СИТУАЦІЙНИЙ ЦЕНТР
ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ
СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Інформаційні матеріали щодо способів реалізації кібератак на месенджери та рекомендації з їх попередження

Механізми реалізації кібератаки на комерційні месенджери

Фішинг через запрошення до групи

Один із поширених способів компрометації акаунту в месенджері Signal полягає у використанні фішингових повідомлень із запрошенням до групи. Зловмисники надсилають повідомлення, яке виглядає офіційно та викликає довіру (наприклад, запрошення до участі в робочій групі або обговоренні важливої теми, яке може надходити від записаного у Вас контакту).

Після переходу за фішинговим посиланням отримувач потрапляє у групу в додатку Signal. В цій групі він зазвичай бачить знайомі імена контактів, що створює ілюзію автентичності та підвищує рівень довіри до групи.

Спершу в групі зловмисники можуть відправляти нейтральні повідомлення без вкладень чи посилань, щоб не викликати підозри. Після цього, коли рівень довіри зростає, надходить повідомлення з посиланням або вкладеним файлом, в якому зазначається, що файл важливий і його потрібно переглянути на комп'ютері, оскільки "на телефоні він не відкривається". Після переходу за посиланням або відкриття файлу на ПК зазвичай відбувається або компрометація пристрою або особа втрачає доступ до сесії в месенджері.

Механізми реалізації кібератаки на комерційні месенджери

Вразливість прив'язки нового пристрою через текстове повідомлення

Раніше в Signal існувала вразливість, яка дозволяла зловмисникам надсилати текстове повідомлення, що маскувалося під посилання для прив'язки нового пристрою.

Посилання, відображене у вигляді QR-коду, при відкритті запускало процес, який дозволяв зловмисникам отримати доступ до акаунту користувача.

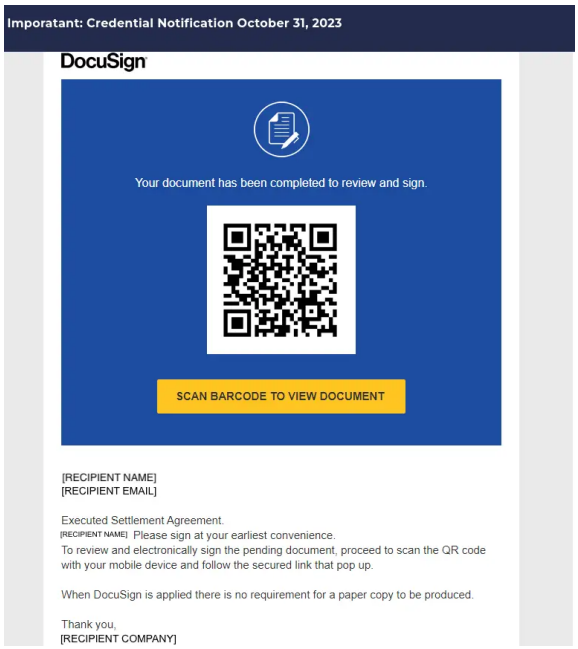
Цю вразливість уже виправлено, але до будь-яких посилань у месенджері варто ставитися з обережністю. Навіть якщо повідомлення надходить від знайомого контакту, варто додатково зателефонувати та уточнити деталі перед тим, як відкривати посилання. Також слід пам’ятати, що такі посилання можуть слугувати причиною зламу інших месенджерів або сервісів, тому необхідно завжди залишатися пильними.

Механізми реалізації кібератаки на комерційні месенджери

Використання QR-коду для авторизації

Ще одним поширеним методом атаки є використання підробленого сайту, який дублює зовнішній вигляд відомого ресурсу (наприклад, інтернет-магазину), де зловмисники запрошують користувача пройти авторизацію через месенджер Signal, запропонувавши відсканувати QR-код. Однак цей код генерується на пристрої зловмисників і, після його сканування, створюється сесія, яка дає їм доступ до акаунту жертви в Signal. QR-код дублюється на комп'ютер жертви, що створює ілюзію легітимності процесу.

Зазвичай інтернет-магазини не використовують метод авторизації через QR-коди, надаючи перевагу SMS-підтвердженню з кодом. У разі отримання подібного запиту слід ставитися до нього з обережністю та уникати сканування QR-кодів із невідомих або неперевірених джерел, так як також існує багато інших векторів атак із використанням QR-кодів (наприклад, прохання відсканувати код для отримання доступу до файлу).



Механізми реалізації кібератаки на комерційні месенджери

Використання десктопної версії Signal

Десктопна версія месенджера Signal є більш вразливою до зламу порівняно з мобільною версією. Її використання створює додаткові ризики, особливо якщо пристрій працює на операційній системі Windows, яка є пріоритетною ціллю для більшості розробників шкідливого програмного забезпечення. Зловмисники часто надсилають файли із ШПЗ (як в наведеному нижче скріншоті), закликаючи відкрити їх саме на комп'ютері. Це дозволяє їм скористатися вразливостями операційної системи для отримання віддаленого виконання коду та встановлення контролю над пристроєм жертви.

Зловмисники часто використовують ботів для автоматизації листування з метою швидкої взаємодії з великою кількістю потенційних жертв. Боти здатні автоматично реагувати на певні слова або запити, створюючи ілюзію реального діалогу, хоча відповідає запрограмований алгоритм. Їх також використовують для відправки шкідливих файлів або посилань, які можуть містити ШПЗ чи посилання на фішингові сайти. Крім того, боти можуть імітувати емоційно забарвлені відповіді, додаючи патріотичні мотиви, для того щоб викликати довіру. Підозрілі чи незграбні відповіді, наприклад, незв’язні фрази, відсутність логіки, повторення шаблонних повідомлень або невідповідність контексту, мають викликати підозру.

Рекомендується уникати використання десктопної версії Signal без нагальної необхідності. У разі її використання слід забезпечити належний рівень захисту системи, включаючи оновлення програмного забезпечення та використання антивірусного захисту. Також важливо уникати відкриття будь-яких підозрілих файлів або посилань, навіть якщо вони здаються легітимними, варто вжити заходи для їх перевірки.

Відновлення контролю над акаунтом в Signal

Для відновлення контролю над обліковим записом Signal необхідно володіти фізичною SIM-карткою.

Для цього на іншому смартфоні встановіть додаток Signal та вставте SIM картку з номером телефону, який відповідає втраченому акаунту.

При першому запуску додатка проводиться верифікація зазначеного номеру через перевірочний код у вигляді SMS повідомлення на наявний номер телефону. За правилами додатку Signal користувач з фізичною карткою має пріоритет у отриманні автентифікаційних даних, що створює перевагу перед зловмисником.

Після відновлення контролю активуйте двофакторну аутентифікацію Signal у вигляді буквено-цифрового PIN-коду з використанням великих та малих літер, цифр та спеціальних знаків.

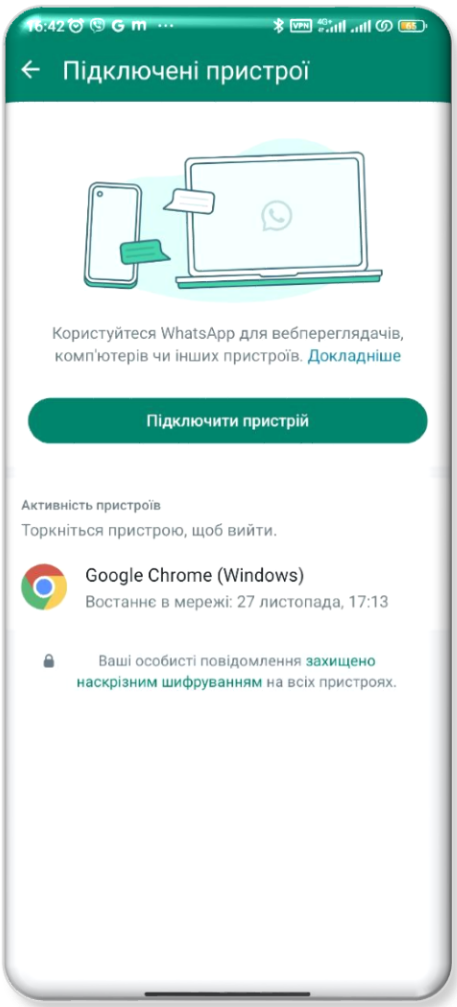
Загальні рекомендації щодо захисту смартфону

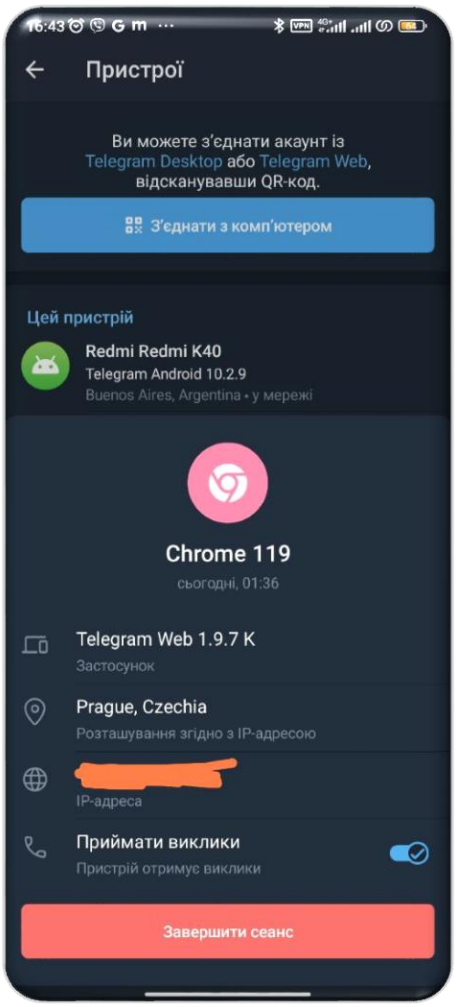
Виявлення паралельних сесій в месенджерах

Перевірка паралельних сесій у месенджерах дозволяє виявити і вчасно зреагувати на несанкціонований доступ до вашого аккаунта.

Отримання доступу до вашого месенджера на іншому пристрої може призвести до витоку особистої інформації, перехоплення повідомлень, або навіть шахрайства від вашого імені.

