



# Основи інформаційної та кібербезпеки



# Лекція 8.

## Методи і засоби соціального інжинірингу

**1** Техніки та види соціоінженерних атак

**2** Етапи атаки із використанням CI

**3** Методи протидії атакам CI

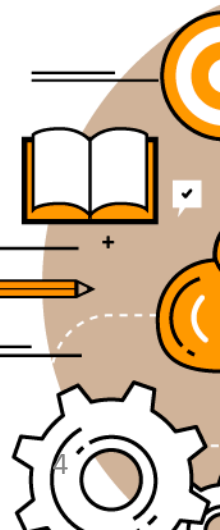


«У світі є тільки один спосіб переконати будь-кого щось зробити. ...  
Він полягає в тому, щоб інша людина захотіла цього. Запам'ятайте  
— це єдиний спосіб.»  
*Дейл Карнегі*

У контексті інформаційної безпеки **соціальна інженерія** — це психологічне маніпулювання людьми з метою примушення їх до виконання певних дій або розголошення конфіденційної інформації.



- 98% кібератак припадають на соціальну інженерію.
- 43% IT-фахівців вказали, що протягом останнього року вони були мішенню схем соціальної інженерії.
- Нові співробітники найбільш сприйнятливі до атак із соціальною інженерією: 60% IT-фахівців вважають, що нещодавно найняті люди піддаються високому ризику.
- 21% нинішніх чи колишніх співробітників використовують соціальну інженерію для отримання фінансової переваги, для помсти, цікавості чи для розваги.
- Кількість випадків порушення за типом:
  - Крадіжка особистих даних – 65%
  - Доступ до облікового запису – 17%
  - Доступ до фінансів – 13%
  - Неприємність – 4%
  - Екзистенційні дані – 1%



У своїй книжці «Психологія впливу» професор психології Роберт Чалдіні виділив шість принципів або рушіїв впливу на людей:

## □ Взаємність

- людина намагається відповісти добром на добро, послугою на послугу, щоб сплатити свій «борг». Почувати себе «зобов'язаним» комусь не комфортно, тому ми намагаємось якнайшвидше позбутися цього обов'язку

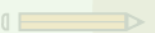


## ❑ Прихильність та Послідовність

- людині властиво дотримуватися тих дій або вчинків, які вона вже робила у минулому. Коли людина дає обіцянку, то вважає за свій обов'язок зробити все, щоб її дотримуватися. Варто попросити людину про кілька дрібних послуг, які вона зазвичай виконує, а у потрібний момент попросити про «головну» послугу і людині буде вже незручно відмовити.

## ❑ Слідуванню прикладу (соціальний конформізм)

- людина погоджується з тим, що робить більшість.
- Особливо в ситуаціях, коли людина не впевнена, що робити, вона швидше зробить те, що робить більшість.



## ❑ Авторитет

- людині притаманно слідувати за тими, кому вона довіряє, кого знає, хто для неї є авторитетом. Хакери користуються цим принципом, коли телефонують, представляючись співробітниками правоохоронних органів, працівниками банку; коли надсилають фішингові листи від імені керівників компаній чи відомих брендів.

