Тема 2. Базові правила убезпечення роботи в комп'ютерній мережі

Соціальна інженерія

План лекції

Вступ
1. Зміст явища «соціальна інженерія»
2. Популярні вектори атак
3. Методи протидії
Висновки

Рекомендована література
Основна

1. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : BAITE, 2021. 106 с.
2. 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. : BAITE, 2021. 262 с.
3. Oles N. How to Catch a Phish: A Practical Guide to Detecting Phishing Emails. Apress Berkeley, CA, 2023. 147 p. DOI: https://doi.org/10.1007/978-1-4842-9361-4.

Допоміжна

5. 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.
6. 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.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.
8. Ви вмієте розпізнавати фішинг? URL: https://phishingquiz.withgoogle.com/?hl=uk.

Текст лекції

Вступ

Соціальна інженерія як явище зародилося ще на початку історії людства і було часто пов'язано з потребою вивчення людської поведінки для прийняття побутових, військових, політичних та інших рішень, вчинення правопорушень. У 1894 році термін «соціальна інженерія» було введено в обіг нідерландським підприємцем Якобом Корнелісом (Жаком) ван Маркеним. З появою засобів комп'ютерної техніки та розвитком мережі Інтернет про комп'ютерну соціальну інженерію дізналися люди з усього світу, а її інструментарій став активно застосовуватися правопорушниками у межах різного виду протиправної поведінки у кіберсфері.

1. Зміст явища «соціальна інженерія»

Соціальну інженерію у широкому розумінні можна розглядати як науку, яка вивчає поведінку людей та фактори, що на неї впливають. У більш вузькому контексті соціальна інженерія – це інструмент психологічного маніпулювання, спрямований на досягнення бажаної поведінки суб'єкта або групи суб'єктів за певних умов.

Соціальна інженерія як інструмент застосовується у більшості видах кібератак та нерідко спрямована на заволодіння персональними даними.

Безпосередньо здійснюючи відповідні кібератаки, зловмисники можуть використовувати соціальну інженерію (рис. 1):

- взагалі не вступаючи в контакт з людьми (підбирання паролю, в якому міститься день народження жертви, номер мобільного телефону тощо, взаємодія із системами відновлення паролів у частині відповіді на секретне питання на кшталт «дівоче прізвище матері»);
- не вступаючи в контакт з цільовою особою (комунікація зі службами підтримки провайдерів цільової особи, її друзями, знайомими, родичами);
- під час комунікації з цільовою особою (назватися службою підтримки банку, начальником керівного підрозділу, поліцейським тощо).

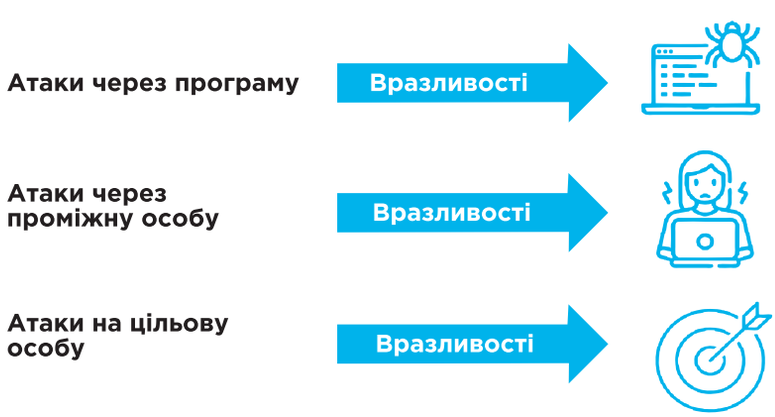


Рис. 1. Напрями застосування інструментарію соціальної інженерії

Розглянемо популярні техніки соціальної інженерії.

Фішинг (англ. phishing, від fishing – риболовля) – вид маніпуляції, який передбачає створення підроблених об'єктів у кіберсфері, які викликають довіру в цільової групи користувачів та спрямовані на отримання від таких користувачів чутливої інформації або вчинення певних дій, вигідних атакуючому. Цілями зловмисників можуть бути автентифікаційні дані облікових записів, отримання коштів від жертви тощо.

Телефонний вид фішингу називають **вішингом** (англ. vishing – voice fishing). Він передбачає використання голосового контакту телефоном атакуючого з жертвою з метою вплинути на поведінку цільової особи. Популярними схемами вішингу є повідомлення жертви про те, що її дитина потрапила в аварію, спричинила жертви і тепер терміново потрібні кошти, або це може бути банківське шахрайство тощо. У будь-якому разі сценарій вішингу продумується заздалегідь та передбачає вибір певного часу телефонного дзвінка, окремі підходи до спілкування з різними віковими групами тощо.

Жителька м. Чернігова заявила у кіберполіцію, що стала жертвою шахрайства. Так, зловмисники зателефонували їй та представившись оператором зв'язку, повідомили, що у зв'язку зі складнощами у роботі мережі можливі збої, а тому є можливість тимчасово безкоштовно перейти у режим роумінгу, аби залишатись на зв'язку.
Погодившись, жінка повідомила коди підтвердження з СМС, які насправді були від її систем авторизації. З банківської картки жінки вивели 48 тис. грн., а з її месенджерів почали надсилати інформацію контактам з проханням позичити кошти. Таким чином, злочинці додатково отримали ще 3 тис. грн.