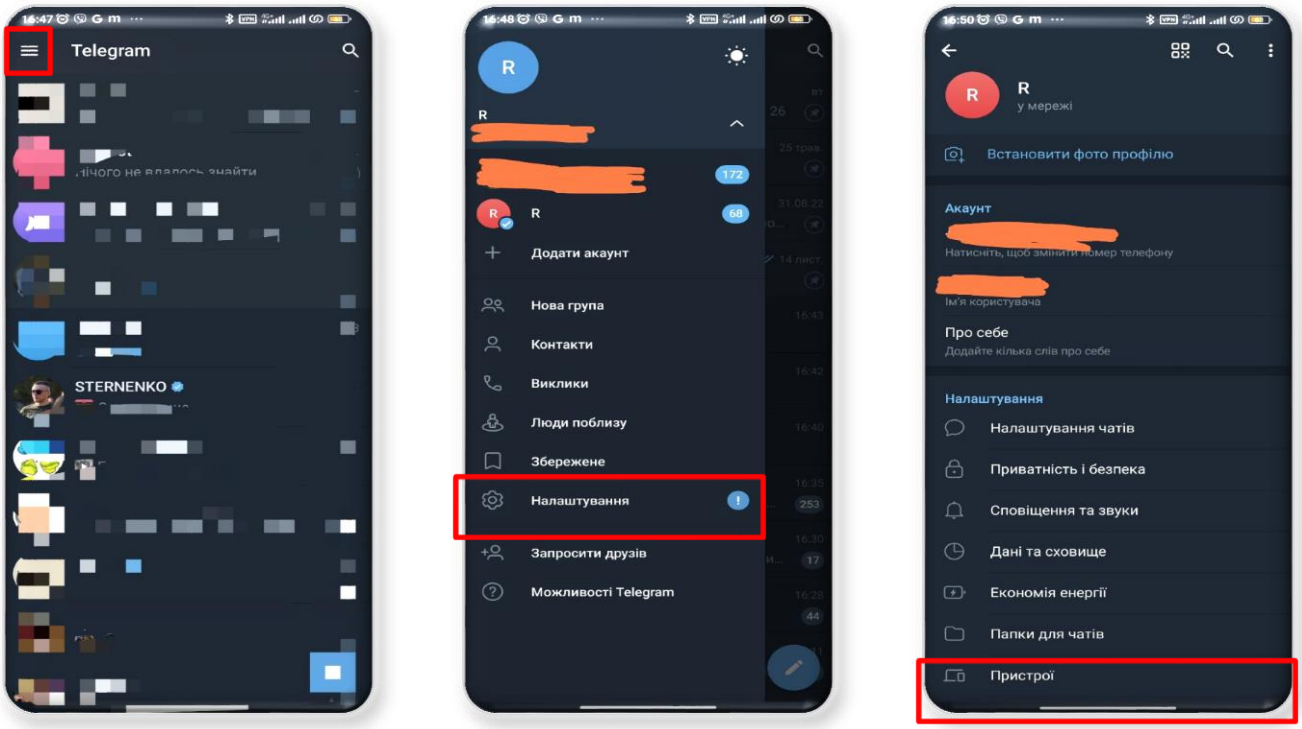
Регулярна перевірка активних сесій та їх закриття, якщо вони вам невідомі, є ключовою для забезпечення вашої цифрової безпеки.

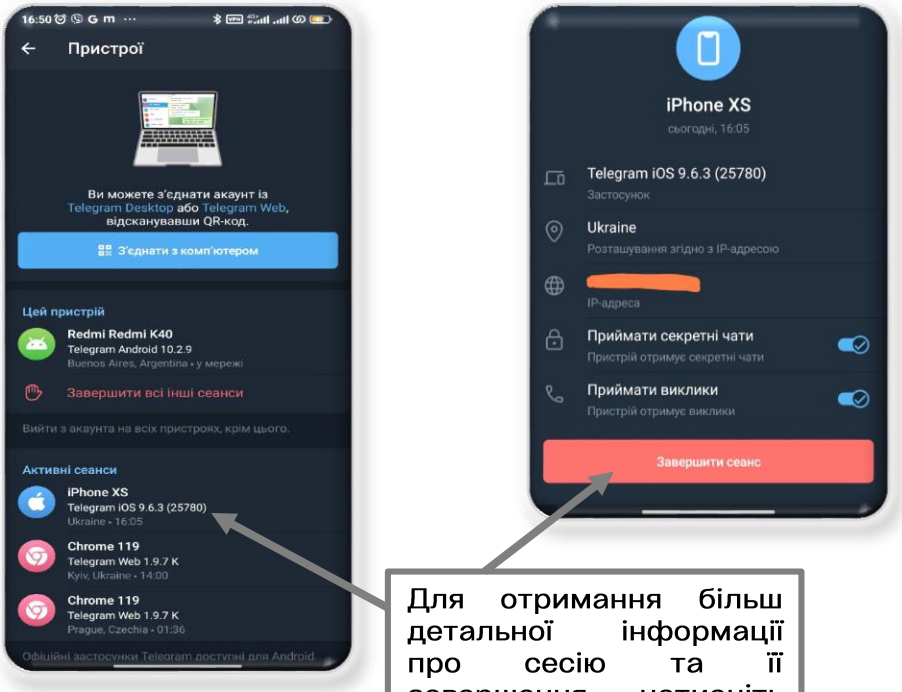




Загальні рекомендації щодо захисту смартфону

Виявлення паралельних сесій в Telegram для Android

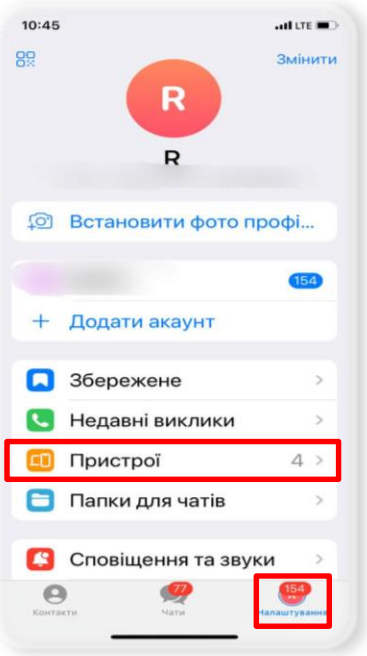


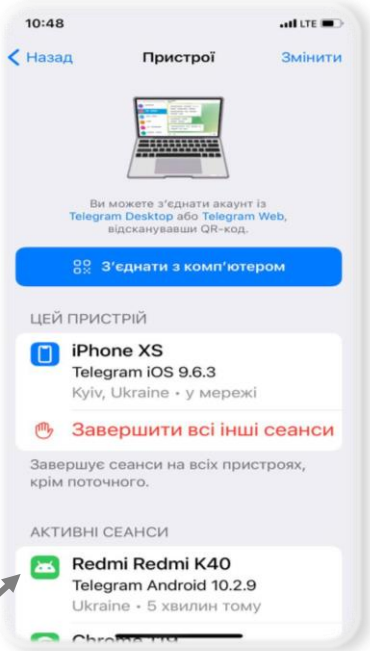


Для отримання більш детальної інформації про сесію та її завершення, натисніть на відповідну вкладку

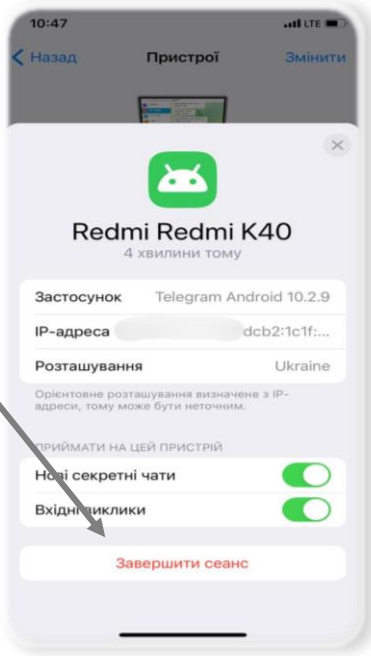
Загальні рекомендації щодо захисту смартфону

Виявлення паралельних сесій в Telegram для Apple IOS



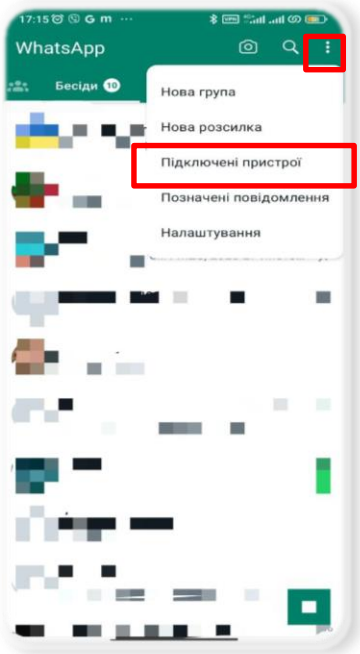


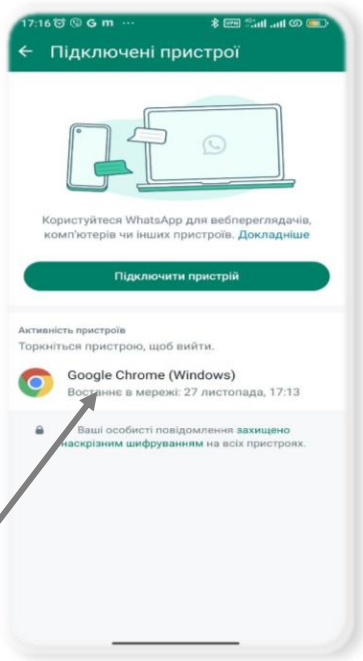
Для отримання більш детальної інформації про сесію та її завершення, натисніть на відповідну вкладку



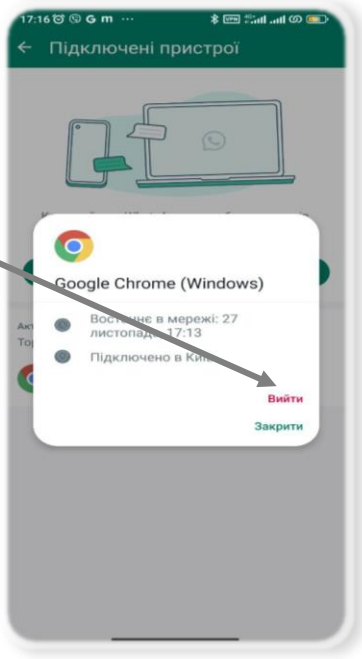
Загальні рекомендації щодо захисту смартфону

Виявлення паралельних сесій в WhatsApp для Android



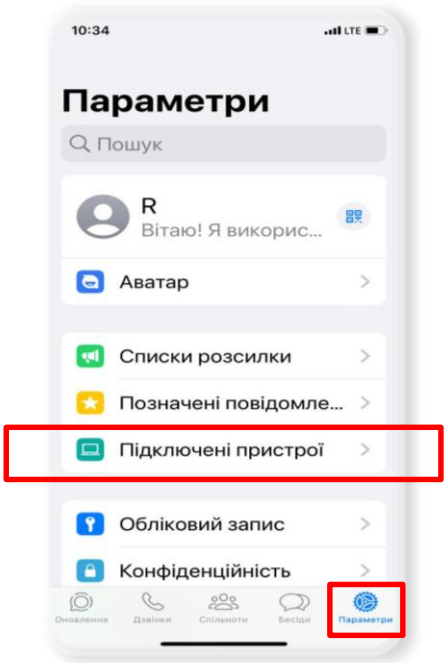


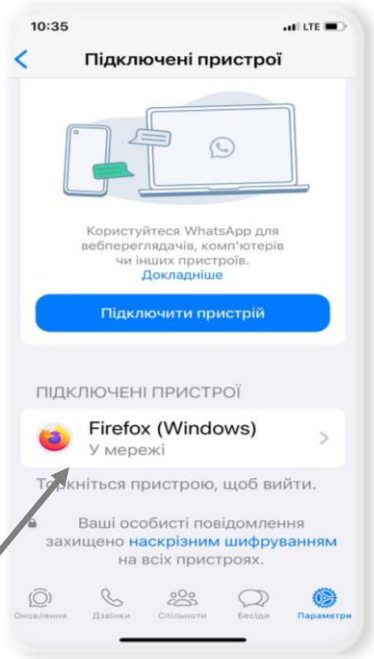
Для отримання більш детальної інформації про сесію та її завершення, натисніть на відповідну вкладку