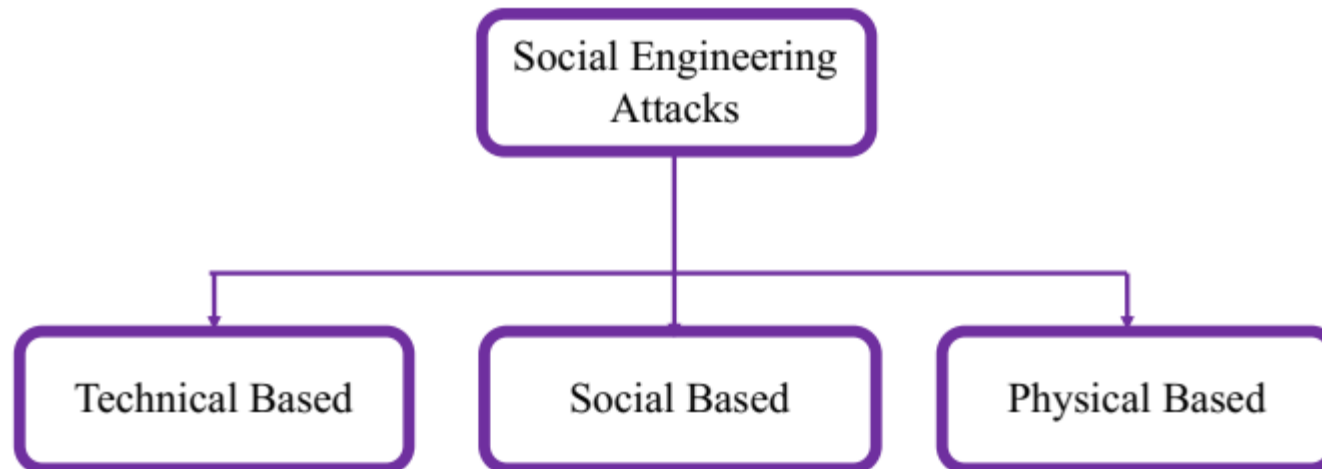
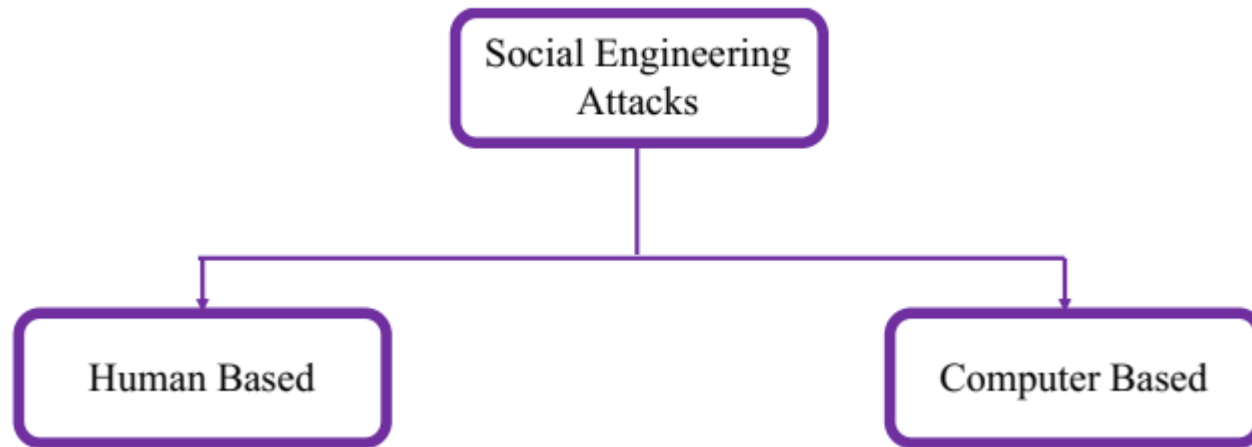
## ❑ Симпатія

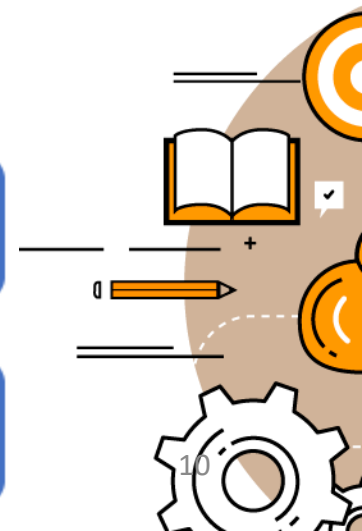
- людина охочіше та швидше виконує прохання тих, хто їй симпатичний, або зробить те, що їй подобається. Використовуючи цей принцип, хакер може розпочати процес «вербування» жертви із зробленого компліменту, до прикладу, щодо фотографій із відпустки, нової зачіски чи взуття.

## ❑ Дефіцит

- людина завжди більше бажає того, що їй недоступно. Коли речі стають менш доступними, вони здаються нам більш бажаними. Якщо у нас є вибір отримати це зараз або, можливо, отримати в майбутньому, ми обираємо зараз. Цей принцип активно застосовують маркетологи у продажах.
- Хакери також можуть використовувати цей підхід у своїх атаках. Наприклад, створивши відчуття, що документ, файл тощо може стати скоро недоступним, хакер може значно підвищити ймовірність того, що користувач завантажить його.
- створення штучного відчуття «дефіцит часу» на прийняття рішення покладаються шахраї у схемах «Ваш родич потрапив до поліції».
- маніпулювання прагненням отримати «швидкі гроші».

