DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

NCSCC
NATIONAL CYBERSECURITY
COORDINATION CENTER

World Vision
ROMÂNIA

СОЮЗ УКРАЇНЦІВ РУМУНІЇ
Uniunea Ucrainenilor din România

Посібник із відновлення та захисту облікових записів у соціальних мережах

Ризики та загрози

Заходи з протидії

Facebook

Instagram

TikTok

WhatsApp

YouTube

Повідомлення про інциденти

TLP:CLEAR

Ризики та загрози

Облікові записи у соціальних мережах піддаються різним кіберризикам, і користувачі повинні знати про потенційні загрози, щоб захистити свою особисту інформацію та присутність в Інтернеті. Ось деякі поширені кіберризики, пов'язані з обліковими записами в соціальних мережах:

Захоплення облікового запису **(Account Takeover Attack - ATO**): Кібер-зловмисники можуть спробувати отримати несанкціонований доступ до ваших облікових записів у соціальних мережах, використовуючи вкрадені паролі або вразливі місця. Отримавши контроль, вони можуть викрасти ваші особисті дані, розмістити підроблену інформацію чи шкідливий вміст або отримати доступ до конфіденційної інформації.

Фішингові атаки: Фішинг полягає в тому, що обманним шляхом змушують користувачів надати конфіденційну інформацію, таку як дані про автентифікацію, особисті або фінансові дані. Зловмисникам вдається отримати ці дані від користувачів, пропонуючи різні сценарії та схеми, де потерпілу особу спонукають надати дані. Зловмисники використовують методи соціальної інженерії та елементи візуальної ідентичності, які можуть викликати довіру та виглядають легітимними. Прикладом можуть бути сайти-клони, які виглядають схожими на оригінальні, але вони зареєстровані на інших доменах. З користувачами зв'язуються з допомогою електронної пошти, смс повідомлень, соціальних мереж чи онлайн чатів. Повідомлення містять посилання, які можуть завдати шкоди , призначені для перенаправлення потерпілої особи на шахрайські сторінки для входу, контрольовані зловмисниками та призначені для захоплення облікових даних потерпілих осіб.

Розповсюдження шкідливих програм: Кібер-зловмисники можуть використовувати платформи соціальних мереж для розповсюдження шкідливих програм. Це може статися через шкідливі посилання або або вкладень в повідомленнях чи постах. Переходячи за цими посиланнями можна встановити зловмисне програмне забезпечення на вашому пристрої.

Соціальна інженерія: Кібер-зловмисники можуть використовувати методи соціальної інженерії, щоб змусити користувачів розкрити конфіденційну інформацію. Це може включати зловмисників, які використовували дані друзів потерпілої особи , знайомих або довірених осіб, щоб отримати доступ до конфіденційної інформації.

Заходи з протидії

Захист ваших облікових записів у соціальних мережах має важливе значення для збереження вашої особистої інформації та запобігання несанкціонованому доступу. Деякі поради:

Надійні паролі: Створюйте надійні паролі з поєднанням великих і малих літер, цифр і спеціальних символів. Уникайте очевидних паролів, таких як дати народження або прізвища.

Двоетапна аутентифікація (2FA): Увімкніть двоетапну автентифікацію для додаткового рівня безпеки. Це передбачає надання коду, згенерованого на вашому мобільному пристрої або електронної пошти, як додаток до вашого пароля.

Регулярне оновлення паролів: Регулярно змінюйте паролі та уникайте використання однакового паролю для декількох облікових записів. Пароль має бути різним для кожного облікового запису.

Перегляд налаштувань конфіденційності: Регулярно перевіряйте та змінюйте налаштування конфіденційності, щоб контролювати, хто може бачити вашу інформацію, хто може взаємодіяти та мати доступ до ваших даних.

Уникнення підозрілих посилань: Будьте обережні з посиланнями та вкладеннями, отриманими в повідомленнях або електронною поштою. Не переходьте за підозрілими посиланнями або посиланнями з невідомих джерел.

Остерігайтеся спроб фішингу: Слідкуйте за можливими спробами фішингу та ніколи не надавайте особисту інформацію чи дані для входу після отримання підозрілих запитів.