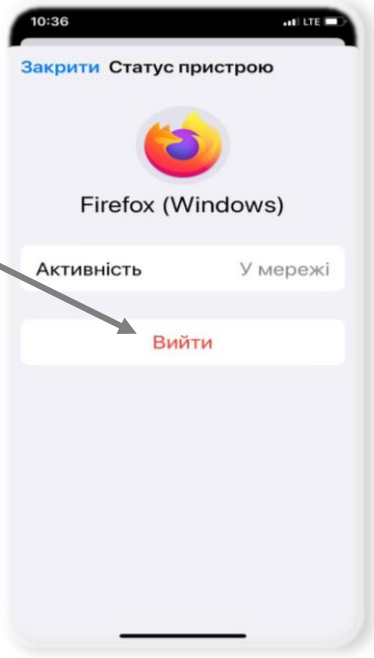
Загальні рекомендації щодо захисту смартфону

Виявлення паралельних сесій в WhatsApp для Apple IOS



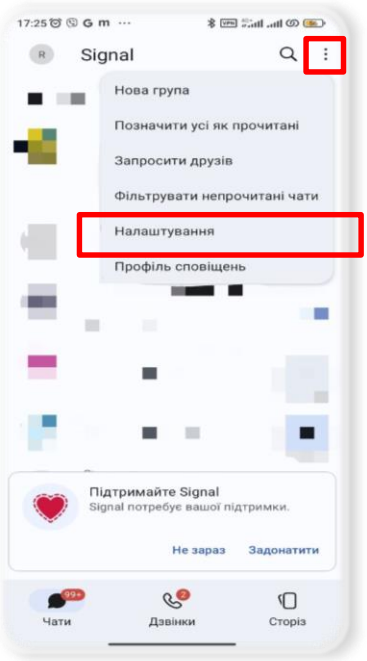


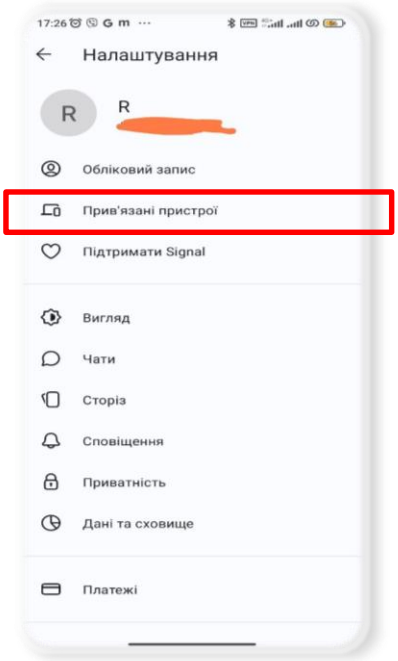
Для отримання більш детальної інформації про сесію та її завершення, натисніть на відповідну вкладку

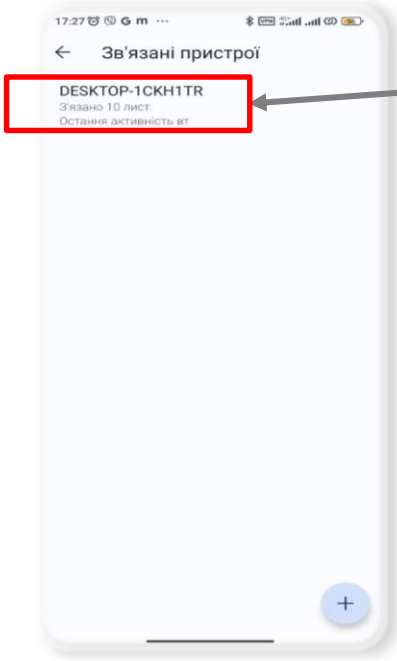


Загальні рекомендації щодо захисту смартфону

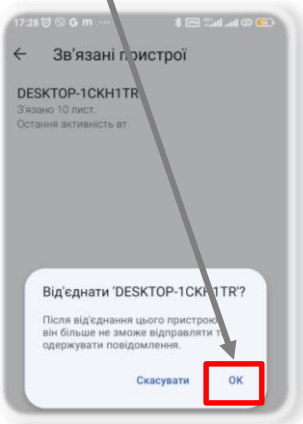
Виявлення паралельних сесій в Signal для Android





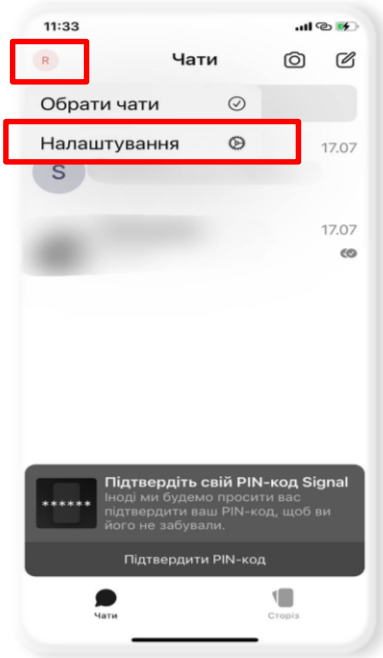


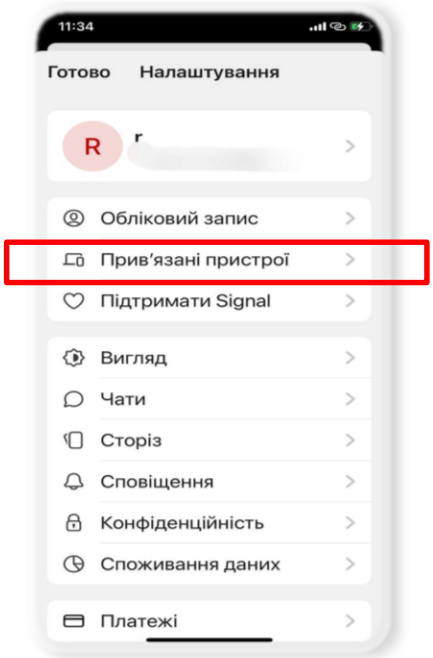
Для завершення сесії натисніть на відповідну вкладку та натисніть «OK»

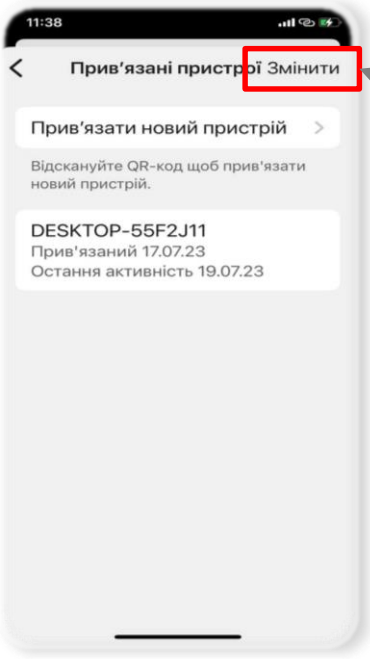


Загальні рекомендації щодо захисту смартфону

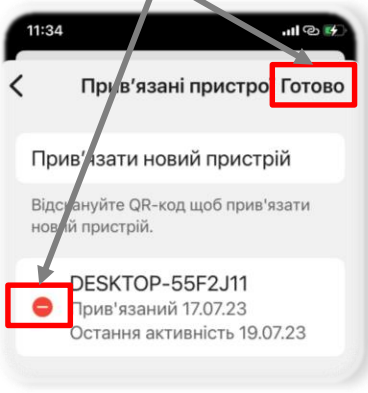
Виявлення паралельних сесій в Signal для Apple IOS





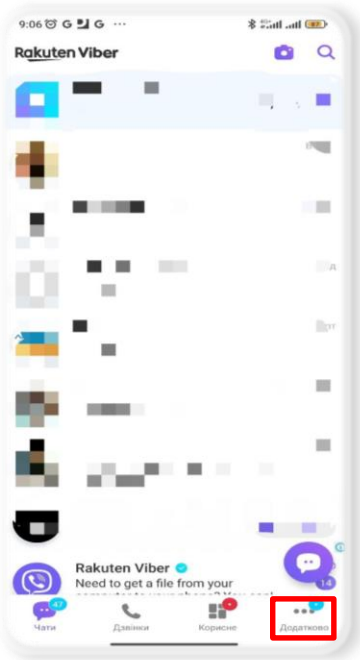


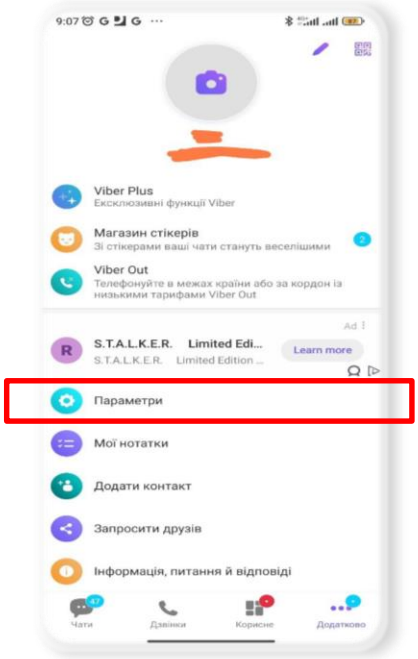
Для завершення сесії натисніть на вкладку «Змінити» та червоний значок біля відповідної вкладки із назвою пристрою. Натисніть «Готово»

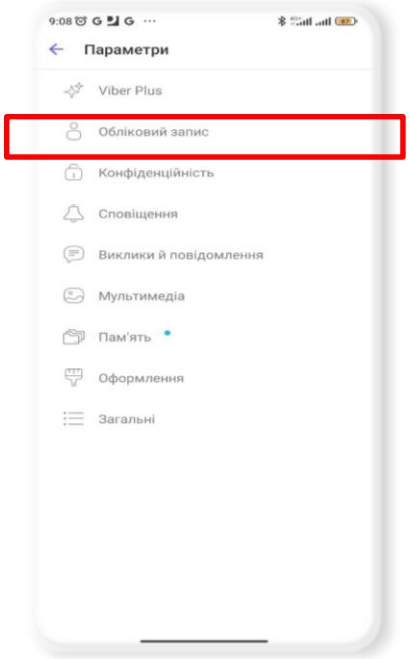


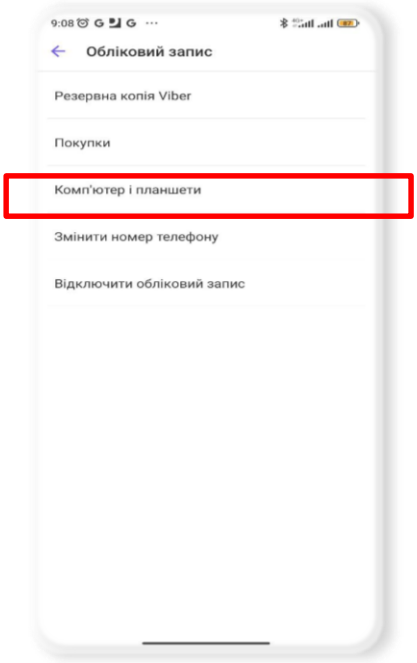
Загальні рекомендації щодо захисту смартфону

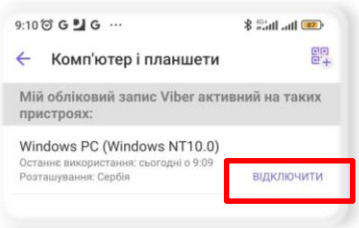
Виявлення паралельних сесій в Viber для Android