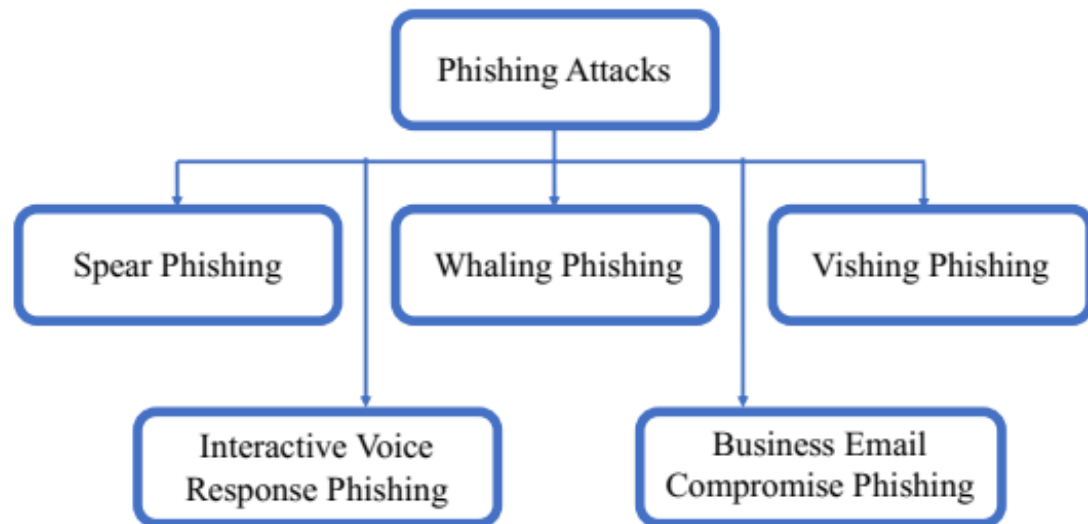






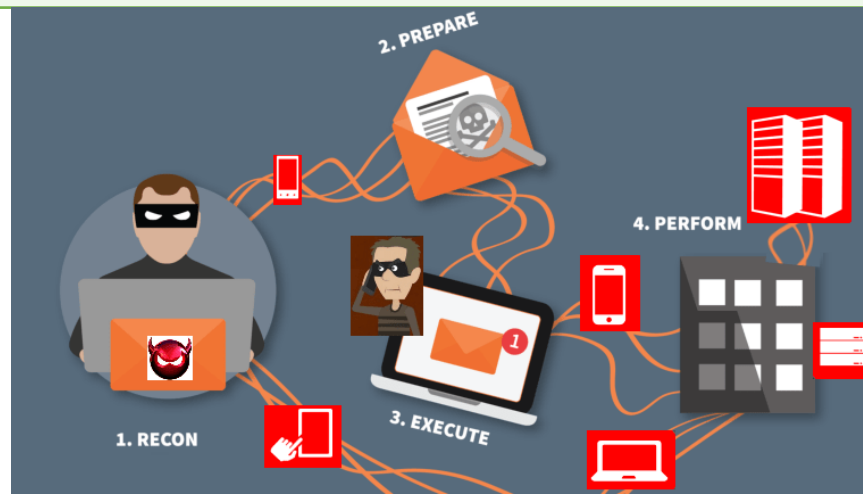
## «Фішинг»

- атака на основі соціальної інженерії, яка здійснюється через слабкості в кібербезпеці для обману користувачів з метою крадіжки їх логінів, паролів і грошових коштів. Техніки фішингу досить численні і складні, серед яких такі, які спонукають користувача перейти за посиланням на зловмисний сайт.



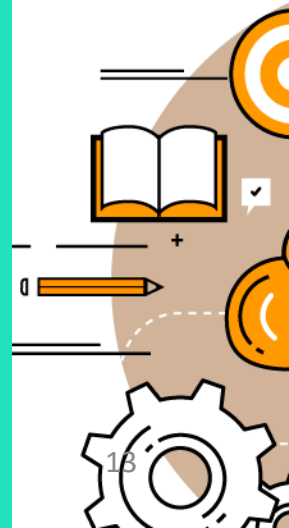
## «Претекстинг»

- атака, проведена за заздалегідь підготовленим сценарієм. Такі атаки спрямовані на розвиток почуття довіри жертви до зловмисника. Атаки зазвичай здійснюються по телефону. Цей метод часто не вимагає попередньої підготовки і пошуку даних про жертви. Претекстинг полягає у видачі жертви себе за іншу людину для отримання бажаних даних. Отримати інформацію про людину можна через джерела відкритого доступу, в основному зі сторінок соціальних мереж.