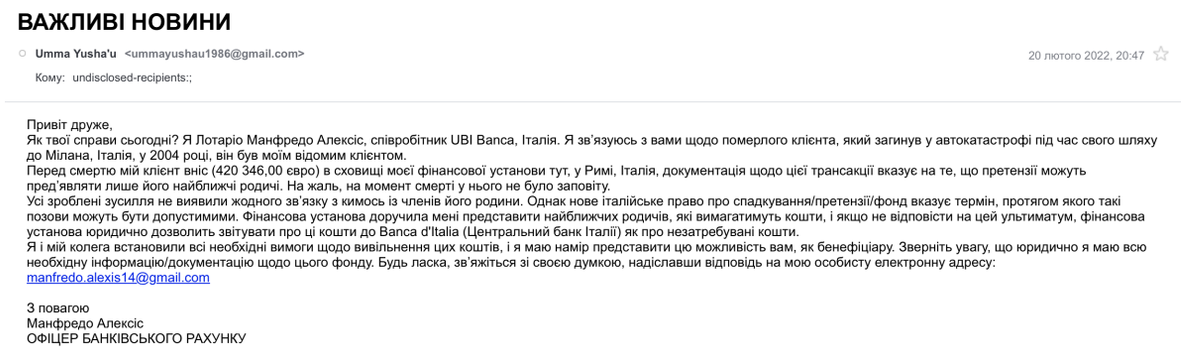
Одним з ключових елементів фішингу є фейк – неправдива інформація словесного, мультимедійного та іншого характеру. Фейки можуть бути як простими, так і досить складними, які вкрай важко відрізнити від оригінальної інформації.

Серед засобів, за допомогою яких найчастіше здійснюють фішингові атаки, слід виділити такі:

- електронна пошта, в тому числі спам-розсилка;
- фейкові веб-сайти;
- рекламні повідомлення та їх різновид у вигляді спливаючих вікон;
- контрафактні програми або дані іншого виду;
- месенджери тощо.

Як правило, фішингові атаки передбачають використання кількох з наведених засобів. Так, якщо згадати класичну кваліфіковану схему фішингу, то цільовій особі спочатку може надходити електронний лист з підробленим заголовком, де вказується довірена електронна пошта відправника листа, а

в самому тілі листа дається закамуфльоване посилання на фейковий ресурс банку, державної установи, певного підприємства, установи, організації, з якою взаємодіє або потенційно може взаємодіяти жертва атаки. Все може бути і набагато простішим (рис. 2).



ВАЖЛИВІ НОВИНИ

Umma Yusha'u <ummayushau1986@gmail.com> 20 лютого 2022, 20:47

Кому: undisclosed-recipients:;

Привіт друже,
Як твої справи сьогодні? Я Лотаріо Манфредо Алексіс, співробітник UBI Banca, Італія. Я зв'язуюсь з вами щодо померлого клієнта, який загинув у автокатастрофі під час свого шляху до Мілана, Італія, у 2004 році, він був моїм відомим клієнтом.
Перед смертю мій клієнт вніс (420 346,00 євро) в сховищі моєї фінансової установи тут, у Римі, Італія, документація щодо цієї трансакції вказує на те, що претензії можуть пред'являти лише його найближчі родичі. На жаль, на момент смерті у нього не було заповіту.
Усі зроблені зусилля не виявили жодного зв'язку з кимось із членів його родини. Однак нове італійське право про спадкування/претензії/фонд вказує термін, протягом якого такі позови можуть бути допустимими. Фінансова установа доручила мені представити найближчих родичів, які вимагатимуть кошти, і якщо не відповісти на цей ультиматум, фінансова установа юридично дозволить звітувати про ці кошти до Banca d'Italia (Центральний банк Італії) як про незатребувані кошти.
Я і мій колега встановили всі необхідні вимоги щодо вивільнення цих коштів, і я маю намір представити цю можливість вам, як бенефіціару. Зверніть увагу, що юридично я маю всю необхідну інформацію/документацію щодо цього фонду. Будь ласка, зв'яжіться зі своєю думкою, надіславши відповідь на мою особисту електронну адресу:
manfredo.alexis14@gmail.com

З повагою
Манфредо Алексіс
ОФІЦЕР БАНКІВСЬКОГО РАХУНКУ

Рис. 2. Приклад шахрайського повідомлення

Якщо атака не цільова, то часто відповідні листи шахрайського змісту розсилаються масово і нерідко потрапляють до спаму (рис. 3).

Рис. 3. Посилання на приклад листів з маніпулятивним змістом
(https://docs.google.com/document/d/
11oTX14GzEcaZMgyKIKejVQKn6BjWCPzQVjh5p3vEfG0/edit)

У листі може міститися пропозиція з переходом на сайт зловмисників, який, як правило, є фейком справжнього відомого ресурсу (рис. 4, 5).

i.ua

Вхід для користувачів

Логін

Пароль

Увійти

© I.UA, 2006-2023.
Зворотний зв'язок

каталог сайтів i.ua

Рис. 4. Фейкова сторінка сайту i.ua
(i-ua.website станом на 06.07.2023)

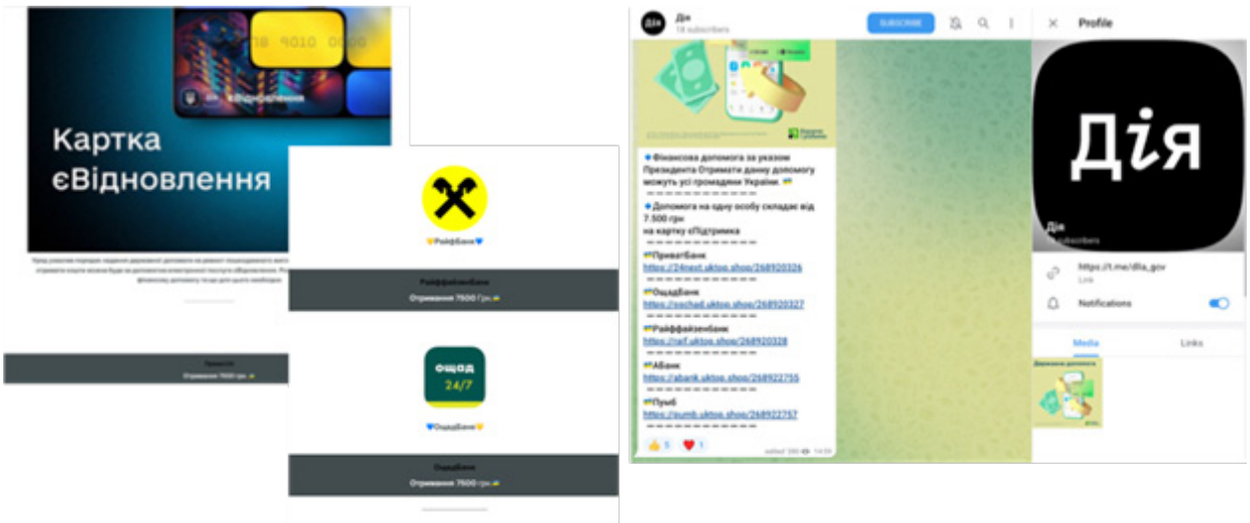


Рис. 5. Зміст фейкового сайту надання допомоги
(viplataua.art.blog станом на 24.07.2023)