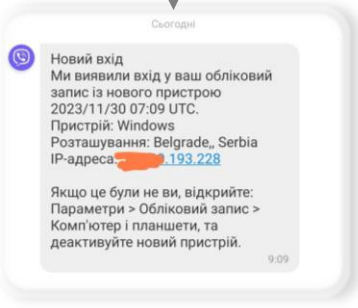






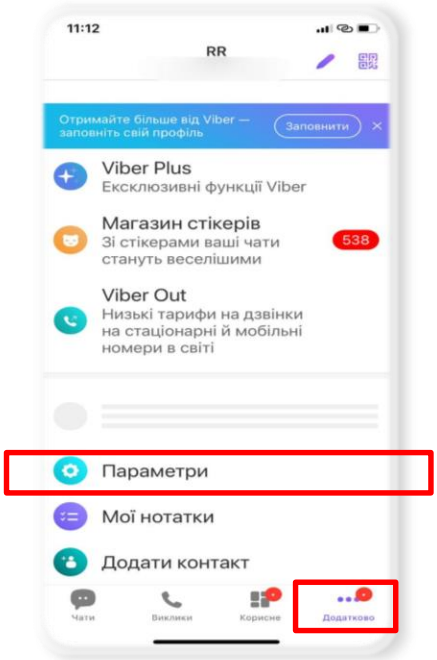


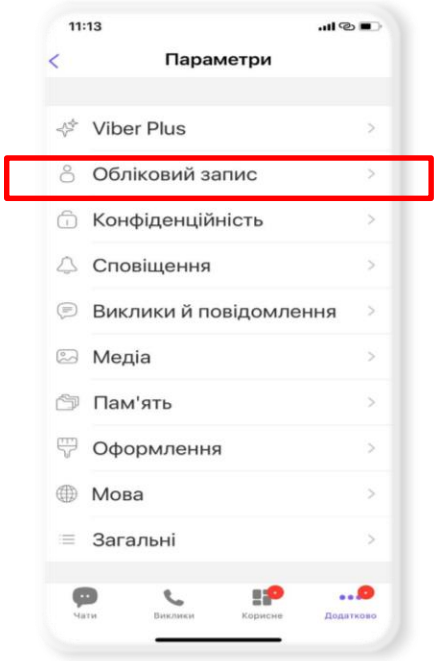
Для перегляду дати, часу, місця та IP-адреси, з якої було здійснено вхід до акаунту перегляньте службовий чат із Viber.

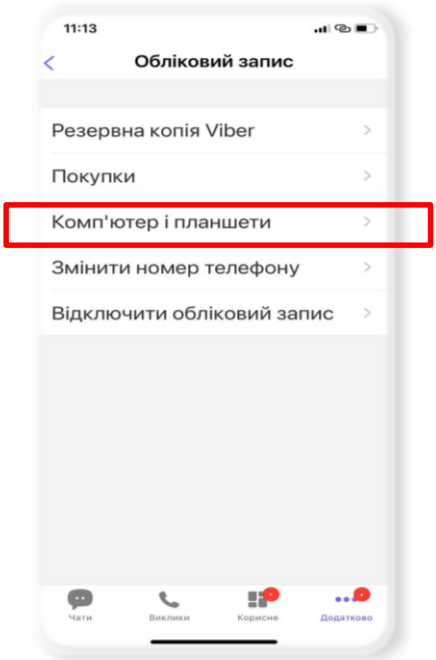


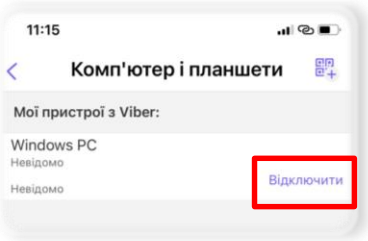
Загальні рекомендації щодо захисту смартфону

Виявлення паралельних сесій в Viber для Apple IOS

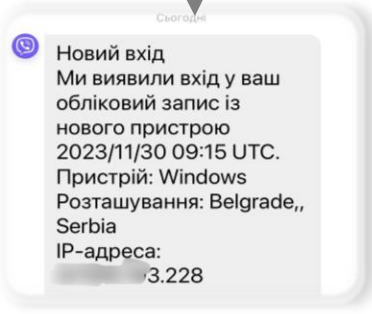






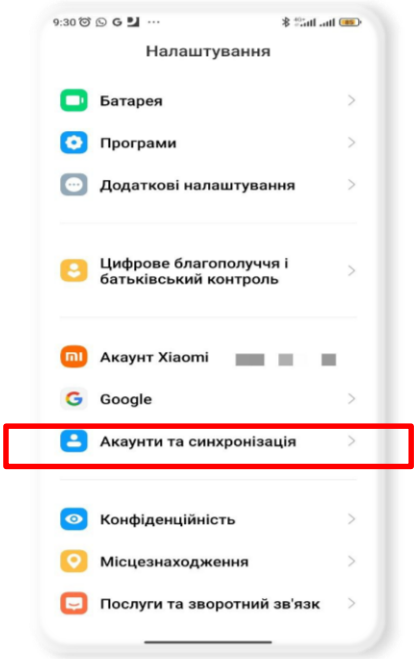


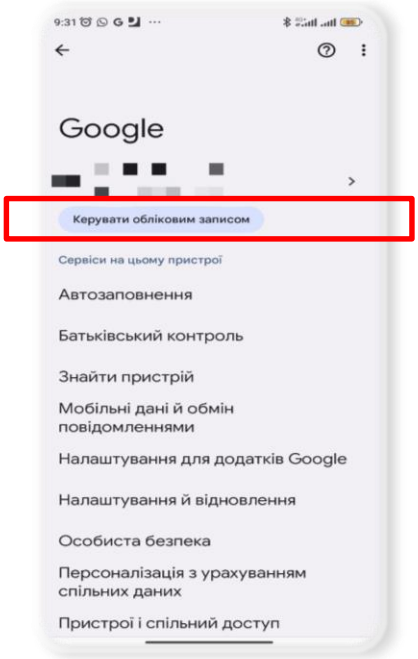
Для перегляду дати, часу, місця та IP-адреси, з якої було здійснено вхід до акаунту перегляньте службовий чат із Viber.

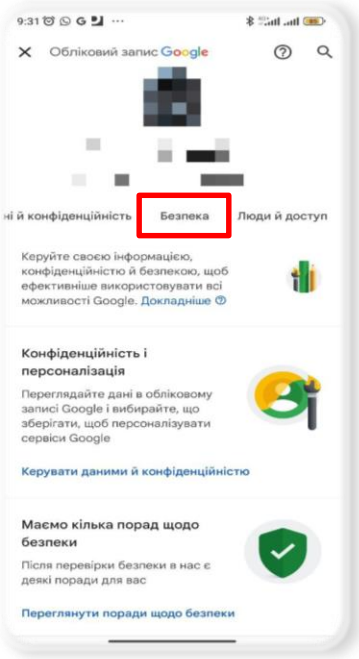


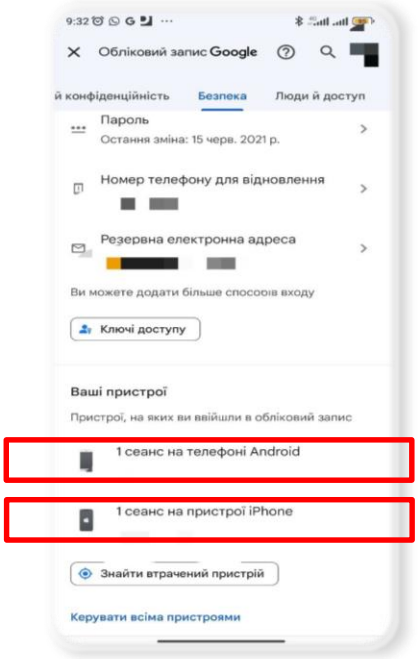
Загальні рекомендації щодо захисту смартфону

Виявлення підключених пристроїв до Google Account







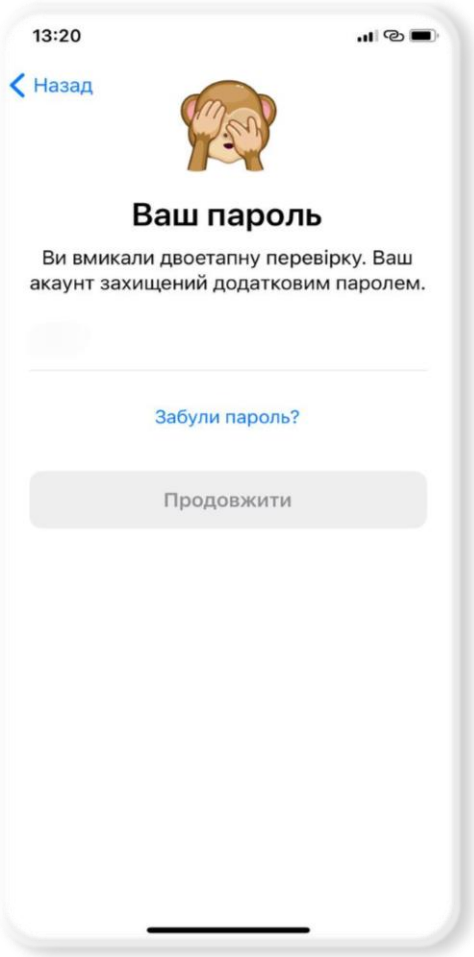


Загальні рекомендації щодо захисту смартфону

Фішинг через запрошення до групи

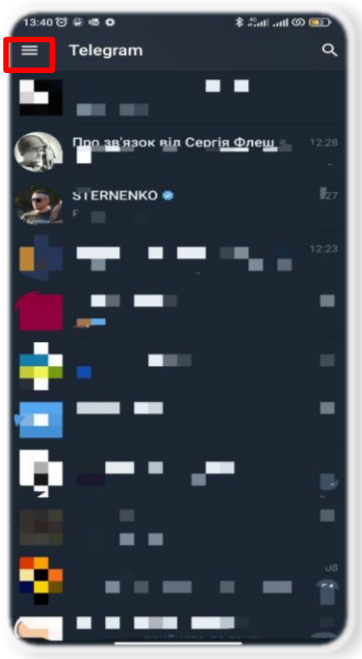
Двофакторна автентифікація (2FA) є критично важливою для забезпечення безпеки Ваших облікових записів. Цей метод додає додатковий шар захисту, вимагаючи два різні типи інформації для входу у ваш акаунт — щось, що ви знаєте (наприклад, пароль) і щось, що у вас є (наприклад, мобільний телефон).

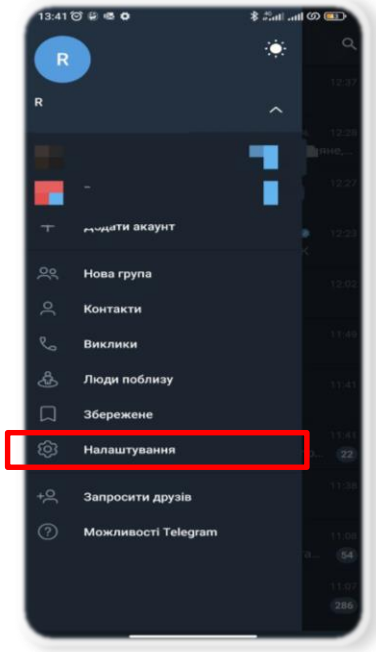
2FA запобігає несанкціонованому доступу до вашого облікового запису, навіть якщо хтось дізнається ваш пароль (або отримає доступ до телефону чи СМС-повідомлень, необхідних для успішного входу до Вашого акаунту).