## «Троянський кінь»

- використовує такі якості потенційної жертви, як цікавість і жадібність. Соціальний інженер відправляє електронного листа з безкоштовним відео або оновленням антивірусу у вкладенні. Жертва зберігає вкладені файли, які насправді є троянськими програмами. Така техніка залишиться ефективною до тих пір, поки користувачі продовжують бездумно зберігати або відкривати будь-які вкладення.



## «Квіпрокво (quid pro quo)»

- При використанні цього виду атаки зловмисники обіцяють жертві вигоду в обмін на факти. Наприклад, зловмисник дзвонить в компанію, представляється співробітником технічної підтримки і пропонують встановити «необхідне» програмне забезпечення. Після того, як отримано згоду на установку програм, порушник отримує доступ до системи і до всіх даних, що зберігаються в ній.



## «Дорожнє яблуко» («road apple»)

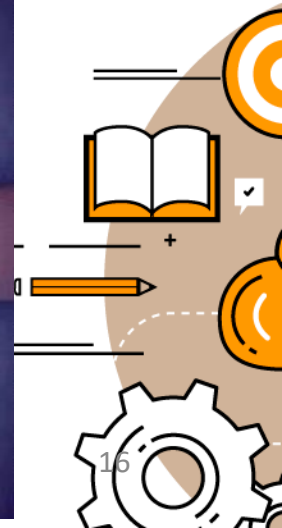
- це метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний носій інформації (флеш-накопичувач, диск) із шкідливим програмним забезпеченням. Носій може мати логотип компанії чи напис, що зацікавить співробітника, наприклад «список на звільнення», «заробітна плата за жовтень» тощо. Як тільки співробітник вставить такий носій до комп'ютеру, запуститься шкідливий код, який активує бекдор та надасть атакуючому доступ до мережі.





## «Зворотна соціальна інженерія»

- особа сама звертається до шахрая та повідомляє свої конфіденційні дані. Одним із можливих сценаріїв є, коли шахрай надсилає співробітникам компанії нібито нові номери телефонів служби технічної підтримки. Цілком імовірно, що через деякий час хтось із співробітників зателефонує і шахрай зможе вивідати інформацію, яка його цікавить.



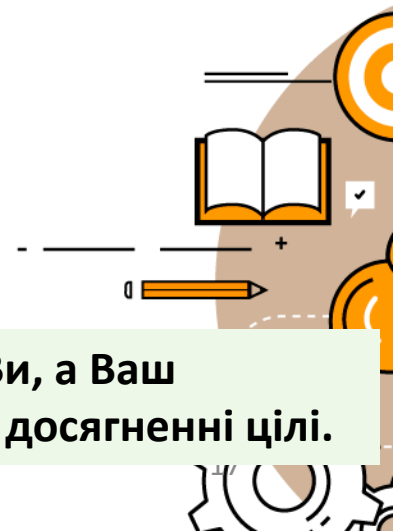


## «Складна атака через проміжну ціль (“Supply chain attack”)»

- хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компрометує ту ціль, яка від самого початку його цікавила.