У більш витончених атаках фішингу можуть використовуватися вразливості в роботі великих компаній та застосовуватися комерційна реклама. Так, у липні 2023 року компанія MalwareBytes виявила фішингову атаку, націлену на американських громадян, під маркою великої поштової компанії USPS (https://www.malwarebytes.com/blog/threat-intelligence/2023/07/malicious-ad-for-usps-phishes-for-jpmorgan-chase-credentials).

Зловмисники замовили в Google рекламу фейкового сайту поштової служби від імені громадянки України Анастасії Іващенко. В результаті користувачі після введення в пошуку USPS tracking бачили у пошуковій видачі на перших позиціях рекламне посилання на фейковий сайт зловмисників (рис. 6).

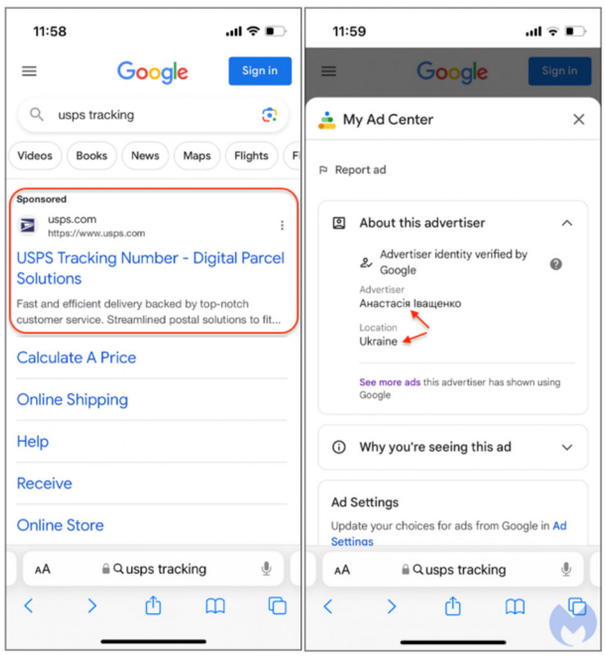


Рис. 6. Результати пошукової видачі

Зверніть увагу, що зловмисники вказали українського замовника реклами, проте вже після викриття атаки, якщо перейти за посиланням фейкового сайту https://super-trackings.com/, можна побачити відомості, які опосередковано вказують на російський слід атакуючих (рис. 7).

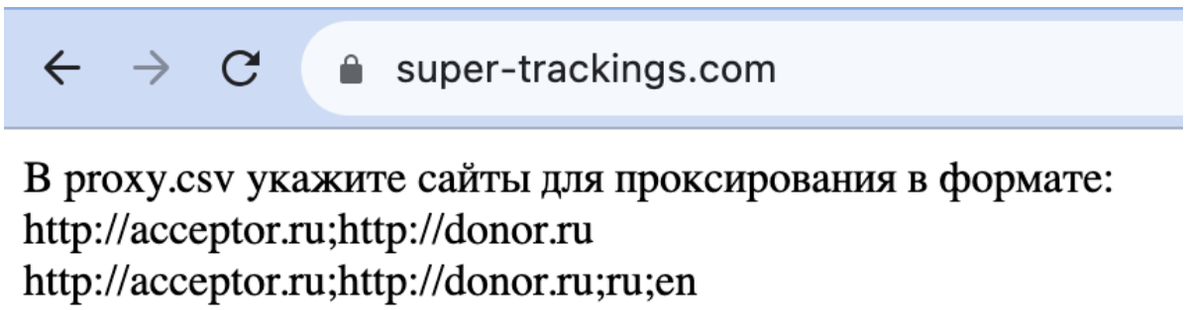


Рис. 7. Результати переходу на сайт зловмисників
(станом на 27.07.2023)

Схожа атака через рекламу Google була здійснена зловмисниками у 2015 році стосовно веб-банкінгу Ощад 24/7, у серпні 2023 року стосовно компанії Amazon (https://www.bleepingcomputer.com/news/security/sneaky-amazon-google-ad-leads-to-microsoft-support-scam/).

Ще одним інструментом здійснення фішингу є неліцензійне (контрафактне) програмне забезпечення. Користувачі, намагаючись «зекономити», нерідко стають жертвами зловмисників, що в свою чергу може потягнути тяжкі наслідки. Наприклад, восени 2022 року з російського боку була ініційована багаторівнева атака через **проміжну ланку** (supply chain), спрямована проти урядових установ України (https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government). Так, на кількох російськомовних та україномовних торрент-трекерах зловмисники поширили троянізований образ неліцензійної збірки Windows 10 (рис. 8).