Регулярні оновлення додатків: Переконайтеся, що ваші соціальні мережі та пов'язані з ними додатки оновлені до останньої версії, щоб скористатися найновішими параметрами безпеки.

Перевірка активних сеансів: Відстежуйте активні сеанси та пристрої, підключені до вашого облікового запису в соціальних мережах. Відключіть несанкціоновані сеанси.

Використання VPN: Якщо ви підключаєтеся до своїх облікових записів у соціальних мережах, використовуйте віртуальну приватну мережу (VPN), щоб захистити своє з'єднання.

Уникайте неофіційних додатків: Завантажуйте офіційні додатки з платформ соціальних мереж і уникайте використання неофіційних або сумнівних додатків.

Як відновити обліковий запис Facebook

Якщо ви більше не можете отримати доступ до свого облікового запису Facebook, можливо, хтось змінив ваші дані доступу, і ваш обліковий запис зламано. *Що вам зробити?*

1. Увійдіть на сторінку за адресою https://www.facebook.com/login/identify
2. Введіть електронну адресу, яку ви використали в момент реєстрації, або номер телефону
3. Дотримуйтеся вказівок на екрані, щоб скинути пароль облікового запису

Ви можете попросити допомоги у друга. *Що вам зробити?*

1. Попросіть друга знайти ваш обліковий запис
2. Увійдіть у свій обліковий запис. Праворуч ви побачите три крапки (...)
3. Натисніть на них, і з'явиться меню
4. Виберіть- **Отримати допомогу або повідомити**
5. Тут виберіть один із варіантів та пройдіть усі запропоновані кроки

Підозрілі дії у вашому обліковому записі

Якщо ви бачите у своєму обліковому записі будь-які підозрілі дії, це означає, що його могли зламати і зловмисники мають до нього доступ. *Якщо ви помітили зміни:*

- Ваше ім'я, день народження, адреса електронної пошти або пароль раптово змінюються
- Запити друзів з вашого облікового запису надсилаються людям, яких ви не знаєте
- Повідомлення, які ви не писали, надсилаються з вашого облікового запису
- Пости, які ви не створювали, з'являються у вашій хронології

Якщо ви виявили подібні дії у своєму обліковому записі, але все ще можете отримати доступ до нього, виконайте наведені нижче кроки:

1. Перейдіть у свій профіль Facebook і знайдіть **Налаштування та конфіденційність**, а потім **Налаштування**
2. Натисніть на **Пароль і безпека**, щоб побачити **Змінити пароль**
3. Введіть поточний пароль, а потім введіть новий пароль (мінімум 6 символів, включаючи літери, цифри та спеціальні символи)
4. Краще використовувати більше 10 символів. Гарний приклад пароля: Ял10бл10!3ди7инам0р3 (Я люблю їздити на море)
5. Натисніть **Змінити пароль**

Перевірте, чи не зламано ваш обліковий запис Facebook

Як перевірити, що ваш обліковий запис зламали? Виконайте наступні дії, щоб дізнатися, чи хтось інший увійшов у ваш обліковий запис Facebook:

1. Перейдіть у свій профіль Facebook і знайдіть **Налаштування та конфіденційність**, а потім **Налаштування**
2. Натисніть на **Пароль і безпека**, щоб побачити, **Де ви увійшли**, потім **Подивитися все** (на мобільному пристрої) і перевірте, чи впізнаєте ви пристрої, які відображаються у списку
3. Якщо ви бачите пристрій, який ви не впізнаєте, натисніть на його назву, а потім на **Вибрати пристрої, від яких потрібно відключитися**
4. Позначте пристрої, які потрібно від'єднати, а потім натисніть на **Від'єднати**

Як відновити обліковий запис Instagram

Якщо у вас є сумніви щодо свого облікового запису у Instagram або ви більше не можете увійти до нього, відвідайте офіційну сторінку довідкового центру Instagram (https://www.instagram.com/hacked/), щоб розпочати заходи з відновлення. Щоб ідентифікувати свій обліковий запис Instagram, вам знадобиться ваше **ім'я користувача, номер телефону** або **адресу електронної пошти**.

