РАДА
ВЕРХОВНА РАДА УКРАЇНИ

Комітет Верховної Ради України з питань свободи слова

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

СИТУАЦІЙНИЙ ЦЕНТР ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СБУ

ОБСЄ

Організація з безпеки і співробітництва в Європі

НАЦІОНАЛЬНА РАДА УКРАЇНИ З ПИТАНЬ ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ

ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ

«МОБІЛЬНІ ПРИСТРОЇ»

РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА

ЧАСТИНА І

2025

Вступ

В умовах повномасштабного військового вторгнення на територію України противник продовжує застосовувати широкий арсенал кіберзброї для отримання розвідувальної інформації, дестабілізації функціонування державних установ, критичної інфраструктури та суспільства в цілому, зокрема через медіа.

Так, з 24 лютого 2022 року спецслужбами рф здійснено понад 100 цілеспрямованих кібератак на мережеву інфраструктуру українського медіа (топові українські телеканали та регіональні ЗМІ) з метою виведення її з ладу,проведення інформаційно-психологічних операцій або здійснення іншихпротиправних дій для дестабілізації у суспільстві, що може призвести до загроз національній безпеці України.

Для цього російські хакерські угрупування, підконтрольні спецслужбам рф, використовують різні методи атак (використання вразливостей в програмних продуктах або технічних налаштуваннях мережевої інфраструктури, DDOS-атак, розповсюдження шкідливого програмного забезпечення через електронні адреси та месенджери тощо).

Однак, одним із основних факторів вдалого проведення кібероперацій є людський, що обумовлений недостатньою кваліфікацією, нехтуванням правилами кібергігієни, низькою обізнаністю методів соціальної інженерії, а в контексті повномасштабної війни, за умов психологічного тиску, людський фактор стає найуразливішим елементом, що підвищує ризик інсайдерських загроз.

Все перелічене створює додаткові можливості хакерам проводити цільові кібератаки на визначені об’єкти або осіб з метою отримання потрібних чутливих даних або для іншої протиправної діяльності.

Метою цих методичних рекомендацій є забезпечення базовими технічними знаннями, зокрема для представників медіа, з метою підвищеннярівня знань у сфері кібербезпеки для мінімізації в подальшому негативних наслідків від майбутніх кібератак та підвищення уваги щодо важ**ливості питання кібербезпеки в національному кіберпросторі.**

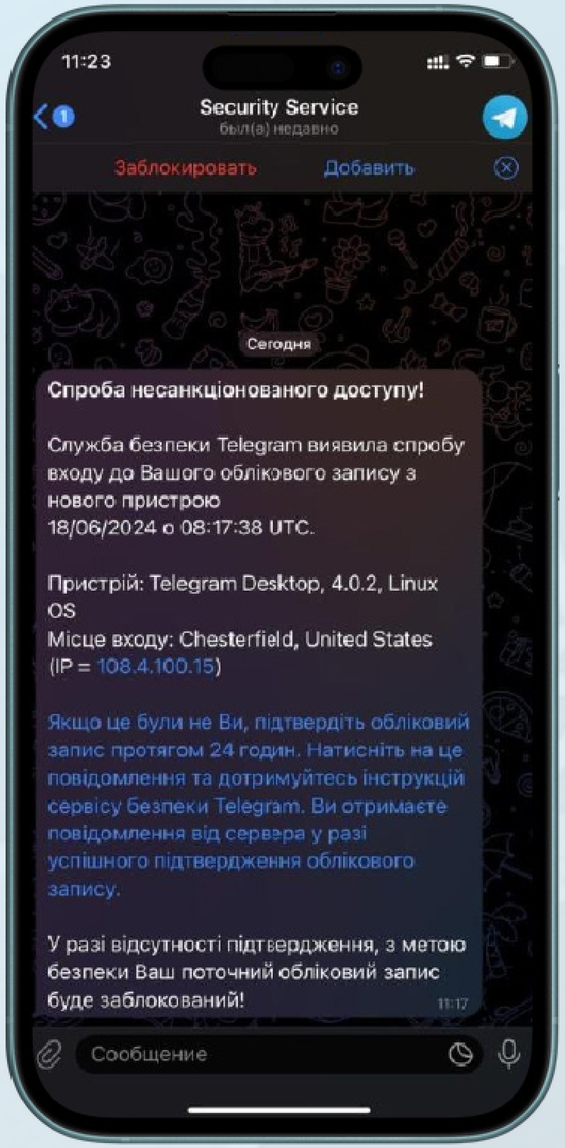
У наведених прикладах атак зловмисники імітують офіційні повідомлення від служби безпеки Telegram та Signal, використовуючи низку ефективних психологічних та технічних маніпуляцій:

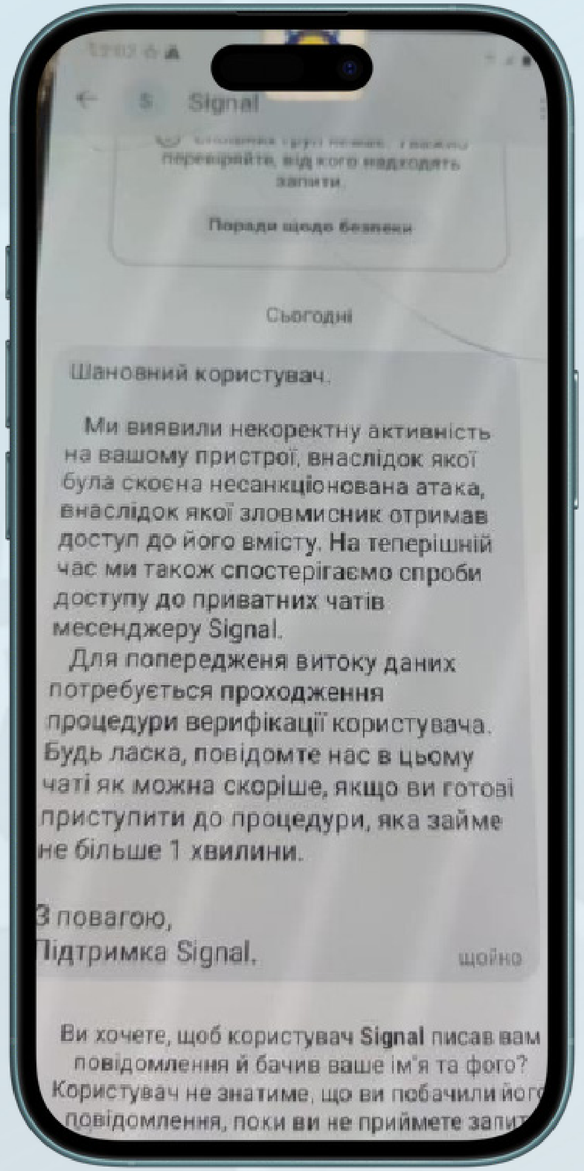
1. **Імітація офіційної структури та стилю**. Атакуючі копіюють стиль повідомлень реальних служб підтримки, зокрема логотип, неймінг, технічну термінологію та формат оформлення, що створює враження легітимності повідомлення.

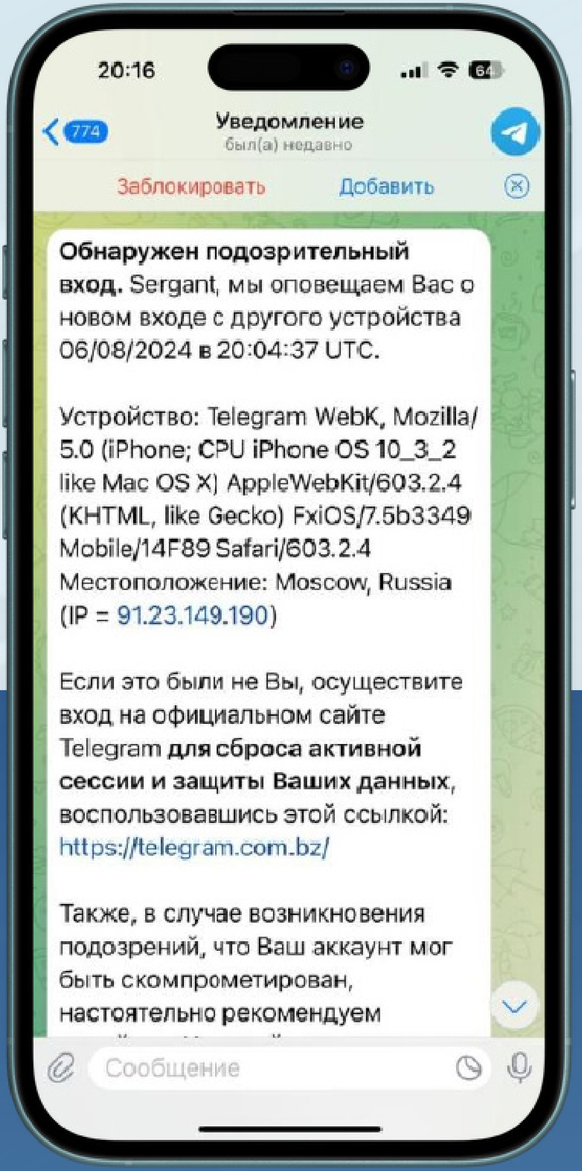
2. **Повідомлення про загрозу втрати доступу до облікового запису**. В усіх випадках користувачу повідомляється про «несанкціонований вхід» або «підозрілу активність», що викликає відчуття терміновості та тривоги. Це суттєво підвищує ймовірність виконання вказівок, не перевіряючи їх справжність.

3. **Вказання технічних деталей (IP, пристрій, місцезнаходження) та посилання на зовнішній фішинговий сайт**. У двох прикладах Telegram-фішингу вказано IP-адресу та місто — Chesterfield (США) та Moscow (РФ). Це створює додатковий рівень правдоподібності та акцентує увагу на «зовнішньому втручанні». У третьому прикладі вказано домен, схожий на офіційний — telegram.com.bz, що імітує реальну адресу, але насправді веде на фішингову сторінку. Це класичний приклад підміни URL з використанням схожого доменного імені.

4. **Мова та стиль повідомлення**. Усі тексти написано грамотною, формальною мовою — українською або російською. Це усуває типову ознаку фішингу — орфографічні помилки і ускладнює виявлення атаки.







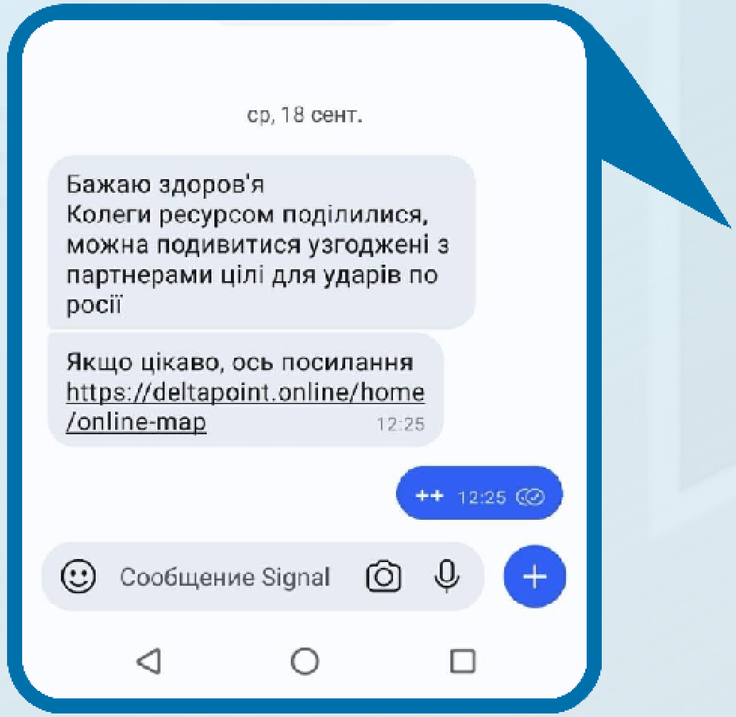
ВАЖЛИВО!