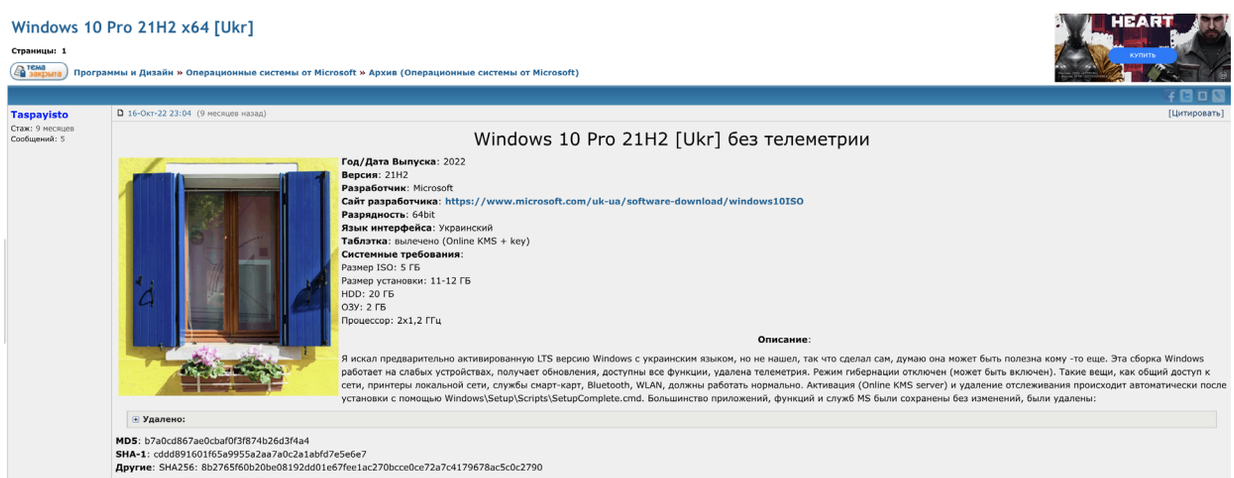


Рис. 8. Результати переходу на сторінку з описом небезпечного образу ОС Windows на одному з торрент-трекерів
(станом на 28.07.2023)

У наведеному образі були передбачені завдання, призначені для отримання команд через PowerShell. Це давало змогу збирати дані з відповідних комп'ютерів, встановлювати шкідливе програмне забезпечення та передавати вкрадені дані на контрольовані зловмисниками сервери. Після попередньої розвідки в систему встановлювалися бекдори, через які зловмисники управляли системою. У процесі атаки зловмисники проводили аналіз заражених пристроїв та атакували ті з них, які належали працівникам урядових структур.

Крім вже наведених інструментів здійснення фішингових атак, слід також згадати розсилання небезпечних повідомлень з використанням месенджерів. Як правило, сценарій таких атак та використовуване програмне забезпечення розробляється під конкретний вид месенджеру. Так, восени 2022 року відбулася хвиля атак на громадян України через месенджери WhatsApp та Telegram.

У першому випадку йшла масова розсилка повідомлень від імені компанії Amazon з пропозицією працевлаштування (рис. 9).

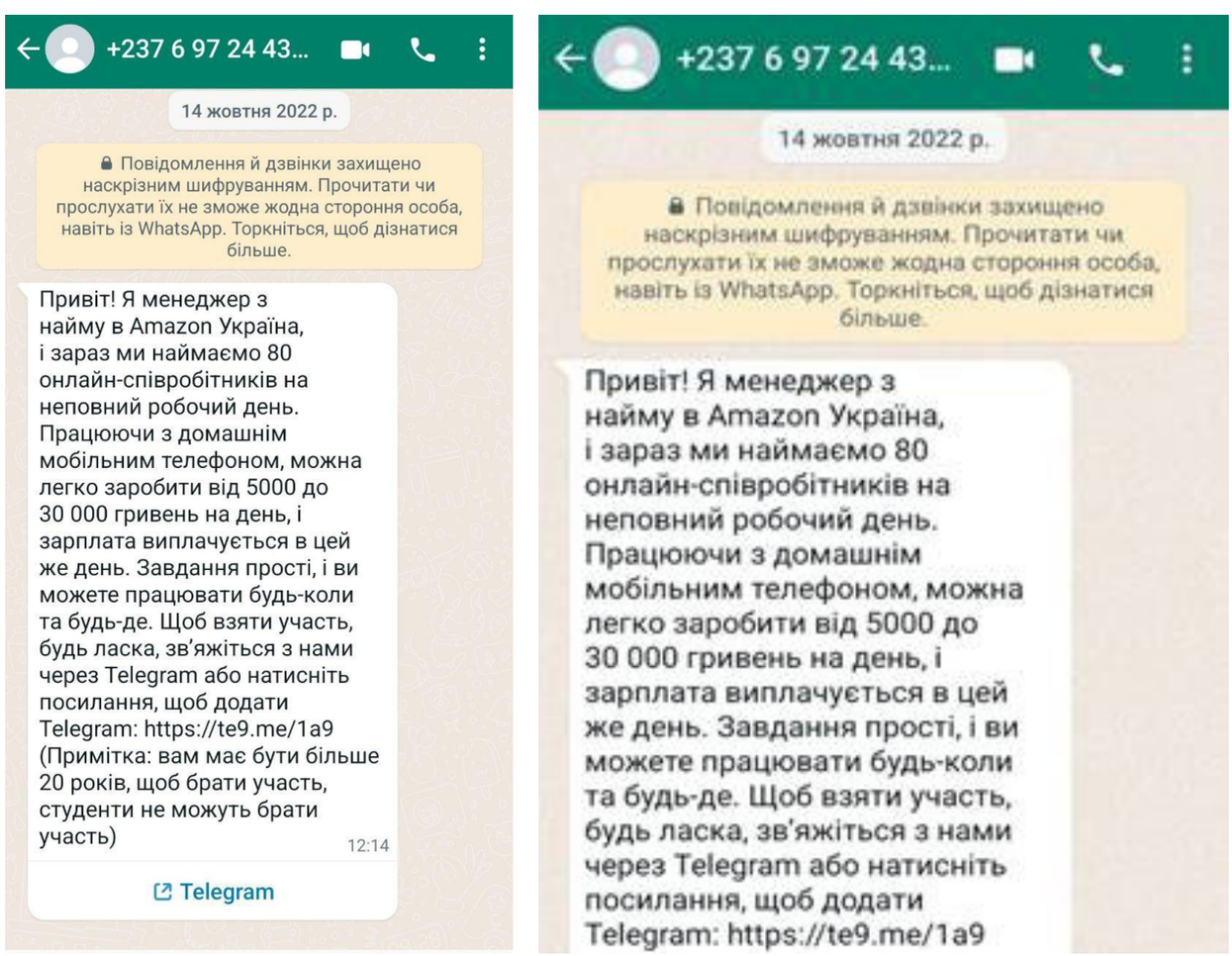


Рис. 9. Пропозиція з працевлаштування

Якщо переглянути реєстраційну інформацію про ресурс te9.me, вказаний в оголошенні, то можна побачити, що його створили нещодавно, при цьому усіляко намагаючись приховати відомості про реєстратора (рис. 10).