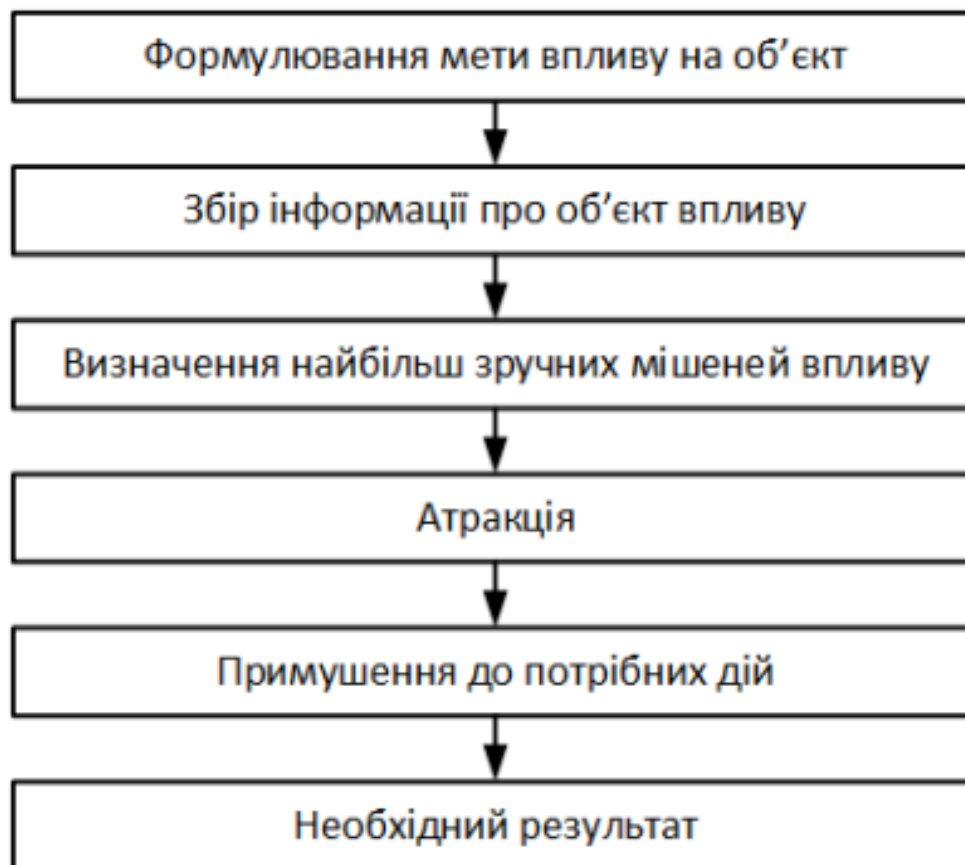
Яскравим прикладом “supply chain”-атаки була масштабна хакерська атака 2017 року з використанням різновиду вірусу Petya, що спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, «Укртелеком», «Укрпошта», «Ощадбанк», «Укрзалізниця» та низки інших великих підприємств. Ця атака розпочалася із компрометації системи оновлення програми M.E.Doc. Інфіковані файли з оновленнями M.E.Doc були встановлені на тисячі систем та спричинили блискавичне розповсюдження вірусу Petya.

**Висновок: пам’ятайте, справжньою ціллю хакера можете бути не Ви, а Ваш керівник чи установа, де Ви працюєте, а Ви – це лише інструмент у досягненні цілі.**



## 2 Етапи атаки із використанням СІ

Всі атаки соціальних хакерів укладаються в одну досить просту схему



## 2 Етапи атаки із використанням СІ

### Розвідка та збір інформації із відкритих джерел

Яка інформація може цікавити хакера?

Якщо це стосується конкретної особи, урядовця, співробітника:

- наявність акаунтів в соціальних мережах;
- емейли, номери телефонів та адреси інтернет-месенджерів;
- деталі щодо сімейного стану, дітей, дружини/чоловіка, батьків тощо;
- місце роботи, заняття, хобі, як проводить вільний час, відпустку;
- деталі щодо посади, як давно працює у компанії/установі, чи задоволений місцем праці, посадою тощо;
- наявність автотранспорту, нерухомості, іншого майна;
- соціальна та громадська діяльність.



## 2 Етапи атаки із використанням СІ

### Розвідка та збір інформації із відкритих джерел

Яка інформація може цікавити хакера?

Якщо це стосується компанії чи державної установи:

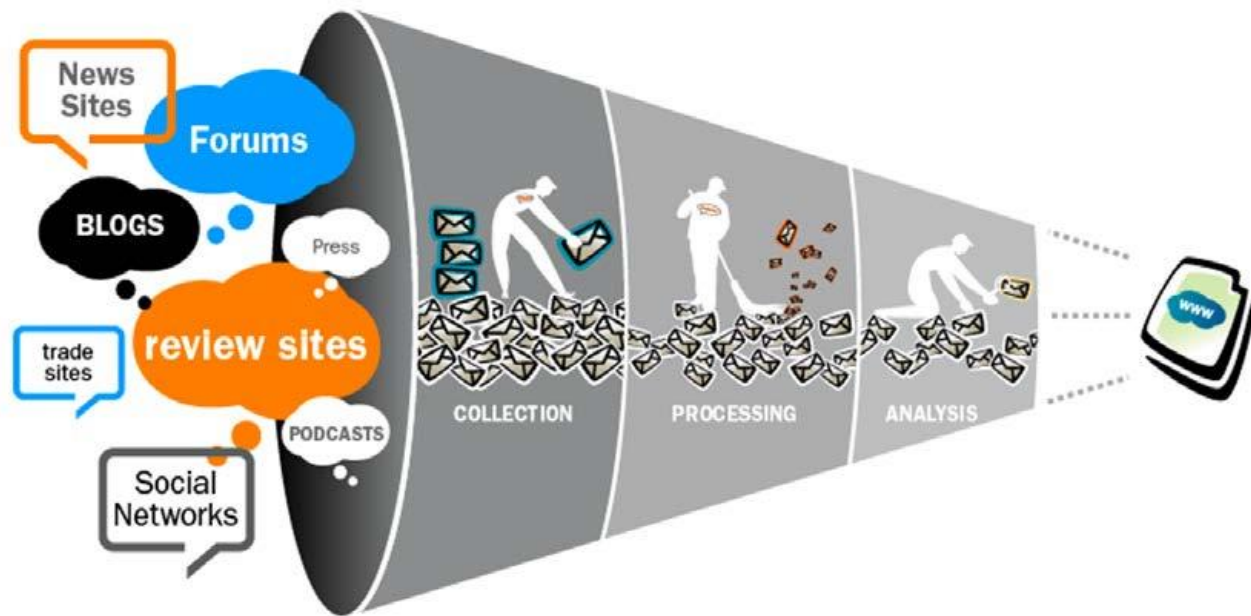
- як побудована мережева інфраструктура (наприклад, чи використовуються групові політики), яким чином здійснюється доступ до мережі «Інтернет»;
- чи використовують (яке?) антивірусне програмне забезпечення;
- версія операційної системи;
- як побудований бізнес, партнери компанії та підрядні організації;
- адреси головного офісу чи філіалів.