Якщо Ви отримали повідомлення, що нібито надійшло від офіційної служби підтримки месенджера, зверніть увагу на інтерфейс чату. В чаті зі справжнім обліковим записом сервісу Ви не зможете виконати дії, доступні Вам в чатах зі звичайними контактами (на кшталт: «заблокувати користувача», «додати до контактів» або «дозволити надсилати повідомлення»). Наявність цих опцій — ознака, що перед Вами звичайний акаунт, а не офіційний обліковий запис сервісу.

Фішинг від імені керівництва

У наведених прикладах атаки реалізовано через скомпрометовані або фейкові акаунти, які імітують керівників або колег. Основною метою є змусити жертву перейти за фішинговим посиланням, щоб отримати доступ до важливої інформації або корисних ресурсів.

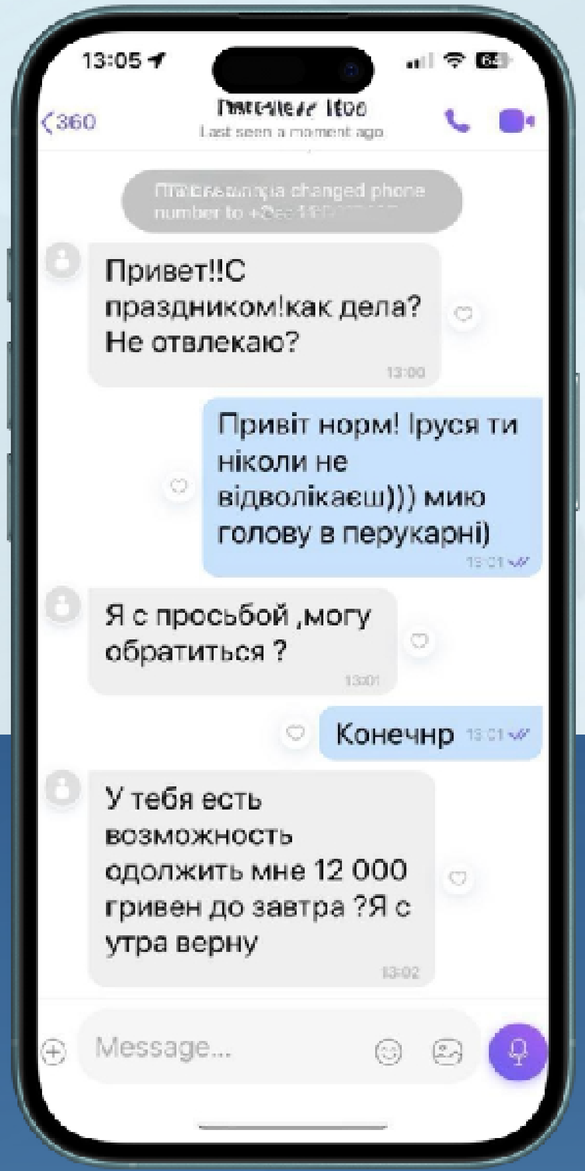
1. **Використання авторитету знайомої особи**. Повідомлення надходять нібито від керівника, старшого офіцера або довіреного колеги. Атакуючі використовують справжнє ім'я в акаунті, знайоме фото, іноді — збережений історичний чат. Це дозволяє миттєво зняти психологічні бар'єри у жертви.

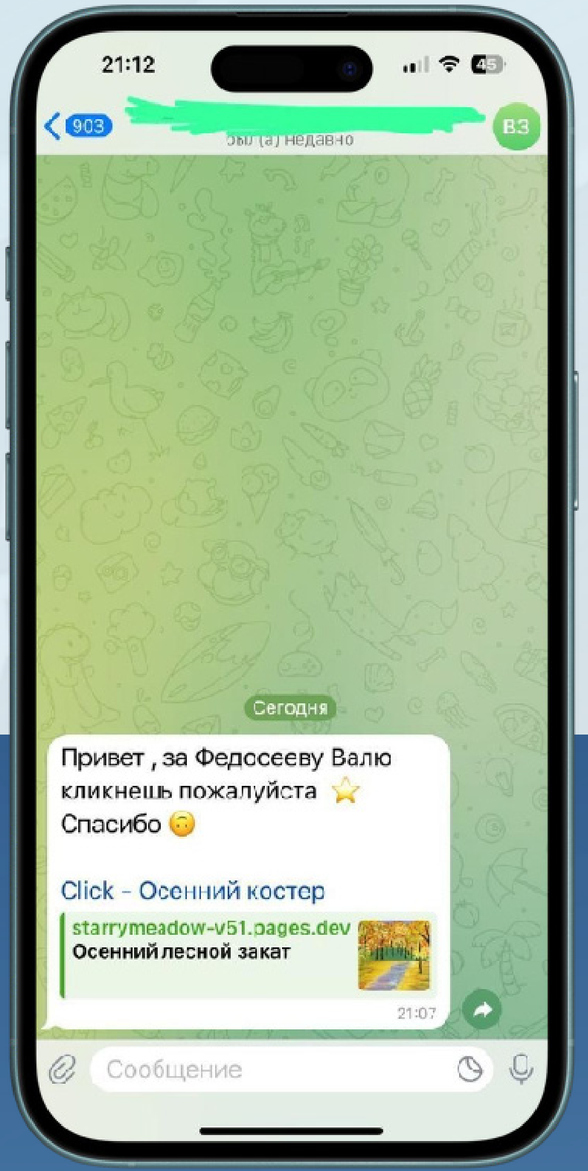


2. **Терміновість**. Усі три повідомлення супроводжуються фразами, які натякають на критичність інформації: «доведення інформації», «по ракетному оповіщенню», «цілі для ударів по росії». Це формує у користувача відчуття залученості до важливої справи.

3. **Маскування шкідливих посилань**. Фішингові домени імітують офіційні сервіси — наприклад, signal-groups.tech замість справжнього signal.group, або deltapoint.online як псевдоаналітичний ресурс. Усі посилання виглядають легітимно, але ведуть на фішингові сайти або сайти із шкідливим вмістом.

4. **Імітація звичних робочих процесів**. Повідомлення побудовані так, ніби це частина рутинної комунікації: приєднання до групи, передача розпорядження, ознайомлення з документом. У результаті жертва діє автоматично, без додаткової перевірки. Крім того, повідомлення складено коректною українською мовою з використанням лексики, притаманної внутрішній комунікації. Це додатково знижує ризик виникнення підозри з боку отримувача.





ВАЖЛИВО!

У разі виникнення підозри, що повідомлення може бути фішинговим, найкращим рішенням буде особисто зв’язатися з відправником, але не через той самий месенджер, у якому Ви отримали повідомлення. Використайте інший перевірений канал зв’язку — наприклад, телефонний дзвінок або альтернативний месенджер, щоб переконатися в достовірності звернення.

Фішинг через зламані акаунти знайомих осіб

У наведених випадках зловмисники використовують уже скомпрометовані облікові записи або створюють фейкові акаунти близьких друзів і родичів жертви.

1. **Встановлення довірливого тону**. Атака розпочинається з короткого неформального привітання та загальних запитань, наприклад про справи або настрій. Така модель спілкування імітує звичну буденну переписку між знайомими, що дозволяє швидко знизити пильність жертви.

2. **Використання шкідливих посилань або особисте прохання**. У першому прикладі жертві надсилають посилання з нібито «голосуванням» чи «підтримкою», оформлене як художній контент. Насправді, сайт із вказаним доменом є фішинговим — після переходу можливий збір облікових даних або зараження пристрою. У другому випадку зловмисник звертається з проханням позичити гроші, що є типовим сценарієм шахрайства через соцмережі.

3. **Невимушеність комунікації**. Ключ до успіху таких атак — природність діалогу. Жодних формальних загроз чи службової термінології. Це створює ілюзію безпеки та знижує обережність жертви.

ВАЖЛИВО!

Рекомендації є аналогічними тим, що були у попередньому випадку: не реагуйте на сумнівні повідомлення, навіть якщо вони надійшли від знайомої особи. Зателефонуйте або напишіть через інший месенджер, аби перевірити, чи справді ця людина надсилала повідомлення. Пам’ятайте: той акаунт, через який Вам надійшло повідомлення, може бути скомпрометованим.

Фішинг від імені стороннього сервісу

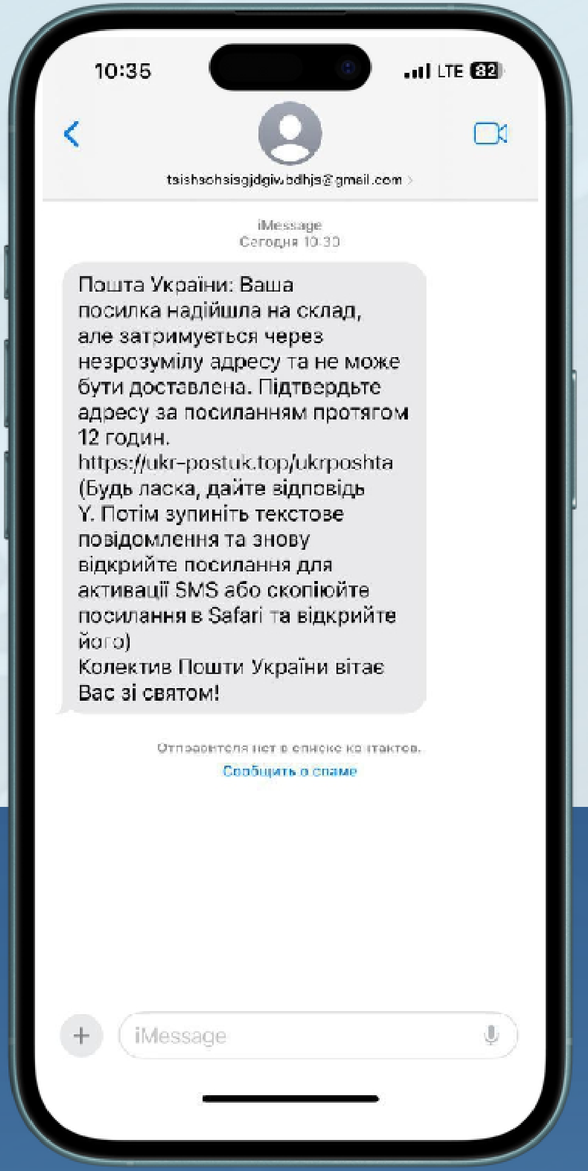
Цей приклад демонструє типову фішингову атаку, реалізовану під виглядом повідомлення від служби доставки. Зловмисники імітують офіційне повідомлення про проблему з доставкою посилки.