Address lookup

canonical name **te9.me.**

aliases

addresses **104.21.37.163**
172.67.210.147
2606:4700:3034::ac43:d293
2606:4700:3037::6815:25a3

Domain Whois record

Queried **whois.nic.me** with "**te9.me**"...

```
Domain Name: TE9.ME
Registry Domain ID: D425500000339260668-AGRS
Registrar WHOIS Server: whois.rrpproxy.net
Registrar URL: http://www.key-systems.net
Updated Date: 2023-03-29T09:08:30Z
Creation Date: 2022-04-17T00:26:40Z
Registry Expiry Date: 2024-04-17T00:26:40Z
Registrar Registration Expiration Date:
Registrar: Key-Systems GmbH
Registrar IANA ID: 269
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: c/o whoisproxy.com
Registrant State/Province: VA
Registrant Country: US
Name Server: COBY.NS.CLOUDFLARE.COM
Name Server: PAIGE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-07-28T11:58:52Z <<<
```

Рис. 10. Відомості про сайт te9.me

Докладніше про цю атаку можна прочитати за адресою https://gwaramedia.com/fejk-amazon-rozsilaie-povidomlennya-z-propozicziieyu-roboti-dlya-ukrainczіv/.

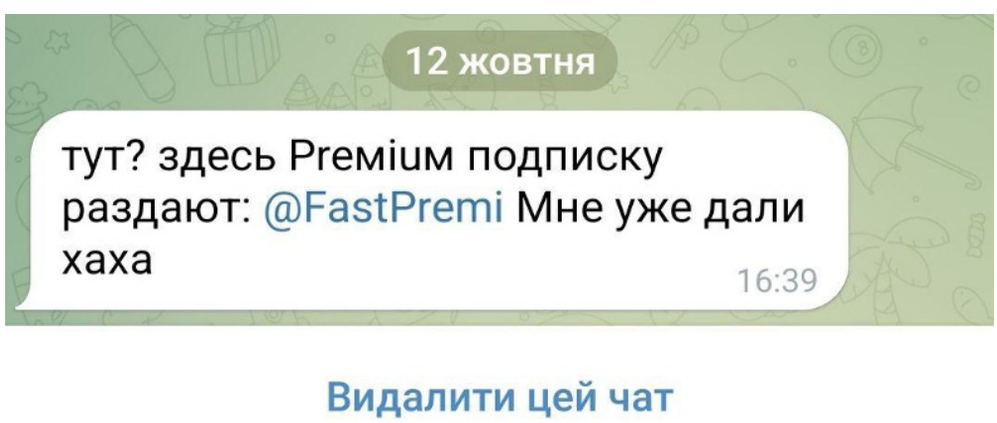


Рис. 11. Шахрайське повідомлення у Telegram

У випадку переходу за наведеним у повідомленні посиланням користувачеві пропонувалося знову авторизуватися в Telegram. У разі виконання цих дій захоплювалася сесія Telegram жертви. Надалі від імені користувача, чия сесія була захоплена, серед його контактів починалася розсилка аналогічного шахрайського повідомлення. Маючи захоплену сесію Telegram, зловмисники мали змогу не тільки дістатися синхронізованих контактів, а й завантажити відповідне листування тощо.

Крім фішингу, популярною технікою соціальної інженерії є збирання інформації з відкритих джерел.

Розвідка з відкритих джерел (OSINT) з'явилася вже досить давно, проте саме з появою глобальних мереж вона набула суттєвого значення для збирання інформації про певні об'єкти в усьому світі. Якщо раніше значна частина чутливої інформації зловмисниками добувалася з використанням різноманітних зламів, то сьогодні можна спостерігати збільшення ролі OSINT в цьому процесі. Немаловажним є той факт, що навіть якщо в мережі відсутня безпосередня інформація про розшукуваний об'єкт, її можна спробувати знайти через пов'язані з об'єктом зв'язки, що робить OSINT універсальним інструментом.

На ринку технічних пошукових сервісів зараз присутня велика кількість комплексних спеціалізованих рішень, які за окремим ідентифікатором дозволяють зібрати інформацію про особу чи інший об'єкт (рис. 12). Вказані обставини значно спрощують роботу атакуючих, в тому числі щодо збирання інформації про жертву.