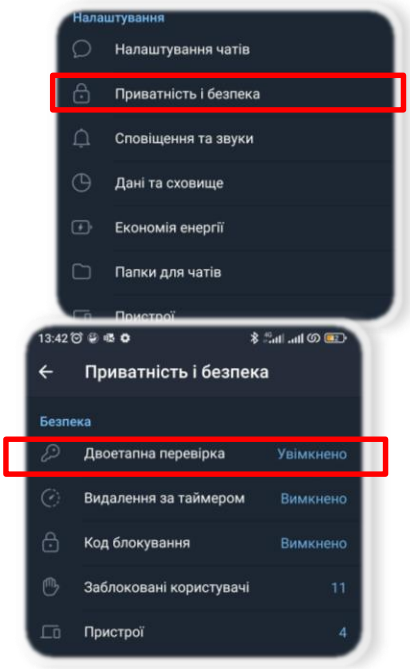


Загальні рекомендації щодо захисту смартфону

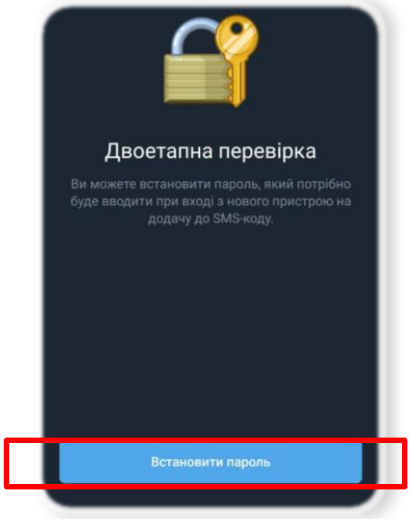
Налаштування двофакторної автентифікації в Telegram для Android

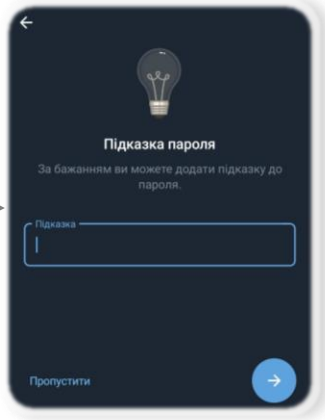






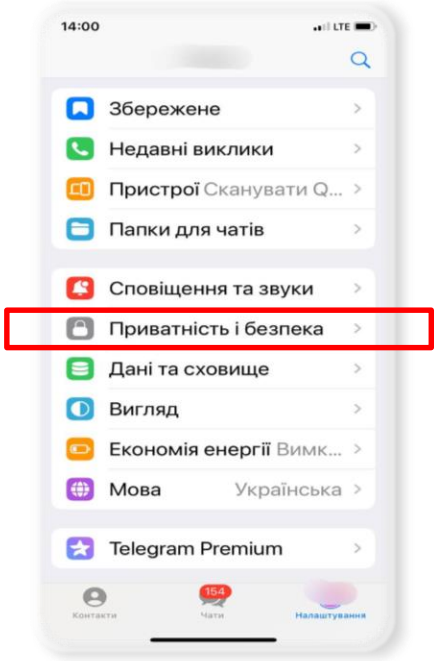
КРИТИЧНО ВАЖЛИВО!
В разі налаштування підказки до паролю двофакторної автентифікації подбайте про те, щоб з допомогою неї Ваш пароль не могли підібрати потенційні зловмисники.

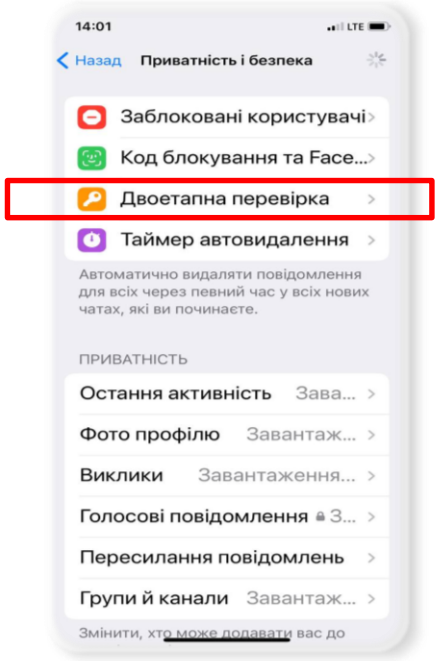


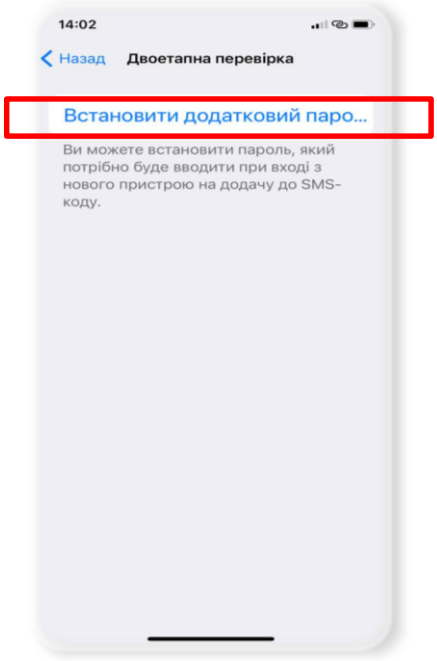


Загальні рекомендації щодо захисту смартфону

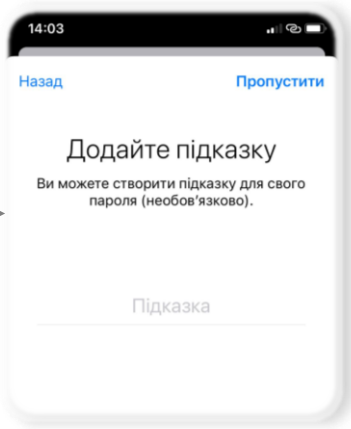
Налаштування двофакторної автентифікації в Telegram для Apple iOS





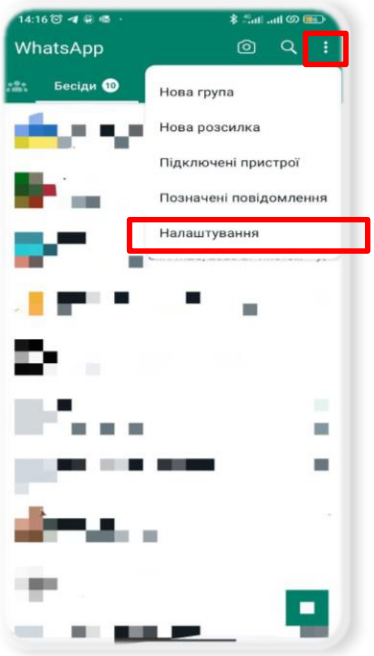


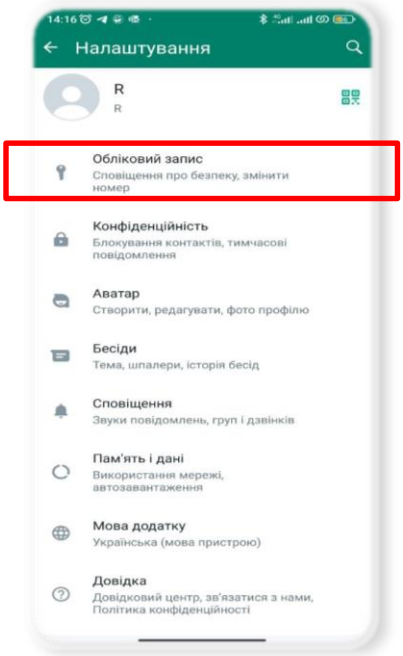
КРИТИЧНО ВАЖЛИВО!
В разі налаштування підказки до паролю двофакторної автентифікації подбайте про те, щоб з допомогою неї Ваш пароль не могли підібрати потенційні зловмисники.