1. **Використання фейкової назви організації**. Атака здійснюється від імені «Пошти України» — неіснуючої структури, яка намагається маскуватися під державного оператора «Укрпошта». Це є першим індикатором недостовірності повідомлення.

2. **Шкідливе посилання з імітацією справжнього домену**. Використано домен **ukr-postuk.top**, який лише імітує назву офіційного сайту, але насправді не має жодного стосунку до «**Укрпошти**». Це класична тактика створення фальшивих ресурсів зі схожими назвами.

3. **Граматичні та стилістичні помилки.** У тексті присутні некоректні формулювання, зокрема фраза «зупиніть текстове повідомлення», яка не має логічного сенсу. Такі помилки часто є ознакою фішингового характеру повідомлення.

4. **Терміновість**. Користувачу повідомляється, що потрібно «підтвердити адресу протягом 12 годин». Подібні часові обмеження — типовий елемент соціальної інженерії, спрямований на те, щоб жертва не встигла критично оцінити ситуацію.



ВАЖЛИВО!

У разі отримання повідомлень від імені сторонніх сервісів доставки або інших організацій — ніколи не переходьте за підозрілими посиланнями з SMS чи месенджерів. Замість цього зверніться до компанії напряму через офіційний сайт або перевірені контакти, які вказані на її офіційній сторінці.

Захист облікового запису WhatsApp: перевірка сесій та налаштування двоетапної перевірки

Для запобігання несанкціонованому доступу до Вашого акаунту в WhatsApp, важливо регулярно перевіряти підключені пристрої та увімкнути двоетапну перевірку.

1. **Перевірка сторонніх сесій**. iOS

На iPhone (iOS): Відкрийте **WhatsApp** > перейдіть у вкладку «**Параметри**» > оберіть «**Пов'язані пристрої**». У цьому розділі Ви побачите всі пристрої, що мають доступ до Вашого акаунту (наприклад, Google Chrome на Windows). Якщо Ви не впізнаєте пристрій — негайно торкніться його та натисніть «**Вийти**».

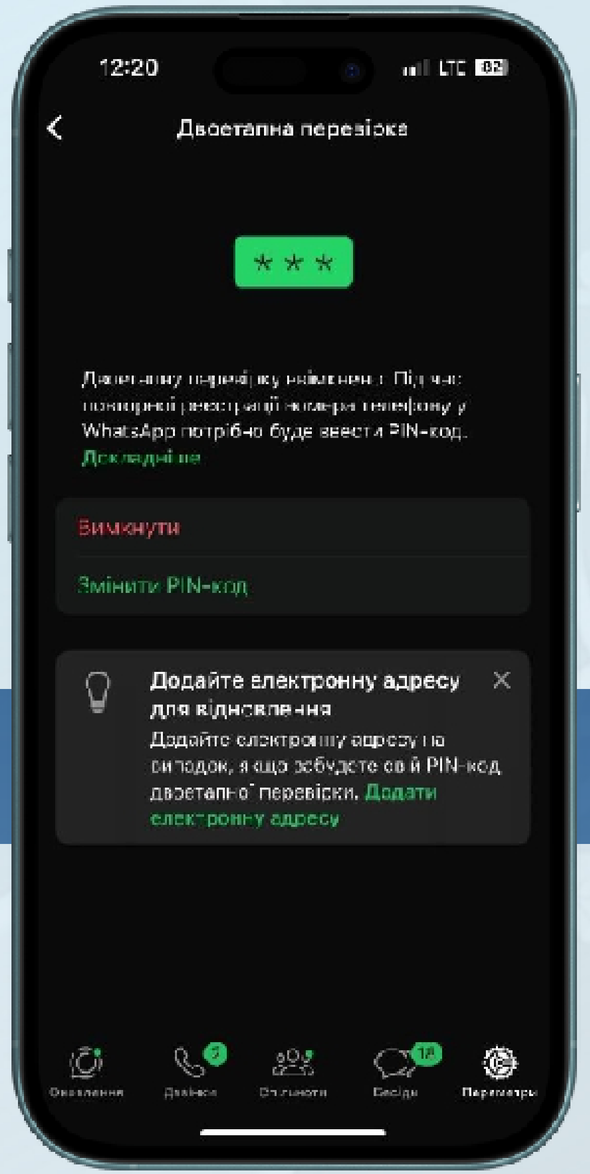
На Android: Відкрийте **WhatsApp** > натисніть три крапки у верхньому правому куті > «**Пов'язані пристрої**». Так само перевірте список активних сесій і завершіть ті, що здаються підозрілими.

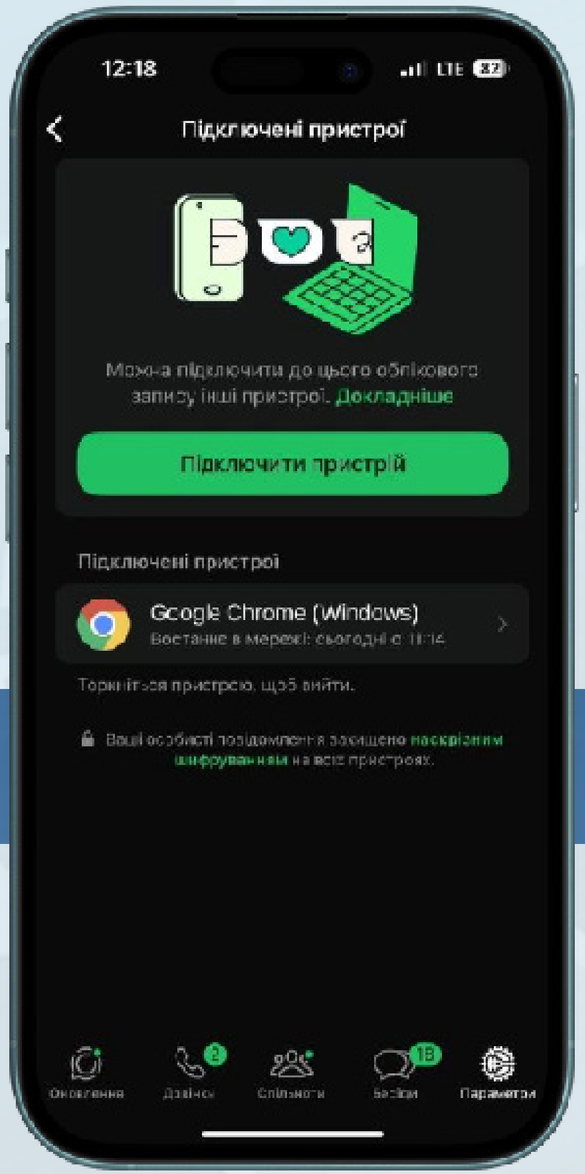
Чому це важливо: У разі компрометації облікового запису зловмисник може непомітно під'єднати пристрій до Вашого акаунту й отримувати копії повідомлень у реальному часі.

2. **Налаштування двоетапної перевірки**.

На iPhone (iOS): Перейдіть до «**Параметри**» > «**Обліковий запис**» > «**Двоетапна перевірка**» > Натисніть «**Увімкнути**» > встановіть **6-значний PIN-код**, а також вкажіть **адресу електронної пошти** для відновлення доступу у разі втрати коду.

На Android: Відкрийте «**Налаштування**» > «**Обліковий запис**» > «**Двоетапна перевірка**» > «**Увімкнути**». Так само встановіть PIN-код та додайте електронну пошту.





Чому це важливо: Без двоетапної перевірки зловмисник може перереєструвати ваш номер на своєму пристрої, якщо отримає доступ до SMS. Увімкнена перевірка блокує таку спробу без введення PIN-коду.

Вимкнення автозавантаження файлів у WhatsApp

Одним із простих, але ефективних способів убезпечити свій пристрій від шкідливих вкладень є вимкнути автоматичне завантаження медіафайлів у WhatsApp.

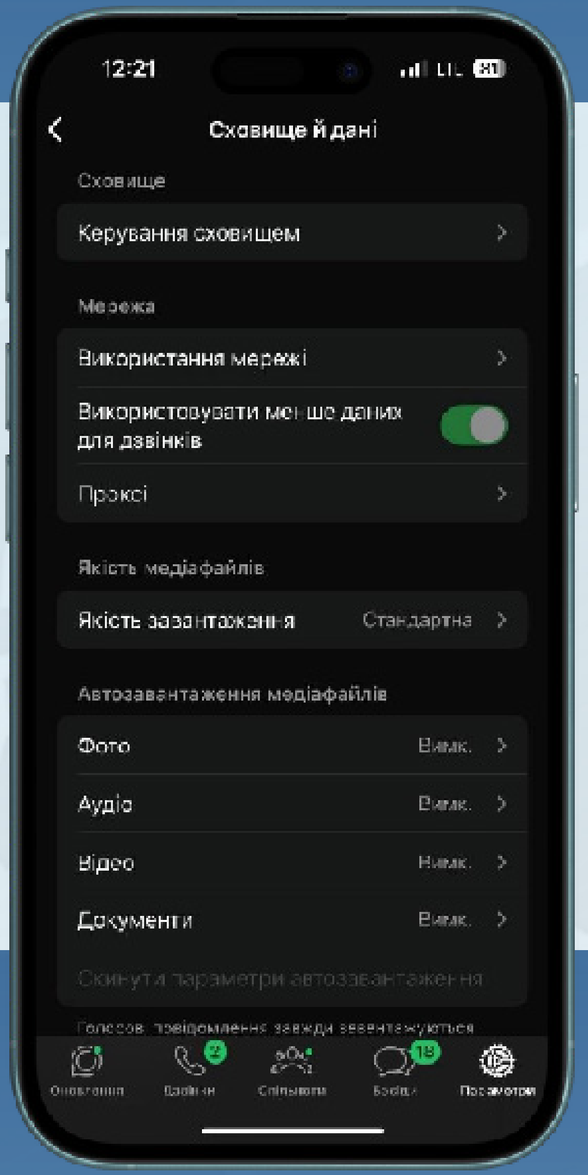
Як вимкнути автозавантаження медіа:

На iPhone (iOS):

Відкрийте **WhatsApp** > перейдіть у вкладку «**Параметри**» > Оберіть «**Сховище й дані**» > У розділі «**Автозавантаження медіафайлів**» окремо відкрийте **Фото**, **Аудіо**, **Відео та Документи**. > У кожному з пунктів виберіть «**Ніколи**» або «**Вимк.**» — залежно від версії застосунку.

На Android:

Відкрийте **WhatsApp** > натисніть **три крапки** у верхньому правому куті > «**Налаштування**» > Перейдіть до розділу «**Дані й сховище**» > У секції «**Автозавантаження медіа**» (по мобільній мережі, Wi-Fi і в роумінгу) зніміть усі прапорці для **Фото**, **Аудіо**, **Відео** та **Документів**.



Чому це важливо: Автоматичне завантаження фото, відео, аудіо або документів може призвести до непомітного потрапляння шкідливого програмного забезпечення на Ваш пристрій. Завантаження файлів повинно відбуватися **тільки за згодою користувача**, після ручного перегляду та оцінки довіри до джерела повідомлення. Завантажуйте лише ті файли, джерело яких Вам відоме та довірене. Ніколи не відкривайте вкладення з незнайомих номерів або у підозрілих повідомленнях.