Перевірте, чи була змінена адреса електронної пошти, пов'язана з обліковим записом

Якщо ви отримали електронний лист від **security@mail.instagram.com** зі сповіщенням про те, що ваша адреса електронної пошти змінилася, ви можете скасувати цю зміну, обравши в повідомленні пункт **Захистити обліковий запис**. Якщо інша інформація була змінена (пароль, ім'я користувача) і ви не можете змінити адресу електронної пошти, буде запропоновано ввести посилання для входу або код безпеки з Instagram.

Надішліть запит на посилання для входу в Instagram

Ви можете надіслати запит на посилання для входу на свою електронну адресу або номер телефону, виконавши наведені нижче дії:

- На екрані входу натисніть **Отримати допомогу** щодо входу
- Введіть ім'я користувача, адресу електронної пошти або номер телефону, пов'язані з вашим обліковим записом, а потім натисніть на опцію **Надіслати посилання для входу**. Якщо у вас немає доступу до імені користувача, адреси електронної пошти чи номера телефону, пов'язаного з вашим обліковим записом, перейдіть на цю сторінку та дотримуйтесь інструкцій на екрані. Завершіть перевірку **captcha**, щоб підтвердити, що ви справжня людина, а потім натисніть **Продовжити**.
- Натисніть на посилання для входу в отриманому електронному або текстовому повідомленні (SMS) і дотримуйтесь інструкцій

Відправте запит на код безпеки або підтримку від Instagram:

Якщо ви не можете відновити обліковий запис за допомогою посилання для входу, ви можете подати запит на допомогу на мобільному пристрої. Переконайтеся, що ви ввели безпечну адресу електронної пошти, доступ до якої маєте лише ви. Після надсилання запиту ви маєте отримати електронний лист від Instagram із інструкціями, які слід виконати. Дізнайтеся більше про те, що ви можете зробити, якщо ви не знаєте свого імені користувача.

Підтвердьте свою особу

Якщо ви подаєте запит на підтримку **облікового запису, який містить ваші фотографії**, вам буде запропоновано записати відеоселфі, на якому ви повертаєте голову в різні боки, щоб підтвердити, що ви справжня людина. Коли ви надішлете відеоселфі, ви отримаєте електронний лист від Instagram на вказану вами електронну адресу. Цей відеоролик буде використано для підтвердження вашої особи.

Якщо ви надіслали запит на підтримку для **облікового запису, який не містить ваших фотографій**, ви маєте отримати автоматичну відповідь електронною поштою від команди підтримки Meta. Вам потрібно буде вказати адресу електронної пошти або номер телефону, за допомогою якого ви зареєструвалися, і інформацію щодо пристрою, який ви використовували під час реєстрації.

Якщо ви все ще маєте можливість ввійти у свій обліковий запис Instagram:

Якщо ваш обліковий запис зламано, але ви все ще маєте можливість в нього ввійти, ось що ви можете зробити, щоб захистити свій обліковий запис:

- Переконайтеся, що номер телефону та адреса електронної пошти в налаштуваннях вашого облікового запису правильні
- Змініть свій пароль або надішліть електронний лист для зміни пароля
- Увімкніть двофакторну автентифікацію для додаткової безпеки
- Перейдіть до «Керування обліковими записами» та видаліть пов'язані облікові записи, які ви не впізнаєте

- Скасуйте доступ до будь-яких підозрілих або сторонніх додатків

Як відновити обліковий запис TikTok

Якщо ви помітили будь-яку з наступних підозрілих дій, ваш обліковий запис, швидше за все, було зламано:

- Ваш пароль або номер телефону було змінено
- Ім'я користувача або псевдонім вашого облікового запису було змінено
- Відеоролики були видалені або опубліковані без вашого дозволу
- Повідомлення, які ви не писали, були надіслані з вашого облікового запису

Ви повинні повідомити про інцидент:

1. Натисніть на **Профіль** внизу праворуч
2. Натисніть на **піктограми з 3 лініями** у верхньому правому куті
3. Натисніть на **Налаштування та конфіденційність**
4. Натисніть на **Повідомити про проблему**
5. Виберіть тему для повідомлення

Ви також можете виконати наведені нижче дії, щоб захистити свій обліковий запис.

Зміна пароля

- Якщо ви вважаєте, що ваш обліковий запис зламано, якнайшвидше змініть пароль. Виберіть пароль, який запам'ятається вам, але іншим користувачам важко вгадати.
- Дізнайтеся, як скинути пароль TikTok

Увімкніть двоетапну перевірку

- Двоетапна перевірка додає додатковий рівень безпеки до вашого облікового запису на випадок, якщо ваш пароль зламано. Це також допомагає захистити ваш обліковий запис від нерозпізнаних/неавторизованих пристроїв або програм сторонніх розробників. Дізнайтеся, як увімкнути двоетапну перевірку

Перевірте пристрої, до яких ви підключені

- Ви можете переглядати усі інші мобільні пристрої, які зараз використовують або нещодавно отримували доступ до вашого облікового запису TikTok. Дізнайтеся, як отримати доступ до підключених пристроїв

Перевірте наявність сповіщень безпеки

- Щоб переглянути сповіщення безпеки, перейдіть до налаштувань програми TikTok, натисніть на **Безпека та вхід**, а потім натисніть на **Сповіщення безпеки**.

Як відновити обліковий запис WhatsApp

Радимо повідомити своїх друзів і родину, якщо ви підозрюєте, що хтось інший використовує ваш обліковий запис WhatsApp, оскільки зловмисники можуть використовувати ідентифікаційні дані, згенеровані цим обліковим записом, у розмовах і групах. Майте на увазі, що WhatsApp повністю зашифрований і повідомлення зберігаються на вашому пристрої, тому, якщо хтось отримає доступ до вашого облікового запису з іншого пристрою, він не зможе прочитати ваші попередні розмови.

Нікому не повідомляйте код підтвердження WhatsApp, отриманий через SMS, навіть друзям чи членам родини! Без цього коду будь-який користувач, який намагається підтвердити ваш номер, не зможе завершити процес підтвердження та не зможе використовувати ваш номер телефону в WhatsApp.

Якщо хтось шахрайським шляхом отримав ваш код і ви втратили доступ до свого облікового запису WhatsApp, виконайте наведені нижче інструкції, щоб відновити його.

- Увійдіть у WhatsApp за допомогою свого номера телефону, а потім підтвердьте свій номер, використовуючи 6-значний код, який ви отримаєте через SMS
- Після введення 6-значного коду, отриманого через SMS, **особа, яка використовує ваш обліковий запис, буде автоматично відключена**
- Вас також можуть попросити ввести код для двоетапної перевірки. Якщо ви не знаєте цей код, можливо, особа, яка використовувала ваш обліковий запис, увімкнула двоетапну перевірку
- Вам потрібно **зачекати 7 днів**, перш ніж ви зможете увійти без **коду двоетапної перевірки**. Незалежно від того, знаєте ви цей код підтвердження чи ні, особу, яка використовувала ваш обліковий запис, буде відключено в момент, коли ви введете 6-значний код, отриманий через SMS









WhatsApp надає підтримку користувачам, яка доступна на телефоні, у додатку, у розділі **WhatsApp > Налаштування > Довідка > Зв'язатися з нами** або на офіційному веб-сайті програми, у розділі Зв'язатися з нами.

Якщо ваш телефон загублено або вкрадено, служба підтримки WhatsApp нічого не зможе зробити. Неможливо деактивувати ваш обліковий запис WhatsApp, оскільки неможливо підтвердити, що ви є власником номера телефону, пов'язаного з цим обліковим записом.

Як відновити обліковий запис YouTube

Перш ніж вживати заходів, важливо ще раз перевірити наявність ознак того, що ваш канал зламано. Кожен канал YouTube пов'язаний принаймні з одним обліковим записом Google. Коли канал YouTube зламано, це означає, що принаймні один із облікових записів Google, пов'язаних із каналом, також зламано.