## 2 Етапи атаки із використанням CI

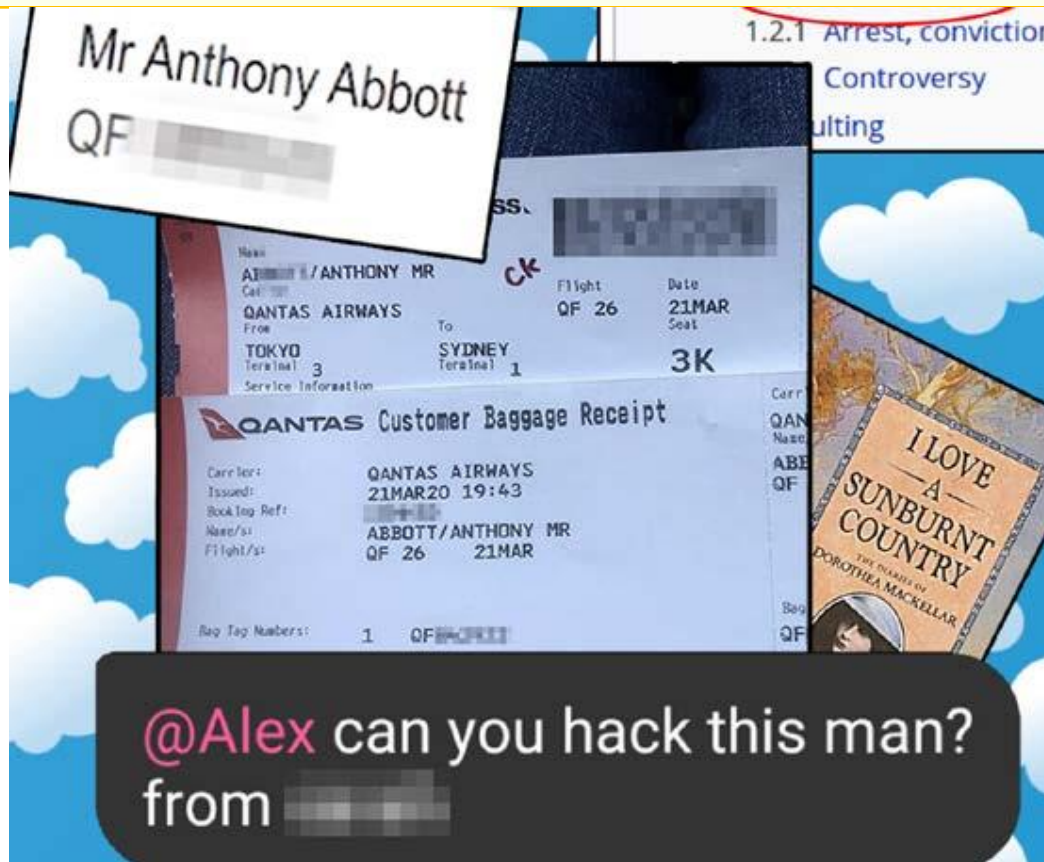
### Розвідка та збір інформації із відкритих джерел

Для збору даних хакери проводять розвідку відкритих джерел інформації або **OSINT (Open source intelligence)**. Інформація отримується з різних джерел, зіставляється, аналізується та формулюється у «звіт», який хакер використовує для планування та здійснення CI-атаки.