Налаштування параметрів конфіденційності в WhatsApp

Важливо регулярно перевіряти розділ «**Конфіденційність**» у налаштуваннях WhatsApp та обирати ті параметри, які відповідають Вашій ролі та рівню відкритості. Особливо це критично для державних службовців, журналістів, військових і громадських активістів.

Рекомендовані параметри конфіденційності

> Фото профілю, статус, геодані, востаннє в мережі, дзвінки, групи >

Рекомендується обрати: «Мої контакти», «Мої контакти, окрім…» або «Ніхто».

Не рекомендується: «Усі», оскільки це дозволяє будь-кому (включно з шахраями) отримати базову інформацію про Вас.

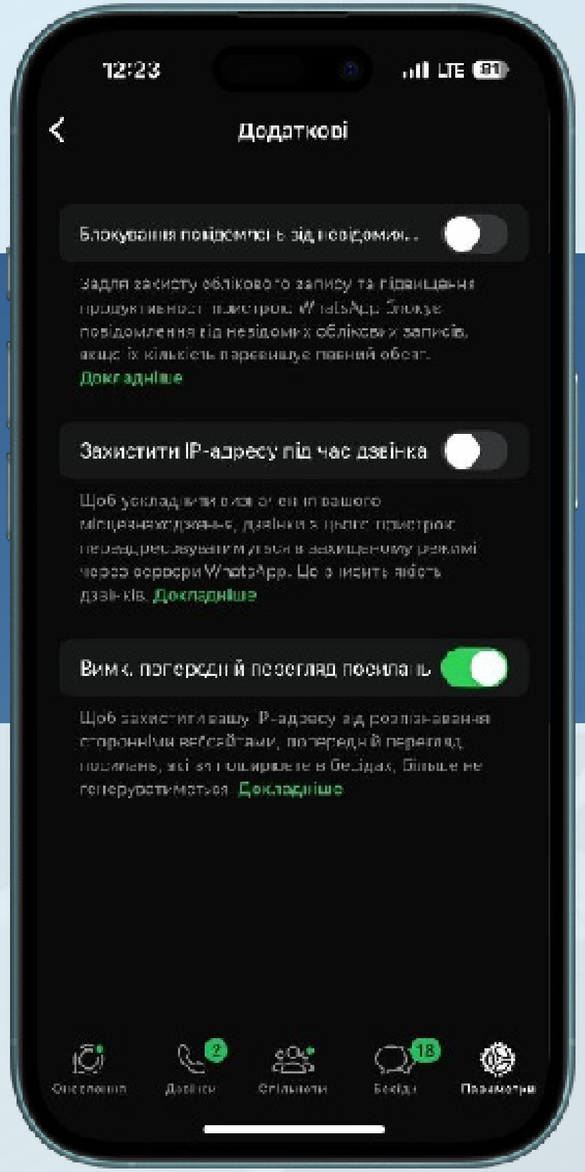
Розділ «Додаткові» — важливі налаштування захисту. У підрозділі «Додаткові» особливої уваги заслуговують три налаштування:

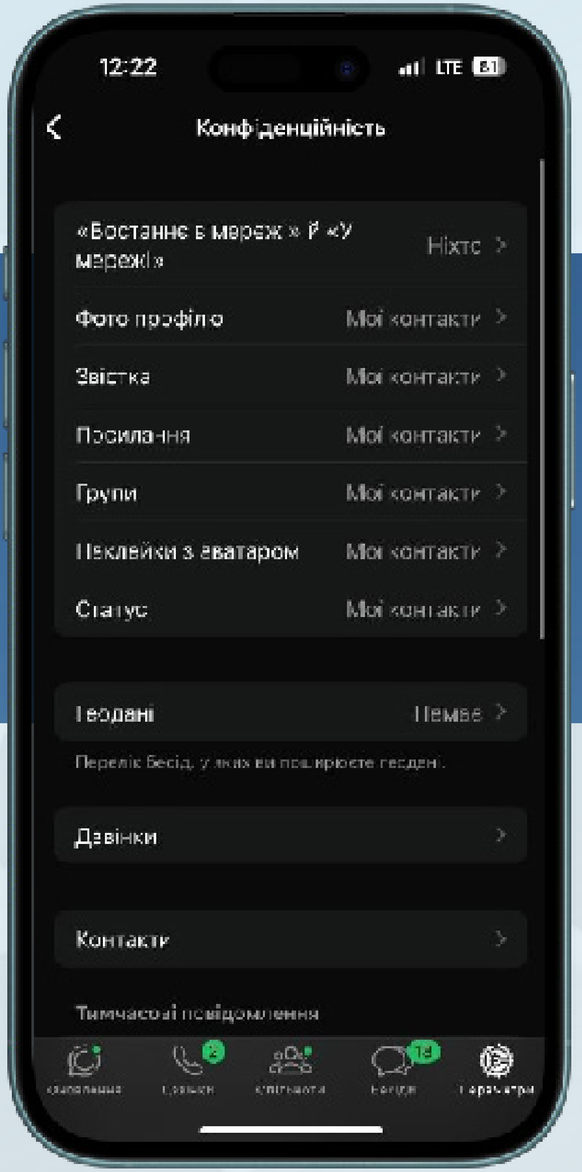
1. Вимкнення попереднього перегляду посилань — **КРИТИЧНО ВАЖЛИВО**

WhatsApp автоматично звертається до будь-якого надісланого в чаті посилання з IP-адреси Вашого пристрою, навіть якщо Ви не натискали на нього. Це створює ризик розкриття Вашого місцезнаходження та цифрового сліду.

Рекомендується: Увімкнути опцію «Вимк. попередній перегляд посилань»

2. Захист IP-адреси під час дзвінка. Увімкнення цієї функції перенаправляє дзвінки через сервери WhatsApp. Але з огляду на обмежений контроль над такими серверами та належність WhatsApp до компанії Meta, яка відома збутом персональних даних своїх користувачів третім сторонам (зокрема, рекламним сервісам), краще використовувати платні VPN сервіси.





Рекомендується: залишити вимкненим, натомість використовувати VPN

3. Блокування повідомлень/дзвінків з невідомих номерів. Ця функція може автоматично блокувати важливі вхідні дзвінки або повідомлення, зокрема від нових або екстрених контактів.

Рекомендується: залишити вимкненою, якщо не ведете комунікацію лише з вузьким колом осіб

! **Чому це важливо**: Конфіденційність у WhatsApp — це питання контролю за тим, хто може бачити Ваші дані. Відкриті профілі — це точка входу для більшості соціоінженерних атак. Обирайте обмеження, які відповідають Вашим потребам, і не залишайте жоден параметр відкритим для всіх («Усі»).

Захист облікового запису Signal: перевірка сесій та налаштування двоетапної перевірки

1. **Перевірка підключених пристроїв (сторонніх сесій)**. Щоб переконатися, що Ваш обліковий запис не використовується на інших пристроях без. Вашого відома, регулярно перевіряйте список зв'язаних пристроїв.

На iPhone (iOS): Відкрийте **Signal** > перейдіть у «**Налаштування**» > «**Пристрої**» > Ви побачите всі прив'язані комп'ютери або планшети. Якщо Ви не впізнаєте пристрій — натисніть на відповіну опцію і розірвіть зв'язок.

На Android: Відкрийте **Signal** > «**Налаштування**» > «**Зв'язані пристрої**»> Перевірте список підключень.

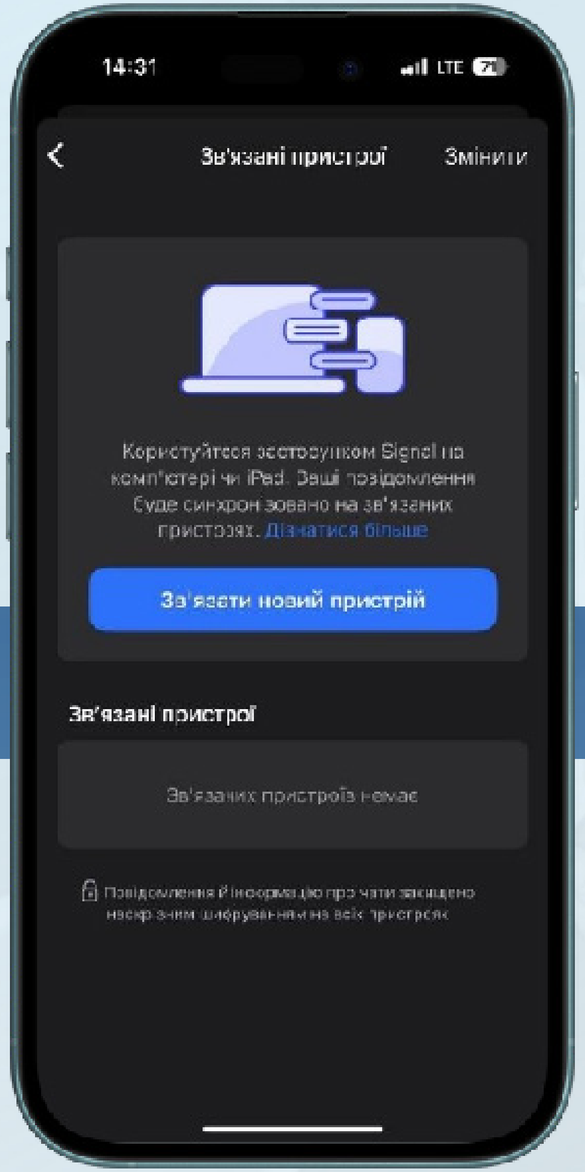
Якщо щось виглядає підозріло — **видаліть** відповідний пристрій.

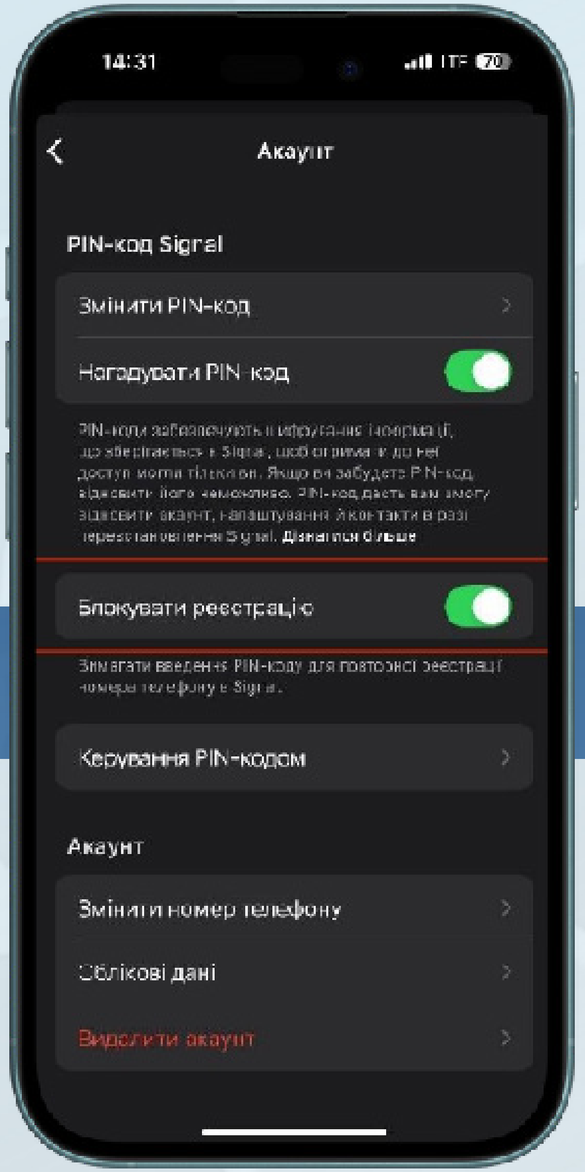
Чому це важливо: Зловмисник, який фізично або дистанційно отримав доступ до Вашого телефону, може отримувати копії повідомлень, залишаючись непоміченим.

