# Як захистити свої акаунти

**Технічна безпека в умовах воєнного стану — це особистий обов'язок кожного. В той момент, коли наші солдати захищають нас на воєнному фронті, а делегати — на дипломатичному, безпеку особистих даних кожен з нас повинен забезпечити самостійно. Ми зібрали перелік рекомендацій для того, щоб приховати свої дані від зловмисників, яких, на жаль, в цей непростий час забагато.**

## TELEGRAM

Найуразливіше місце Телеграм-акаунту зустрічає користувачів при першому запуску застосунку. Якщо зловмиснику відомий Ваш номер телефону, то за допомогою стороннього софту не важко буде перехопити повідомлення із кодом авторизації.

Щоб уникнути втрати Телеграм-акаунту, рекомендуємо зробити дві важливі дії: «сховати» свій акаунт та увімкнути двофакторну аутентифікацію.

Для того, щоб «сховати» свій акаунт, необхідно перейти в розділ «Приватність і конфіденційність».

- У пункті «Хто може бачити мій номер» обираємо «Мої контакти», щоб ваш номер телефону не було можливо знайти у вільному доступі Телеграм;
- У пункті «Відвідини та стан у мережі» обираємо «Мої контакти», щоб тільки ваші близькі знали, коли ви були в мережі;
- У пункті «Фото профілю» обираємо «Мої контакти», щоб ніхто не міг використати саме те фото, яке стоїть у вашому профілі Телеграм;
- У пункті «Виклики» обираємо «Мої контакти», щоб запобігти дзвінкам від третіх осіб;
- У пункті «Пересилання повідомлень» обираємо «Ніхто», щоб сторонні користувачі не могли пересилати ваш акаунт будь-яким повідомленням;
- У пункті «У групах і каналах» обираємо «Мої контакти», щоб ваш акаунт не можна було додавати стороннім особам в групи або канали Телеграм.

Як можна помітити, вказані налаштування сильно зав'язані на тому, які контакти є у вашому телефоні. Тому, буде важливим нагадати необхідність фільтрувати свою телефонну книжку та раз на місяць чистити її на наявність сторонніх контактів насправді незнайомих вам осіб.

Щоб додатково захистити ваш акаунт, рекомендуємо встановити двофакторну автентифікацію. Ця опція дозволяє запросити персональний пароль вже після того, як користувачем буде введено разовий SMS-код. Цей пароль ви можете створити особисто.

Також, додаток рекомендує підв'язати електрону скриньку на той випадок, якщо Ви забудете пароль. Насправді з одного боку, це доволі

комфортний метод, але ми не рекомендуємо це робити, адже, якщо зловмисник матиме доступ до вашої електронної скриньки, то не важко буде отримати доступ до цього пароля. Однак, треба зазначити, якщо ви забудете цей пароль, то не зможете ніяким чином відновити акаунт Телеграм, тому, будьте обачні.

Для підключення переходимо в розділ «Приватність і конфіденційність», обираємо пункт «Двоетапна перевірка», створюємо пароль та за бажанням робимо собі невеличку підказку.

Окрім віртуального захисту свого Телеграму, рекомендуємо також поставити на сам додаток код-пароль без використання «Face ID» або «Touch ID».

Обов'язково, не забудьте встановити автоблокування на 5 або 10 хвилин замість стандартної години. Цей простий момент не дасть скористуватися Вашим акаунтом, якщо телефон буде втрачено.

Взагалі, рекомендуємо особисто переглянути усі пункти в розділі «Приватність і конфіденційність», щоб налаштувати додаток під себе, мінімізувати дискомфорт та збільшити ступінь захисту.

## VIBER

«Вайбер», попри свою популярність, має багато налаштувань, які ми з тих чи інших причин не звикли міняти. І нехай за статистикою Вайбер піддається кібератакам значно рідше, все одно не буде зайвим трішки «похімічити» із його параметрами безпеки.

Переходимо в меню «Додатково» (три крапки в правому нижньому кутку), обираємо розділ «Параметри», заходимо в «Конфіденційність».

Пункти «Показувати стан «В мережі», «Надсилати стан «Переглянуто» та «Пропонувати друзів» рекомендуємо відключити. Це необхідно для того, щоб Ваш акаунт зайвий раз було важче моніторити на момент активності.

В «Настройках додавання в групи» обмежуємо коло людей до списку ваших контактів. Це потрібно для того, щоб вас не додавали в чати сусіднього під'їзду або інші нерелевантні спільноти.

