Параметри  > Родина під пунктом [ваше ім'я].
2. Торкніть своє ім'я, а потім торкніть «Припинити використання Сімейного доступу».






### **Припинення Сімейного доступу на iPhone чи iPad з iOS 17, iPadOS 17 або попередньою версією**

Вимкнути «Сімейний доступ» може тільки організатор родини.

1. Перейдіть у Параметри  > [ваше ім'я] > Сімейний доступ.
2. Торкніть своє ім'я, а потім торкніть «Припинити використання Сімейного доступу».


### **Припинення Сімейного доступу на Mac**

Щоб припинити Сімейний доступ, ви повинні:

- Бути організатором родини.
  - Перенести облікові записи дітей до іншої родини.
1. Виконайте одну з таких дій:
    - На Mac з macOS 15 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть «Родина» під пунктом [ваше ім'я].
    - На Mac з macOS 13 або macOS 14. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Сімейний доступ» , а потім виберіть «Сімейний доступ» на бічній панелі.
    - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Сімейний доступ» , а потім виберіть «Сімейний доступ».
  2. Натисніть > біля свого імені, а потім клацніть «Припинити використання Сімейного доступу».

### **Вилучення учасників із сімейної групи на iPhone чи iPad з iOS 18, iPadOS 18 або новішою версією**


Якщо ви — організатор родини:

1. Перейдіть у Параметри  > Родина під пунктом [ваше ім'я].
2. Торкніть [ім'я учасника], торкніть «[Ім'я учасника]: вилучити з родини», а потім знову торкніть «[Ім'я учасника]: вилучити».

*Примітка.* Якщо ви є організатором родини, ви не можете вилучити себе з групи Сімейного доступу.

## Вилучення учасників із сімейної групи на iPhone чи iPad з iOS 17, iPadOS 17 або попередньою версією







Якщо ви — організатор родини:

1. Перейдіть у Параметри  > [ваше ім'я] > Сімейний доступ.
2. Торкніть [ім'я учасника], потім торкніть «[Ім'я учасника]: вилучити з родини».

*Примітка.* Якщо ви є організатором родини, ви не можете вилучити себе з групи Сімейного доступу.

## Вилучення учасників із сімейної групи на Mac

Якщо ви є організатором родини, ви можете вилучати учасників із сімейної групи, але не можете вилучити самих себе.

1. Виконайте одну з таких дій:
  - На Mac з macOS 15 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», а потім клацніть «Родина» під пунктом [ваше ім'я].
  - На Mac з macOS 13 або macOS 14. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Сімейний доступ» , а потім виберіть «Сімейний доступ» на бічній панелі.
  - На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть «Сімейний доступ» , а потім виберіть «Сімейний доступ».
2. Виконайте одну з таких дій:
  - На Mac з macOS 15 або новішою версією. Виберіть учасника зі списку, клацніть «[Ім'я учасника]: вилучити з родини», а потім знову клацніть «[Ім'я учасника]: вилучити».
  - На Mac з macOS 14 або попередньою версією. Виберіть учасника в списку, потім натисніть , а тоді клацніть, щоб підтвердити намір вилучити його.



## Безпечне зберігання ваших даних в iCloud

iCloud надійно зберігає ваші фото, відео, документи, музику, програми, резервні копії пристроїв тощо і синхронізує їх на всіх ваших пристроях. iCloud також дає змогу поширювати фотографії, календарі, геопозицію тощо для друзів і родини. Увійти в iCloud можна на своєму пристрої або в інтернеті за допомогою облікового запису Apple.

Докладніше про дані, які зберігаються в iCloud, перегляньте в документі [Посібник користувача iCloud](https://support.apple.com/guide/icloud/) (<https://support.apple.com/guide/icloud/>).



## Безпекові опції iCloud






Apple пропонує користувачам дві опції шифрування й захисту даних, які зберігаються в iCloud:

- *Стандартний захист даних (усталений параметр)*. Ваші дані iCloud шифруються, ключі шифрування надійно зберігаються в центрах зберігання даних Apple, і компанія Apple може сприяти вам у відновленні ваших даних і облікового запису. Наскрізне шифрування застосовується лише до певних даних iCloud — це 14 категорій, включно з даними про здоров'я та паролями у В'язці iCloud.
- *Розширений захист даних для iCloud*. Необов'язковий параметр, який пропонує найвищий рівень захисту від компанії Apple для ваших хмарних даних. Якщо ви вирішите увімкнути розширений захист даних, ваші довірені пристрої матимуть виключний доступ до ключів шифрування для більшості ваших даних в iCloud, які захищені методом наскрізного шифрування. За використання розширеного захисту даних кількість категорій даних, до яких застосовуватиметься наскрізне шифрування, збільшується до 23 і включає резервні копії iCloud, Фотографії, Нотатки тощо.

Більше інформації наведено в статтях служби підтримки Apple про те, [як увімкнути розширений захист даних для iCloud](https://support.apple.com/108756) (https://support.apple.com/108756) і [огляд безпеки даних iCloud](https://support.apple.com/102651) (таблиця «Категорії даних і шифрування») (https://support.apple.com/102651).






### Перегляд і редагування параметрів iCloud

Ви можете переглядати та змінювати налаштування iCloud на кожному пристрої, зокрема програми (Apple та сторонніх розробників), які використовують iCloud, а також резервні копії iCloud тощо:


- *На iPhone або iPad.* Перейдіть у Параметри  > [ваше ім'я] > iCloud.  
У разі вимкнення цієї функції ви не зможете використовувати її, якщо ваш пристрій буде втрачено або вкрадено й вимкнено.
- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , а потім — iCloud.
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , а потім — iCloud.

### Вихід з iCloud

Ви також можете повністю вийти з iCloud на пристрої. Якщо ви вийдете з iCloud, резервне копіювання інформації на цьому пристрої більше не буде виконуватися.

- *На iPhone або iPad.* Перейдіть у Параметри  > [ваше ім'я], прокрутіть униз і торкніть «Вийти».
- На Mac з macOS 13 або новішою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , клацніть «Огляд», а потім — «Вийти».
- На Mac з macOS 12 або попередньою версією. Виберіть меню Apple , виберіть «Системні параметри», клацніть обліковий запис Apple , клацніть «Огляд», а потім — «Вийти».

## Керування параметрами безпеки в Повідомленнях

У програмі «Повідомлення»  можна надсилати текстові повідомлення двома відмінними способами:



- Через Wi-Fi чи стільникову службу, коли iMessage використовується для обміну звітками з тими, хто користується службою iMessage на iPhone, iPad чи Mac. У такому разі ваші повідомлення iMessage з'являтимуться в синіх бульбашках.
- Шляхом пересилання SMS/MMS-повідомлень із вашого iPhone чи інших пристроїв. У такому разі ваші SMS/MMS-повідомлення з'являтимуться в зелених бульбашках.

За допомогою iMessage можна надсилати повідомлення, фотографії або відео на інший iPhone, iPad або Mac через Wi-Fi чи стільникові мережі. Ці повідомлення завжди шифруються й відображаються в блакитних текстових бульбашках на ваших iPhone, iPad і Mac.




### Як обмежити використання Повідомлень одним пристроєм

Якщо ви хочете обмежити використання Повідомлень одним пристроєм, потрібно деавторизувати обліковий запис у Повідомленнях на пристроях, де ви більше не хочете отримувати повідомлення, а потім вимкнути Повідомлення в iCloud.

