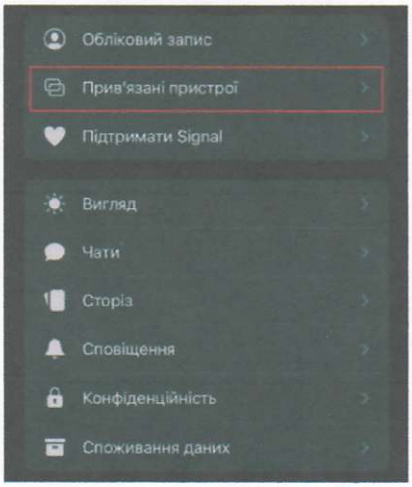
СИТУАЦІЙНИЙ ЦЕНТР ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ
СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ОБЛІКОВИХ ЗАПИСІВ В МЕСЕНДЖЕРАХ ТА СОЦІАЛЬНИХ МЕРЕЖАХ

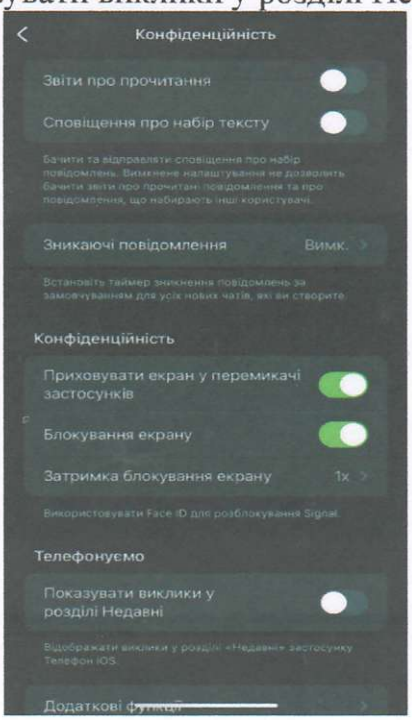
Київ 2024

1. Месенджер Signal

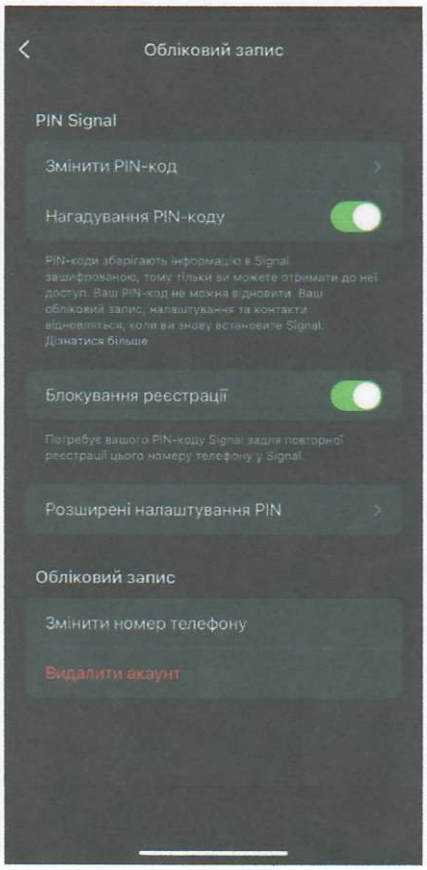
Рекомендуємо періодично перевіряти інші активні сесії Вашого Signal-акаунту та закривати підозрілі чи невідомі. Перевірити Ви можете натиснувши на піктограму акаунту та перейшовши в пункт "Прив'язані пристрої".



Також, в меню "Конфіденційність" увімкніть пункти "Приховувати екран в перемикачі застосунків", "Блокування екрану" та встановіть затримку на блокування екрану на 1хв. Крім того, для користувачів iOS рекомендується вимкнути пункт "Показувати виклики у розділі Недавні".



В пункті меню "Обліковий запис" увімкніть пункт "Блокування реєстрації" для унеможливлення використання Вашого номеру для повторної реєстрації акаунту в Signal та доступу до Ваших повідомлень.



При отриманні повідомлення від невідомого номеру з файлом чи посиланням наполегливо рекомендуємо не відкривати файли, не зберігати їх на пристрій та не переходити за підозрілими посиланнями.

2. Месенджер WhatsApp

Для безпечного користування WhatsApp налаштуйте двохфакторну автентифікацію. Для цього перейдіть в "Параметри" та меню "Обліковий запис". Там при переході в меню "Двоетапна перевірка" керуючись підказками застосунку налаштуйте двофакторну автентифікацію (необхідно буде вказати шестизначний пароль та електронну пошту).

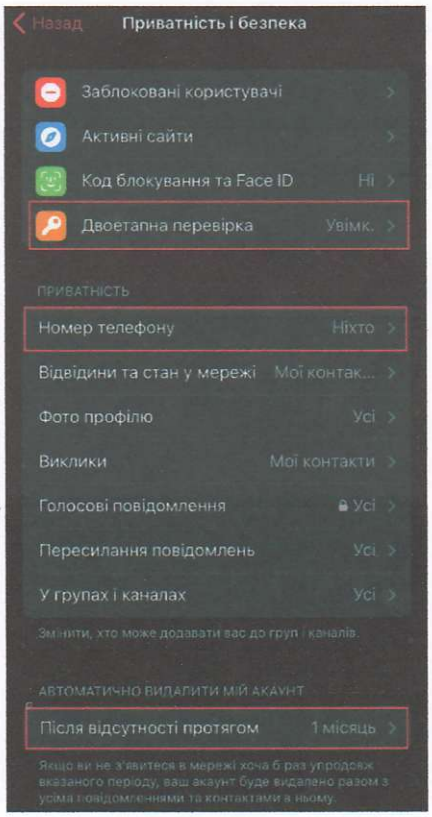
Крім того, періодично перевіряйте пристрої, на яких авторизовано Ваш акаунт WhatsApp в меню "Підключені пристрої", а також в меню "Обліковий запис" перейшовши в пункт "Безпека" увімкніть функцію "Показувати сповіщення системи безпеки".