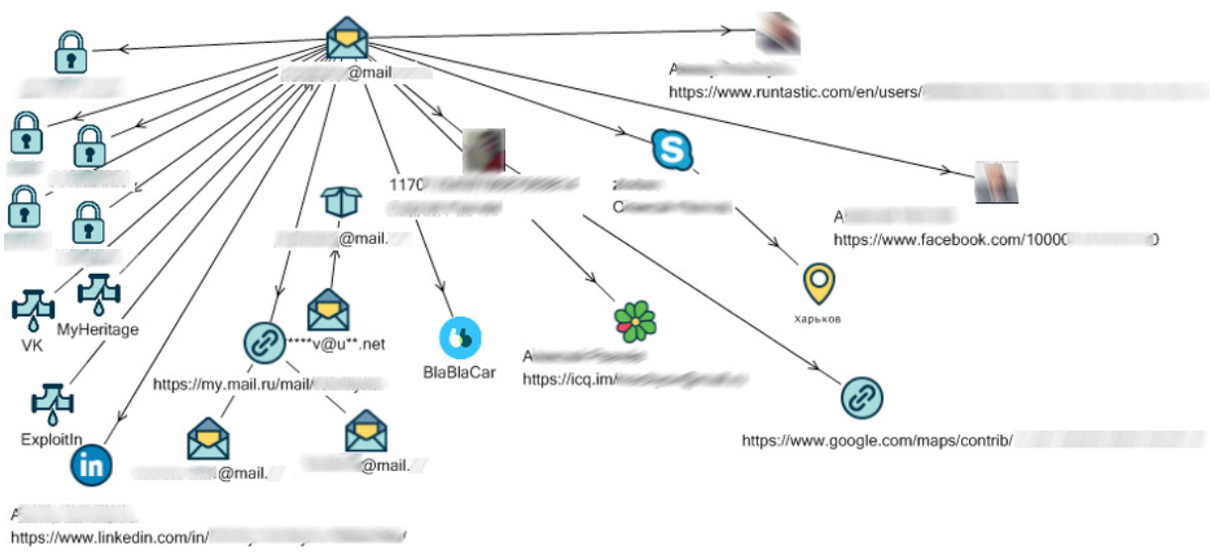


Рис. 12. Результати роботи комплексного рішення з пошуку інформації

У цьому випадку за електронною поштою вдалося знайти п’ять старих паролів до різних ресурсів із вказівкою джерела витоку, прив’язані до електронної пошти облікові записи Skype, LinkedIn, Facebook, ICQ, Google, BlaBlaCar, Runtastik, резервні та пов’язані облікові записи, місто знаходження. Обліковий запис на runtastic.com свідчить, що його володілець, імовірніше за все, користується фітнес-браслетом, а відтак – існує ймовірність відслідкувати його переміщення.

Варто відзначити, що навіть без наявності спеціалізованих інструментів кваліфіковані зловмисники здатні зібрати суттєву інформацію про об’єкт атаки за незначний проміжок часу. Так, наприклад, знаючи електронну пошту на сервері Gmail або номер телефону, прив’язаний до такої пошти, можливо дізнатися GAIA ID (Google user ID), знання якого за певних обставин може допомогти зібрати інформацію про об’єкт атаки (рис. 13).

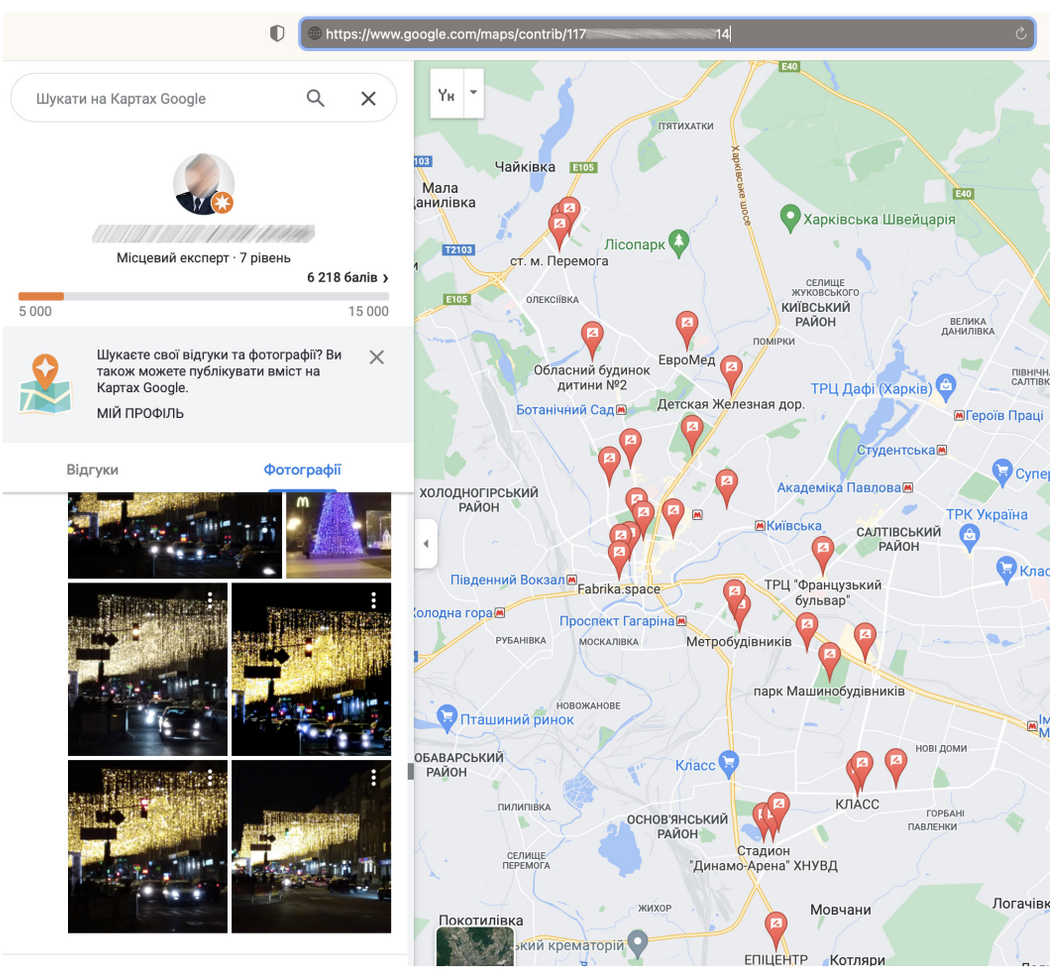


Рис. 13. Виведення карти з відмітками користувача за його GAIA ID

Потрібно наголосити, що OSINT не є самодостатнім інструментом. Тому під час здійснення атаки зловмисники застосовують пошук інформації з відкритих джерел разом із іншими техніками соціальної інженерії.