2. **Увімкнення PIN-коду та блокування реєстрації**. Signal дозволяє встановити PIN-код для додаткового захисту даних і налаштувань. Проте сам PIN-код не захищає від повторної реєстрації номеру на іншому пристрої. Тому надзвичайно важливо активувати ще й блокування реєстрації.

Як налаштувати на iOS та Android:

Відкрийте **Signal** > «**Налаштування**» > «**Обліковий запис**» > Оберіть пункт > «**Змінити PIN-код**» > встановіть **надійний PIN-код** > Після цього **обов'язково** увімкніть опцію «**Блокувати реєстрацію**».





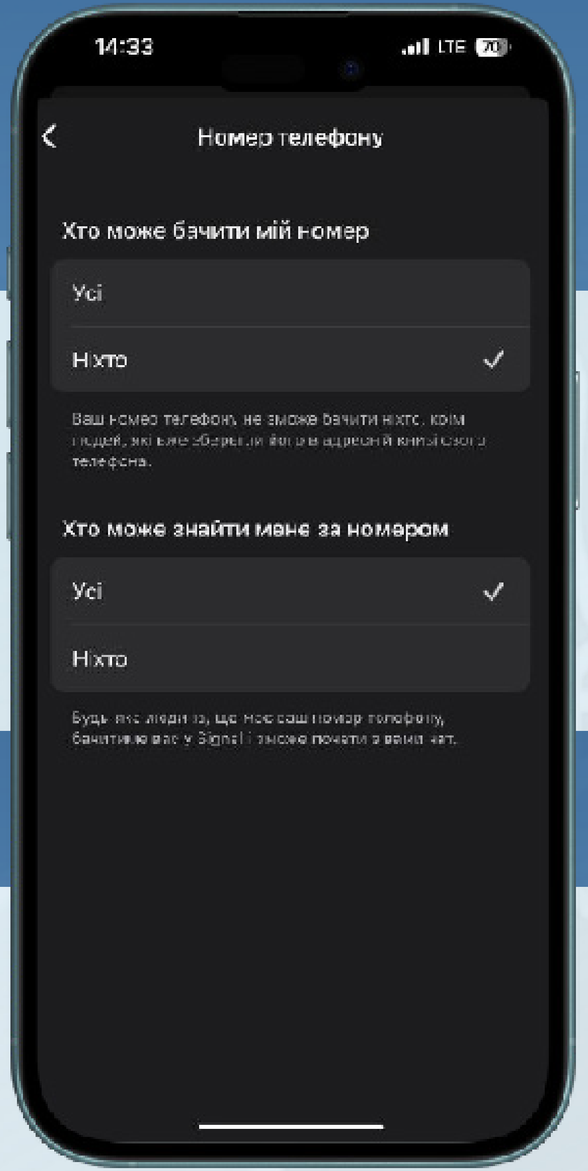
Чому це важливо: Увімкнене **блокування реєстрації** гарантує, що при спробі реєстрації Вашого номера на іншому пристрої буде вимагатися введення PIN-коду. Без цієї функції, зловмисник, який отримає SMS-код, зможе отримати доступ до Ваших чатів, навіть якщо Ви встановили PIN. Тому, ніколи не залишайте активним лише PIN-код без блокування реєстрації. Це створює хибне враження захищеності, не забезпечуючи при цьому реального захисту Вашого акаунту від перереєстрації.

Налаштування параметрів конфіденційності в Signal

1. **Приховування номера телефону: обов'язково вимкнути публічний доступ**

На iOS та Android: в меню «Конфіденційність» **>** «Номер телефону» потрібно налаштувати обмеження видимості номера:

- **Хто може бачити мій номер: «Ніхто»**
- **Хто може знайти мене за номером: «Ніхто»**



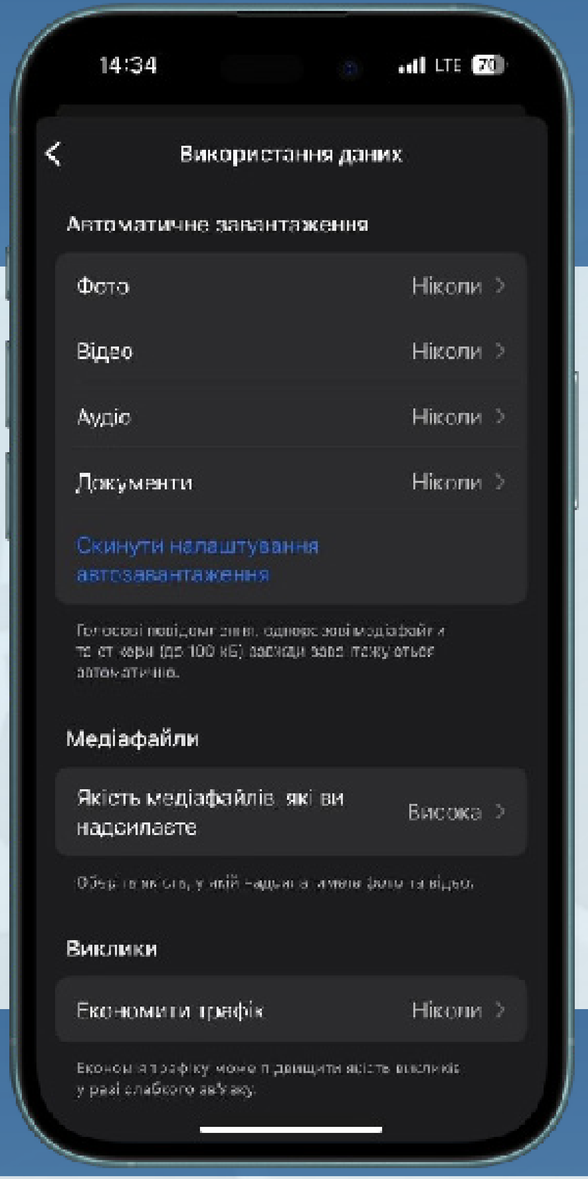
Чому це важливо: Якщо залишити налаштування на «Усі», будь-хто, хто має Ваш номер телефона (навіть випадковий шахрай), зможе дізнатися, що Ви користуєтеся Signal, побачити Ваш профіль та почати спілкування.

2. **Блокування доступу до застосунку на фізичному рівні**

Як налаштувати: На **iOS** та **Android**: Signal **>** **Налаштування** **>** **Конфіденційність** **>** Увімкнути **>** «**Приховувати екран у перемикачі програм**» **>** «**Блокування екрана**» **>** Установити «**Затримку блокування екрана**» (наприклад, 5 хвилин)

Чому це важливо: Якщо Ваш пристрій потрапить у чужі руки або Ви випадково відкриєте перемикач застосунків у публічному місці, сторонні не зможуть переглянути або швидко сфотографувати вміст відкритих чатів. Крім того, **ввімкнене блокування екрана** дозволяє Signal запитувати Face ID, пароль або інший метод автентифікації при кожному запуску застосунку.

Примітка: Індикатори читання повідомлень та набору тексту не впливають на рівень безпеки — їх можна залишити увімкненими або вимкненими залежно від Ваших уподобань.



Захист від шкідливих вкладень у Signal: вимкнення автозавантаження медіа

Signal за замовчуванням може автоматично завантажувати фото, відео, аудіо та документи, що надходять у чатах. Це створює потенційний вектор атаки, коли шкідливий файл потрапляє на пристрій без відома користувача.

Рекомендація: Встановіть значення «Ніколи» для всіх типів файлів — фото, відео, аудіо та документи. Усі медіа повинні завантажуватись виключно вручну, після того як Ви переглянете повідомлення й усвідомлено приймете рішення.

Як налаштувати:

На iPhone (iOS): 1. Відкрийте **Signal** > Перейдіть до «**Налаштування**» > «**Використання даних**» > У розділі «**Автоматичне завантаження**» відкрийте кожен пункт (**Фото**, **Відео**, **Аудіо**, **Документи**) > Для кожного — оберіть значення «**Ніколи**»

На Android: Відкрийте **Signal** > Перейдіть до «**Налаштування**» > «**Дані та сховище**» > У розділі «**Автоматичне завантаження медіа**» (окремо для мобільної мережі, Wi-Fi та роумінгу) > Зніміть усі прапорці для всіх типів файлів > Збережіть налаштування

Чому це важливо: Якщо злочинець надішле файл зі шкідливим вмістом — вірусом, шпигунським кодом або експлойтом — він може одразу завантажитися на пристрій, навіть якщо його не було відкрито. Вимкнення автоматичного завантаження дозволяє контролювати, які саме файли потрапляють у пам'ять телефону.

Захист облікового запису Telegram: перевірка сесій

Telegram дозволяє використовувати один обліковий запис на кількох пристроях одночасно. Це зручно, але водночас створює ризик несанкціонованого доступу, якщо Ви втратите контроль над хоча б одним із підключених пристроїв.

