

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

щодо використання месенджерів: як убезпечити свої дані

Технічна безпека в умовах воєнного стану — це особистий обов'язок кожного. В той момент, коли військові захищають нас на воєнному фронті, захист особистих даних кожен з нас повинен забезпечити самостійно.

Витоки даних відбуваються постійно, і не всі розуміють важливість конфіденційності. Багато витоків даних відбувається через програми обміну повідомленнями, оскільки багато з них мають уразливі місця.

Ми зібрали кілька найефективніших порад щодо безпеки, які допоможуть захистити ваш месенджер.

1. Налаштуйте конфіденційність облікового запису.

Налаштуйте «конфіденційність», щоб контролювати, хто може бачити вашу фотографію профілю і хто може додавати вас до груп;

В розділі «Приватність і безпека» або «Конфіденційність» змініть налаштування, як вказано нижче:

- Помер телефону —> Хто може бачити номер телефону - Ніхто
- Номер телефону —> Хто може знайти за номером - Мої контакти
- Остання активність —> Хто може бачити час моєї останньої активності - Ніхто
- Фотографії профілю —> Хто може бачити фото та відео мого профілю - Мої контакти
- Дзвінки —> Хто може мені телефонувати - Мої контакти (або Ніхто, якщо хочете).
- Дзвінки —> Peer-to-peer - Мої контакти (або Ніхто, якщо ви волієте не повідомляти свою IP-адресу абонентам, що викликають).
- Пересилання повідомлень —> Хто може додавати посилання на мій обліковий запис під час надсилання моїх повідомлень - Мої контакти.

2. Налаштуйте захист облікового запису:

- Одним із найефективніших заходів безпеки є використання надійних паролів
- Пароль слід використовувати лише один раз та не використовуватися в іншому місці.
- Намагайтесь часто змінювати паролі.
- Довжина пароля повинна складатися з семи або більше символів. Чим довший пароль, тим він надійніший.

Використовуйте цифри, літери та спеціальні символи. Це робить пароль складним і його важко зламати.

- Не зберігайте паролі у своїх браузерях. Крім того, не варто дозволяти месенджеру запам'ятовувати ваш пароль.

- Увімкніть Автоблокування Телеграм на 1 хвилину чи 5 хвилин
- Увімкніть двофакторну автентифікацію для свого облікового запису
- Для безпеки IP-адреси використовуйте сервіси VPN.

3. Захистіть себе під час використання месенджерів

- Діліться конфіденційною (особистою) інформацією лише з тими, кому ви довіряєте. Перевіряйте, чи є людина, з якою ви розмовляєте, тим, за кого вона себе видає, зателефонувавши або передавши голосове повідомлення;

- Використовуйте «зникаючі повідомлення» або «одноразовий перегляд»
- Ніколи й нікому не давайте коди підтвердження SMS — навіть якщо ви знаєте цих людей.

- Активуйте двофакторну автентифікацію, щоб додатково захистити свій обліковий запис. Це означає, що вхід в месенджер прив'язаний до номеру телефону та/або до електронної пошти, а не тільки до паролю (який, як ви вже знаєте, має бути складнішим,

ніж дата народження).

- Двічі перевіряйте точність повідомлень, що пересилаєте;
- Не відкривайте лінки чи файли, які ви отримуєте від людей, яких не знаєте.
- Якщо повідомлення надійшло від знайомих, проте виглядає підозріло, не має супровідного тексту - не поспішайте відкривати вкладення. Це може бути автоматичне завантаження вірусних програм на ваш телефон або ж акаунт вашого знайомого могли зламати.

- Скаржтеся на будь-які контакти, які здаються шахрайськими або розсилають погрози або інші небезпечні повідомлення.

- Для того, щоб незнайомі користувачі не змогли додавати вас у сторонні чати месенджеру, зайдіть у налаштування конфіденційності застосунку і поставте галочку «Мої контакти» розділі «Хто може додавати вас у групи». У розділі «Особисті дані» с налаштування визначення точного розташування, а також збору даних, які можна вимкнути.

- Перегляньте історію чату та членство в групах. Розглядайте можливість очищення історії чату;

- Не забувайте, що месенджери мають доступ до ваших галерей фото та мікрофону, тому якщо ви не використовуєте ці функції постійно, їх краще відключати. Використовуйте месенджер, який зашифрований і не зберігає дані на своїх серверах. Бажано, щоб номер телефону для месенджера не збігався з тим, до якою прив'язана ваша банківська картка.

Не покладайтесь на політики конфіденційності месенджерів.

Постулат, який працює в епоху онлайн: «Якщо ви не хочете, щоб щось стало публічним, не пересилайте цю інформацію навіть приватними повідомленнями».

Рекомендуємо дотримуватись основних правил кібергігієни, опублікованих на сайті CERT-UA (<https://cert.gov.ua/recommendation/31>), зокрема налаштуванням двофакторної аутентифікації на всіх облікових записах.

Під час проведення аудіо- та відеоконференцій слід дотримуватись наступних заходів безпеки:

підготувати середовище для роботи та переконатись, що в полі зору вебкамери не має жодних конфіденційних даних;

увімкнути функцію шифрування аудіо- та відеозв'язку; не поширювати посилання на конференції у відкритому доступі та встановити пароль для входу, який необхідно змінювати для кожної нової сесії; контролювати підключення учасників;

під час спільного використання екрану поширювати лише необхідні дані; налаштувати безпечну передачу файлів, для чутливих даних додатково налаштувати шифрування та парольний захист.

При використанні особистих електронних пристроїв для підключення до відкритих каналів зв'язку, рекомендуємо здійснити наступні налаштування: заборонити автоматичне встановлення додатків з невідомих джерел; обмежити доступ додатків до функціоналу пристрою, в якому немає потреби;

відключити функцію автоматичного підключення до незахищених точок доступу.

Корисно: якщо ви хочете повідомити якусь важливу інформацію, наприклад, код від під'їзду, то краще запишіть це аудіоповідомленням. Так ви убезпечите себе від того, що інформацію отримають сторонні особи, адже здебільшого, коли зламують чати, шахраї мають доступ до текстових повідомлень.