Ще однією технікою соціальної інженерії є **претекстинг.** Він передбачає як раз попереднє збирання інформації про жертву з відкритих джерел для того, щоб потім представитися жертві особою з певними повноваженнями та стимулювати її виконати дії, вигідні зловмисникам. Прикладом такого виду атаки може слугувати ситуація, коли особа намагається влаштуватися на роботу до правоохоронних органів. Зловмисник, довідавшись про це, вступає в контакт з кандидатом на посаду та представляється керівником певного рівня, від якого може залежати рішення про працевлаштування. Надалі атакуючий намагається, користуючись своїми «повноваженнями», маніпулювати жертвою. Під час здійснення претекстингу застосовується такий інструмент, як *імперсонація,* в межах якої зловмисник може використовувати фізичне маскування типу уніформи, гриму, документів прикриття, створення легенди тощо.

Для набуття даних іншої особи в сучасних умовах нерідко застосовуються засоби штучного інтелекту, які дозволяють створити реалістичні фейкові зображення (рис. 14), відео, підробити голос атакуючого тощо.

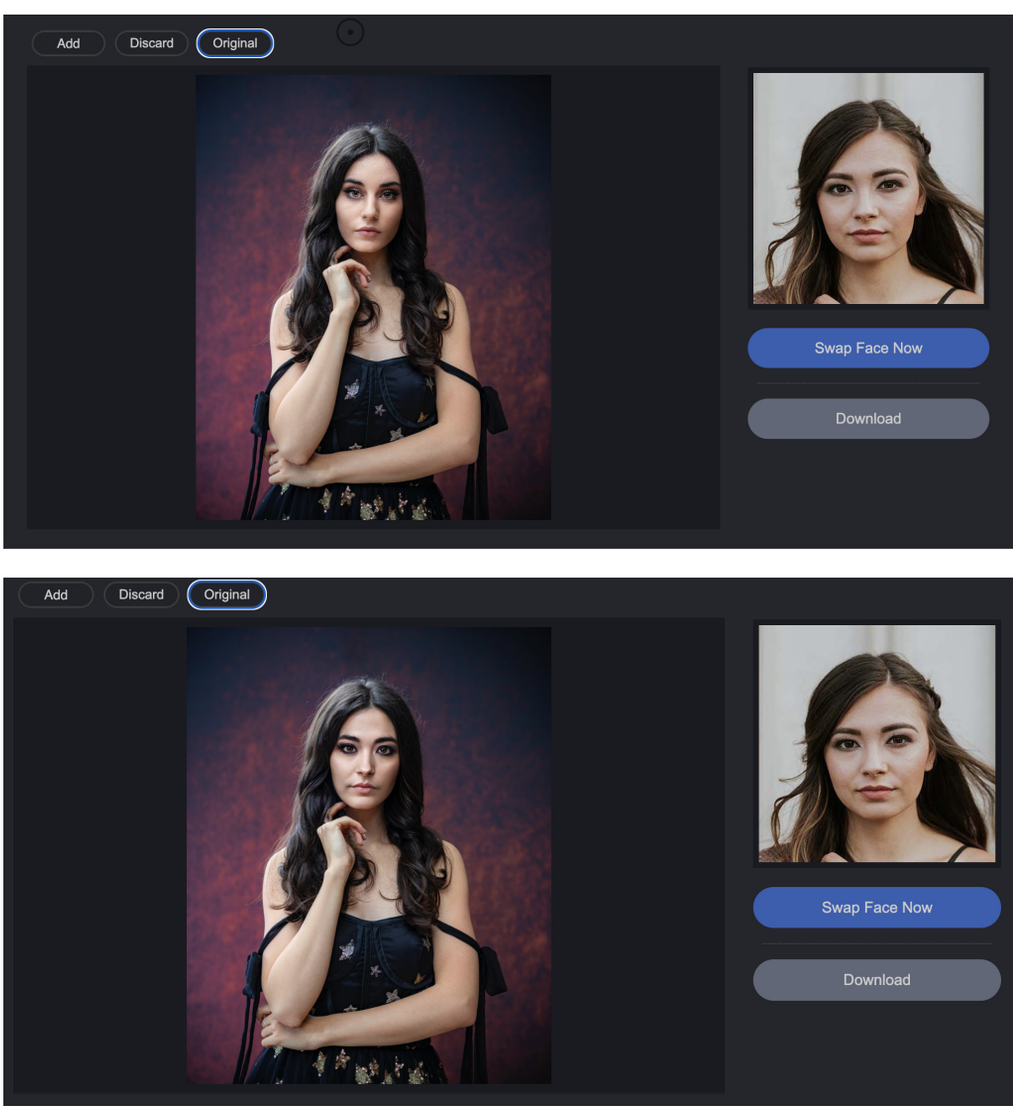


Рис. 14. Заміна обличчя особи (https://unsplash.com/photos/QK_NtQtmL8M) за допомогою сервісу faceswapper.ai

Певний сценарій атаки з використанням соціальної інженерії може реалізовуватися без контакту з фізичними особами, як, зокрема, в техніці **«дорожнє яблуко».** У межах цього методу здійснюється підкидання співробітнику фізичного носія інформації зі шкідливим програмним забезпеченням. Носій може мати певний логотип чи напис, що викличе інтерес, на кшталт «фото ню [ПРІЗВИЩЕ_ПРАЦІВНИКА]» тощо. Щойно співробітник вставить такий носій у комп'ютер, запуститься шкідливий код, який виконуватиме завдання, запрограмовані зловмисником.

Серед небезпечного виду носіїв, які можуть використовуватися в такого виду атаках, слід назвати флеш-накопичувач Rubber Ducky (рис. 15), який під час приєднання до комп'ютера визначається як клавіатура, а скрипт, записаний на такій флешці, виконується на комп'ютері жертви.