Якщо ви помітили будь-яку з наведених нижче дій у своєму обліковому записі Google, можливо, ваш обліковий запис Google було зламано або скомпрометовано:

- Зміни, які ви не вносили: фотографія профілю, описи, налаштування електронної пошти, зв'язок облікового запису AdSense або надіслані повідомлення відрізняються
- Завантажені відеоролики, які вам не належать: хтось опублікував відеоролики з вашого облікового запису Google. Ви можете отримувати сповіщення електронною поштою про ці відеоролики щодо штрафів або попереджень за неприйнятний вміст

Щоб відновити зламаний канал YouTube, спершу потрібно відновити зламаний обліковий запис Google, пов'язаний із каналом YouTube. Три кроки для відновлення каналу YouTube:

1. Відновіть і захистіть зламаний обліковий запис Google, пов'язаний із каналом YouTube
2. Негайно треба видалити е небажані зміни у своєму каналі YouTube, щоб уникнути наслідків політики, таких як правила спільноти чи попередження щодо авторських прав
3. Зменшіть ризик несанкціонованого доступу до вашого облікового запису Google, використовуючи найкращі методи безпеки для всіх пов'язаних користувачів каналу

Відновіть обліковий запис Google

Якщо ви все ще можете ввійти у свій обліковий запис Google, важливо оновити пароль і захистити свій обліковий запис Google. Якщо ви не можете ввійти у свій обліковий запис Google:

1. Дотримуйтеся вказівок, щоб відновити обліковий запис Google або Gmail. Вам буде запропоновано декілька запитань, щоб підтвердити, що це ваш обліковий запис, і надати правильні відповіді . Якщо у вас виникли проблеми, дотримуйтесь порад, щоб завершити кроки відновлення облікового запису
2. Скиньте свій пароль, коли буде запитано. Виберіть надійний пароль, який ви раніше не використовували для цього облікового запису. Дізнайтеся, як створити надійний пароль
3. Попросіть менеджерів/власників каналів виконати ті самі дії, щоб захистити свій обліковий запис Google

Повідомлення про інциденти

Повідомити можна за допомогою онлайн-форми на веб-сайті www.dnsc.ro, alerts@dnsc.ro або зателефонувавши за номером 1911, який є унікальним національним номером екстреної служби, призначеним для повідомлення про інциденти кібербезпеки.

- Якщо ви отримали **підозрілий електронний лист**, надішліть його на alerts@dnsc.ro або зателефонуйте за номером 1911
- Якщо ви отримали підозріле текстове повідомлення, повідомте про це через онлайн-форму на веб-сайті www.dnsc.ro, надішліть його на alerts@dnsc.ro або зателефонуйте за номером 1911
- Якщо ви отримали підозрілі телефонні дзвінки, покладіть слухавку, заблокуйте користувача та зверніться до свого оператора зв'язку.
- У разі отримання підозрілого повідомлення на Вашу електронну пошту (робочу або особисту у соціальних мережах або месенджерах у телефонах):
- Інформуйте безпосереднього керівника за фактом;
- Для вжиття заходів реагування повідомте про кіберінцидент Урядову команду реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України (CERT.UA) :
- E-mail: incidents@cert.gov.ua
- Пн - Чт: 8:00 - 17:00, Пт: 8:00 - 15:45:
- Тел..: +38 (044) 281-88-25
- Тел.: +38 (044) 281-88-05
- Вихідні та святкові дні (цілодобово):
- Тел.: +38 (044) 281-88-01
- Або скористайтеся формою «Повідомте нас про кіберінцидент» на сайті CERT.UA :
- https://cert.gov.ua/recommendations/21
- Про злочинні схеми в кіберпросторі, злочинців, у разі виявлення випадків шахрайства в тому числі фінансового, у кіберпросторі повідомляйте Департамент кіберполіції Національної поліції України:
- Тел..: 0800-505-170
- E-mail: callcenter@cyberpolice.gov.ua
- https://cyberpolice.gov.ua
- Про загрози національній безпеці України в мережі Інтернет, зокрема спроби та фатки кіберрозвідки інших держав, кібертероризму та кібершпигунства, кіберінциденти в органах державної влади України – інформуйте Ситуаційний Центр забезпечення кібербезпеки Служби безпеки України (СБУ):
- incident@dis.gov.ua
- cyber_security@dis.gov.ua
- Або скористайтеся сайтом:
- https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

Цей посібник був розроблений та підготовлений експертами Національного управління кібербезпеки: **Міхаєм Ротаріу, Даніелєм Аботезатоей, Даном Андріеш, Міхаелою Дан, Іриною Немояну, Крістіаном Ністор**

У перекладі посібника на українську мову допомогли співробітники World Vision Румунія, **Василій Гуцу та Наталія Лебідь.**