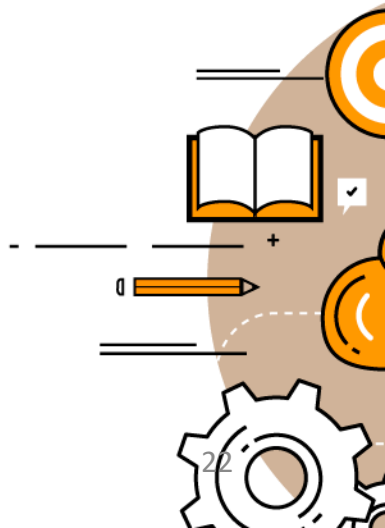


## 2 Етапи атаки із використанням CI

### Розвідка та збір інформації із відкритих джерел



<https://www.theverge.com/2020/10/15/21516842/tony-abbott-passport-boardingpass-instagram-hacking-cybersecurity>





## 2 Етапи атаки із використанням СІ

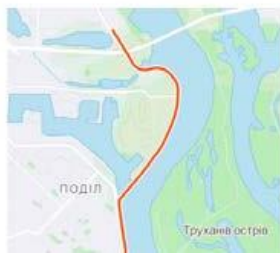
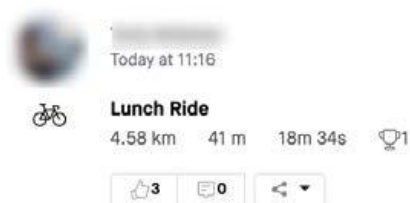
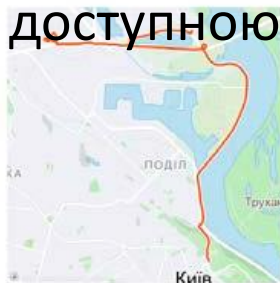
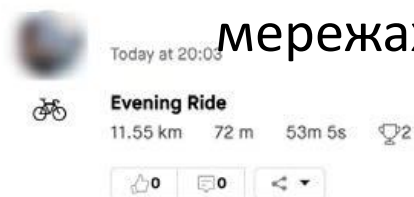
Розвідка та збір інформації із відкритих джерел



## 2 Етапи атаки із використанням СІ

Чи можуть хакери визначити місце Вашого проживання, якщо Ви обмежили користування соціальними мережами та не розміщуєте там свої фотографії?

Так, якщо Ви користуєтесь популярними фітнес-трекерами. Наприклад, фітнестрекер Strava фіксує усі Ваші тренування, які в подальшому стають доступними для перегляду Вашим контактам, а якщо Ви розміщуєте цю інформацію в соціальних мережах, то вона стає доступною ще більшій аудиторії.





## 2 Етапи атаки із використанням СІ

Чи можуть хакери визначити місце Вашого проживання, якщо Ви обмежили користування соціальними мережами та не розміщуєте там свої фотографії?



Tobias Schneider

@tobiaschneider

Follow

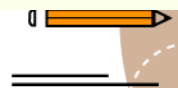


So much cool stuff to be done. Outposts around Mosul (or locals who enjoy running in close circles around their houses):



11:37 AM - 27 Jan 2018

Розміщуючи фото в мережі Інтернет не забувайте про метадані фотографії (**метадані** – це службова інформація, доступна у кожному файлі, яка вказує, коли, як, ким було створено тощо).



## 2 Етапи атаки із використанням СІ

Цікавим прикладом використання OSINT для збору інформації про особу є стаття, опублікована на сайті інтернет-видання “Bellingcat” (<https://www.bellingcat.com/news/uk-and-europe/2019/03/19/locating-the-netherlands-most-wanted-criminal-by-scrutinising-instagram/>). “Bellingcat” на базі аналізу фотографій розміщених у соціальних мережах змогло визначити точне місце розташування злочинця-втікача, який переховувався від поліції Нідерландів.

Злочинець активно постив фотографії в соціальних мережах, знущаючись із поліції, закликаючи «зловіть мене, якщо можете».




## 2 Етапи атаки із використанням CI


### Легендування та планування атаки

На цьому етапі хакер підготує весь необхідний інструментарій: створить фішинговий лист, напише текст (на практиці це зазвичай роблять спеціальні сервіси і хакери купують фішинговий пакет

[ПРОДАЖА] 🏠 New Exploit and Corona Virus Phishing Method!