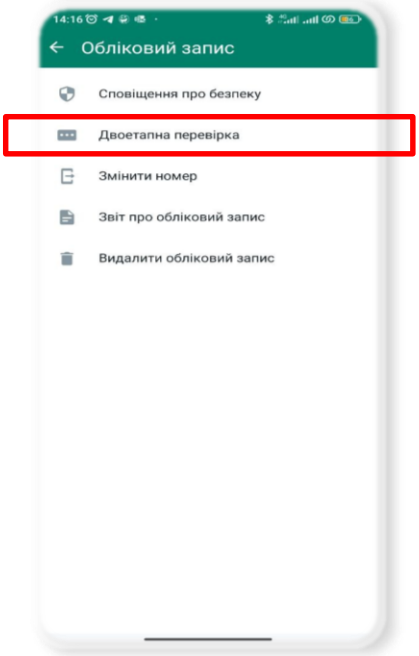


Загальні рекомендації щодо захисту смартфону

Налаштування двофакторної автентифікації в WhatsApp для Android

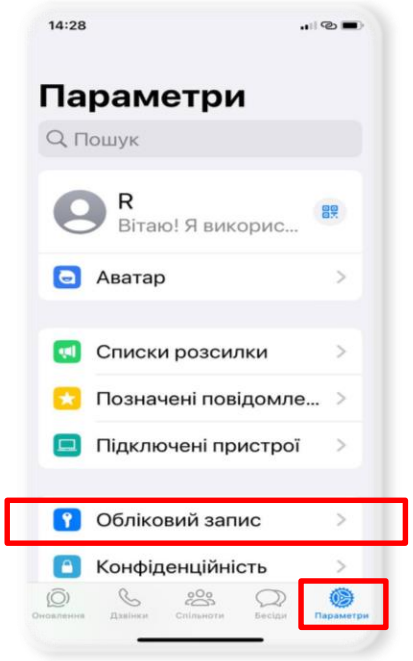


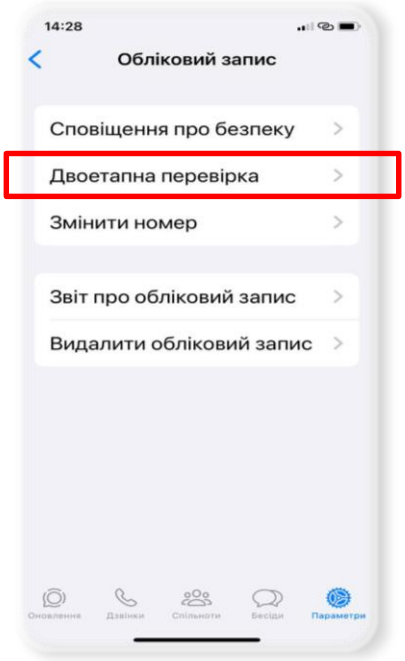


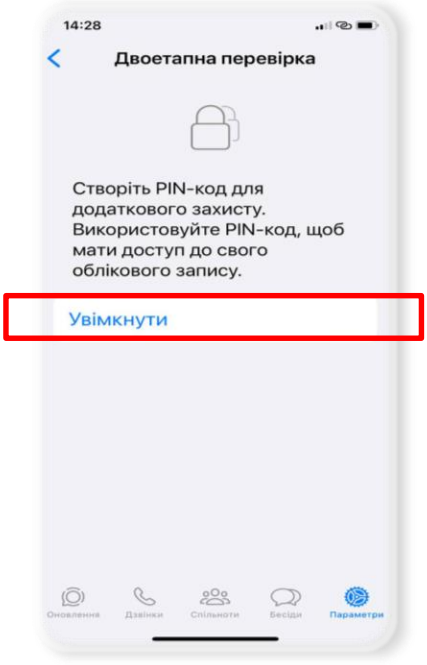


Загальні рекомендації щодо захисту смартфону

Налаштування двофакторної автентифікації в WhatsApp для Apple iOS

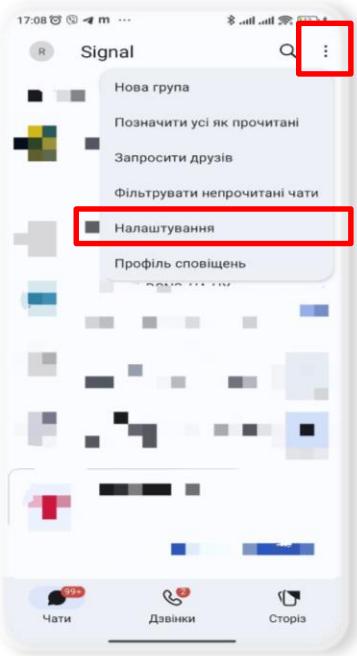


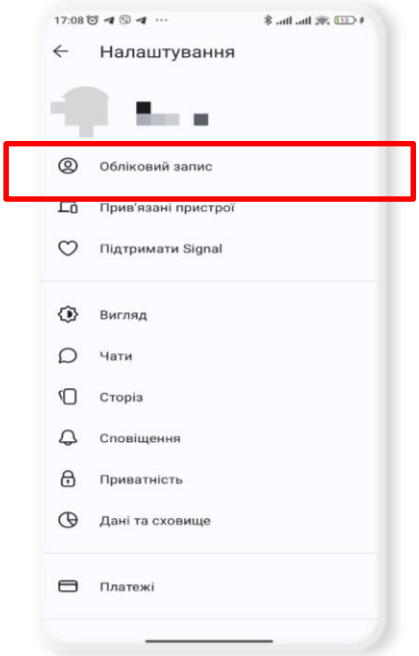


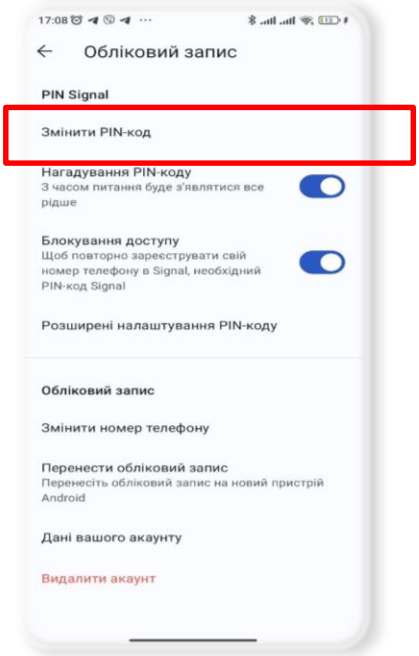


Загальні рекомендації щодо захисту смартфону

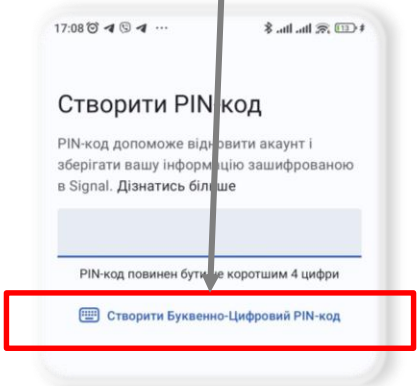
Налаштування двофакторної автентифікації в Signal для Android





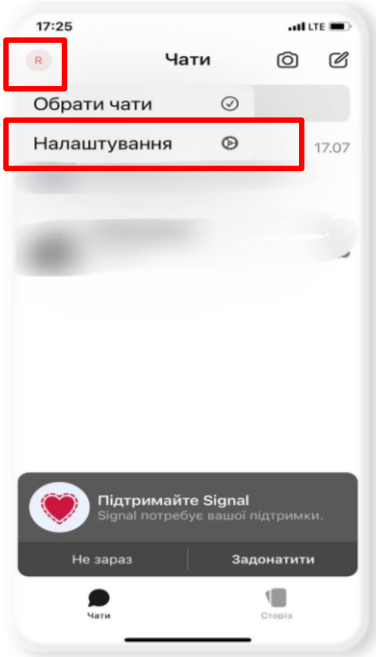


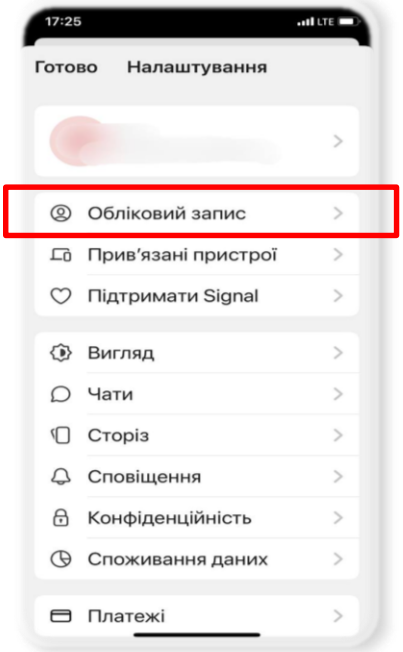
Серед доступних варіантів варто налаштувати саме «Буквенно-Цифровий PIN-код»

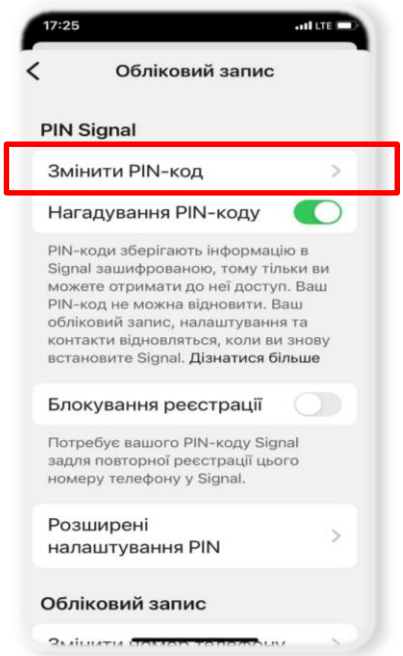


Загальні рекомендації щодо захисту смартфону

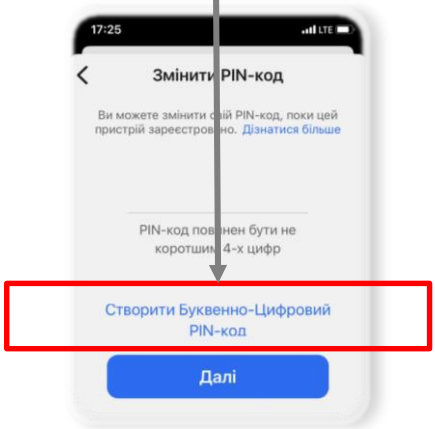
Налаштування двофакторної автентифікації в Signal для Apple iOS





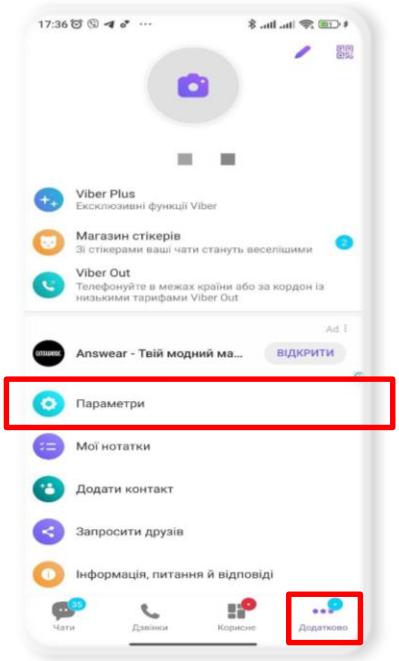


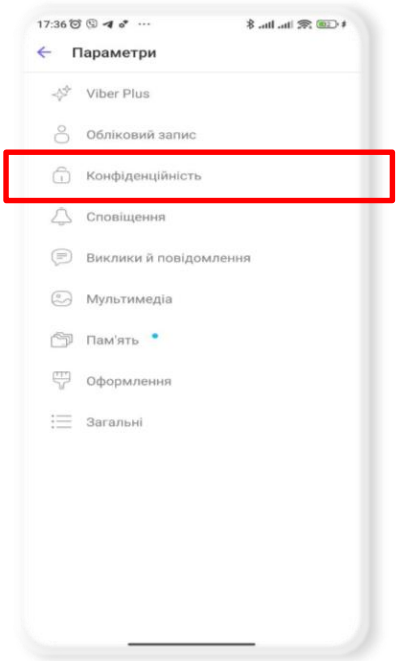
Серед доступних варіантів варто налаштувати саме «Буквенно-Цифровий PIN-код»

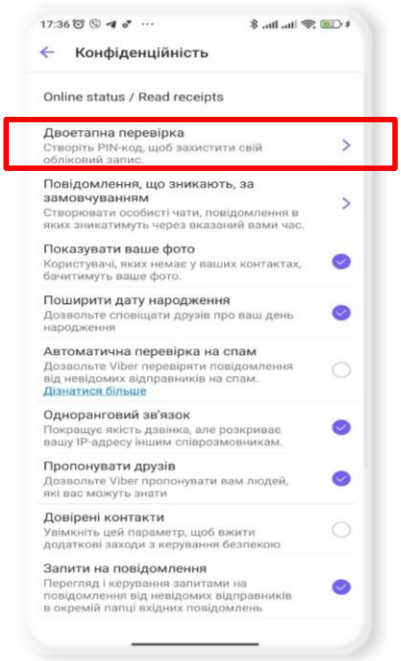


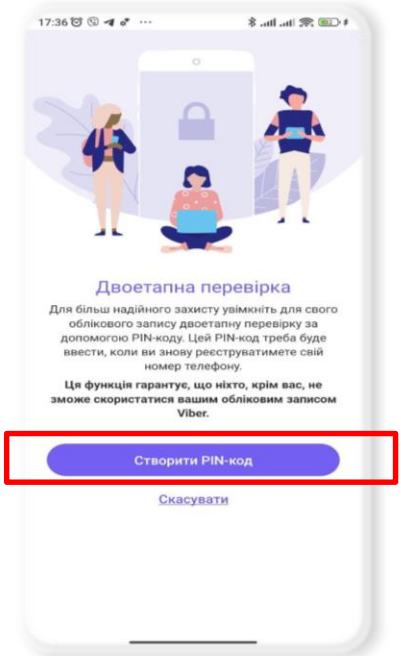
Загальні рекомендації щодо захисту смартфону

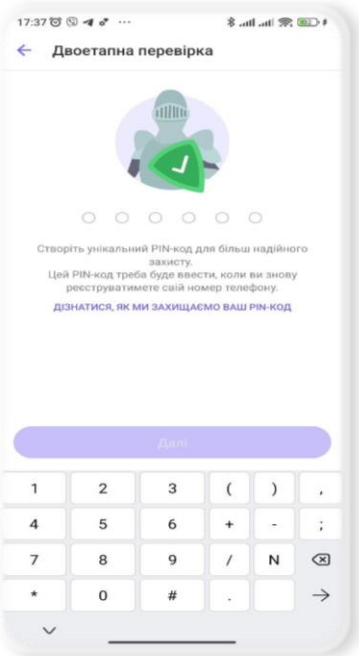
Налаштування двофакторної автентифікації в Viber для Android