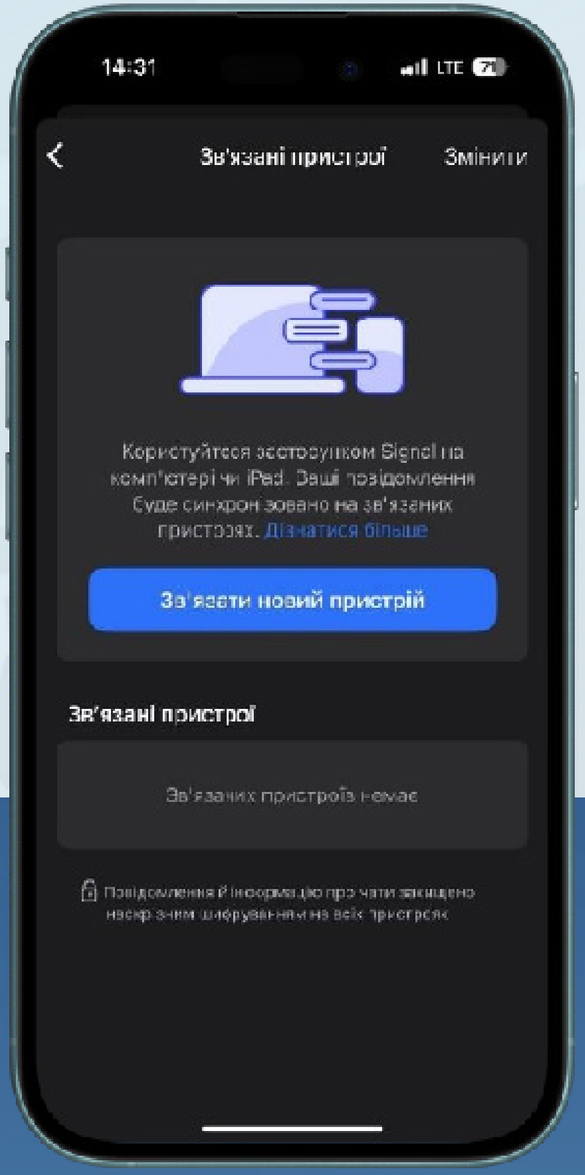
1. Перевірка активних сесій у Telegram

На iPhone (iOS): Відкрийте **Telegram** > Перейдіть до «**Налаштування**» > «**Пристрої**» > У розділі «**Активні сесії**» Ви побачите перелік усіх пристроїв, підключених до Вашого акаунту > Якщо виявлено незнайомий пристрій — натисніть «**Завершити всі інші сеанси**», щоб відключити всі сесії, окрім поточної

На Android: Відкрийте **Telegram** > Перейдіть у «**Меню**» (три смужки у верхньому лівому куті) > «**Налаштування**» > «**Пристрої**» > Перевірте список усіх активних сесій > Натисніть «**Завершити всі інші сесії**», щоб миттєво вийти з усіх підозрілих пристроїв

2. Налаштування автоматичного завершення сесій

У нижній частині цього ж розділу є опція «**Автозавершення старих сеансів**» (або «**Автоматичне завершення при відсутності**»). Встановіть **мінімальний доступний інтервал часу** (**1 тиждень**). Це гарантує, що підключення з пристроїв, якими Ви давно не користуєтесь, буде автоматично завершено, зменшуючи ризик несанкціонованого доступу до Ваших повідомлень.



Чому це важливо: Якщо Ви коли-небудь входили у Telegram з робочого або спільного комп'ютера, планшета чи іншого телефону — сесія могла залишитись активною. Зловмисник, який отримає доступ до цього пристрою, зможе читати Ваші повідомлення у фоновому режимі. Регулярна перевірка активних сесій — обов'язковий елемент цифрової гігієни.

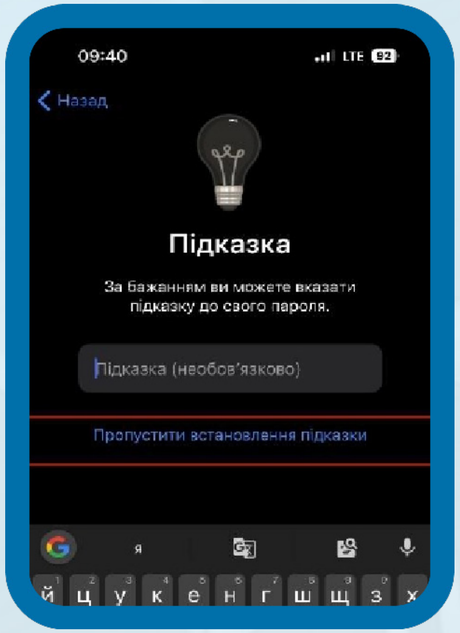
Налаштування двоетапної перевірки в Telegram

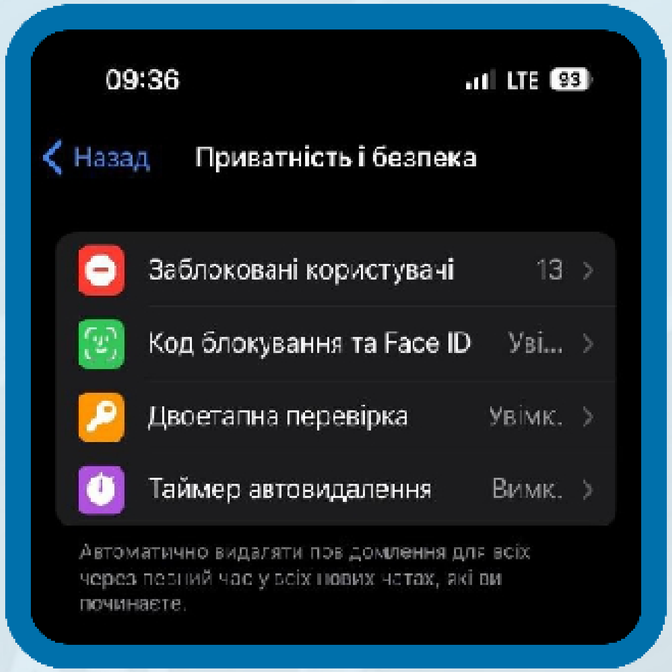
Telegram дозволяє налаштувати **двоетапну перевірку** — це додатковий пароль, який запитуватиметься під час входу у Ваш обліковий запис із нового пристрою. Його не можна обійти навіть при перехопленні коду з SMS.

Як налаштувати двоетапну перевірку

На iPhone (iOS): Відкрийте **Telegram** > Перейдіть у **Налаштування** > **Приватність і безпека** > Оберіть пункт «**Двоетапна перевірка**» > Натисніть «**Увімкнути пароль**», встановіть надійний пароль

На Android: Відкрийте **Telegram** > Перейдіть у **Налаштування** > **Приватність і безпека** > Натисніть «**Двоетапна перевірка**» > «**Увімкнути пароль**», після чого встановіть свій пароль



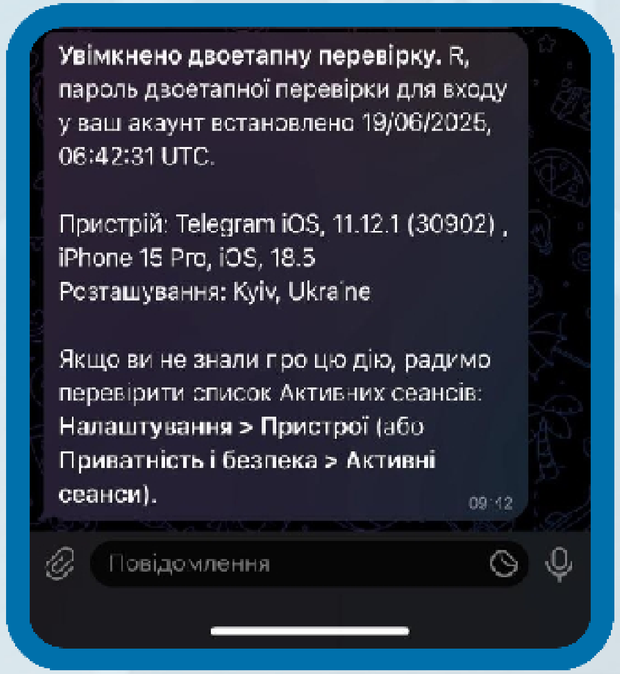


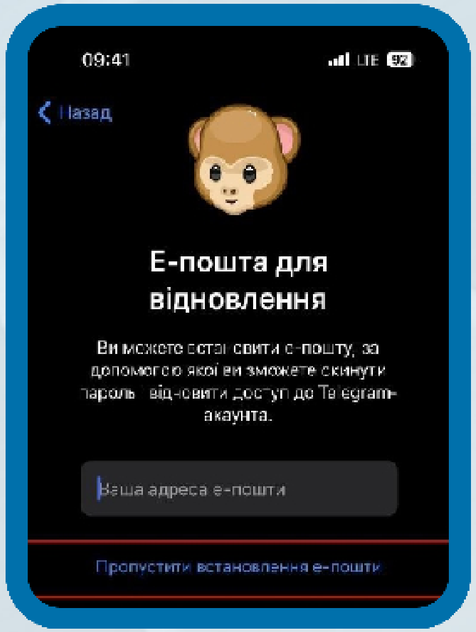
Рекомендації з безпеки

• **Не встановлюйте підказку до пароля**. Ваша підказка буде видимою у разі втрати пароля. Якщо вона очевидна або базується на особистій інформації, її можуть використати зловмисники.

• **Не додавайте електронну пошту**. Електронна адреса — це додатковий вектор атаки. Її можна скомпрометувати через фішинг або підбір пароля, після чого відновити доступ до Telegram. Також це додатковий ідентифікатор, який може призвести до деанонімізації.

Щоб переконатися, що двоетапну перевірку в Telegram налаштовано правильно, слід звернути увагу на системне повідомлення, яке автоматично надійде в офіційний чат Telegram після активації захисту. У ньому буде зазначено, що двоетапну перевірку увімкнено, а також вказано дату й час її активації, модель пристрою, на якому встановлено пароль, і приблизне місце розташування — місто та країну. Якщо Ви не здійснювали ці дії, необхідно негайно перейти до налаштувань, відкрити розділ «Пристрої» та завершити всі інші сесії, окрім поточної.





Налаштування параметрів конфіденційності в Telegram

У розділі «**Приватність і безпека**» рекомендується змінити низку параметрів для підвищення рівня анонімності та захисту Вашого облікового запису, найважливішими серед яких є:

1. **Номер телефона**. Вкрай важливо обмежити видимість Вашого номера. Рекомендується встановити значення «Ніхто» або принаймні «Мої контакти», залежно від мети використання акаунту. У жодному разі не обирайте опцію «Усі», оскільки це створює додатковий ризик Вашої деанонімізації.

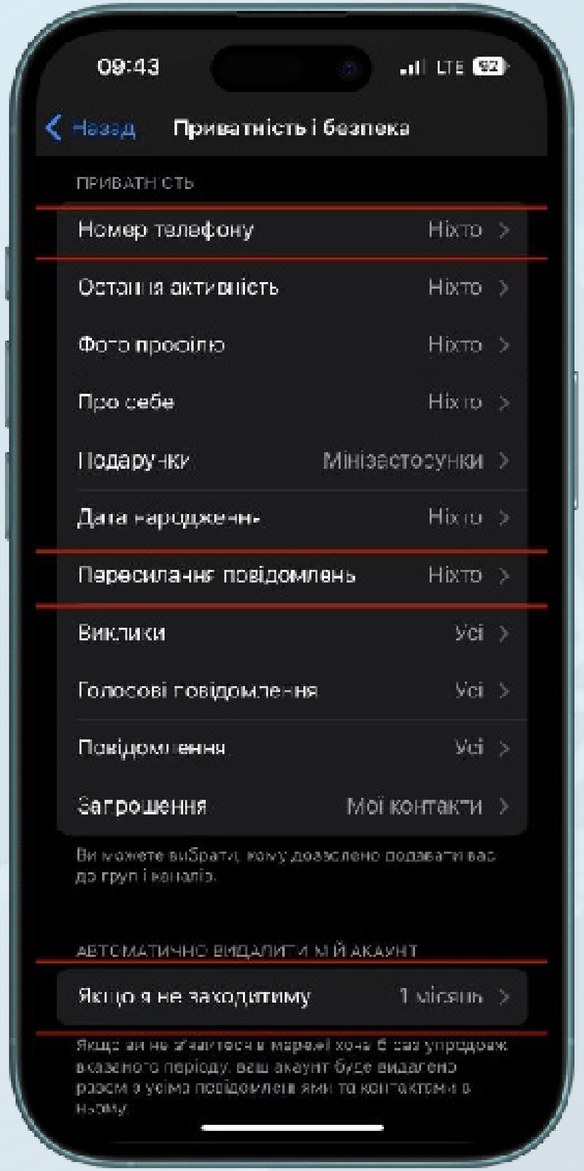
2. **Пересилання повідомлень**. Необхідно повністю вимкнути цю функцію. Якщо її залишити увімкненою, Ваші повідомлення можуть бути переслані іншим користувачам або ботам, які за допомогою Telegram API можуть дізнатися Ваш Telegram ID. Надалі через цей ID потенційно можна отримати історичні дані про зміну нікнеймів або пов'язані з акаунтом телефонні номери.