1. Виконайте одну з таких дій:
  - *На iPhone або iPad.* Перейдіть у Параметри  > Повідомлення, а потім увімкніть або вимкніть iMessage.
  - *На Mac.* У програмі «Повідомлення»  виберіть Повідомлення > Параметри, клацніть iMessage, а потім — «Вийти». Підтвердьте свій намір вийти, а потім клацніть «Вийти» ще раз.


### Вимкнення повідомлень в iCloud на iPhone та iPad

Коли ви використовуєте Повідомлення в iCloud, усі повідомлення, які ви надсилаєте, отримуєте й видаляєте, автоматично синхронізуються на всіх ваших пристроях Apple.

1. *На iPhone або iPad.* Перейдіть у Параметри  > [ваше ім'я], а потім торкніть iCloud.
2. У розділі «Програми, які використовують iCloud» торкніть «Показати всі».
3. Торкніть «Повідомлення», а потім вимкніть опцію «Синхронізувати цей [iPhone] [iPad]».
4. Повторіть ці дії для кожного пристрою, щоб вилучити повідомлення з iCloud.

## Вимкнення повідомлень в iCloud на Mac

Коли ви використовуєте Повідомлення в iCloud, усі повідомлення, які ви надсилаєте, отримуєте й видаляєте, автоматично синхронізуються на всіх ваших пристроях Apple.

1. У програмі Повідомлення  на Mac оберіть Повідомлення > Параметри, а потім клацніть iMessage.
2. Клацніть «Параметри», а потім скасуйте вибір параметра «Увімкнути повідомлення в iCloud».
3. Виберіть один із варіантів нижче.
  - *Вимкнути всі.* Буде вимкнено повідомлення в iCloud на всіх ваших пристроях. Повідомлення більше не зберігатимуться в iCloud — натомість вони зберігатимуться на кожному пристрої.
  - *Вимкнути на цьому пристрої.* Буде вимкнено повідомлення в iCloud лише на вашому Mac. Повідомлення з вашого Mac більше не зберігатимуться в iCloud. На інших пристроях, де увімкнуто повідомлення в iCloud, повідомлення й далі зберігатимуться в iCloud.

## Увімкнення та вимкнення iMessage

iMessage використовує наскрізне шифрування, захищаючи ваші повідомлення на всіх ваших пристроях, щоб ніхто не міг отримати до них доступ без вашого коду допуску, включно з Apple. Оскільки обмін повідомленнями iMessage відбувається через Wi-Fi і стільникові мережі, інформація про адресата ваших повідомлень не відображається у вашому рахунку за користування телефоном. Ви можете створювати резервні копії повідомлень iMessage: якщо ваш пристрій загубиться або його вкрадуть, ви матимете змогу відновити важливі обговорення.

**Важливо!** Щоб повідомлення зберігалися в iCloud, необхідно увімкнути резервне копіювання. Якщо цього не зробити, повідомлення не відновляться. Перегляньте розділ [Налаштування iCloud для Повідомлень на всіх ваших пристроях](https://support.apple.com/guide/icloud/mm0de0d4528d) (<https://support.apple.com/guide/icloud/mm0de0d4528d>) у Посібнику користувача iCloud.




## Коли iMessage увімкнено

Ви можете надсилати повідомлення iMessage через Wi-Fi, коли немає доступу до стільникової служби. Функція «Недавно видалені» зберігає видалені повідомлення протягом щонайбільше 30 днів, тому якщо ви вважаєте, що хтось видалив повідомлення з вашого пристрою, їх можна знайти на цій вкладці.

## Коли iMessage вимкнено

Коли iMessage вимкнено, такі функції, як редагування повідомлень, ненадіслані повідомлення та звіти про прочитання недоступні. Натомість повідомлення надсилаються за допомогою SMS/MMS.

**Важливо!** Під час використання SMS/MMS записи про ці повідомлення можуть відображатися у вашому рахунку за користування телефоном, і ці записи цього номера телефону через оператора можуть потрапляти до власника рахунку.




- *На iPhone або iPad.* Перейдіть у Параметри  > Повідомлення, а потім увімкніть або вимкніть iMessage.
- На Mac з macOS 13 або новішою версією. Відкрийте програму «Повідомлення» , виберіть Повідомлення > Параметри, клацніть iMessage, а потім — «Вийти». Підтвердьте свій намір вийти, а потім клацніть «Вийти» ще раз.
- На Mac з macOS 12 або попередньою версією. Відкрийте програму «Повідомлення» , виберіть Повідомлення > Параметри, клацніть iMessage, а потім — «Вийти». Підтвердьте свій намір вийти, а потім клацніть «Вийти» ще раз.

## Увімкнення та вимкнення звітів про прочитання

Звіти про прочитання iMessage дають змогу користувачам iMessage дізнаватися, коли їхні повідомлення прочитують. Увімкнувши звіти про прочитання, автор отриманого вами повідомлення iMessage побачить індикатор прочитання під звісткою, коли ви її прочитаєте. Якщо вимкнути звіти про прочитання, автори повідомлень бачитимуть лише звіт про доставку.

Ви можете надсилати звіти про прочитання для всіх розмов або лише для вибраних. Якщо ви ввімкнули звіти про прочитання для всіх розмов, ви потім усе одно зможете вимкнути їх для певних бесід.

*Примітка.* Звіти про прочитання не підтримуються під час обміну SMS-звістками, а також груповими текстовими повідомленнями.



- *На iPhone або iPad.* Перейдіть у Параметри  > Повідомлення, а потім увімкніть або вимкніть звіти про перегляд.
- На Mac з macOS 13 або новішою версією. Відкрийте програму «Повідомлення» , перейдіть у Повідомлення > Параметри, клацніть вкладку iMessage, а потім виберіть параметр «Звіти про перегляд» або скасуйте його вибір.
- На Mac з macOS 12 або попередньою версією. Відкрийте програму «Повідомлення» , перейдіть у Повідомлення > Параметри, клацніть вкладку iMessage, а потім виберіть параметр «Звіти про перегляд» або скасуйте його вибір.

## Редагування надісланого повідомлення

У системах iOS 16, iPadOS 16.1 і macOS 13 або новіших ви можете редагувати нещодавно надіслані повідомлення до п'яти разів протягом 15 хвилин після надсилання. Це дає змогу виправляти друкарські помилки. Одержувачі бачитимуть, що повідомлення редагувалося й зможуть переглянути історію змін.

*Примітка.* SMS-повідомлення не можна редагувати.


Якщо ваші одержувачі мають пристрої Apple із ранішими версіями iOS, iPadOS чи macOS, вони отримуватимуть подальші повідомлення з префіксом «Змінено на» та вашим новим повідомленням у лапках.

- *На iPhone або iPad.* Торкніть «Повідомлення» , торкніть і утримуйте бульбашку повідомлення, торкніть «Редагувати», а потім змініть повідомлення та надішліть його повторно.
- *На Mac з macOS 13.* Відкрийте Повідомлення , клацніть бульбашку повідомлення, утримуючи Control, виберіть «Редагувати», а потім змініть повідомлення та надішліть його повторно.


## Як відмінити надсилання повідомлення

В iOS 16, iPadOS 16.1 і macOS 13 або новіших версіях ви можете скасовувати надсилання нещодавно надісланих повідомлень протягом 2 хвилин після надсилання. Це дає змогу відкликати повідомлення, яке було випадково надіслано хибному адресату. Одержувачі бачать, що надсилання повідомлення було скасовано.

*Примітка.* Надсилання SMS-повідомлень не можна скасувати.

- *На iPhone або iPad.* Торкніть «Повідомлення» , торкніть і утримуйте бульбашку повідомлення, а потім торкніть «Відмінити надсилання».

Примітка з підтвердженням того, що надсилання повідомлення скасоване, з'явиться в записі розмови у вас і в одержувача.

- *На Mac з macOS 13 або новою версією.* Відкрийте «Повідомлення» , клацніть бульбашку повідомлення, утримуючи Control, а потім виберіть «Відмінити надсилання».

Примітка з підтвердженням того, що надсилання повідомлення скасоване, з'явиться в записі розмови у вас і в одержувача.

## Реагування на шахрайські запити спільного доступу до інформації

Будьте обережні, якщо ви отримуєте небажані повідомлення з пропозицією прийняти подарунки, завантажити документи, встановити програмне забезпечення або перейти за підозрілими посиланнями. Люди, які хочуть отримати доступ до ваших персональних даних, використовують будь-які засоби, як-от підроблені е-листи й текстові повідомлення, оманливу спливу рекламу, недостовірні викачування, календарний спам і навіть шахрайські телефонні виклики, щоб обманом отримати від вас інформацію, зокрема ваш обліковий запис Apple чи пароль, або щоб змусити вас надати код підтвердження для двофакторної автентифікації.

Щоб отримати поради щодо того, як уникнути обману та не скомпрометувати свої облікові записи або особисту інформацію, перегляньте статтю служби підтримки Apple про [розпізнавання та уникнення фішингових повідомлень, оманливих служб підтримки та інших проявів шахрайства](https://support.apple.com/102568) (<https://support.apple.com/102568>).

*Примітка.* Фішинг — це шахрайські спроби отримати від вас особисту інформацію.

## Блокування викликів і повідомлень від певних осіб

Якщо ви отримуєте дзвінки, дзвінки FaceTime, повідомлення або е-листи від небажаних абонентів, ви можете заблокувати їх, щоб вони не могли зв'язуватися з вами в майбутньому. Якщо ви заблокуєте когось на одному пристрої, цю особу буде заблоковано на всіх пристроях Apple, на яких виконано вхід з використанням того самого облікового запису Apple.

▼ **ВАЖЛИВО.** Особа, яку ви блокуєте, не отримає сповіщення про те, що її заблокували, і ви й далі можете телефонувати, надсилати повідомлення чи е-листи заблокованим контактам, не розблоковуючи їх. Але якщо ви ділилися із цією людиною своєю геопозицією, вона *отримає* сповіщення про те, що ви припинили ділитися своєю геопозицією після того, як заблокували її.

Блокування контакту в одній із програм «Телефон», FaceTime, «Повідомлення» або «Пошта» блокує його в усіх чотирьох програмах.



## Блокування голосових викликів, викликів у FaceTime, повідомлень та Пошти від певних людей

- *Програма «Телефон» на iPhone.* У програмі «Телефон» торкніть «Улюблені», «Недавні» або «Гол. пошта», торкніть ⓘ поруч з іменем, номером телефону або адресою е-пошти контакту, який ви хочете заблокувати, прокрутіть униз, торкніть «Заблокувати абонента», а потім — «Заблокувати контакт».
- *Програма FaceTime на iPhone чи iPad.* В історії викликів FaceTime торкніть ⓘ поруч з іменем, номером телефону або адресою е-пошти контакту, який ви хочете заблокувати, прокрутіть униз, торкніть «Заблокувати абонента», а потім — «Заблокувати контакт».
- *Програма FaceTime на пристрої Mac.* В історії викликів FaceTime натисніть, утримуючи клавішу Control, ім'я, номер телефону або адресу е-пошти контакту, який потрібно заблокувати, а потім виберіть «Заблокувати абонента».
- *Програма «Повідомлення» на iPhone чи iPad.* У Повідомленнях торкніть обговорення, торкніть ім'я або номер угорі обговорення, торкніть ⓘ, прокрутіть униз, а потім торкніть «Заблокувати абонента».
- *Програма «Повідомлення» на Mac.* В історії програми «Повідомлення» виберіть ім'я, номер телефону або адресу е-пошти людини, яку треба заблокувати. У меню «Бесіди» виберіть «Блокувати особу», потім клацніть «Блокувати».
- *Програма «Пошта» на iPhone або iPad.* Відкрийте програму «Пошта» ✉, виберіть повідомлення е-пошти від відправника, торкніть його ім'я у верхній частині листа, виберіть «Блокувати цей контакт», а потім торкніть пункт «Блокувати цей контакт».
- *Програма «Пошта» на Mac.* Відкрийте програму «Пошта», виберіть повідомлення е-пошти від відправника, клацніть його ім'я у верхній частині листа, а потім у спадному меню виберіть «Блокувати цей контакт».





Іконка блокування 🚫 з'являється поруч з іменем відправника в списку повідомлень, а до їхніх повідомлень додається банер, який указує на блокування. Банер також містить посилання на панель «Заблоковані» в параметрах Пошти, звідки можна керувати заблокованими відправниками.

*Примітка.* Якщо відправника раніше було позначено як VIP у пошті, слід спочатку натиснути «Вилучити з VIP», перш ніж його можна буде заблокувати.



## Керування заблокованими контактами

Керувати своїми заблокованими контактами можна за допомогою будь-якої з чотирьох програм, які дозволяють блокування: «Телефон», «FaceTime», «Повідомлення» та «Пошта». Розблокування в одній програмі призведе до розблокування в усіх чотирьох програмах. Щоб переглянути список заблокованих номерів, виконайте будь-які з таких дій:

- *iPhone*. Перейдіть у Параметри  > Телефон, а потім торкніть «Заблоковані контакти».
- *FaceTime на iPhone чи iPad*. Перейдіть у Параметри  > FaceTime, а потім у розділі «Виклики» торкніть «Заблоковані контакти».
- *FaceTime на Mac*. Відкрийте FaceTime, перейдіть у FaceTime > Параметри, а потім клацніть «Заблоковані».
- *Програма «Повідомлення» на iPhone чи iPad*. Перейдіть у Параметри  > Повідомлення, а потім у розділі «SMS/MMS» торкніть «Заблоковані контакти».
- *Програма «Повідомлення» на Mac*. Відкрийте програму «Повідомлення», перейдіть у Повідомлення > Параметри, клацніть iMessage, а потім клацніть «Заблоковані».
- *Програма «Пошта» на iPhone або iPad*. Перейдіть у Параметри > Пошта, а потім у розділі «Групування» торкніть «Заблоковані».
- *Програма «Пошта» на Mac*. Відкрийте програму «Пошта», перейдіть у Пошта  > Параметри, клацніть «Спам-фільтр», а потім — «Заблоковані».

## Безпечне використання NameDrop

### Що таке NameDrop?

Завдяки функції NameDrop (що є частиною AirDrop) користувачі iPhone і Apple Watch можуть легко ділитися своєю контактною інформацією, просто наблизивши свої пристрої один до одного. Ви можете обрати конкретні контактні дані, якими хочете або не хочете ділитися.


Функція NameDrop працює автоматично. Якщо потрібно вимкнути NameDrop, перегляньте розділ [Вимкнення NameDrop](#) далі в цьому посібнику.

*Примітка.* Для використання NameDrop необхідно, щоб на обох пристроях було встановлено iOS 17.1, iPadOS 17.1, watchOS 10.1 або новішу версію на iPhone, Apple Watch SE 2-го покоління, Apple Watch Series 7, Apple Watch Ultra або новішій моделі.

## Огляд і оновлення відомостей у своїй картці контакту

Ви можете оновлювати інформацію, яка поширюється через NameDrop шляхом оновлення своєї картки контакту (наприклад, якщо ви хочете лише поділитися своїм ім'ям чи ініціалами).

*Примітка.* Функція NameDrop поширює лише вибрані вами ім'я, номер телефону чи е-адресу, а також інформацію про обкладинку контакту, пов'язану з картою контакту. Ця функція не поширює іншу інформацію з вашої картки контакту, як-от домашню адресу чи день народження. Коли ви ділитесь своєю інформацією через програму «Контакти» чи NameDrop, стандартно ваші займенники не повідомляються. Коли ви ділитесь чиеюсь інформацією, їхні займенники ніколи не повідомляються.

1. Відкрийте програму «Контакти» .
2. Торкніть Моя картка > Редагувати.
3. Перегляньте й оновіть відомості про своє ім'я, номери телефонів і е-адреси, які ви хочете поширювати через NameDrop.


Докладніше дивіться в розділі:

- [Додавання або редагування контактної інформації та фото на iPhone](https://support.apple.com/guide/iphone/iph18b749db1) у посібнику користувача iPhone (https://support.apple.com/guide/iphone/iph18b749db1)
- [Додавання або редагування контактної інформації та фото на iPad](https://support.apple.com/guide/ipad/ipadfcfa2d42) у посібнику користувача iPad (https://support.apple.com/guide/ipad/ipadfcfa2d42)

## Поширення контактних даних

Ви можете ділитися своєю контактної інформацією з іншими людьми.

1. Виконайте одну з таких дій:
  - *Надсилання з iPhone чи iPad.* Тримайте свій iPhone на відстані кількох сантиметрів над iPhone або Apple Watch іншої людини.
  - *Надсилання з Apple Watch на Apple Watch.* Відкрийте програму «Контакти»  на своєму Apple Watch, торкніть зображення у верхньому правому куті, торкніть «Поширити», а потім піднесіть годинник до Apple Watch іншої людини.
  - Екрани обох пристроїв почнуть світитися, а Apple Watch почне вібрувати, вказуючи на встановлення з'єднання.
2. Продовжуйте тримати пристрої поруч, поки на їх екранах не з'явиться NameDrop.
3. Виберіть поширення своєї картки контакту (або певного номера телефону чи е-адресу) й отримання відомостей іншої людини або лише отримання інформації іншої людини.


Якщо ви поширюєте свою контактну картку, можете торкнутися , вибрати поля, які потрібно включити, а потім торкнутися «Зберегти». Наступного разу, під час використання NameDrop, буде вибрано ті самі поля.

Щоб скасувати, перемістіть пристрої подалі один від одного або замкніть свій iPhone, перш ніж завершиться передавання через NameDrop.

Докладніше дивіться в розділі:

- [Використання NameDrop на Apple Watch для поширення контактних даних у посібнику користувача Apple Watch \(https://support.apple.com/guide/watch/apd8ebed6c09#apdd22da5d51\)](https://support.apple.com/guide/watch/apd8ebed6c09#apdd22da5d51)

## Вимкнення NameDrop

1. Відкрийте програму «Параметри» .
2. Торкніть Загальні > AirDrop.
3. Вимкніть параметр «Піднесення пристроїв один до одного».

## Керування параметрами спільного доступу до Фотографій на пристроях Apple

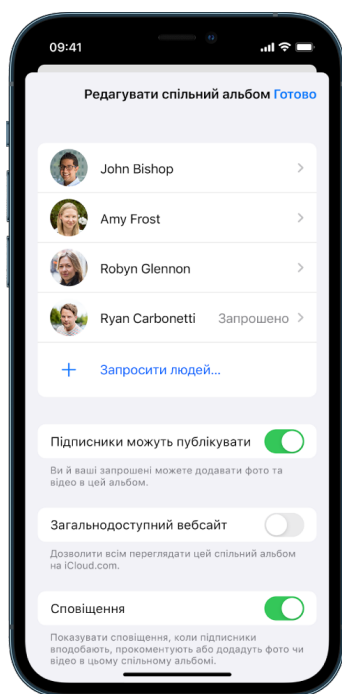
За допомогою спільних альбомів у Фотографіях можна вибрати фото і відео, якими ви хочете поділитися, а також людей, яким ви хочете надати доступ до них. Ви також можете будь-коли змінити параметри спільного доступу. Якщо ви припините поширення фотографії чи альбому для когось із користувачами, ця людина більше не матиме доступу до спільного альбому та його вмісту.

Якщо ви підписалися на спільний альбом, то можете видалити будь-які фотографії, якими ви поділилися. Ви також можете вибрати «Скасувати підписку», щоб відмовитися від підписки на спільний альбом.



Щоб керувати тим, для кого ви поширюєте вміст зі свого Mac, дивіться розділ [Керування параметрами «Поширено для вас» на пристроях Apple](#) далі в цьому посібнику.

## Керування параметрами поширення для спільних альбомів у Фотографіях на iPhone або iPad



1. Виберіть спільний альбом на своєму iPhone чи iPad, а потім торкніть «Запросити людей».
2. Виконайте будь-які з таких дій:
  - *Щоб запросити нових підписників.* Торкніть «Запросити людей», а потім введіть імена підписників, яких ви хочете додати.  
Підписники можуть додавати фото й відео до цього альбому. Вимкніть кнопку «Підписники можуть публікувати» для того, щоб тільки ви могли додавати фото й відео.
  - *Щоб вилучити підписників.* Торкніть ім'я підписника, потім торкніть «Вилучити підписника».
  - *Щоб вилучити себе зі спільного альбому.* Виконайте одну з таких дій:
    - Торкніть три крапки у верхньому правому куті, а потім — «Відписатися».
    - Торкніть іконку облікового запису iCloud у верхньому правому куті, а потім — «Відписатися».
  - *Щоб вимкнути сповіщення.* Проведіть пальцем, щоб вимкнути «Сповіщення».

Докладніше дивіться в розділі:

- «[Поширення фото й відео на iPhone](https://support.apple.com/guide/iphone/iphf28f17237)» у Посібнику користувача iPhone (<https://support.apple.com/guide/iphone/iphf28f17237>)
- «[Поширення фото й відео на iPad](https://support.apple.com/guide/ipad/ipad4f44c78f)» у Посібнику користувача iPad (<https://support.apple.com/guide/ipad/ipad4f44c78f>)

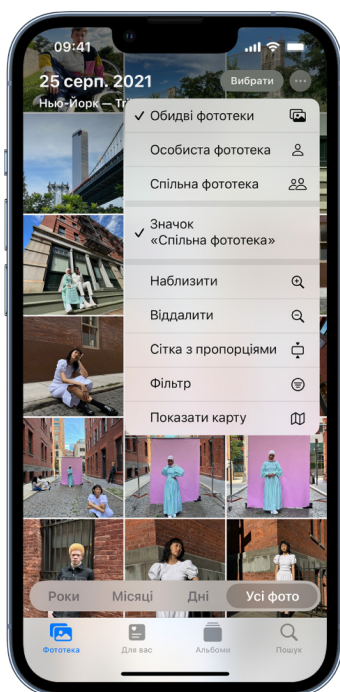
## Керування параметрами Спільної фототеки iCloud на iPhone або iPad


Спільна фототека iCloud дає змогу легко ділитися фотографіями та відео з п'ятьма іншими людьми. Коли ви додаєте фото й відео в Спільну фототеку iCloud, вони переміщуються з вашої персональної фототеки в спільну. За допомогою спільної фототеки можна обирати вміст для поширення та автоматично ділитися вмістом безпосередньо з камери. Усі учасники мають однакові дозволи на додавання, редагування та видалення вмісту в спільній фототеці. Водночас особа, яка налаштувала спільну фототеку, тобто автор фототеки, надає сховище iCloud для всього вмісту.

Учасники можуть вийти зі спільної фототеки в будь-який момент.

Якщо ви є автором фототеки, ви можете вилучати учасників зі спільної фототеки або видалити її в будь-який момент. Коли ви вилучаєте учасників зі своєї спільної фототеки, вони отримують сповіщення й можуть скопіювати всі елементи зі спільної фототеки у свої особисті фототеки. Учасник не може вилучати інших учасників.

*Примітка.* Для використання спільних фототек у Фотографіях потрібна iOS 16, iPadOS 16.1 або новіша версія. Щоб дізнатися версію програмного забезпечення, інсталюваного на вашому пристрої, перейдіть у Параметри > Загальні, а потім торкніть «Про пристрій».



- Перейдіть у Параметри  > Фотографії > Спільна фототека, а потім виконайте будь-які з таких дій:
  - *Щоб вилучити учасників зі Спільної фототеки.* Торкніть «Видалити учасників».
  - *Щоб вийти зі Спільної фототеки.* Торкніть «Вийти зі Спільної фототеки».

Коли ви виходите зі спільної фототеки, ви можете скопіювати все зі спільної фототеки у власну фототеку або лише той вміст, який додавали ви.

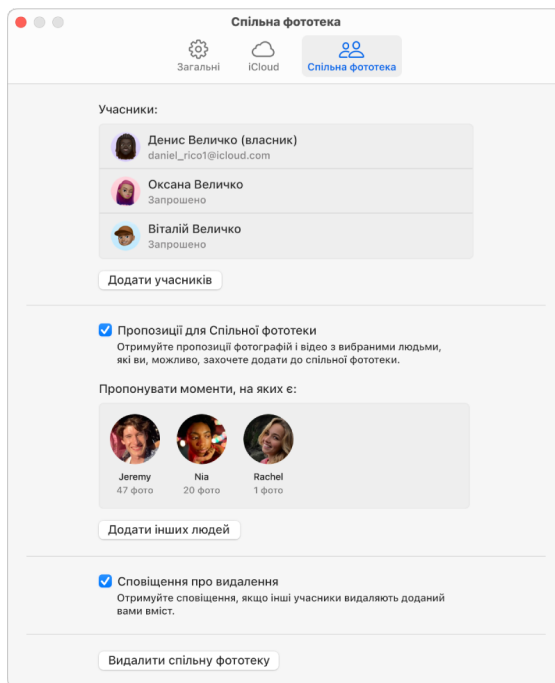
  - *Щоб видалити Спільну фототеку (ви повинні бути її організатором).* Торкніть «Видалити Спільну фототеку».



Усі учасники отримують сповіщення, що спільну фототеку видалено.

Докладніше дивіться в розділі:

- [Налаштування Спільної фототеки iCloud або приєднання до неї у Фотографіях у Посібнику користувача iPhone \(https://support.apple.com/guide/iphone/iph28ac9ea81\)](https://support.apple.com/guide/iphone/iph28ac9ea81)
- [Налаштування Спільної фототеки iCloud або приєднання до неї у Фотографіях у Посібнику користувача iPad \(https://support.apple.com/guide/ipad/ipad94c5ed43\)](https://support.apple.com/guide/ipad/ipad94c5ed43)

## Керування параметрами поширення для спільних альбомів у Фотографіях на Mac



1. Відкрийте програму «Фотографії»  на своєму Mac, а потім клацніть спільний альбом у розділі «Спільні альбоми» на бічній панелі.
2. Клацніть  на панелі інструментів.
3. У полі «Запросити людей» виконайте одну з наведених нижче дій:
  - *Запросити нових підписників* Введіть адресу е-пошти.


Якщо особа, яку ви запрошуєте, не використовує iCloud, ви можете встановити прапорець «Публічний вебсайт», щоб створити URL-адресу для вашого спільного альбому. Будь-хто із цією URL-адресою може переглядати та викачувати вміст спільного альбому.

- *Вилучити підписників.* Виберіть адресу е-пошти підписника, а потім натисніть «Видалити».
- *Повторно запросити підписника.* Клацніть стрілку вниз біля імені абонента та виберіть «Відправити запрошення ще раз».



Докладніше дивіться в розділі:

- [Що таке спільні альбоми у Фотографіях на Mac](https://support.apple.com/guide/photos/pht7a4c765b) у Посібнику користувача Фотографій (https://support.apple.com/guide/photos/pht7a4c765b)
- [Підписка на спільні альбоми у Фотографіях на Mac](https://support.apple.com/guide/photos/pht884a8908) у Посібнику користувача Фотографій (https://support.apple.com/guide/photos/pht884a8908)

### **Вилучення учасників зі Спільної фототеки iCloud на Mac**

*Примітка.* Для роботи спільних бібліотек у Фотографіях на Mac потрібна macOS 13 або новіша версія. Щоб дізнатися версію операційної системи, яку встановлено на вашому пристрої, відкрийте меню Apple  у верхньому лівому куті свого екрана та виберіть «Про цей комп'ютер».

Якщо учасник мав доступ до Спільної фототеки менше ніж 7 днів, він може отримувати лише ті елементи, які додав сам.

1. У програмі «Фотографії»  на Mac оберіть меню Фотографії > Параметри, а потім клацніть «Спільна фототека».
2. Клацніть  поряд з особою, яку потрібно вилучити, а потім виберіть «Вилучити».
3. Клацніть «Вилучити» в меню «Спільна фототека».

Докладніше дивіться в розділі:


- [Що таке Спільна фототека iCloud у Фотографіях на Mac](https://support.apple.com/guide/photos/pht153ab3a01) у Посібнику користувача Фотографій (https://support.apple.com/guide/photos/pht153ab3a01)




## Як вийти зі Спільної фототеки iCloud або видалити її у Фотографіях на Mac

Учасники можуть вийти зі спільної фототеки в будь-який момент. Якщо ви є автором спільної фототеки, ви можете її видалити. Коли ви видаляєте спільну фототеку, усі учасники отримують сповіщення й можуть зберегти всі елементи зі спільної фототеки у своїй особистій фототеці.

Якщо ви вийдете зі спільної фототеки протягом 7 днів після приєднання, ви можете залишити лише ті, елементи які самі додали.

*Примітка.* Для роботи спільних бібліотек у Фотографіях на Mac потрібна macOS 13 або новіша версія. Щоб дізнатися версію операційної системи, яку встановлено на вашому пристрої, відкрийте меню Apple  у верхньому лівому куті свого екрана та виберіть «Про цей комп'ютер».

1. У програмі «Фотографії»  на Mac оберіть меню Фотографії > Параметри, а потім клацніть «Спільна фототека».
2. Клацніть «Вийти зі Спільної фототеки» (якщо ви учасник) або «Видалити спільну фототеку» (якщо ви автор).
3. Виберіть одну з наведених нижче опцій.
  - *Залишити все.* Додайте всі фотографії зі спільної фототеки у свою особисту фототеку.
  - *Залишити лише додане мною.* Додайте всі фотографії, додані вами в спільну фототеку, у свою особисту фототеку.
4. Клацніть «Видалити спільну фототеку», а потім клацніть «Видалити спільну фототеку» знову, щоб підтвердити видалення.

Докладніше дивіться в розділі:

- [Що таке Спільна фототека iCloud у Фотографіях на Mac](https://support.apple.com/guide/photos/pht153ab3a01) у Посібнику користувача Фотографій (https://support.apple.com/guide/photos/pht153ab3a01)
- [Як вийти зі спільної фототеки або видалити її](https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22) у Посібнику користувача Фотографій (https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22)

## Керування спільними групами вкладок у Safari



Ви можете поділитися групою вкладок і співпрацювати з людьми, які використовують iCloud. Доступ до спільної групи вкладок можуть мати загалом 100 учасників. Учасники можуть додавати й вилучати вкладки в меню «Група вкладок», і всі учасники бачитимуть зміни в реальному часі.

Кожен, з ким ви співпрацюєте, повинен увійти у свій обліковий запис Apple, увімкнути Safari в параметрах iCloud (<https://support.apple.com/guide/iphone/iphde0f868fd>) і увімкнути двофакторну автентифікацію.



### Керування спільними групами вкладок у Safari на iPhone або iPad

Якщо кнопка «Співпраця» не відображається, це означає, що у вас немає спільних груп вкладок.



1. Торкніть Safari , а потім торкніть  у верхньому правому куті.
2. Торкніть «Керувати спільною групою вкладок», а потім виконайте будь-які з таких дій:
  - *Вилучення учасника.* Торкніть ім'я людини, а потім торкніть «Вилучити доступ».
  - *Припинення спільного доступу для всіх.* Торкніть «Припинити поширення».
  - *Додавання учасника.* Торкніть «Поширити для інших людей» та запросіть учасників.

Докладніше дивіться в розділі:

- [Додавання та вилучення людей зі спільної групи вкладок](https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659) у Посібнику користувача iPhone (<https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659>)
- [Додавання та вилучення людей зі спільної групи вкладок](https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8) у Посібнику користувача iPad (<https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8>)

## Керування спільними групами вкладок у Safari на Mac

Якщо кнопка «Співпраця» не відображається, це означає, що у вас немає спільних груп вкладок.

1. У програмі Safari  на Mac клацніть  на панелі інструментів.
2. Клацніть «Керувати спільною групою вкладок», а потім виконайте будь-які з таких дій:
  - *Вилучення учасника.* Клацніть ім'я, клацніть «Заборонити доступ», а потім клацніть «Продовжити».
  - *Припинення спільного доступу для всіх.* Клацніть «Припинити поширення», а потім клацніть «Продовжити».
  - *Додавання учасника.* Клацніть «Поширити для інших людей», відтак клацніть «Повідомлення», щоб запросити людей.

Докладніше дивіться в розділі:

- [Додавання та вилучення людей зі спільної групи вкладок](https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659) у Посібнику користувача Safari (<https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659>)

## Забезпечення приватності історії перегляду в Safari і на Картах

Варто переглядати й очищувати історію пошуку та збоїв браузерів та інших програм, якщо вас непокоїть доступність вашого пристрою для інших користувачів. Багато програм зберігають інформацію про ваші пошукові запити та перегляди, щоб у майбутньому вам було легше знайти раніше переглянуте. Наприклад, коли ви використовуєте програму «Карти», історія місць, які ви шукали та переглядали, допоможе легше переходити до нещодавно відвіданих місць.



Якщо ви перебуваєте в небезпечній особистій ситуації та вам потрібно шукати стратегії безпеки онлайн, але ви не хочете, щоб браузер Safari зберігав записи про те, що ви переглядали, можна відкрити вікно приватного перегляду на iPhone, iPad і Mac. Під час використання режиму «Приватний перегляд» деталі вашого перегляду не зберігаються і не поширюються на ваших інших пристроях. Крім того, якщо ви оновили операційну систему пристроїв до iOS 17, iPadOS 17 або macOS 14, Safari замикає вкладки приватного перегляду через певний період неактивності, тож відкрити їх можна, тільки ввівши пароль, код допуску, Face ID або Touch ID. Це захищає приватність ваших даних, коли ви відходите від пристрою. Ви можете очистити історію перегляду й відкрити вікно приватного перегляду на iPhone, iPad і Mac.

Дізнайтеся, як відкрити вікно приватного перегляду на iPhone, iPad або Mac, далі в цьому посібнику.



### Очищення історії перегляду в Safari

Якщо ви шукали інформацію про стратегії безпеки в Інтернеті й стурбовані тим, що хтось може побачити вашу історію перегляду, ви можете видалити всі записи Safari про ваш перегляд.



- *На iPhone або iPad.* Перейдіть у Параметри  > Safari > «Стерти історію і дані сайтів».
- *На Mac.* Відкрийте програму Safari , виберіть Історія > Очистити історію, клацніть спливне меню, а потім виберіть період, який ви хочете видалити.

Під час очищення історії Safari видаляє дані, збережені в результаті вашого перегляду, зокрема:


- історію відвіданих вебсторінок;

- список переходів із відкритих вебсторінок та на них;
- список часто відвідуваних сайтів;
- останні пошуки;
- іконки для вебсторінок;
- миттєві знімки, збережені для відкритих вебсторінок;
- список елементів, які ви завантажили (завантажені файли не видаляються);
- вебсайти, які ви додали для швидкого пошуку вебсайтів;
- вебсайти, які запитували дозвіл на використання вашої геопозиції;
- вебсайти, які запитували дозвіл на надсилання вам сповіщень.



### **Очищення нещодавніх маршрутів і улюблених елементів у Картах на iPhone або iPad**

1. Відкрийте програму «Карти» , відтак прокрутіть список результатів у полі пошуку до розділу «Недавні».
2. Виконайте одну з таких дій:
  - Змахніть нещодавній маршрут ліворуч.
  - Торкніть «Більше» безпосередньо над списком, а потім змахніть нещодавній маршрут ліворуч, або щоб видалити групу маршрутів, торкніть «Очистити» над групою.
3. Якщо ви хочете вилучити улюблене місце, прокрутіть сторінку до розділу «Улюблене», а потім торкніть «Більше». Проведіть справа наліво по улюбленому місцю, яке потрібно видалити, або торкніть «Редагувати», а потім — , щоб вилучити кілька улюблених елементів.

### **Очищення нещодавніх маршрутів і улюблених елементів у «Картах» на Mac**



1. Відкрийте програму «Карти» , а потім прокрутіть сторінку до розділу «Недавні» на бічній панелі.
2. Під розділом «Недавні» клацніть «Очистити недавні».
3. Якщо ви хочете вилучити улюблене місце, клацніть місце, утримуючи Control (на бічній панелі під елементом «Улюблені»), а потім виберіть «Вилучити з Улюблених».


## Відкриття вікна приватного перегляду на iPhone

1. Відкрийте програму Safari.
2. Торкніть .
3. Торкніть  унизу по центру смуги вкладок у нижній частині екрана, а потім торкніть «Приватні».

Вкладка автоматично додається до групи вкладок під назвою «Приватні». У групі можна відкрити кілька приватних вкладок.

Ви можете легко перевірити, що ви перебуваєте в режимі «Приватний перегляд», переконавшись, що рядок поля пошуку сірий або відображає слово «Приватно».


Щоб приховати сайти й вийти з режиму «Приватний перегляд», торкніть , а потім — , щоб відкрити іншу групу вкладок у меню внизу екрана. Приватні сайти з'являться знову, коли ви наступного разу скористаєтеся режимом «Приватний перегляд».

Щоб закрити приватні вкладки, торкніть , а потім проведіть пальцем ліворуч по кожній із вкладок, які потрібно закрити.


## Відкриття вікна приватного перегляду на iPad

- У програмі Safari торкніть , потім торкніть «Приватно».

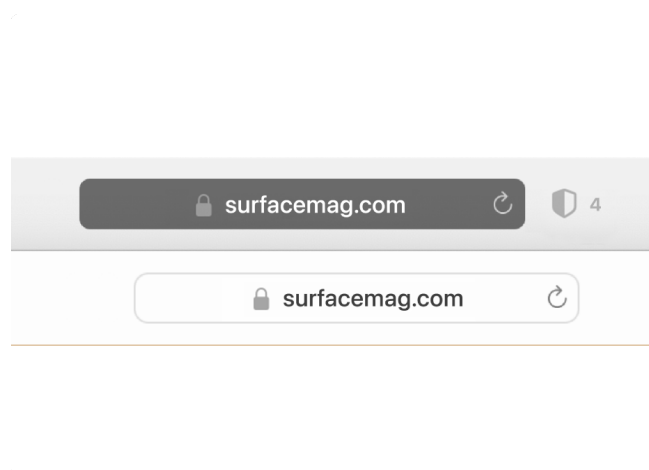
Коли ввімкнено режим приватного перегляду, фон поля пошуку чорний замість білого, а сайти, які ви відвідуєте, не відображаються в історії на iPad або в списку вкладок на інших ваших пристроях. У групі приватних вкладок можна відкрити кілька приватних вкладок.

Щоб приховати сайти й вийти з режиму «Приватний перегляд», торкніть , а потім перейдіть до іншої групи вкладок. Вкладки з'являться знову, коли ви наступного разу скористаєтеся режимом «Приватний перегляд».

## Відкриття вікна приватного перегляду на Mac

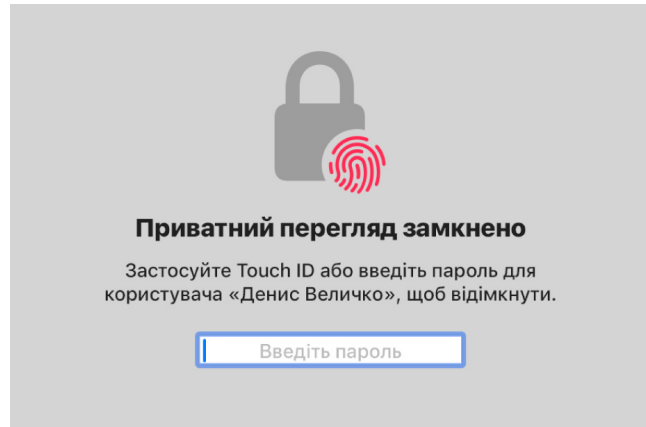
1. У програмі Safari  виберіть «Файл» > «Нове приватне вікно», або перемкніться на вікно Safari, у якому вже використовується режим «Приватний перегляд».

У вікні приватного перегляду є темне поле динамічного пошуку з білим текстом.




2. Переглядайте вебсайти як зазвичай.





*Примітка.* Коли пристрій замкнено або він перебуває в режимі сну, а також якщо ви не використовуєте Safari, ваші приватні вікна в Safari замикаються. Коли ви відмикаєте пристрій чи виводите його з режиму сну, а також якщо знову починаєте використовувати Safari, просто відімкніть приватне вікно за допомогою Face ID, Touch ID, коду допуску пристрою або пароля.



### Якщо необхідно завжди відкривати вікна в режимі приватного перегляду на Mac

1. У програмі Safari  виберіть Safari > «Параметри», потім клацніть «Загальні».
2. Клацніть спливне меню «Під час запуску Safari відкривати» та потім виберіть «Нове приватне вікно».

Якщо ця опція не відображається, виконайте одну з наведених нижче дій:

- На Mac з macOS 13 або новішою версією. Відкрийте меню Apple , виберіть «Системні параметри», клацніть «Робочий стіл і Dock» , а потім переконайтеся, що вибрано параметр «Закривати вікна в разі завершення роботи програми».
- На Mac з macOS 12 або попередньою версією. Відкрийте меню Apple , виберіть «Системні параметри», клацніть «Загальні» , а потім переконайтеся, що вибрано параметр «Закривати вікна в разі завершення роботи програми».

### Для подальшого підвищення конфіденційності Safari

- Видаліть усі елементи з папки «Викачане», які були викачані під час використання вікон приватного перегляду.
- Закрийте будь-які інші вікна приватного перегляду, які все ще відкриті, щоб інші люди не могли використовувати кнопки «Назад» і «Уперед» для перегляду сторінок, які ви відвідали.


## Керування параметрами «Поширено для вас» на пристроях Apple

Коли хтось ділиться з вами вмістом із програм «Музика», Apple TV, News, «Фотографії», «Подкасти» та Safari, ви можете автоматично впорядкувати такий вміст у розділ «Поширено для вас» для легкого доступу. Вміст, яким із вами поділилися в програмі «Повідомлення», автоматично впорядковується в розділ «Поширено для вас» у програмах «Музика», Apple TV, News, «Фотографії», «Подкасти» та Safari.



### Керування за конкретною людиною на iPhone або iPad

Якщо ви не хочете відображати певний вміст, поширений для вас через програму «Повідомлення», у пов'язаних програмах, ви можете вимкнути цю функцію для конкретного користувача.

1. Торкніть «Повідомлення»  на своєму iPhone або iPad, а потім торкніть розмову із вмістом, який ви не хочете відображати в пов'язаних програмах.
2. Коли розмова відкриється, торкніть ім'я користувача у верхній частині.
3. Вимкніть «Показати» в розділі «Поширено для вас», потім торкніть «Готово».



Докладніше дивіться в розділі:

- [Використання Повідомлень для отримання та поширення вмісту для друзів у Посібнику користувача iPhone](https://support.apple.com/guide/iphone/iphb66cfeaad) (<https://support.apple.com/guide/iphone/iphb66cfeaad>)
- [Використання Повідомлень для отримання та поширення вмісту для друзів у Посібнику користувача iPad](https://support.apple.com/guide/ipad/ipad5bf3d77b) (<https://support.apple.com/guide/ipad/ipad5bf3d77b>)



## Керування за конкретною людиною на Mac

Якщо ви не хочете відображати певний вміст, поширений для вас через програму «Повідомлення», у пов'язаних програмах, ви можете вимкнути цю функцію для конкретного користувача.

1. Відкрийте програму «Повідомлення»  на своєму Mac, а потім виберіть розмову.
2. Натисніть  у верхньому правому куті обговорення, а потім зніміть прапорець «Показувати в розділі "Поширено для вас"», щоб вилучити спільний вміст із розділу «Поширено для вас».


Якщо «Поширено для вас» вимкнено, ви все одно можете закріпити спільний вміст, щоб відображати його у відповідній програмі.

Докладніше дивіться в розділі:

- [Відстеження поширеного вмісту в Повідомленнях на Mac](https://support.apple.com/guide/messages/ichtdc9ebc32) у посібнику користувача Mac (<https://support.apple.com/guide/messages/ichtdc9ebc32>)


## Керування за конкретною програмою на iPhone або iPad

Якщо ви хочете вимкнути функцію «Поширено для вас» у програмах «Музика», Apple TV, News, «Фотографії», «Подкасти» або Safari, можете змінити параметри.

- На своєму iPhone або iPad перейдіть у Параметри  > Повідомлення > Поширено для вас, а потім вимкніть «Автоматичне поширення» або вимкніть параметр «Поширено для вас» для певної програми.

## Керування за конкретною програмою на Mac

Якщо ви хочете вимкнути функцію «Поширено для вас» у програмах «Музика», Apple TV, News, «Фотографії», «Подкасти» або Safari, можете змінити параметри.

1. Відкрийте програму «Повідомлення»  на своєму Mac.
2. Виберіть Повідомлення > Параметри.
3. Клацніть «Поширено для вас» і виконайте одну з наведених нижче дій:
  - *Щоб вимкнути всі програми.* Клацніть «Вимкнути».
  - *Щоб вимкнути вибрані програми.* Скасуйте вибір програм.

Докладніше дивіться в розділі:

- [Відстеження поширеного вмісту в Повідомленнях на Mac](https://support.apple.com/guide/messages/ichtdc9ebc32) у посібнику користувача Mac (<https://support.apple.com/guide/messages/ichtdc9ebc32>)

# Додаткова інформація

## Міркування безпеки

Перед тим як вносити зміни чи видаляти інформацію, майте на увазі:

- Може бути доцільно зробити запис підозрілої активності. Дивіться також розділ [Отримання доказів, пов'язаних з іншим обліковим записом Apple](#).
- Зміни, які ви вносите в параметри поширення чи доступу, можуть побачити інші люди. У цьому посібнику інформацію, що стосується безпеки і яку може бути доцільно взяти до уваги, перш ніж вживати заходів, позначено такою іконкою: .
- Коли ви вносите зміни в спільний доступ до інформації, ви можете втратити доступ до важливих для вас інструментів і даних.
- Програми, розроблені іншими компаніями (як-от Youtube або Instagram), мають власні параметри, на які Apple не має впливу. Перегляньте інструкції для кожної окремої програми щодо перевірки того, чи надсилають ці програми сповіщення про зміни, а також керування цим процесом. Для отримання додаткової інформації дивіться розділ [Параметри сторонніх програм](#).

## Інші ресурси з питань безпеки, пов'язаних із технологіями

Додаткову інформацію або підтримку з питань безпеки, пов'язаних із технологіями, можна знайти на зазначених нижче вебсайтах.

### США

- [The Safety Net Project](#) при National Network to End Domestic Violence
- [National Center for Victims of Crime](#)

### Велика Британія

- [Refuge UK](#)

### Австралія

- [WESNET Safety Net Australia](#)

Дата опублікування: 28 жовтня 2024 року

## Інші допоміжні ресурси

Щодо інших питань, що стосуються Apple, звертайтеся до зазначених нижче ресурсів.

### Служба підтримки Apple

Загальна підтримка з питань, пов'язаних з Apple, у вигляді ресурсів для самопомоги або зв'язку з експертом. Служба підтримки Apple має вкрай обмежений доступ до вашої інформації без вашого явного дозволу і не має доступу до ваших даних і паролів.

- [Служба підтримки Apple](https://support.apple.com) (https://support.apple.com)
- США: 1-800-275-2273; Канада: 1-800-263-3394

### Безпека на платформах Apple

На сайті [безпеки на платформах Apple](#) можна знайти інформацію про безпеку на рівні обладнання й системи, шифрування та захист даних, а також безпеку служб, як-от обліковий запис Apple, iCloud, Вхід з Apple, Apple Pay, Повідомлення, FaceTime і Локатор.

### Конфіденційність Apple

На вебсторінці [конфіденційності Apple](#) можна знайти інформацію про функції, які захищають ваші дані, та параметри, що дають вам змогу керувати ними, переглянути відомості про поживну цінність для програм і звіти для забезпечення прозорості для урядових запитів, а також ознайомитися з Політикою конфіденційності Apple.

### Ваші дані та конфіденційність

Увійдіть на [вебпортал «Дані та конфіденційність»](#) зі своїм обліковим записом Apple, щоб дізнатися більше про дані, які збирає Apple, отримати або передати копію своїх даних, а також виправити, деактивувати чи видалити свої дані.

### Спільнота підтримки Apple

На сайті [спільноти підтримки Apple](#) можна отримувати відповіді на запитання від інших клієнтів Apple (у всьому світі).

# Авторське право

© 2024 Apple Inc. Усі права захищено.

Використання «клавіатурного» логотипа Apple (Option+Shift+K) у комерційних цілях без попередньої письмової згоди корпорації Apple може вважатися порушенням прав на торговельну марку та недобросовісною конкуренцією, що порушує федеральні закони й закони штату.

Apple, логотип Apple, AirDrop, AirPods, AirTag, Apple Books, Apple Music, Apple Pay, Apple TV, Apple Wallet, Apple Watch SE, Apple Watch Series, Apple Watch Ultra, Digital Crown, Face ID, FaceTime, FileVault, Finder, Find My, HomeKit, HomePod, HomePod mini, iMac, iMessage, iPad, iPadOS, iPad Pro, iPhone, iTunes, Launchpad, Lightning, Mac, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, OS X, Safari, Siri, Time Machine і Touch ID є торговельними марками компанії Apple Inc., зареєстрованими в США та інших країнах і регіонах.

App Store, iCloud, iCloud+, iCloud Keychain та iTunes Store є знаками обслуговування Apple Inc., зареєстрованими в США та інших країнах і регіонах.

Apple  
One Apple Park Way  
Cupertino, CA 95014  
[apple.com](https://apple.com)

IOS є торговельною маркою або зареєстрованою торговельною маркою компанії Cisco в США та інших країнах і використовується відповідно до умов ліцензії.

Словесний знак та логотипи Bluetooth® є зареєстрованими торговельними марками, що належать корпорації Bluetooth SIG, Inc.; будь-яке використання подібних знаків корпорацією Apple відбувається згідно з ліцензією.

Інші назви компаній і продуктів, згадані в цій інструкції, можуть бути торговельними марками відповідних компаній.

Для гарантування точності посібника докладено всіх можливих зусиль. Корпорація Apple не несе відповідальності за друкарські або канцелярські помилки.

Деякі програми доступні не в усіх регіонах. Доступність програм може змінюватися.

UA028-00796