

Розділ 3. Захист даних і конфіденційність

Вступ до кібербезпеки (I2CS)



Мета розділу

Розділ 3. Захист даних і конфіденційність

Мета розділу: пояснити, як захистити себе в Інтернеті.

Назва теми	Мета вивчення теми
Захист ваших пристроїв та мережі	Визначити способи захисту своїх комп'ютерних пристроїв.
Обслуговування даних	Використовувати бездротові мережі безпечно.
Хто володіє вашими даними?	Створення та збереження надійних паролів.
Захист конфіденційності в Інтернеті	Впровадити методи безпечного збереження даних.
Дослідіть ризики своєї поведінки в Інтернеті	Пояснити способи підвищення безпеки онлайн-даних.

3.1. Захист ваших пристроїв та мережі


Захист ваших пристроїв та мережі

Захистіть ваші цифрові пристрої

- Деякі головні поради щодо захисту ваших пристроїв:

Увімкніть міжмережний екран	Ви повинні використовувати принаймні один тип міжмережних екранів (програмний або апаратний на маршрутизаторі), щоб захистити свій пристрій від несанкціонованого доступу. Міжмережний екран слід увімкнути та постійно оновлювати, щоб хакери не змогли отримати доступ до ваших особистих даних або даних організації.
Встановіть антивірусне і анти-шпигунське програмне забезпечення	Шкідливе програмне забезпечення, таке як віруси та шпигунські програми, призначене для отримання несанкціонованого доступу до вашого комп'ютера та ваших даних. Після встановлення віруси можуть знищити ваші дані та сповільнити роботу комп'ютера. Вони навіть можуть заволодіти вашим комп'ютером і розсилати спамові листи за допомогою вашого облікового запису. Шпигунське програмне забезпечення може контролювати ваші дії в Інтернеті, збирати вашу особисту інформацію або відкривати небажані спливаючі вікна з рекламою у вашому веб-браузері під час роботи в Інтернеті. Щоб запобігти цьому, завантажуйте програмне забезпечення лише з надійних веб-сайтів. Однак ви завжди повинні використовувати антивірусне програмне забезпечення, щоб забезпечити інший рівень захисту. Це програмне забезпечення, яке часто містить антишпигунське програмне забезпечення, призначене для сканування комп'ютера та вхідної електронної пошти на наявність вірусів та їх видалення.
Контролюйте вашу операційну систему та браузер	Хакери завжди намагаються скористатися уразливостями в операційній системі та веб-браузерах. Тому щоб убезпечити свій комп'ютер і дані, встановіть середній або високий рівень захисту на вашому комп'ютері та у веб-браузері. Ви повинні регулярно оновлювати операційну систему, веб-браузер, регулярно завантажуйте та встановлюйте останні виправлення програмного забезпечення та оновлення системи безпеки від постачальників ПЗ.
Налаштуйте захист паролем	Усі ваші комп'ютерні пристрої мають бути захищені паролем, щоб запобігти несанкціонованому доступу. Будь-яка збережена інформація, особливо конфіденційні дані, повинна бути зашифрована. Ви повинні зберігати лише необхідну інформацію на своєму мобільному пристрої на випадок його крадіжки або втрати. Якщо будь-який з ваших пристроїв скомпрометовано, злочинці можуть мати доступ до всіх ваших даних через вашого постачальника послуг хмарного сховища, наприклад iCloud або Google Drive.

Безпека бездротової мережі вдома

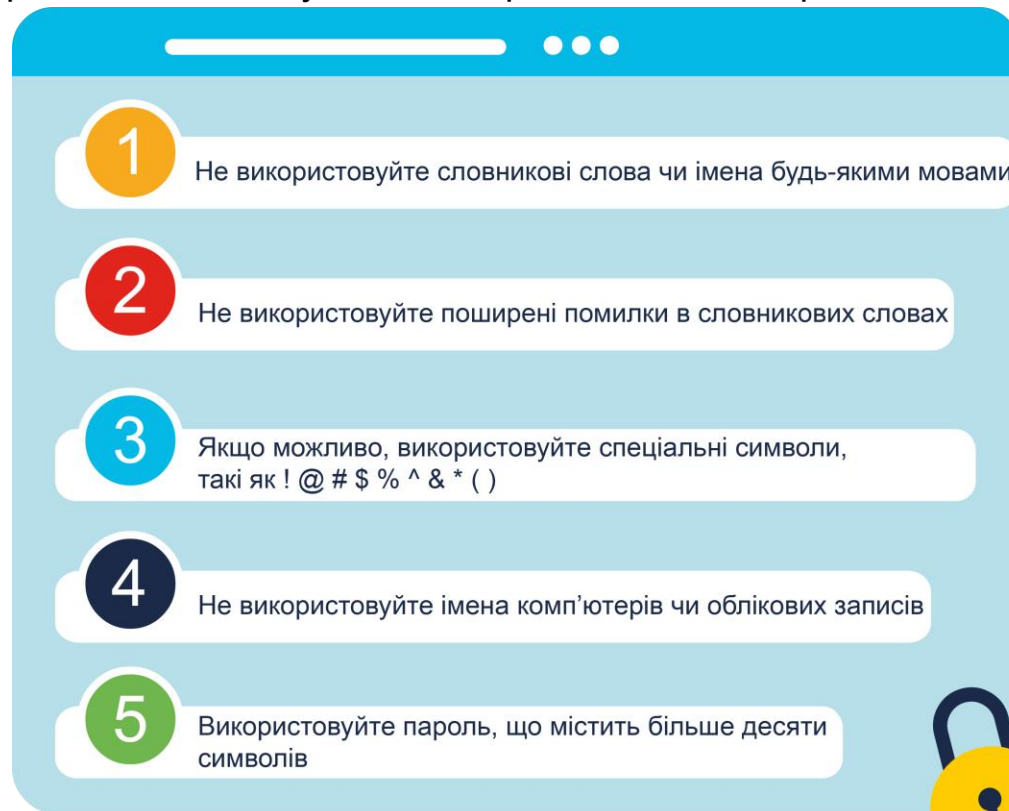
- Бездротові мережі дозволяють пристроям з підтримкою Wi-Fi підключатися до мережі за допомогою SSID.
 - Хоча бездротовий маршрутизатор можна налаштувати так, щоб він не транслював SSID, це не слід вважати достатньою безпекою для бездротової мережі.
 - Хакерам буде відомий попередньо встановлений SSID і пароль за замовчуванням, тому, щоб запобігти проникненню зловмисників у вашу домашню бездротову мережу, вам слід змінити ці дані.
 - Крім того, слід шифрувати бездротове з'єднання, активувавши бездротову безпеку та функцію шифрування WPA2 на вашому бездротовому маршрутизаторі.
 - Але майте на увазі, навіть якщо ввімкнено шифрування WPA2, бездротова мережа все ще може бути вразливою.
 - **Виявлення недоліку безпеки в протоколі WPA2 у 2017 році**
 - Атаки перевстановлення ключа (KRACK) зловмисниками, які порушують шифрування між бездротовим маршрутизатором і бездротовим пристроєм, надаючи їм доступ до мережних даних, можуть використовувати цю вразливість.
 - Цей недолік впливає на всі сучасні захищені мережі Wi-Fi, і щоб пом'якшити цю ситуацію, ви повинні:
 - оновлювати всі бездротові пристрої, такі як маршрутизатори, ноутбуки та мобільні пристрої, щойно стануть доступними оновлення безпеки
 - використовувати дротове підключення для будь-яких пристроїв з дротовою мережною інтерфейсною картою (NIC)
-  використовувати надійну службу віртуальної приватної мережі (VPN) під час доступу до бездротової мережі.

Ризики загально-доступного Wi-Fi

- Коли ви не вдома, публічні точки доступу до Wi-Fi (hot spot) дають змогу отримувати доступ до вашої онлайн-інформації та переглядати Інтернет.
- Однак існують певні ризики, які означають, що краще не отримувати доступ до будь-якої особистої інформації та не надсилати її під час використання загальнодоступного Wi-Fi.
- Завжди перевіряйте, що на вашому пристрої не налаштовано спільний доступ до файлів і медіа, а також що він вимагає автентифікації користувача за допомогою шифрування.
- Ви також повинні використовувати зашифровану службу VPN, щоб не допустити перехоплення вашої інформації іншими особами (відомої як «підслуховування») через загальнодоступну бездротову мережу.
- Ця послуга надає вам безпечний доступ до Інтернету, шифруючи з'єднання між вашим пристроєм і сервером VPN.
- Навіть якщо хакери перехоплять передачу даних у зашифрованому тунелі VPN, вони не зможуть її розшифрувати.

Надійний пароль

- Ось кілька простих порад, які допоможуть вам вибрати надійний пароль.



Використання парольної фрази

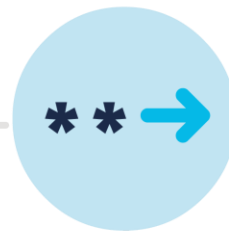
- Для запобігання несанкціонованому доступу до ваших пристроїв було б корисно використовувати парольні фрази замість паролів.
- Парольна фраза зазвичай має форму речення («Acat th@tlov3sd0gs.»), що полегшує вам запам'ятовування.
- І оскільки вона довша, ніж звичайний пароль, вона менш уразлива до атак із використанням словника або грубої сили.
- Ось кілька порад щодо створення хорошої парольної фрази.



Виберіть фразу,
яка для вас має
значення



Додайте спеціальні
символи, такі як
! @ # \$ % ^ & * ()



Чим довше,
тим краще



Уникайте поширених чи
відомих висловлювань,
наприклад, текстів
популярної пісні

Правила вибору паролів

- Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) Сполучених Штатів опублікував удосконалені вимоги до паролів.
- Стандарти NIST призначені для державного застосування, проте можуть також слугувати стандартом для інших.
- Ці рекомендації мають на меті покласти відповідальність за перевірку користувачів на постачальників послуг і забезпечити кращий досвід для користувачів загалом.
- У них зазначено:
 - Паролі повинні містити не менше восьми символів, але не більше 64 символів.
 - Не слід використовувати паролі, які легко вгадати, такі як «пароль» або «abc123».
 - Не повинно існувати жодних правил складання, включаючи малі та великі літери та цифри.
 - Користувачі повинні мати можливість бачити пароль під час введення, щоб підвищити точність.
 - Дозволяється використовувати усі друковані символи та пробіли.
 - Підказок на пароль бути не повинно.
 - Термін дії пароля повинен бути відсутній.
 - Не повинно бути аутентифікації на основі знань, наприклад, надання відповідей на секретні запитання або перевірка історії транзакцій.

3.2 Обслуговування даних

Що таке шифрування?

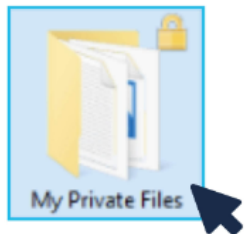
- Шифрування – це перетворення інформації у форму, непридатну для сприйняття неавторизованою стороною.
- Лише довірена, уповноважена особа, яка має секретний ключ або пароль, може розшифрувати дані та отримати їх в оригінальній формі.
- Зауважте, що саме лише шифрування не може завадити перехопленню даних.
- Воно може тільки завадити неавторизованій особі переглядати або отримувати доступ до вмісту даних.
- Фактично, злочинці можуть просто зашифрувати ваші дані, унеможлививши їх використання до сплати вами викупу.

Як ви шифруєте ваші дані?

- Існують програми, які використовуються для шифрування файлів, тек і навіть цілих дисків.
- Система шифрування файлів (Encrypting File System - EFS) - це функція Windows, яка може шифрувати дані. Лише користувач, який зашифрував дані, матиме доступ до них після того, як вони будуть зашифровані EFS.
- Щоб зашифрувати дані за допомогою EFS для всіх версій Windows, виконайте наступні кроки:

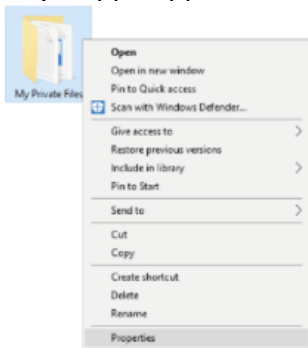
Крок 1

Виберіть один або декілька файлів або тек.



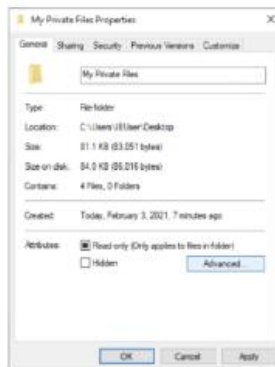
Крок 2

Натисніть праву кнопку миші на вибраних даних і перейдіть до



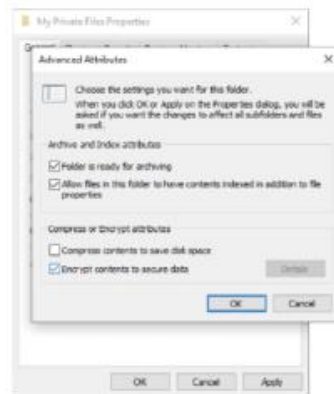
Крок 3

Знайдіть і натисніть «Додатково».



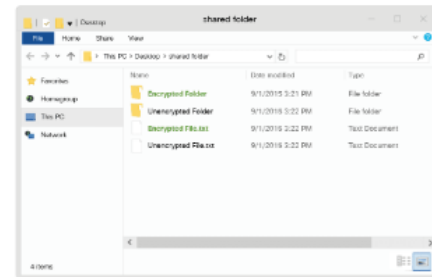
Крок 4

Встановіть прапорець «Шифрувати вміст для



Крок 5

Файли та теки, зашифровані EFS, відображаються зеленим кольором, як показано на рисунку.



Резервні копії ваших даних

- Наявність резервних копій зможе запобігти втраті унікальних даних, наприклад, сімейних фотографій.
- Для належного виконання резервного копіювання даних, вам знадобиться додаткове сховище даних, до якого потрібно копіювати дані регулярно.

Натисніть на шпильки, щоб вивчити деякі з цих додаткових місць зберігання.

Домашня мережа	Зберігання даних локально означає повний контроль над ними.
Вторинне розташування	Ви можете скопіювати всі свої дані до мережного сховища (Network Attached Storage, NAS), на звичайний зовнішній жорсткий диск або, можливо, зберегти лише кілька важливих тек на флеш-накопичувачі, CD/DVD-диску або навіть стрічці. За таким сценарієм ви як власник даних несете повну відповідальність за витрати на придбання та технічне обслуговування пристрою зберігання.
Хмара	Ви можете підписатися на службу хмарного сховища, як-от Amazon Web Services (AWS). Вартість цієї послуги буде залежати від необхідного обсягу пам'яті, тому вам може знадобитися бути більш розбірливим у виборі даних, які ви копіюєте. Доступ до резервних копій зберігається доки у вас є доступ до вашого облікового запису. Однією з переваг використання служби хмарного сховища є те, що ваші дані в безпеці в разі виходу з ладу пристрою зберігання даних або в екстремальних ситуаціях, таких як пожежа або крадіжка.

Як видалити свої дані назавжди?

- Чи доводилося вам коли-небудь видаляти дані або позбавлятися від жорсткого диска?
- Якщо так, то чи вжили ви будь-яких запобіжних заходів, щоб захистити дані, щоб вони не потрапили в чужі руки?
- Натисніть на зображення, щоб дізнатися, що вам потрібно зробити, щоб гарантувати, що ви видалите свої файли безпечно і назавжди.
 - Щоб видалити дані остаточно, без можливості відновлення, потрібно кілька разів перезаписати поверх них одиниці та нулі, використовуючи спеціально розроблені для цього інструменти.
 - SDelete від Microsoft за ствердженням виробника, надає можливість видаляти конфіденційні файли остаточно.
 - Shred для Linux та Secure Empty Trash для Mac OSX можуть надати аналогічний сервіс.
 - Єдиний спосіб переконатися, що дані або файли не підлягають відновленню, - це фізичне знищення жорсткого диску або іншого пристрою зберігання.
 - Багато злочинців скористалися файлами, які вважалися недоступними або невідновними!

3.3 Хто володіє вашими даними?

Хто володіє вашими даними?

Ознайомтеся з умовами

- Умови надання послуг містять ряд розділів, починаючи від прав та обов'язків користувачів до застережень та умов щодо зміни облікового запису.
- Політика використання даних визначає, як постачальник послуг збирає, використовує та передає ваші дані.
- Налаштування конфіденційності дозволяють вам контролювати, хто бачить інформацію про вас і хто може отримати доступ до вашого профілю або даних облікового запису.
- Політика безпеки визначає, що компанія робить для захисту даних, які вона отримує від вас.

Хто володіє вашими даними?

На що ви погоджуєтеся?

- Ви успішно створили обліковий запис @Apollo та погодилися з Умовами надання послуг компанії, яка обмінюється фотографіями в Інтернеті.
- Чи знаєте Ви під чим підписалися?



ПРИЙНЯТИ УМОВИ:



Я погоджуюся з умовами обслуговування та
політика конфіденційності.

Хто володіє вашими даними?

Перш ніж зареєструватися

- Які фактори слід враховувати, перш ніж зареєструватися в онлайн-сервісі?
- Чи ознайомилися Ви з Угодою про надання послуг?
- Які права Ви маєте щодо своїх даних?
- Чи можете Ви запросити копію Ваших даних?
- Що може робити постачальник послуг із даними, які Ви завантажили?
- Що відбувається з вашими даними, коли Ви закриваєте свій обліковий запис?

3.4. Захист конфіденційності в Інтернеті

Двофакторна аутентифікація

- Популярні онлайн-сервіси, такі як Google, Facebook, Twitter, LinkedIn, Apple та Microsoft, використовують двофакторну автентифікацію для забезпечення додаткового рівня захисту при вході до облікових записів.
- Крім імені користувача та пароля, або особистого ідентифікаційного номера (PIN), для двофакторної автентифікації потрібен другий токен для підтвердження вашої особи.
- Це може бути:
 - фізичний об'єкт, такий як кредитна картка, мобільний телефон або брелок
 - біометричне сканування, наприклад відбиток пальців або розпізнавання обличчя та голосу
 - код підтвердження, надісланий через SMS або електронну пошту.

Відкрита авторизація

- Відкрита авторизація (Open Authorization, OAuth) - це протокол відкритого стандарту, який дає змогу вам використовувати ваші облікові дані для отримання доступу до сторонніх застосунків, не розкриваючи пароль.
- Що це означає на практиці?
- Ви з нетерпінням чекаєте реєстрації на курс Cisco «Основи кібербезпеки», наступний курс із цієї серії, який допоможе вам розвинути свою кар'єру. Але для цього потрібно увійти на портал електронного навчання.
- Ви не можете згадати свої дані для входу, але не хвилюйтесь. Портал дає вам можливість увійти, використовуючи свої облікові дані з веб-сайту соціальних мереж, наприклад Facebook, або через інший обліковий запис, наприклад Google.
- Тож замість того, щоб скидати дані для входу, ви входите на портал електронного навчання за допомогою наявних облікових записів у соціальних мережах та легко реєструєтесь на наступний курс. Ви не можете дочекатися, щоб почати!

Відео – Не піддавайтеся обману

Простий підроблений або фальсифікований електронний лист може призвести до масового витоку даних і, можливо, завдати непоправної шкоди вашій репутації.

Конфіденційність електронної пошти та веб-браузера

- Цю проблему можна звести до мінімуму, увімкнувши у веб-браузері режим приватного (анонімного) перегляду.
- Більшість популярних веб-браузерів мають свою назву для режиму приватного перегляду:
 - **Microsoft Internet Explorer:** InPrivate
 - **Google Chrome:** Incognito
 - **Mozilla Firefox:** Приватна вкладка чи вікно
 - **Safari:** Приватний серфінг
- Як працює приватний режим?
 - Коли приватний режим увімкнено, файли cookie — файли, збережені на вашому пристрої, щоб позначати, які веб-сайти ви відвідували — вимкнено.
 - Тому будь-які тимчасові файли Інтернету видаляються, а історія перегляду видаляється, коли ви закриваєте вікно або програму.
 - Це може допомогти запобігти тому, щоб інші збирали інформацію про вашу діяльність в Інтернеті та намагалися спонукати вас купити щось за допомогою націленої реклами.
 - Навіть в режимі приватного перегляду із заборonoю використання файлів cookie, компанії постійно розробляють нові способи спостереження за активністю користувачів, щоб відстежувати їх поведінку в Інтернеті.

3.5 Дослідження власних ризиків, зумовлених поведінкою в Інтернеті

3.6 Контрольна робота

Що нового я дізнався у цьому розділі?

- Важливо організувати безпеку своїх пристроїв.
- Деякі поради щодо цього: увімкніть брандмауер, установіть антивірусне та антишпигунське програмне забезпечення, керуйте браузером операційної системи та налаштуйте захист паролем.
- Хакерам буде відомий попередньо встановлений SSID і пароль за замовчуванням, тому, щоб запобігти проникненню зловмисників у вашу домашню бездротову мережу, вам слід змінити ці дані.
- Крім того, слід шифрувати бездротове з'єднання, активувавши бездротову безпеку та функцію шифрування WPA2 на вашому бездротовому маршрутизаторі.
- Але майте на увазі, навіть якщо ввімкнено шифрування WPA2, бездротова мережа все ще може бути вразливою.
- Однак існують певні ризики, які означають, що краще не отримувати доступ до будь-якої особистої інформації та не надсилати її під час використання загальнодоступного Wi-Fi.
- Завжди перевіряйте, що на вашому пристрої не налаштовано спільний доступ до файлів і медіа, а також що він вимагає автентифікації користувача за допомогою шифрування.
- Ви також повинні використовувати зашифровану службу VPN, щоб не допустити перехоплення вашої інформації іншими особами через загальнодоступну бездротову мережу.
- Завжди використовуйте надійні паролі, не використовуйте паролі з орфографічними помилками звичайних слів словника, а також використовуйте спеціальні символи та паролі, довші за десять символів.
- Слід розглянути можливість використання парольних фраз.
- Шифрування – це перетворення інформації у форму, непридатну для сприйняття неавторизованою стороною.
- Саме лише шифрування не може завадити зловмиснику перехопити дані.
- Воно може тільки завадити неавторизованій особі переглядати або отримувати доступ до вмісту даних.

Що нового я дізнався у цьому розділі? (прод.)

- Існують програми, які використовуються для шифрування файлів, тек і навіть цілих дисків.
- Система шифрування файлів (Encrypting File System - EFS) - це функція Windows, яка може шифрувати дані.
- Наявність резервних копій зможе запобігти втраті унікальних даних, наприклад, сімейних фотографій.
- Деякими місцями зберігання є домашня мережа, вторинне розташування та хмара.
- Щоб видалити дані остаточно, без можливості відновлення, потрібно кілька разів перезаписати поверх них одиниці та нулі, використовуючи спеціально розроблені для цього інструменти.
- Єдиний спосіб переконатися, що дані або файли не підлягають відновленню, - це фізичне знищення жорсткого диску або іншого пристрою зберігання.
- Умови надання послуг містять ряд розділів, починаючи від прав та обов'язків користувачів до застережень та умов щодо зміни облікового запису.
- Перш ніж зареєструватися в онлайн-службі, врахуйте деякі фактори, як-от прочитайте її та знайте свої права.
- Щодо ваших даних, чи можете ви запросити копію своїх даних, зокрема.
- Популярні онлайн-сервіси, такі як Google, Facebook, Twitter, LinkedIn, Apple та Microsoft, використовують двофакторну автентифікацію для забезпечення додаткового рівня захисту при вході до облікових записів.
- Відкрита авторизація (Open Authorization, OAuth) - це протокол відкритого стандарту, який дає змогу вам використовувати ваші облікові дані для отримання доступу до сторонніх застосунків, не розкриваючи пароль.
- Простий підроблений або фальсифікований електронний лист може призвести до масового витоку даних і, можливо, завдати непоправної шкоди вашій репутації.
- Цю проблему можна звести до мінімуму, увімкнувши у веб-браузері режим приватного (анонімного) перегляду.