

## Безпека користування соціальними мережами

### План лекції

Вступ

1. Правила реєстрації
2. Правила парольної безпеки
3. Конфіденційність даних

Висновки

### Рекомендована література

#### Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.

#### Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.

### Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

## Текст лекції

### Вступ

Соціальні мережі, такі як Facebook, LinkedIn, Instagram, TikTok або Snapchat, дозволяють вам ділитися особистою інформацією, спілкуючись з друзями, партнерами і колегами по всьому світу. Хоча мережі дозволяють вам залишатися на зв'язку, ви наражаєтеся на ризик того, що зловмисники можуть дізнатися, де ви, що ви робите, чим ви володієте, а також іншу інформацію.

Безпека і соціальні мережі – речі, на перший погляд, якщо не протилежні, то точно ледь сумісні. Реєструючись у соціальній мережі, користувачі, за рідкісними винятками, не дотримуються анонімності. Ми ділимося фотографіями, уподобаннями в музиці, підписками на сторінки – все це є елементами «профайлу», за якими нас знайдуть друзі й знайомі ... і маркетологи. А отже, всю цю інформацію можна продати.

Проблема в тому, що багато власників сервісів за гроші нададуть не лише інформацію про товари, які ви шукали онлайн, а і більшість особистих даних. Так що інформацію, яку ви не готові афішувати на весь світ, не можна завантажувати в соціальні мережі зовсім: ані в закриті альбоми, ані в особисті повідомлення – нікуди.

У березні 2018 року стало відомо, що британська аналітична компанія «Cambridge Analytica» збирала дані користувачів через свій додаток у Facebook і використовувала для розміщення політичної реклами, зокрема під час президентської кампанії в США і референдуму про вихід Великобританії з Євросоюзу в 2016 році. Втручання в цілому могло торкнутися 87 млн користувачів соцмережі. «Cambridge Analytica» заперечувала свою провину, стверджуючи, що це був звичайний і законний збір даних для онлайн-реклами. Потім компанія втратила всіх клієнтів і оголосила про банкрутство. Засновник соцмережі Марк Цукерберг визнав помилку, зазначивши, що у Facebook зробили недостатньо для запобігання використанню її функціоналу на шкоду. Facebook було оштрафовано більш ніж на 5 млрд дол. США.

Тож далі розглянемо, як варто поводитися онлайн у соціальних мережах, щоб не стати або жертвою зловмисників, або «елементом статистики».

### 1. Правила реєстрації

Ви хочете використовувати своє справжнє ім'я? Деякі мережі раніше дотримувалися «політики справжніх імен», але з часом послабили вимоги. Якщо вам не хочеться використовувати своє справжнє ім'я в соціальних мережах, можете цього не робити.



Під час реєстрації не надавайте більше інформації, ніж потрібно. Якщо ви хочете зберегти свої контактні дані, використовуйте окрему, спеціально створену адресу електронної пошти і не вказуйте свій номер телефону. Основна адреса пошти і номер телефону можуть розкрити вашу особистість і зв'язати вас з іншими обліковими записами.

Будьте обережні, вибираючи фото профілю або інші зображення, які ви завантажуєте. Мало того, що в метаданих файлу може бути вказане місце і час зйомки, власне зображення може також розкрити будь-яку інформацію про вас. Поставте собі питання перед завантаженням зображення: фото було знято поза межами дому або роботи? Чи видно покажчики з назвою вулиць або інші знаки і вивіски? Чи не видно робочих документів або змісту екрану комп'ютера?

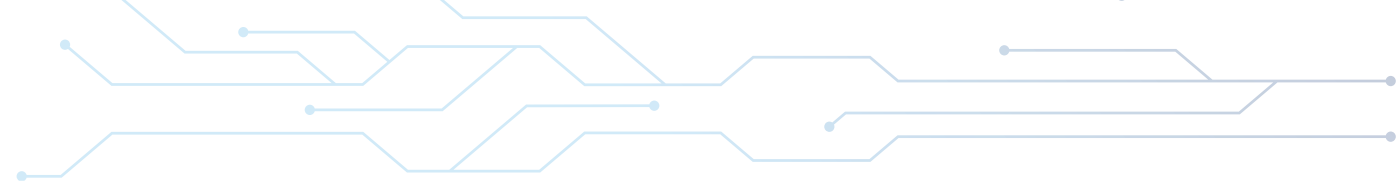
Не слід правильно відповідати на питання для відновлення доступу до облікового запису («В якому місті ви народилися?» або «Яке ім'я вашої домашньої тварини?»), оскільки відповіді на такі питання можуть бути знайдені за допомогою загальнодоступних даних ваших акаунтів у соціальних мережах. Ви можете вказати довільні відповіді на ці питання. Запам'ятати ці відповіді буде важкувато, тому їх можна записати в окремому місці або зберігати за допомогою менеджера паролів.

## 2. Правила парольної безпеки

Захистіть ваш обліковий запис надійним паролем. Надійні паролі довгі, складні та унікальні. Це означає, що вони повинні бути довше 10–16 символів, містити різні типи символів (великі й маленькі літери, цифри, спеціальні символи) та бути різними для кожного облікового запису та системи. Паролі не повинні бути засновані на простих словах, які можна знайти в словниках. Паролі не повинні бути когнітивними – це означає, що вони не повинні бути засновані на даних про вас, що їх можна знайти у вашому ж обліковому записі! Дату народження, ім'я близької людини, кличку собаки та іншу доступну інформацію не варто використовувати як складові паролю. Краще використовуйте парольні фрази, щоб уникнути проблем зі слабкими паролями.

Оберіть фразу, яку ви не зможете легко забути в наступні 2–3 дні: рядок з вірша або пісні, прислів'я, гасло тощо. Потім трансформуйте цю фразу у єдине «слово», видаливши пробіли та замінивши деякі літери схожими на них цифрами або спецсимволами: А->4, В->8, С->3, Е->3, І->1, L->7, S->5, T->7 тощо. Додавання цифр та спецсимволів, а також переведення деяких букв у верхній регістр зроблять парольну фразу ще сильнішою.

Ніхто, крім вас, не повинен знати ваші паролі та парольні фрази. Не розказуйте їх нікому, навіть дружині, батькам, дітям. Ніколи не записуйте ваші паролі



та паролні фрази на папері або в незашифрованому файлі. Захищений паролем файл Excel – це не шифрування. Архів, захищений паролем, не є належним шифруванням. Використовуйте надійні паролні менеджери.

Прикладами надійних паролних менеджерів є:

- ▶ 1Password: <https://1password.com> (платний);
- ▶ Bitwarden: <https://bitwarden.com> (безкоштовний);
- ▶ Dashlane: <https://www.dashlane.com/> (безкоштовний з обмеженнями);
- ▶ KeePassXC: <https://keepassxc.org/> (безкоштовний).

Змінюйте паролі та паролні фрази на регулярній основі та принаймні один раз на рік. Паролі та паролні фрази, які ви використовуєте найчастіше (наприклад, кілька разів на день), повинні змінюватися принаймні щомісячно або раз на два місяці.

### 3. Конфіденційність даних

Інформація, що зберігається третьою стороною, захищена її власною політикою конфіденційності й може бути використана в комерційних цілях та навіть передана іншим компаніям (наприклад, маркетинговим). Оскільки читання всієї політики конфіденційності – майже непосильне завдання для будь-якої людини, спробуйте ознайомитися лише з розділом, у якому йдеться про те, як використовуються ваші дані, в яких випадках дані можуть бути передані кому-небудь ще, а також як компанія реагує на запити правоохоронних органів.

Сайти соціальних мереж – це, в основному, бізнес, зосереджений на отриманні прибутку. Вони часто збирають конфіденційну інформацію, крім наданої вами: де ви перебуваєте, які ваші інтереси і переваги, на яку рекламу ви реагуєте, які сайти ви відвідуєте (за допомогою кнопок «Like»). Ви можете використати розширення (плагін) браузера з блокуванням стеження для запобігання пасивної передачі зайвої інформації стороннім сайтам.

Головна порада: змініть налаштування за замовчуванням. Наприклад, чи хочете ви ділитися своїми публікаціями з усіма або тільки з будь-якою конкретною групою людей? Чи можна дозволити людям шукати вас за номером телефону або адресою електронної пошти? Чи хочете ви публікувати своє місце розташування в автоматичному режимі?

Незважаючи на те, що на кожній платформі соціальних мереж є свої унікальні налаштування, ви можете помітити деяку схожість.

Налаштування конфіденційності надають відповідь на питання: «Хто може це бачити?» Тут ви зможете вибрати аудиторію («Всі», «Друзі друзів», «Тільки



друзі» тощо) для своїх публікацій, розташування, фотографій, контактної інформації, міток і тих, хто може знайти ваш профіль через пошук.

Налаштування безпеки будуть пов'язані з можливістю блокування інших облікових записів і способів оповіщення про спроби неавторизованого доступу до вашого профілю. Іноді в цьому розділі будуть присутні налаштування входу до акаунту: наприклад, включення двофакторної автентифікації та резервна адреса електронної пошти/номер телефону.

Скористайтеся «перевірками» налаштувань безпеки і конфіденційності. Facebook, Twitter і багато інших веб-сайтів пропонують провести «перевірку налаштувань безпеки» облікового запису. Ці перевірки є чудовими покроковими настановами, описаними простою мовою. Вони дуже добре допомагають вам відповідним чином налаштувати безпеку і конфіденційність свого облікового запису.

Пам'ятайте, що налаштування конфіденційності можуть змінитися. Іноді вони можуть ставати більш надійними і докладними, а іноді – навпаки. Звертайте увагу на ці зміни: раптом інформація, раніше конфіденційна, стала вже відкритою для всіх, або нові додаткові налаштування дозволять краще контролювати рівень вашої конфіденційності?

Ось посилання на налаштування безпеки для найпопулярніших соціальних мереж:

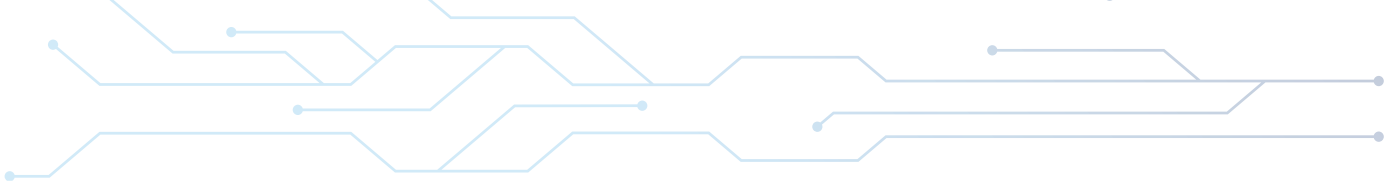
- ▶ Facebook: <https://www.facebook.com/settings?tab=security&section=ap-provals>;
- ▶ Twitter: <https://twitter.com/settings/security>.

Пам'ятайте, що більшість сучасних онлайн-сервісів підтримують двофакторну автентифікацію. Увімкніть її за допомогою програмного коду (доступний у Facebook, Twitter тощо) або за допомогою одноразового паролю з SMS. Надавайте перевагу використанню Google Authenticator, фізичного токена, або перевірці за допомогою мобільного додатку. Використання одноразових кодів через SMS менш безпечно.

Більше інформації про двофакторну автентифікацію тут:  
<https://twofactorauth.org/>.

Не використовуйте сторінку в соціальній мережі для реєстрації на сайтах, які запитують доступ до вашої особистої інформації та інформації про ваших друзів. Багато сайтів зараз пропонують авторизуватися через соцмережі, щоб проголосувати в опитуванні, залишити коментар або дізнатися результати якого-небудь тесту. Побережіть дані, обійдіться без інформації про те, яким є ваш психологічний вік або хто ви з героїв «Гаррі Поттера».





Крім того, не анонсуйте на сторінці свої плани. Інформацією про те, що ви найближчими вихідними збираєтеся в іншу країну, можуть скористатися квартирні крадії.

**Пам'ятайте: все, що ви публікуєте, може бути використано проти вас!**

Чим більше інформації ви публікуєте про своє особисте життя, тим легше зловмиснику підготувати атаку проти вас. Наприклад, якщо ви публікуєте багато інформації про свою родину, захоплення або про майбутню відпустку чи робочу поїздку, зловмисник може зібрати всі ці конкретні дані й створити фішингового електронного листа або зробити телефонний дзвінок, спеціально призначений для вас.

Якщо ви напишете, що серед ваших уподобань є випікання, зловмисник може створити фішинговий лист зі спеціальною рекламою нового набору мисок. До цього електронного листа він може додати вкладення з купоном на 50% знижки на купівлю продукції вашого улюбленого бренду для випікання. **Якщо пропозиція здається занадто гарною, щоб бути правдою, це, ймовірно, шахрайство.**

Крім того, щоб забезпечити безпеку вашого роботодавця, ніколи, з жодної причини не розміщуйте конфіденційну інформацію про вашу роботу в Інтернеті. Завжди звертайте увагу на те, що ви публікуєте і чим ділитесь на своїй сторінці. Слідкуйте за коментарями. Йдеться не тільки про коментарі, які ви залишаєте на інших ресурсах, а й про коментарі, що їх інші залишають на вашій сторінці. Іноді найгіршого удару по онлайн-репутації посадової особи завдають не злами і «зливи» даних, а необдумані жарти, в яких хтось може побачити грубість або необережні висловлювання ваших же друзів.

Як і фішингові атаки електронною поштою, кіберзловмисники можуть спробувати обдурити вас у соціальних мережах. Поширений метод атаки: злочинець отримує доступ до облікового запису в соціальній мережі, наприклад, вашого колеги. Потім він може відправити вам терміновий запит, що його пограбували або він застряг під час відпустки й потрібні гроші, які він просить відправити йому прямо зараз.

Якщо ви отримуєте будь-які дивні або підозрілі повідомлення від колеги, друга або знайомого, дійте обачно і будьте обережні з відповіддю. Не відповідайте безпосередньо через обліковий запис у соціальних мережах. Замість цього зателефонуйте своєму другові по телефону, щоб підтвердити, чи дійсно він опублікував повідомлення і потребує вашої допомоги.

*Закінчення користування*

Чи зможете ви згадати, скільки і в яких соціальних мережах ви створювали облікових записів? А яка частина з них залишаються покинутими через



забутий пароль? Зі зростанням популярності соцмереж кожен такий акаунт може становити інтерес для зловмисників.

Отримавши доступ до покинутого акаунту, можна використовувати його для дискредитації вас, опублікувати рекламну – і не тільки – інформацію.

Щоб уникнути цього, не забувайте про свої старі облікові записи – видаляйте, за можливості, або хоча б блокуйте їх. А якщо не маєте доступу, спробуйте звернутись до служб технічної підтримки по допомогу. Іноді це може спрацювати!

## **Висновки**

І, наостанок, згадайте, що ви – офіційна особа, і навіть якщо обліковий запис ваш особистий, все одно у користувачів буде до нього інше ставлення.