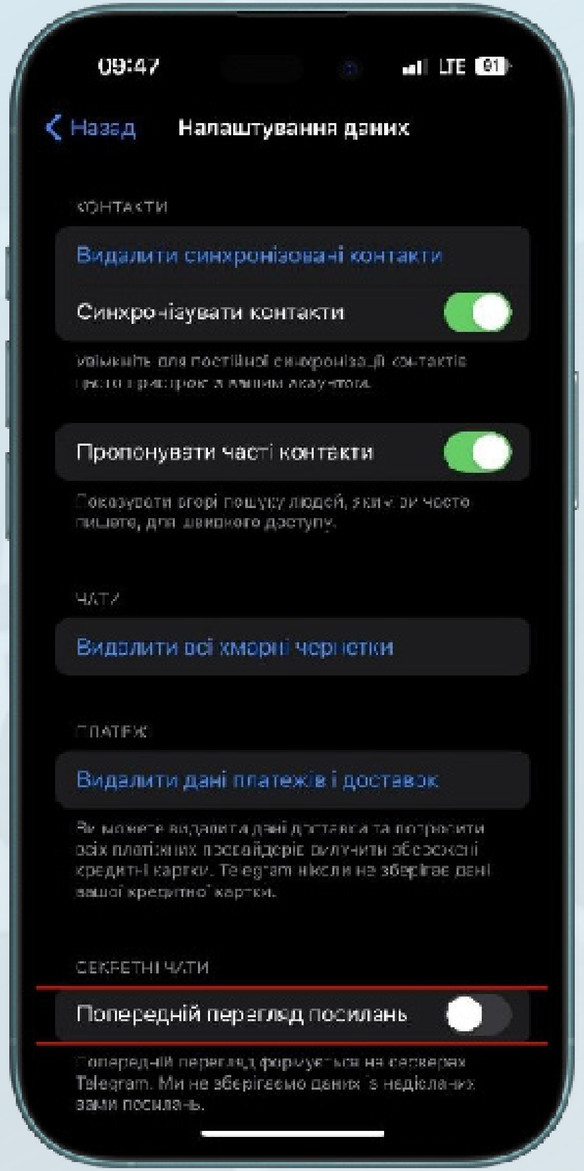
3. **Автоматичне видалення облікового запису**. У параметрі «**Якщо я не заходитиму**» слід обрати мінімальний можливий термін (наприклад, 1 місяць). Це гарантує, що навіть якщо обліковий запис стане недоступним, він буде автоматично видалений разом з усією інформацією.

Додатково, перейдіть до розділу «**Налаштування даних**», де також варто внести низку змін:

4. **Синхронізація контактів**. Якщо Ви використовуєте Telegram для анонімної діяльності або під час проведення чутливих розслідувань, **не синхронізуйте контакти** з телефону. Це дозволить уникнути витоку або ненавмисного розкриття кола Вашого спілкування.

5. **Попередній перегляд посилань**. Хоча Telegram генерує прев'ю посилань зі своїх серверів, а не з Вашої IP-адреси (на відміну від WhatsApp), все ж рекомендується вимкнути цей параметр. Це дозволяє уникнути ситуацій, коли Telegram автоматично відкриває вміст потенційно небезпечного посилання без Вашого відома.





Захист від шкідливих вкладень в Telegram: вимкнення автозавантаження медіа

У Telegram важливо вимкнути **автоматичне завантаження медіа**, щоб зменшити ризик потрапляння на пристрій потенційно шкідливих файлів. Завантаження файлів має відбуватися **лише за ініціативою користувача**, після перевірки повідомлення та відправника.

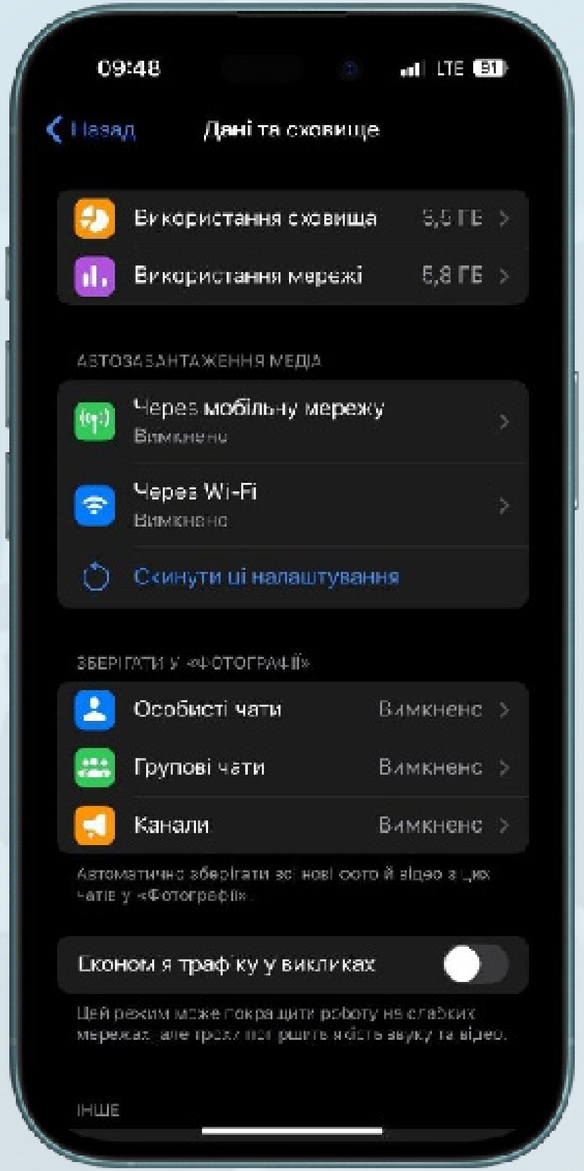
Як вимкнути автозавантаження медіа в Telegram:

На iPhone (iOS): Відкрийте **Telegram** > Перейдіть до меню **Налаштування** > **Дані та сховище** > У розділі **Автозавантаження медіа** зайдіть у **Через мобільну мережу** > Встановіть усі типи медіа на «Ніколи» > Так само зайдіть в **Через Wi-Fi** > Також встановіть усі пункти на «Ніколи».

Після цього жоден файл не буде завантажено без Вашої згоди — Ви самостійно обиратимете, що зберігати.

На Android: Відкрийте **Telegram** > Перейдіть до **Налаштування** > **Дані та сховище** > У блоці **Автозавантаження медіа** натисніть **Мобільна мережа**, **Wi-Fi** та **Роумінг** по черзі > У кожному розділі зніміть позначки з усіх категорій (фото, відео, файли, голосові повідомлення тощо).

Так Ви забезпечите контроль над кожним файлом, який потрапляє на пристрій, і уникнете автоматичного збереження потенційно небезпечного контенту.



Захист облікового запису Viber: перевірка сесій та налаштування двоетапної перевірки

Для безпечного користування месенджером Viber варто налаштувати два важливих параметри: перевірку активних сесій і двоетапну перевірку. По-перше, необхідно регулярно перевіряти, які пристрої підключені до Вашого Viber-акаунту. Це можна зробити у розділі «Комп’ютери і планшети».

Перевірка сторонніх сесій у Viber

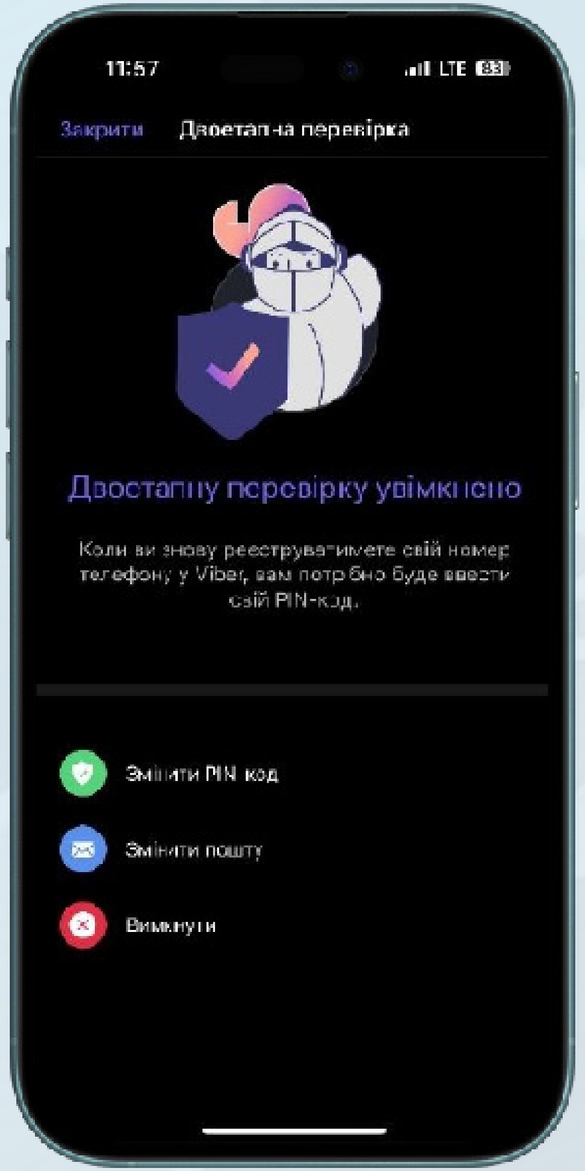
На iPhone: > Відкрийте вкладку «**Додатково**» (праворуч унизу) > Перейдіть у «**Параметри**» > «**Обліковий запис**» > «**Комп’ютери і планшети**» > У цьому розділі перегляньте перелік підключених пристроїв > Якщо виявлено сторонні або незнайомі сесії, натисніть «**Відключити**» навпроти відповідного пристрою.

На Android: > Відкрийте «**Ще**» (або три смужки, залежно від версії застосунку) > Перейдіть у «**Налаштування**» > «**Обліковий запис**» > «**Комп’ютери і планшети**» > Перевірте список підключених пристроїв > У разі виявлення сторонніх — натисніть «**Відключити**».

По-друге, надзвичайно важливо активувати двоетапну перевірку, яка запобігає спробам повторної реєстрації Вашого номера телефона без введення PIN-коду.

На iPhone: Відкрийте вкладку «**Додатково**» > «**Налаштування**» > Перейдіть до розділу «**Обліковий запис**» > «**Двоетапна перевірка**» > Встановіть PIN-код, який буде запитуватись при повторній реєстрації акаунту > Введіть адресу електронної пошти, яка використовуватиметься для відновлення доступу у разі втрати PIN-коду.

На Android: > Відкрийте «**Ще**» > «**Налаштування**» > Перейдіть у «**Обліковий запис**» > «**Двоетапна перевірка**» > Вкажіть PIN-код > Введіть електронну пошту, яка буде прив’язана до акаунту для відновлення доступу.



Налаштування параметрів конфіденційності у Viber

Viber часто піддається критиці за надмірний збір даних, а також за недостатньо прозору політику обробки особистої інформації користувачів. Тому для зниження цифрової експозиції та зменшення ризиків деанонімізації варто налаштувати Viber максимально конфіденційно.

По-перше, у розділі «**Конфіденційність**» рекомендується:

• Вимкнути показ Вашого фото для сторонніх осіб. Це можна зробити, деактивувавши опцію «**Показувати Ваше фото**». Таким чином лише абоненти, які є у Вашому списку контактів, зможуть бачити Вашу фотографію.

• Вимкнути функцію «**Поширити дату народження**», щоб ця інформація не використовувалась для ідентифікації Вас сторонніми особами чи зловмисниками.

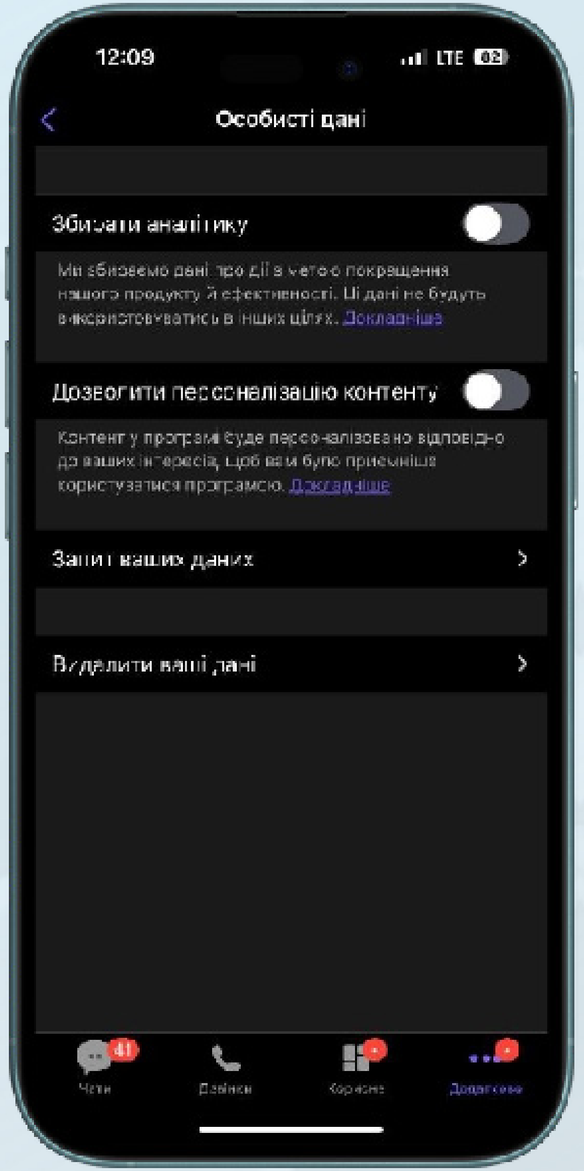
• За можливості не вмикати опцію «**Автоматична перевірка на спам**», оскільки це передбачає додаткову обробку Ваших повідомлень сторонніми серверами.

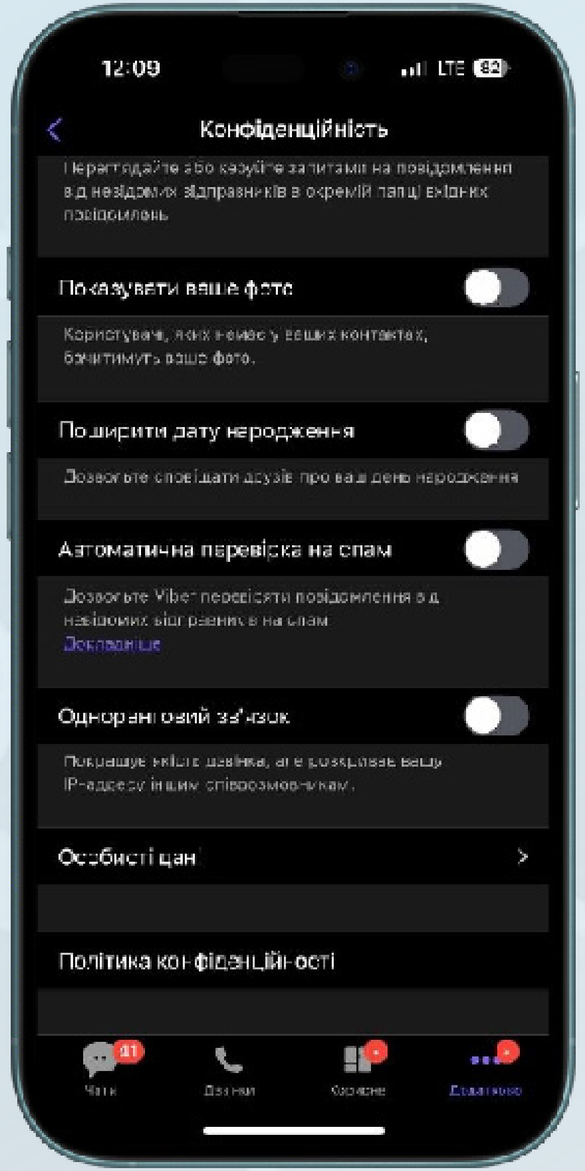
По-друге, у підрозділі «**Особисті дані**» потрібно відмовитися від необов'язкової телеметрії:

• Вимкніть опцію «**Збирати аналітику**», щоб Viber не надсилав дані про Вашу поведінку в застосунку.

• Вимкніть «**Дозволити персоналізацію контенту**», щоб уникнути додаткового збору інформації для побудови Вашого профілю інтересів.

Ці базові налаштування не усувають всіх ризиків, пов'язаних із використанням Viber, однак допомагають зменшити обсяг даних, які застосунок отримує про Вас, і зробити профіль менш видимим для сторонніх осіб.





Захист від шкідливих вкладень у Viber: вимкнення автозавантаження медіа

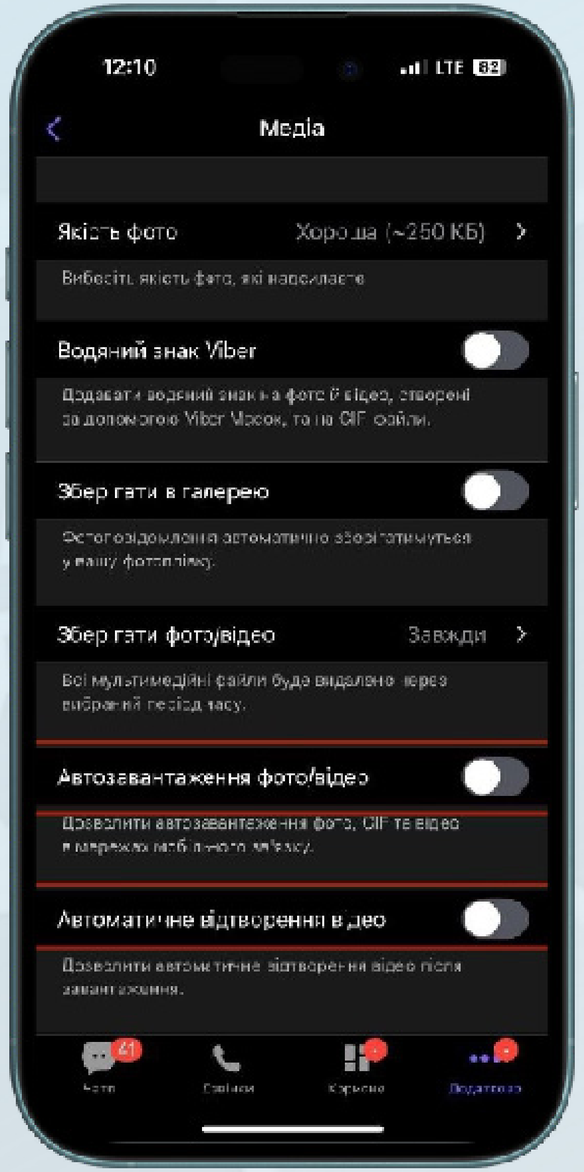
Автоматичне завантаження медіафайлів і автовідтворення відео у Viber є потенційно небезпечними функціями, які можуть призвести до неконтрольованого потрапляння шкідливого контенту на Ваш пристрій. Якщо зловмисник надішле файл, який містить шкідливе програмне забезпечення або експлойт, і функція автозавантаження буде увімкнена, такий файл миттєво збережеться або навіть автоматично відкриється без Вашої участі. Особливо це критично, коли йдеться про атаки, спрямовані на конкретного користувача.

Крім того, автоматичне завантаження зображень і відео може не лише збільшити ризик зараження пристрою, але й призводити до витрат мобільного трафіку, заповнення пам'яті телефону та підвищення навантаження на систему.

Щоби підвищити рівень безпеки, рекомендовано вимкнути автоматичне завантаження файлів і автовідтворення відео, щоб усі дії відбувалися виключно за Вашим свідомим рішенням.

Як вимкнути автозавантаження та автовідтворення у Viber:

Відкрийте **Viber** > Перейдіть у вкладку «**Додатково**» (внизу праворуч) > Оберіть «**Параметри**» > Далі відкрийте розділ «**Медіа**» > У цьому розділі ввимкніть опцію «**Автозавантаження фото/відео**» — це заборонить Viber автоматично завантажувати медіа у мобільній мережі або через Wi-Fi > Вимкніть «**Автоматичне відтворення відео**» — це унеможливить автоматичне відкриття відеофайлів одразу після завантаження. За бажанням також можна вимкнути «**Зберігати в галерею**».



Використання десктопних версій популярних месенджерів, особливо на операційній системі Windows, пов’язане з підвищеними ризиками. Персональні комптери, як правило, є більш вразливими до атак з боку зловмисників, оскільки на них часто встановлено велике число сторонніх програм, а системи безпеки не завжди налаштовані належним чином. У разі зараження ПК шкідливим програмним забезпеченням, скомпрометовані можуть бути не лише особисті файли, а й активні сесії месенджерів, доступ до листування та облікових записів.

З міркувань безпеки доцільніше надавати перевагу використанню **веб-версій месенджерів** (якщо така опція доступна), оскільки вони не зберігають дані постійно на комп’ютері та працюють у контрольованому середовищі браузера. Водночас важливо після завершення роботи **обов’язково завершувати активну сесію** у веб-версії. Це дозволить уникнути ситуацій, коли хтось інший отримає доступ до Вашого листування, якщо матиме фізичний або віддалений доступ до комп’ютера.

Для повідомлення щодо протиправних дій у сфері інформаційної безпеки (Департамент кібербезпеки СБУ):

- E-mail: **cyber_security@dis.gov.ua**

Для невідкладного інформування про кіберінциденти та кібератаки (Ситуаційний центр забезпечення кібербезпеки СБУ)

- E-mail: **incident@dis.gov.ua**