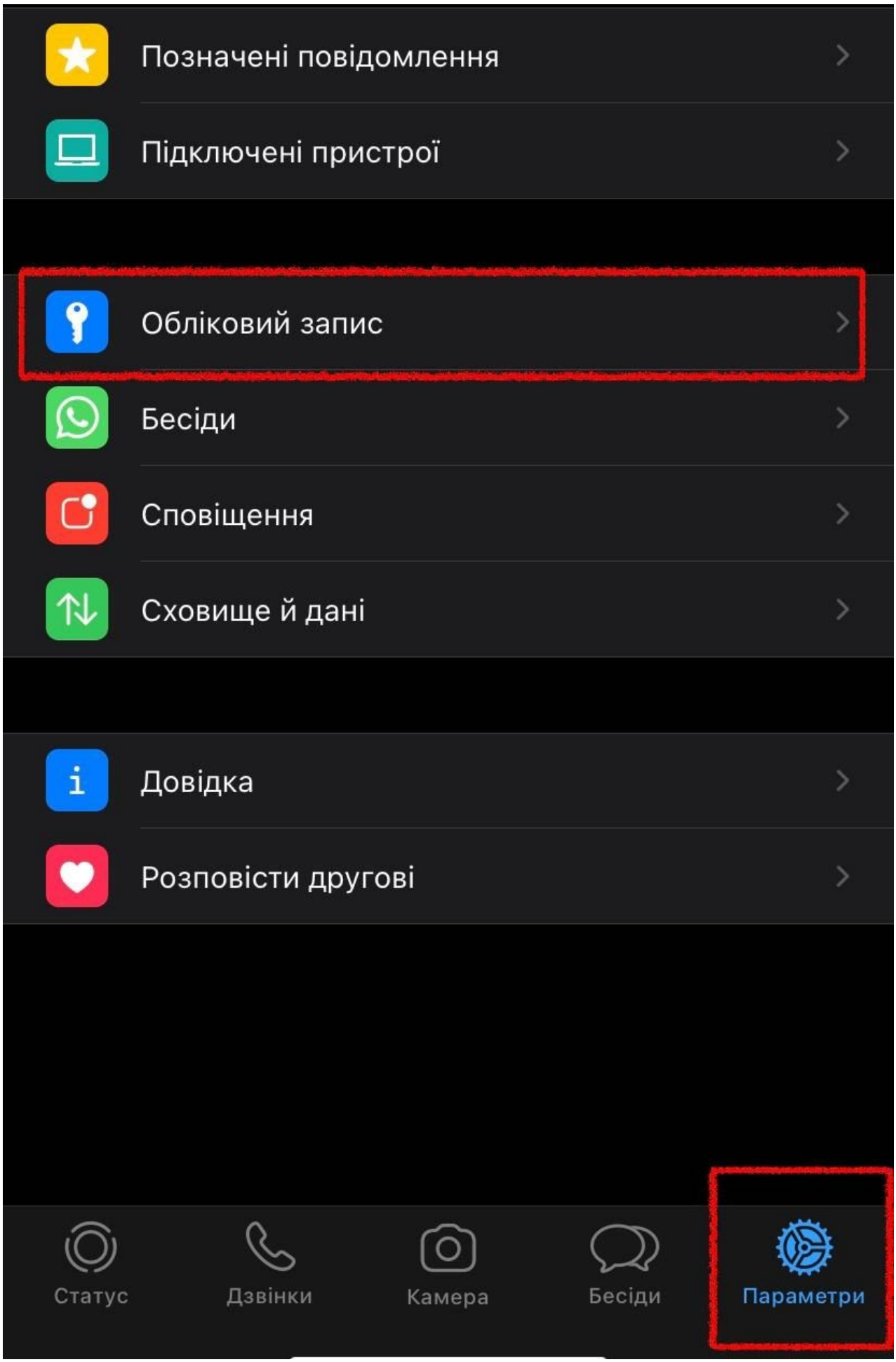
«Довірені контакти», «Показувати ваше фото», «Поширити дату народження» та «Одноранговий зв'язок» виключаємо, а «Запити» та «Автоматичну перевірку на спам» включаємо.

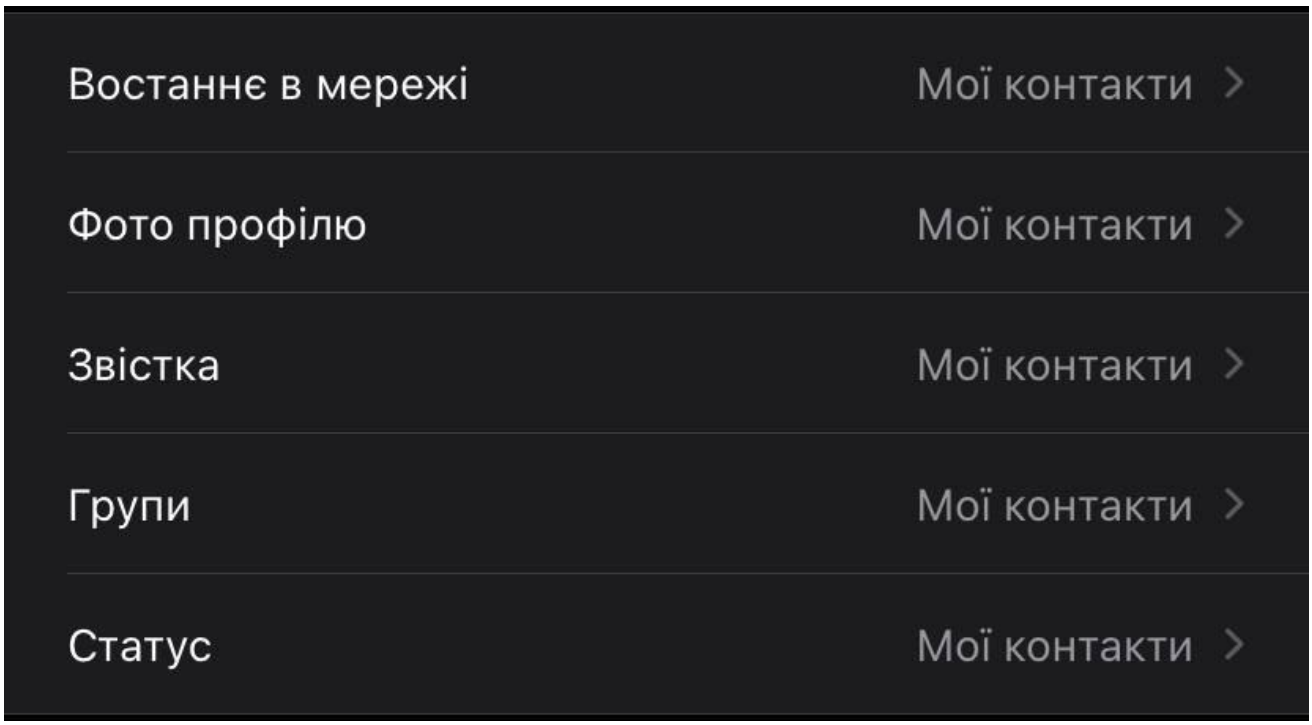
Також в меню «Особисті дані» даємо заборону на «Збір аналітики», «Персоналізацію контенту» та «Служби точної геолокації».

## WHATSAPP

Параметри безпеки «Вотсапу» мало чим відрізняються від тих, що є у «Вайбері» чи «Телеграмі», однак, і їх в обов'язковому порядку необхідно ретельно перевіряти.

Переходимо в «Параметри», «Обліковий запис», «Конфіденційність».


Позначені повідомлення
Підключені пристрої
Обліковий запис
Бесіди
Сповіщення
Сховище й дані
Довідка
Розповісти другові
Статус
Дзвінки
Камера
Бесіди
Параметри




Останній статус в мережі, фото профілю, звістку, додавання до груп та загальний статус робимо доступними лише для ваших контактів.

Інші налаштування в цьому додатку є опціональними. Ви можете змінити їх за бажанням, наприклад, встановити блокування додатку за допомогою Face ID або Touch ID так коду-паролю.

**ІНШІ ЗАСОБИ БЕЗПЕКИ**

Окрім безпеки ваших месенджерів варто не забувати про важливість захищатися від інших зовнішніх факторів. Для цього ми зібрали декілька застосунків, які точно допоможуть будь-якому користувачу.

**GetContact —** додаток**,** який допоможе автоматично визначати абонента, який Вам телефонує і допоможе уберегтися від шахраїв та інших зловмисників. Також надає можливість перевіряти, як підписана людина у інших користувачів. Це корисно тоді, коли ви торгуєте із незнайомцями на маркетплейсах (наприклад, OLX або Prom.ua), влаштовуєтесь на роботу тощо.

Посилання App Store та Google Play

**Psiphon —** безкоштовний VPN-додаток із необмеженим трафіком. Надає можливість безпечно відвідувати сайти, а також надає доступ до тих сайтів, діяльність яких обмежена на території Вашої держави.

Посилання App Store та Google Play

**TunnelBear** — ще один чудовий VPN-сервіс. За повне використання додатку потрібно платити, але для українців компанія безкоштовно дарує 100 гігабайтів захищеного трафіку, що дуже і дуже багато для звичайного користувача.

Посилання App Store та Google Play

**Телеграм-бот @info_baza** — корисний додаток для пошуку інформації про людину по фото. З початком активного вторгнення рф на територію України в ньому стала безкоштовною функція пошуку людини по фото. Дуже комфортно для пошуку диверсантів або шахраїв у соціальних мережах.

Пам’ятайте, що війна — це не тільки коли «стріляють». Війна також відбувається на інформаційному та цифровому фронті. І кожен з нас повинен бути завжди готовим. До речі, Міністерство цифрової трансформації нещодавно звітувало українцям про новинки на цифровому фронті.