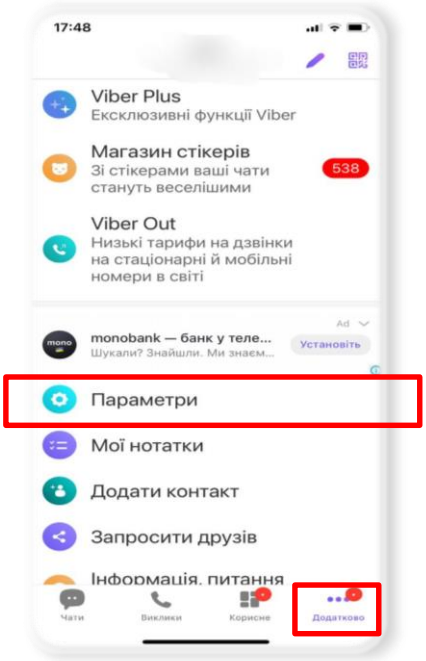


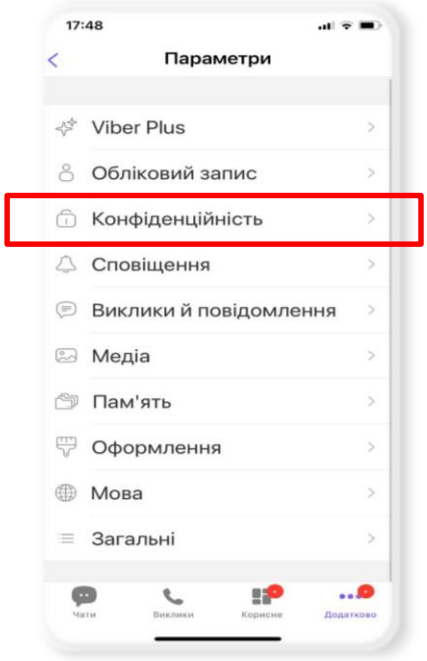


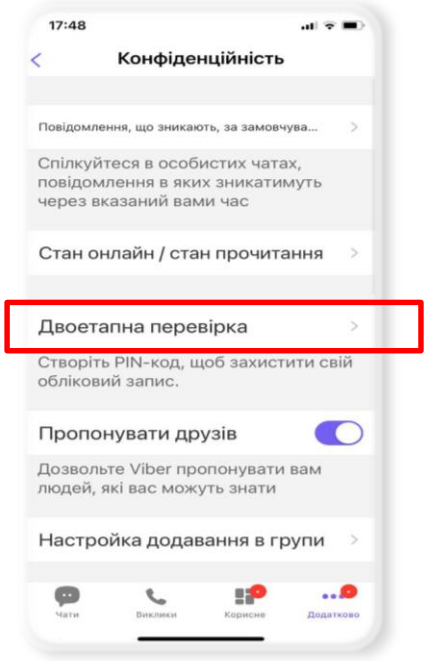


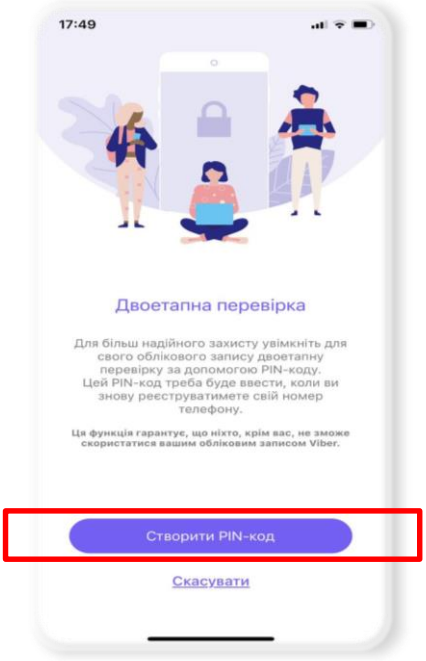
Загальні рекомендації щодо захисту смартфону

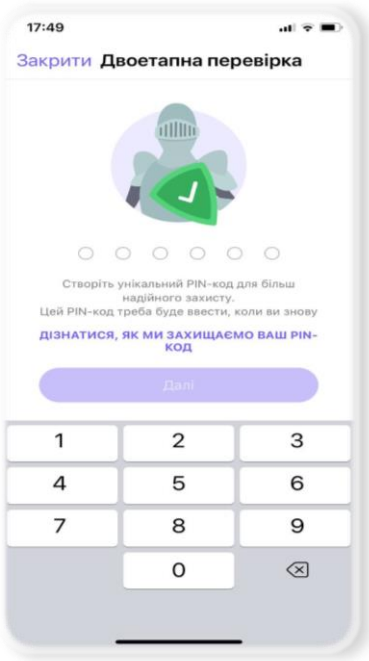
Налаштування двофакторної автентифікації в Viber для Apple iOS







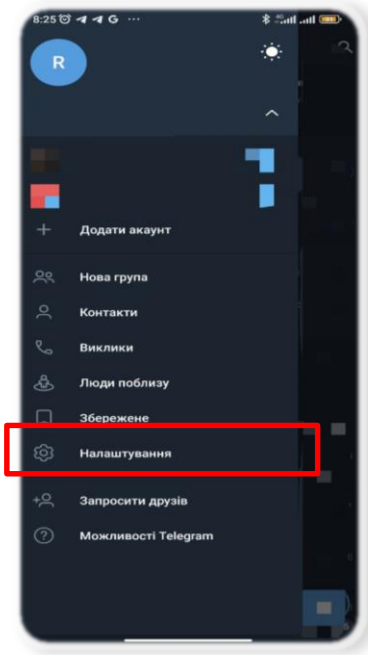


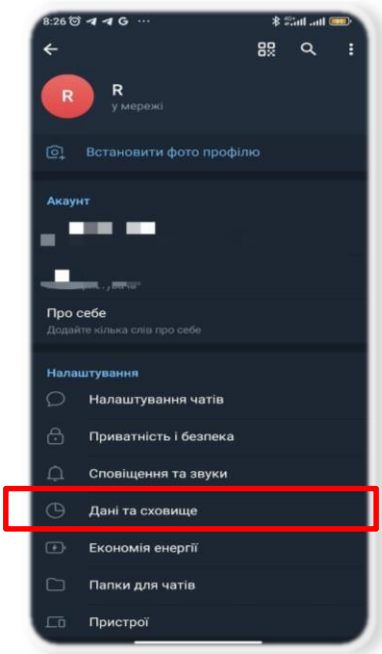


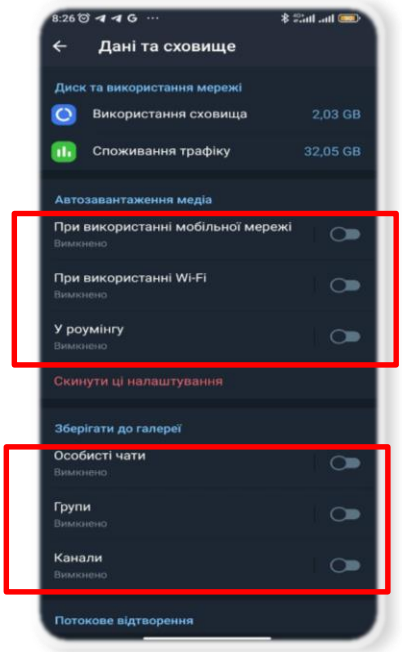
Загальні рекомендації щодо захисту смартфону

Відключення автозавантаження файлів в Telegram для Android

Відключення автозавантаження медіа в Telegram захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами



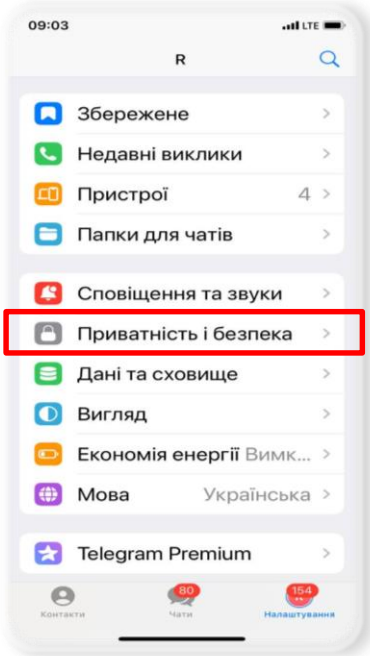


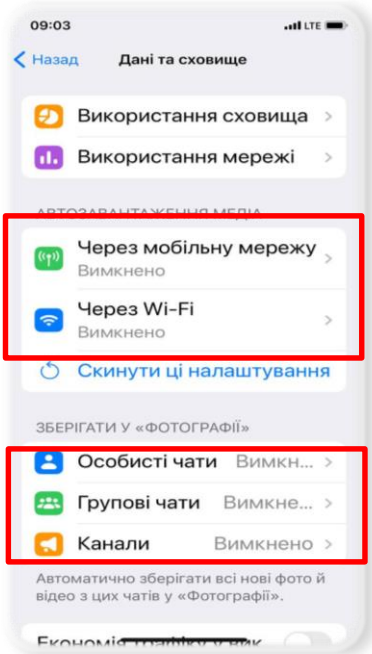


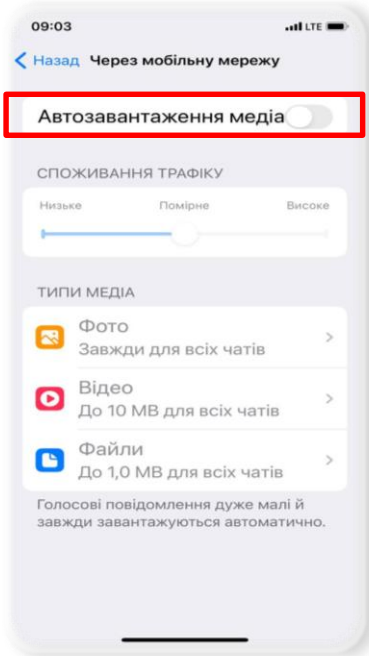
Загальні рекомендації щодо захисту смартфону

Відключення автозавантаження файлів в Telegram для Apple iOS

Відключення автозавантаження медіа в Telegram захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами



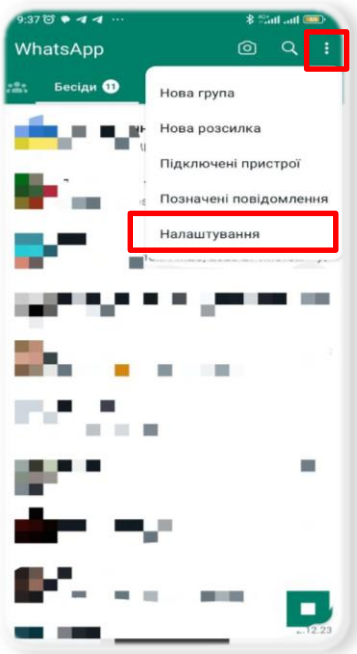


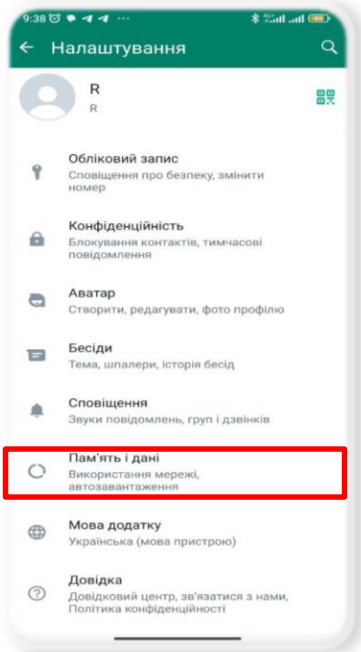


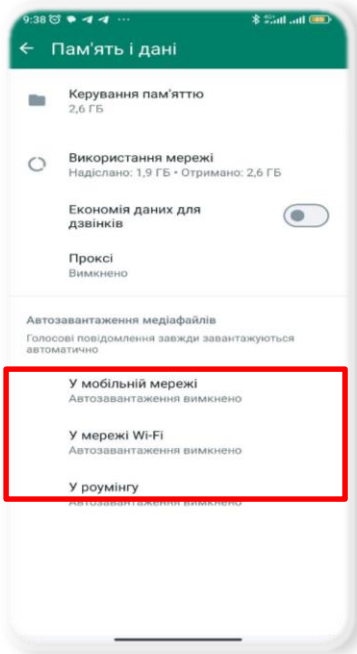
Загальні рекомендації щодо захисту смартфону

Відключення автозавантаження файлів в WhatsApp для Android

Відключення автозавантаження медіа в WhatsApp захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами



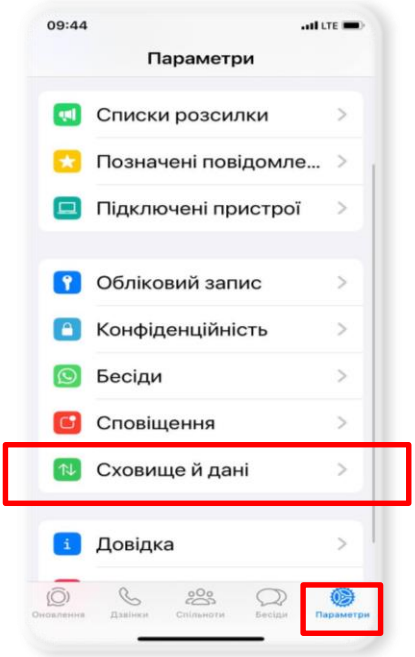


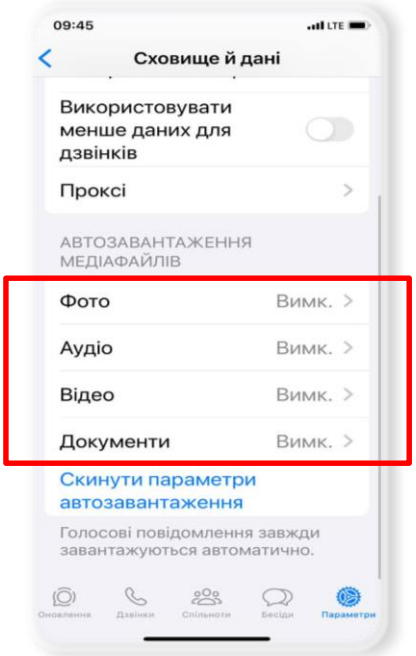


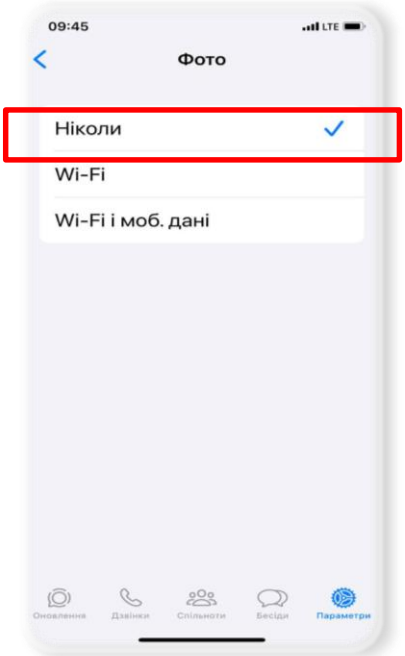
Загальні рекомендації щодо захисту смартфону

Відключення автозавантаження файлів в WhatsApp для Apple iOS

Відключення автозавантаження медіа в WhatsApp захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами



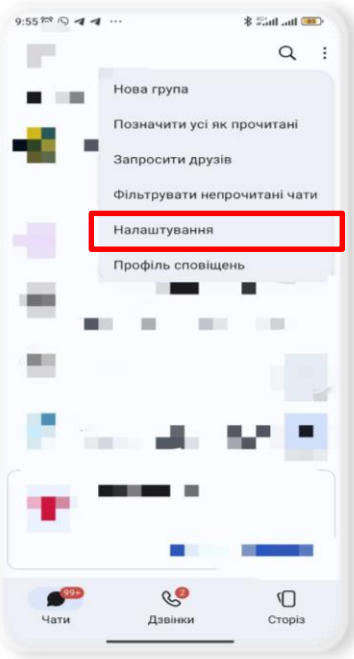


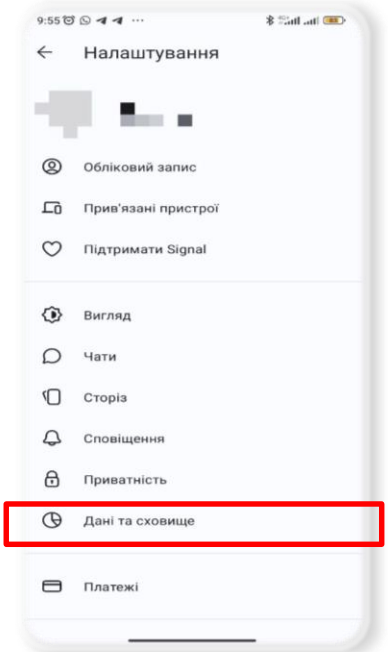


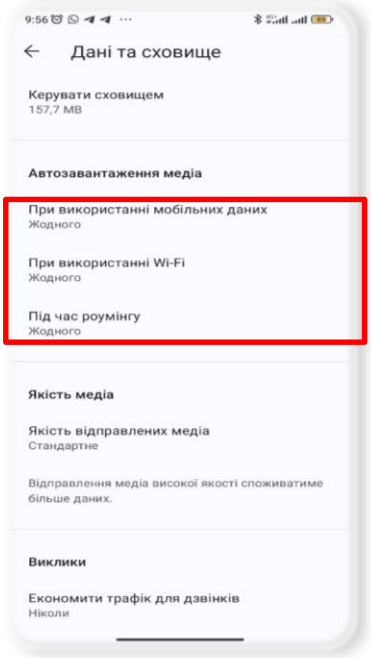
Загальні рекомендації щодо захисту смартфону

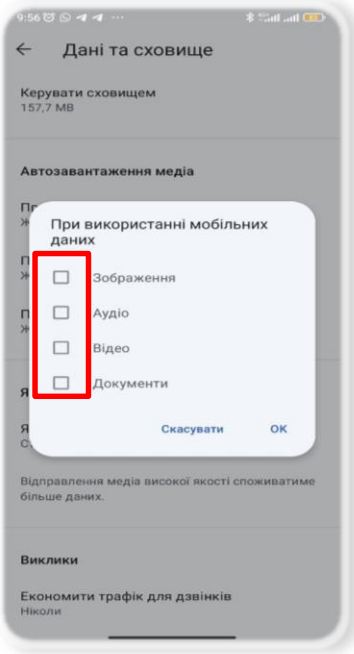
Відключення автозавантаження файлів в Signal для Android

Відключення автозавантаження медіа в Signal захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами





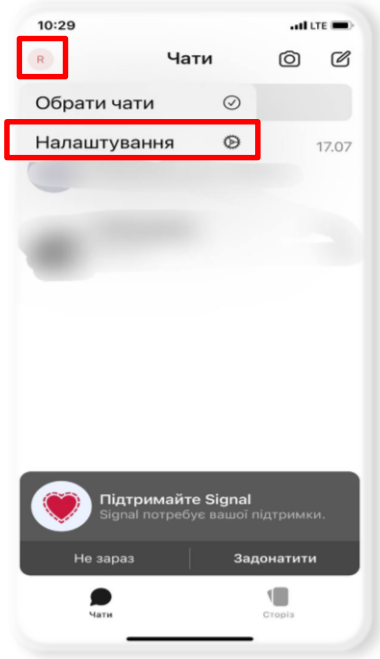


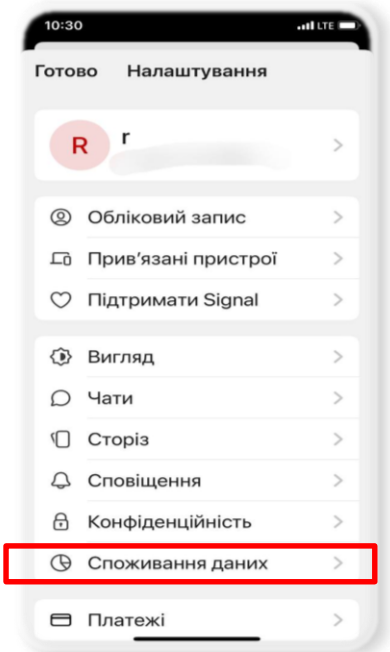


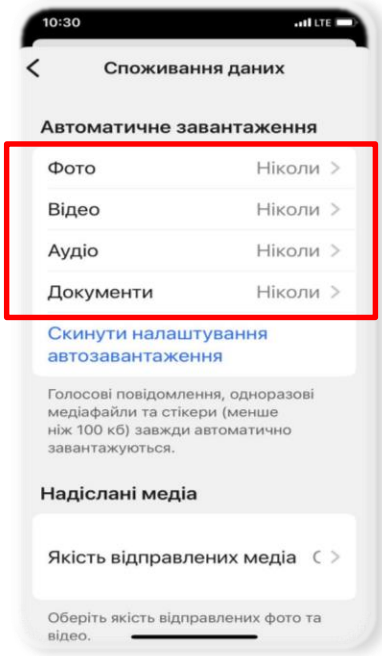
Загальні рекомендації щодо захисту смартфону

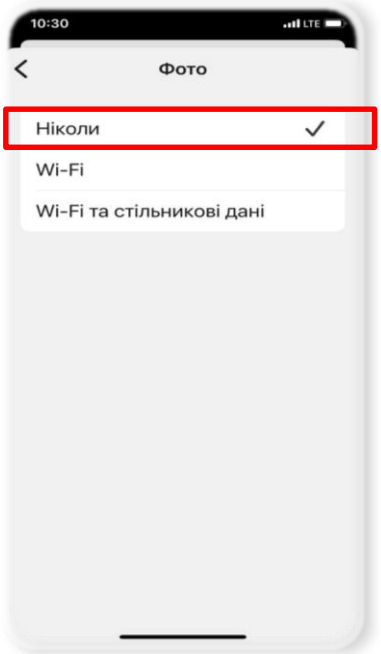
Відключення автозавантаження файлів в Signal для Apple iOS

Відключення автозавантаження медіа в Signal захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами









Загальні рекомендації щодо захисту смартфону

Відключення автозавантаження файлів в Viber для Apple iOS

Відключення автозавантаження медіа в Viber захищає від автоматичного завантаження потенційно шкідливого або небажаного контенту, який може потрапити на Ваш пристрій, знижуючи ризик зараження вірусами