При отриманні повідомлення від невідомого номеру з файлом чи посиланням наполегливо рекомендуємо не відкривати файли, не зберігати їх на пристрій та не переходити за підозрілими посиланнями.

3. Месенджер Telegram

В даному месенджері також варто налаштувати двохфакторну автентифікацію. Для цього перейдіть до "Параметри", та в меню "Приватність і безпека" оберіть "Двоетапна перевірка". Буде запропоновано встановити пароль та електронну пошту для його відновлення. Встановлюйте складний пароль (більше 8 символів, великі та малі літери, символи, цифри) та не використовуйте пароль, який Ви вже використовуєте в іншому месенджері, соц. мережі чи електронній пошті.

Також в цьому ж меню встановіть, щоб Ваш номер телефону не відображався нікому, а також автоматичне видалення акаунту після 1 місяцю відсутності.



Періодично перевіряйте меню "Пристрої" на наявність невідомих Вам пристроїв з яких авторизований Ваш акаунт. Також рекомендується в меню

"Дані та сховища" вимкнути автозавантаження медіа як через мобільну мережу, так і через Wi-Fi.

При отриманні повідомлення від невідомого номеру з файлом чи посиланням наполегливо рекомендуємо не відкривати файли, не зберігати їх на пристрій та не переходити за підозрілими посиланнями.

4. Соціальна мережа Instagram

Для кожного облікового запису рекомендується налаштувати двохфакторну автентифікацію. Для цього відкрийте застосунок, перейдіть у "Налаштування" та відкрийте пункт "Безпека". Натиснувши на пункт "Перевірка безпеки" Ви отримаєте рекомендації від Instagram щодо підвищення рівня захищеності вашого акаунту, зокрема можуть бути рекомендації по зміні пароля на більш надійний, підтвердження електронної пошти, мобільного телефону та встановлення двофакторної автентифікації. Встановити "Двоетапну перевірку" можна шляхом окремого додатку для автентифікації, текстового повідомлення на номер телефону чи за допомогою WhatsApp (попередньо увімкнувши отримання повідомлення за номером).

Також в меню "Безпека" перейдіть до пункту "Входи в обліковий запис" та перевірте чи не було авторизації до Вашого акаунту з невідомого Вам пристрою. У разі виявлення подібного одразу закрийте інший сеанс.

Рекомендується періодично змінювати пароль до облікового запису, встановлюючи складний пароль, що не використовується в інших соц. мережах, месенджерах чи електронних поштах, а також не відкривати можливі посилання, що можуть надійти в особистих повідомленнях або написані в коментарі до посту.

5. Соціальна мережа Facebook

Захист Вашого акаунту Facebook також залежить від правильних налаштувань. Для цього відкрийте застосунок, перейдіть до "Меню", прогортайте до низу і оберіть пункт "Налаштування" після чого відкрийте "Пароль і безпека". В цьому меню Ви можете перевірити важливі налаштування безпеки за рекомендаціями Facebook, а також змінити пароль, що варто робити періодично і встановлювати унікальні та складні паролі. Також варто налаштувати двоетапну перевірку, для цього натисніть "Використання двоетапної перевірки" та керуючись рекомендаціями Facebook оберіть зручний для Вас метод двофакторної автентифікації.

Після налаштування поверніться до попереднього меню "Пароль і безпека", перевірте з яких пристроїв Ви авторизовані до акаунту в пункті "Авторизовані входи", а також відкривши меню "Отримувати сповіщення про підозрілі входи" увімкніть сповіщення на пошті та у додатку.

Не відкривайте та не зберігайте вкладені файли у підозрілі повідомлення отримані у Messenger Facebook, а також не переходьте за посиланнями, отриманими в повідомленнях чи написаних в коментарі до посту. Періодично перевіряйте активні пристрої як описано вище.

6. Соціальна мережа Twitter

Задля підвищення безпеки Вашого облікового запису(-ів) у соціальній мережі Twitter відкрийте застосунок, натиснувши на піктограму профілю відкрийте меню "Налаштування та конфіденційність" та оберіть "Безпека та доступ до профілю". В цьому меню натиснувши на пункт "Безпека" налаштуйте двофакторну автентифікацію за допомогою текстового повідомлення на мобільний телефон, додатку для автентифікації або ключа безпеки. Також рекомендується увімкнути функцію "Захист від скидання пароля" в меню "Безпека" для унеможливлення зміни пароля без Вашого підтвердження.

Перейдіть до меню "Безпека й доступ до профілю" та в пункті "Додатки та сеанси" перевірте наявні інші несанкціоновані сеанси, підключені застосунки а також авторизовані пристрої.

Періодично змінюйте пароль, для цього в меню "Налаштування та конфіденційність" та оберіть "Ваш профіль" та пункт "Змініть свій пароль". Не переходьте за посиланнями, які можете отримати в особистих повідомленнях або в коментарях до твіту.

Ситуаційний центр забезпечення
кібербезпеки СБУ