Рис. 15. USB Rubber Ducky в упаковці

Продовжуючи цикл популярних технік соціальної інженерії, слід згадати про зворотну соціальну інженерію. За сценарієм такої атаки, жертва повинна сама зв'язатися із зловмисником та надати йому потрібні дані. Прикладом подібної атаки може слугувати попереднє повідомлення поштою або телефоном користувача про зміну контактних даних провайдера електронних комунікацій. У подальшому щодо жертви може бути зімітовано «несправність Інтернету» для того, щоб користувач, згадавши, що йому нещодавно надходило повідомлення про зміну контактних даних, сам вийшов на зв'язок з атакуючим. У подальшому зловмисник інструктуватиме жертву, що потрібно зробити для «усунення несправності».

Зворотна соціальна інженерія може бути не тільки цільовою, а й розрахованою на масову аудиторію. Так, свого часу в Україні розсилали підроблені квитанції про комунальні платежі (https://glavred.info/stolica/328199-kiev-navodnili-falshivye-kvitancii-zhkh-kommunalshchiki-rasskazali-kak-vernut-dengi.html). Оплативши відповідну квитанцію, споживачі, по суті, переказували кошти на рахунки шахраїв (рис. 16).

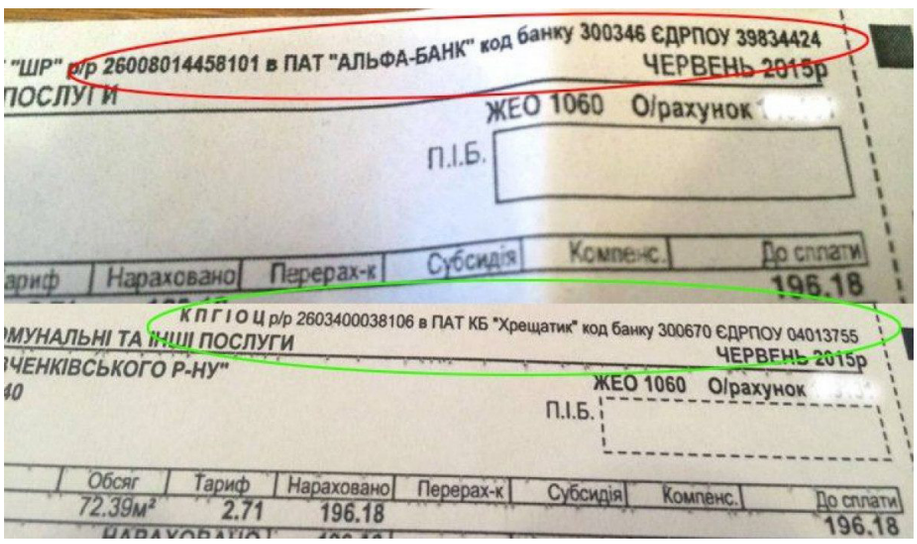


Рис. 16. Зверху – підроблена квитанція, знизу – справжня

Подібні схеми реалізуються шахраями і за кордоном. Так, у США у травні 2023 року була виявлена схема (https://www.kget.com/news/state-news/san-francisco-parking-ticket-scammers-issue-fake-tickets-set-up-fake-payment-site/), в межах якої зловмисники підкладали під двірники автомобілів квитанції для оплати паркування, які відрізнялися від справжніх реквізитами для оплати у QR-коді (рис. 17).

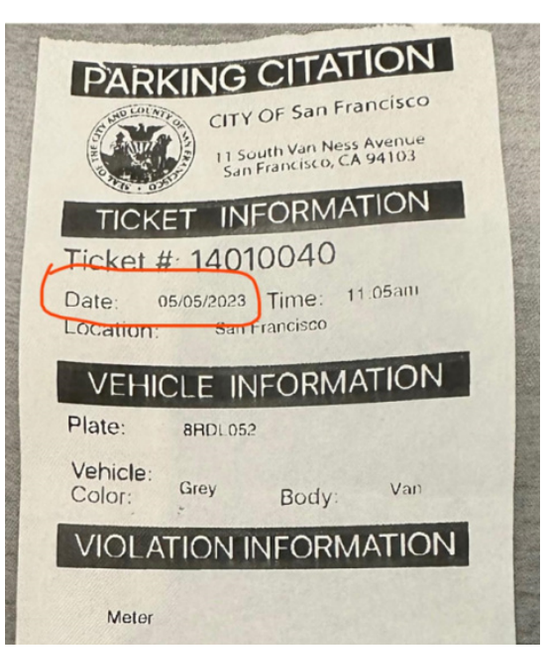


Рис. 17. Підроблена квитанція за паркування

Виявити шахрайство вдалося завдяки тому, що атакуючі вказували у квитанції дату, яка ще не настала.

Крім вже наведених технік, варто також згадати банальне підглядання та підслуховування, аналіз сміття тощо. Взагалі, такі схеми постійно удосконалюються зловмисниками, тому для свого убезпечення користувачам слід дотримуватися базових правил кібергігієни щодо безпечного поводження у кіберсфері. Частина таких правил наведена у висновках.

Висновки

Про застосування щодо користувача технік соціальної інженерії може свідчити:

- надходження нетипового листа з дивним вмістом;
- збурення емоцій відповідним повідомленням або серією повідомлень;
- короткий термін, протягом якого слід надати відповідь на повідомлення;
- зміст повідомлення виглядає надто привабливим, аби бути правдою;
- пропозиція допомоги, яку не просили;
- відправник не може підтвердити особу.

Методи протидії соціальній інженерії:

1. Не довіряйте «підозрілим» повідомленням та предметам.
2. Підтверджуйте особу.
3. Утилізуйте сміття належним чином.
4. Навчіться розрізняти працівників.
5. Не робіть компрометуючі фотознімки та відеозаписи.
6. Перевіряйте інформацію з різних джерел.

Як програмний інструментарій протидії соціальній інженерії в частині фішингу можуть бути запропоновані вітчизняна розробка Ukrainian Malicious URL Blocklist (https://github.com/braveinnovators/url-blocklist) та зарубіжна система, заснована на використанні штучного інтелекту для аналізу сайтів, – CheckPhish (https://checkphish.ai/).