👤 Zaher · 📅 23.02.2020

 NO AVATAR

**Zaher**   
florru'диск

Пользователь

Регистрация: 17.02.2020  
Сообщения: 5  
Реакции: 2  
Баллы: 3

23.02.2020

New Exploit and Corona Virus Map Phishing method

Новая Эксплоит плюс разводка с Карт распространения Корона Вирус



## 2 Етапи атаки із використанням СІ

### **Загальні поради щодо протидії атакам із використанням СІ:**

- Не повідомляйте свої персональні дані чи дані про установу, де ви працюєте іншим особам.
- Уникайте або обмежуйте публікування своїх персональних даних, фотографій в соціальних мережах, на сайтах чи порталах.
- Якщо сам емейл чи телефонний дзвінок, який Ви отримали, а також саме прохання телефонуючого чи автора емейлу викликає у Вас підозру, перевірте легітимність емейлу чи самого запиту.
- Якщо Вам телефонують з невідомого номеру або невідома особа і представляється співробітником банку, поліції, прокуратури тощо та просить повідомити персональні дані, переказати кошти чи повідомити дані платіжної картки – не робіть цього!!! Зазвичай це шахраї. Не піддавайтесь паніці.
- Ігноруйте запити та повідомлення в соціальних мережах від акаунтів, які не мають активності.
- Користуйтесь антивірусами, ліцензійним програмним забезпеченням.
- На всіх сервісах, де це можливо, активуйте двохфакторну аутентифікацію.

### 3 Методи протидії атакам СІ

#### **Превентивні методи захисту від соціотехнічних атак:**

- **правові** (законодавчі та морально-етичні);
- **організаційні** (адміністративні, технічні, економічні);
- **інженерно-технічні** (фізичні, технічні, програмні).



### 3 Методи протидії атакам СІ

#### **Превентивні методи захисту від соціотехнічних атак:**

- **правові** (законодавчі та морально-етичні);
- **організаційні** (адміністративні, технічні, економічні);
- **інженерно-технічні** (фізичні, технічні, програмні).





### 3 Методи протидії атакам СІ

#### **Технології протидії соціальним хакерам:**

- 1) диференціація важливої інформації між кількома співробітниками, чіткий розподіл повноважень як у доступі до агрегованої бази даних, так і в розголошенні інформації;
- 2) обізнаність та навчання персоналу; привертання уваги людей до питань інформаційної безпеки, усвідомлення співробітниками серйозності проблеми, вивчення і використання профілактичних методів і дій для підвищення рівня захисту;



### Технології протидії соціальним хакерам:

3) побудова системи «раціональної довіри», що передбачає побудову здорової атмосфери на підприємстві (відсутність страху перед керівництвом);

4) максимальна автоматизація важливих процесів; розроблення процедури для перевірки особистості та авторизації осіб, які звертаються за інформацією або вимагають якихось дій від співробітників компанії; здійснення ввічливого відхилення запиту працівниками компанії про надання важливої інформації, поки не буде встановлено особу, яка подавала запит на її право на доступ до цієї інформації;



### Технології протидії соціальним хакерам:

5) побудова надійної структури метрик для відстеження прогресу та вимірювання впливу засобами аналітичного пакету; щоб по-справжньому мати зрілу модель протидії соціальному хакерству, підприємство повинне не тільки змінювати поведінку та культуру, а й мати структуру метрик для демонстрації цих змін;

6) підтримка пильності персоналу; проведення тренінгів, які формують розвиток критичного мислення, вміння співставляти факти, аналізувати та тверезо оцінювати ситуацію з позиції «здорового глузду»; не піддаватися на паніку чи шантаж, не приймати «на віру», а раціонально оцінювати будь-які штатні, а тим паче нестандартні ситуації, відхилення; перевіряти підозрілу інформацію; впровадження системи розсилки нагадувань.

### 3 Методи протидії атакам CI

Тест на проникнення методами соціальної інженерії є індикатором на виявлення найбільш сприятливих умов для злочинців:

- здійснюється за допомогою **Social-Engineer Toolkit** та Kali Linux, Cogni-Sense.
- Для цього проводиться навчання стосовно вірогідних сценарії атак соціальної інженерії. За результатами такого навчання удосконалюються технології і політики протидії соціоінженерному впливові. На практиці метод реалізується як **Social Engineering Defensive Framework**.



### 3 Методи протидії атакам CI

## Тест на проникнення методами соціальної інженерії:

