МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ФЕДОРИШИН ОЛЕКСАНДР ОЛЕГОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
прикладної математики та
кібербезпеки,
д – р філософії з математики,
_____ А.В.Луценко
«__»_____20__ р.

МЕТОДИ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ ДЛЯ ПЕРЕСІЧНОГО КОРИСТУВАЧА ІНТЕРНЕТУ

Спеціальність 125 Кібербезпека
Кваліфікаційна (бакалаврська) робота

Керівник:
Д-р техн. наук, професор,
професор кафедри прикладної
математики та кібербезпеки
Крижановський В.Г.

Оцінка:___/___/_____
(бали за шкалою ЄКТС/за
національною шкалою)
Голова ЕК:_____
(підпис)

Вінниця - 2024

АНОТАЦІЯ

Федоришин О.О. Методи протидії соціальній інженерії для пересічного користувача інтернету. Робота присвячена актуальній проблемі захисту від соціальної інженерії в Інтернеті. В роботі розглядаються основні поняття, типи атак та методи соціальної інженерії, аналізуються популярні сценарії атак, а також пропонуються практичні поради щодо захисту від небезпеки. Дослідження проводилось шляхом опитування та практичного тестування групи людей різного віку та професій. Результати тестування продемонстрували, що після короткої навчальної програми рівень обізнаності щодо соціальної інженерії у учасників суттєво покращився.

Ключові слова: соціальна інженерія, кібербезпека, фішинг, смішинг, вішинг, кіберзлочинність, інтернет-безпека, навчання користувачів, обізнаність.

ANNOTATION

Fedoryshyn O.O. Methods of countering social engineering for the average Internet user This work is dedicated to the current issue of protecting against social engineering on the Internet. The paper discusses the basic concepts, types of attacks, and methods of social engineering, analyzes popular attack scenarios, and offers practical advice on how to protect yourself from these threats. The research was conducted through a survey and practical testing of a group of people of different ages and professions. The results of the testing showed that after a short training program, the level of awareness of social engineering among participants significantly improved.

Keywords: social engineering, cybersecurity, phishing, smishing, vishing, cybercrime, internet security, user education, awareness.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

МСІ - Методи соціальної інженерії (Methods of Social Engineering)

КДБ - Комітет державної безпеки (Committee for State Security, USSR)

ЦРУ - Центральне розвідувальне управління (Central Intelligence Agency, USA)

ІС3 - Інтернет-кримінальний центр (Internet Crime Complaint Center)

SET - Social-Engineer Toolkit

SEDF - Social Engineering Defensive Framework

VPN - Virtual Private Network

2FA - Two-Factor Authentication

DNS - Domain Name System

IP - Internet Protocol

ЕК-джерельні - Експертні джерела (Expert Sources)

ЛГ-джерельні - Легковажні джерела (Careless Sources)

КН-джерельні - Контактні джерела (Contact Sources)

ВП-джерельні - Випадкові джерела (Random Sources)

В-доступ - Відкритий доступ (Open Access)

К-доступ - Конфіденційний доступ (Confidential Access)

С-доступ - Секретний доступ (Secret Access)

BEC - Business E-mail Compromise

КЦД-дії - Комбіновані дії (Combined Actions)

Т-віддалені - Телефонні віддалені (Telephone-based Remote)

МТ-віддалені - Мережеві віддалені (Network-based Remote)

К-дієві - Конфіденційність-дієві (Confidentiality-Oriented)

Ц-дієві - Цілісність-дієві (Integrity-Oriented)

Д-дієві - Доступність-дієві (Availability-Oriented)

Мономономні - Одноосібна атака на одну особу (Single attacker, single target)

Полімономні - Багатоосібна атака на одну особу (Multiple attackers, single target)

Монополічні - Одноосібна атака на багатьох осіб (Single attacker, multiple targets)

Поліполічні - Багатоосібна атака на багатьох осіб (Multiple attackers, multiple targets)

Прості MCI - Прості методи соціальної інженерії (Simple Social Engineering Methods)

Складні MCI - Складні методи соціальної інженерії (Complex Social Engineering Methods)

Системні MCI - Системні методи соціальної інженерії (Systemic Social Engineering Methods)

ВСТУП

Актуальність теми дослідження

В сучасному цифровому віці, коли Інтернет став не лише джерелом інформації, а й платформою для взаємодії та спілкування, питання захисту особистої інформації та відвертості важливіше, ніж будь-коли. Соціальна інженерія, або маніпулювання людськими діями та вчинками, стає все поширенішою загрозою для безпеки та конфіденційності користувачів Інтернету.

Мета – дослідити рівень знань користувачів мережі інтернет та ознайомити їх з соціальною інженерією.

Завдання дослідження:

1. Дослідження соціальної інженерії.
2. Визначення понять та видів соціальної інженерії.
3. Аналіз сценаріїв атак на базі соціальної інженерії.
4. Виявлення методів соціальної інженерії та методів протидії.
5. Дослідження та покращення рівня знань пересічного користувача.

Об’єкт дослідження – соціальна інженерія та методи протидії.

РОЗДІЛ 1.
СОЦІАЛЬНА ІНЖЕНЕРІЯ

1.1. Визначення поняття соціальної інженерії

Сьогодні практично кожна людина використовує комп'ютер і має хоча б один обліковий запис у соціальних мережах. Соціальні мережі приваблюють людей, оскільки сучасний світ побудований на комунікаціях, обміні інформацією та нових знайомствах. Деякі люди створюють для себе віртуальний світ, де можуть бути безстрашними та популярними, уникаючи реальності. Однією з найбільш актуальних і складних проблем сьогодення є питання безпеки персональних даних.

Нині як ніколи важливо свідомо використовувати інформаційні потоки та ресурси, оскільки вони можуть впливати на свідомість окремих осіб, груп людей або всього суспільства. Проте, суспільство, яке активно використовує телекомунікації та глобальні комп'ютерні мережі, не завжди може передбачити всі можливості та ризики, пов'язані з цими технологіями.

Термін "соціальна інженерія" точно відображає суть поняття, яке об'єднує підходи та методи, спрямовані на цілеспрямовану зміну соціальних процесів та організаційних структур, що визначають поведінку людей. Використовуючи психологічні особливості людей, такі як зацікавленість, довіра та звички, соціальна інженерія дозволяє контролювати їх поведінку.

Інформаційна війна сьогодні розглядається як процес маніпулювання інформацією або інформаційними потоками, яким довіряє об'єкт впливу (без його відома), щоб змусити його приймати рішення, що суперечать його інтересам. Соціальна інженерія також є формою маніпуляції інформацією, спрямованою на виконання певних дій або розголошення конфіденційної інформації, що призводить до зміни цілісності даних. Таким чином, інформаційна війна включає деструктивні методи та засоби соціальної інженерії.

Аналіз наукових джерел показує, що поняття деструктивної соціальної інженерії відсутнє. На нашу думку, соціальна інженерія - це наука, яка досліджує людську природу та створює соціальне середовище на мікро- та макрорівнях для вирішення соціальних проблем та адаптації соціальних систем до змінних умов. Однак, якщо соціальна інженерія використовується для маніпуляції інформацією деструктивними методами, вона стає деструктивною соціальною інженерією.

Варто зазначити, що сьогодні дослідники та фахівці, особливо в галузі кібербезпеки, часто використовують термін "соціальний інжиніринг", хоча інжиніринг (англ. engineering) означає набір методів для проектування діяльності компанії чи підприємства. Соціальний інжиніринг - це метод несанкціонованого доступу до інформації або систем без використання технічних засобів, спрямований на отримання доступу до захищених систем з метою крадіжки інформації, паролів тощо. Об'єктом атаки є людина, що і робить цей метод деструктивним у вузькому розумінні.

Мета деструктивної соціальної інженерії полягає в тому, щоб змусити особу або групу виконувати дії, які вони за звичайних умов не зробили б. Це може включати розголошення конфіденційної інформації, відвідування небезпечних сайтів, виконання дій за сумнівними посиланнями або використання програм, які крадуть особисті дані.

Деструктивна соціальна інженерія є методом керування діями людей без використання технічних засобів, який базується на слабкостях людського фактору. Вона використовує некомпетентність, непрофесіоналізм або недбалість персоналу для доступу до інформації, демонструючи, що особистість є найслабшою ланкою в системі. З іншого боку, деструктивна соціальна інженерія часто розглядається як незаконний метод отримання інформації, і її активно використовують в Інтернеті для доступу до цінної або конфіденційної інформації. Методи несанкціонованого доступу до інформації можна поділити на ті, що використовують деструктивну соціальну інженерію, і ті, що існують без неї.

Основоположником деструктивної соціальної інженерії є Кевін Мітник, який популяризував цей метод на початку XXI століття. Колишній хакер, Мітник здійснював незаконне проникнення в різні бази даних і вважав, що людський фактор є найвразливішою частиною будь-якої системи.

Методи деструктивної соціальної інженерії були відомі давно, але їх важливість і особливості застосування показав саме Кевін Мітник. Як зазначає Лаптєв С. О., соціальна інженерія (деструктивна) є нетехнічним типом стратегії кібератак, що базується на взаємодії між людьми та маніпуляціях, щоб людина порушила стандартні правила кібербезпеки. Ця тактика не вимагає від зловмисника технічних знань, що робить її привабливою для шахраїв. Важливо підготуватися, зібравши інформацію про жертву, щоб знати, як отримати потрібну інформацію.

Деструктивна соціальна інженерія ґрунтується на тому, що особистість або соціальна група є найслабшою ланкою будь-якої інформаційної системи. Злочинці, використовуючи деструктивний інформаційно-психологічний вплив, спрямовують свої дії на користувача як на найвразливіше місце в системі інформаційної безпеки. Основні напрями деструктивної соціальної інженерії включають:

- Несанкціонований доступ до персональних даних.
- Проникнення в інфраструктуру організації для дестабілізації основних вузлів інформаційної системи та її мережі.
- Загальна дестабілізація роботи організації та подальше руйнування її авторитету і структури.
- Фінансово-економічне шахрайство.
- Викрадення конфіденційної інформації.
- Отримання даних про перспективні плани і проекти організації.
- Отримання інформації про співробітників для їх подальшої дискредитації.

Сучасні кібершахраї та хакери використовують методи деструктивної соціальної інженерії, орієнтуючись на різні аспекти психології особистості. [1]

1.2. Статистика кіберзлочинів з використанням соціальної інженерії

Згідно з проведеними дослідженнями, можна визначити масштаб проблеми та оцінити наслідки для потенційних жертв. Ось деякі ключові статистичні дані щодо випадків застосування соціальної інженерії та втрат, яких зазнали її жертви:

- За даними звіту Verizon 2019 року про кібербезпеку, майже половина збитків від кіберзлочинності у 2019 році були спричинені компрометацією електронної пошти, що принесло шахраям 1,8 мільярда доларів США.
- У 2020 році IC3 повідомила про понад 240 000 індивідуальних жертв фішингу, яким було завдано збитків на суму понад 54 мільйони доларів США.

Соціальна інженерія завдає шкоди як приватному бізнесу, так і великим корпораціям. Однією з головних причин цього є те, що зловмисники, отримавши доступ до одного корпоративного аккаунту, можуть отримати доступ до всієї системи. Це включає конфіденційну інформацію, клієнтські бази даних, фінансові ресурси та інші важливі активи компанії. Такі атаки можуть призвести до значних втрат, пошкоджень та підриву довіри клієнтів і партнерів.

Ці статистичні дані підкреслюють серйозність проблеми соціальної інженерії та її вплив на корпоративний та особистий сектори[2].

1.3. Області застосування соціальної інженерії

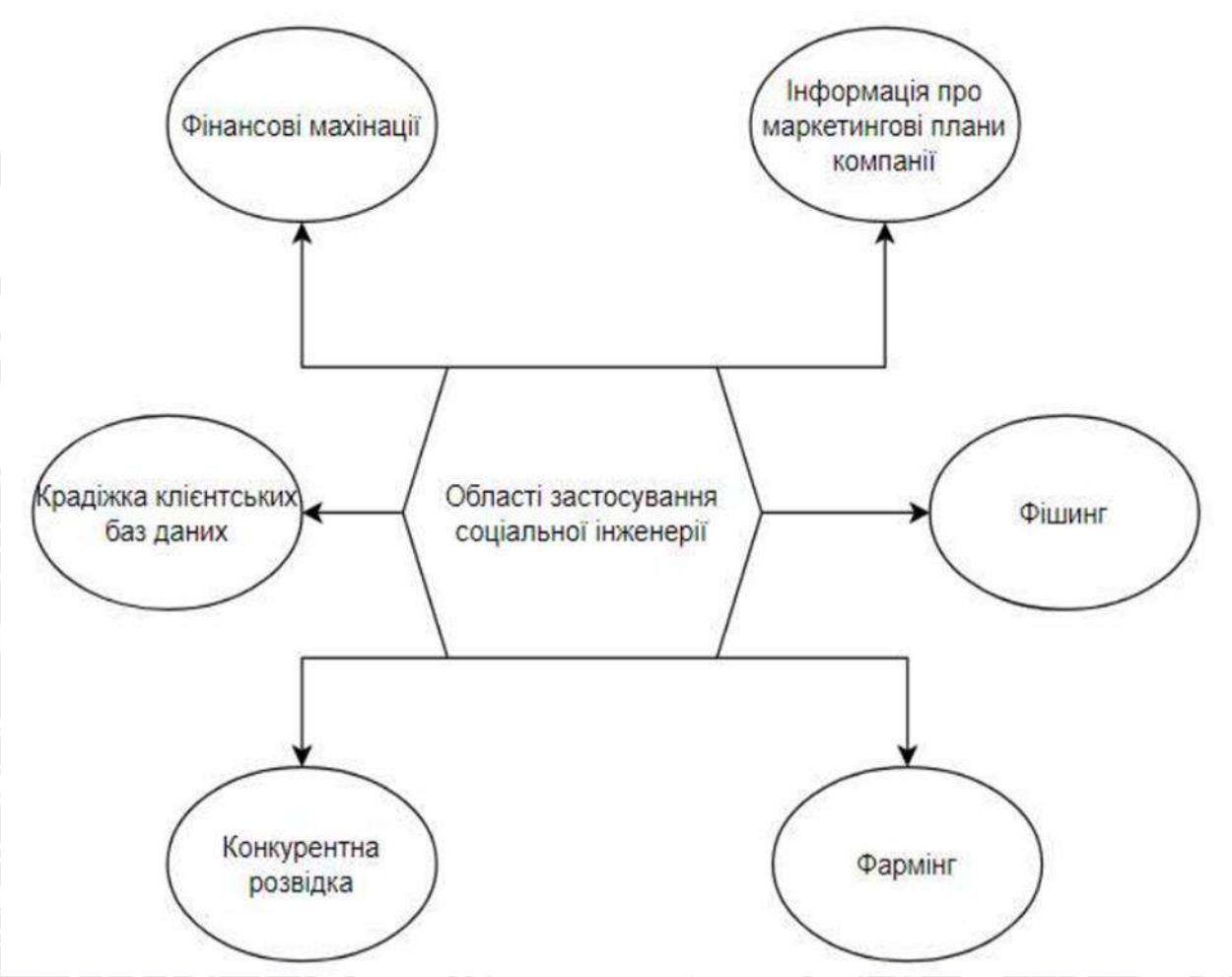


Рисунок 1.1. – Області застосування соціальної інженерії

Давайте розберемо більш детально кожний з них:

Фінансові махінації

Для ілюстрації цієї теми наведено приклад, описаний Кевіном Митником, про злочин, здійснений його колегою Стенлі Марком Ріфкіним. Суть в тому, що найбільший грабіж банку був здійснений без використання комп'ютера, а методами соціальної інженерії. Ріфкін мав контракт з банком, згідно з яким він відповідав за створення резервної системи даних на випадок збою основного комп'ютера. Його рівень доступу дозволяв спостерігати за роботою співробітників банку. Він швидко помітив, що відділ трансферних переведень

використовує числовий пароль, який змінюється щодня. Проте працівники телеграфного приміщення не дотримувалися інструкцій і записували пароль на папірцях, залишаючи їх на видному місці.

Ріфкін скористався цим недбальством. Під виглядом перевірки резервної системи він проник у телеграфне приміщення, знайшов пароль і запам'ятав його. Пізніше, використовуючи таксофон, він зателефонував у відділ трансферів, видав себе за працівника міжнародного відділу банку та замовив переведення 10 мільйонів доларів на рахунок у швейцарському банку, який він заздалегідь відкрив. Він назвав правильний пароль, але не знав внутрішнього паролю офісу. Не розгубившись, він зателефонував у інше відділення банку, знову видав себе за працівника, отримав потрібний код і підтвердив переведення коштів. У Швейцарії він зняв гроші з рахунку, придбав діаманти на всю суму та вивіз їх, сховавши у поясі.

Цей приклад демонструє, що у фінансовій сфері соціальна інженерія є дуже актуальною, оскільки банки є однією з найбільш захищених систем, і зламати їх технічними методами дуже складно. Використання соціальної інженерії дозволяє обійти високі технічні бар'єри з меншими витратами ресурсів.

Інформація про маркетингові плани компанії

Капіталістична модель торгівлі загалом побудована таким чином, що перший, хто закриває собою нішу певних потреб, незалежно від того, яким чином вона утворюється, має перевагу. Головне, що ринкове правило працює так, що перший гравець, навіть якщо його товар не ідеальний і гірший за конкурентів, які випустили свій продукт пізніше, буде домінуючим на ринку. Виправити цю ситуацію майже неможливо, адже домінуючий продукт приносить прибуток, який інвестується в розвиток продукту. Відповідно, більший бюджет означає кращий продукт. Тому абсолютно вирішальну роль грає першість на ринку і випередження конкурентів. Для випередження конкурентів потрібно знати про їхні плани. Проте інформацію про точні глобальні рамки маркетингових планів компанії знає дуже обмежена кількість осіб, тому відправити інформатора на

таку посаду практично неможливо. Тут на допомогу знову приходить соціальна інженерія.

Крадіжка клієнтських баз даних

Якщо розглядати крадіжки баз даних, то технічний канал для цього не завжди ефективний, адже ймовірно, що дані на сервері зашифровані. Тут набагато краще підходить соціальна інженерія. У більшості випадків інформацію перепродають самі працівники, адже рівень доступу до такої інформації відносно низький. Наприклад, системний адміністратор може образитися на керівництво і перед звільненням зробити копію бази даних на цифровий носій. Потім він може її продати за помірну суму або навіть викласти у відкритий доступ, якщо його образа надто сильна.

Або ж, коли системний адміністратор у відрядженні, з'являється його "друг", який налагоджує базу даних, яка несподівано перестала працювати. І хоча база даних дійсно починає працювати краще, вона вже працює в іншому місці. Ці приклади стосуються не лише малих компаній.

Багато хто недооцінює цінність інформації, отриманої через бази даних. Для кого вони потрібні і як використовуються? Це дуже широкий спектр людей. У незаконному світі бази даних потрібні всім — від квартирних злодіїв та авто викрадачів до великих акул, які займаються рейдерськими захопленнями фірм.

У цивільному житті сфера застосування баз даних також велика. Будь-який бізнесмен хоче контролювати розвиток своїх конкурентів, і для цього найкраще підходить база їх клієнтів. Під час укладання договорів між фірмами також відбувається взаємна контррозвідка, де будь-яка інформація є цінною.

Фішинг

Класичне визначення фішингу: «Фішинг (від англ. fishing — риболовля) — вид шахрайства, метою якого є виманювання у користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів». Фішинг є одним з найпоширеніших видів соціальної інженерії, що передбачає вивідування інформації для доступу до

банківських рахунків. Він поширений у країнах з популярним інтернет-банкінгом. Найчастіше фішери використовують підроблені електронні листи від імені банку з проханням підтвердити пароль або повідомлення про переведення грошей. [8]

Суть фішингу полягає у змушуванні користувача надати секретну інформацію (банківські дані, дані кредитних карток). Жертва робить це добровільно, оскільки фішери добре володіють психологічними прийомами.

Основні види фішингу:

- Поштовий фішинг
- Онлайн фішинг
- Комбінований фішинг

Першим з'явився поштовий фішинг, відомий з 1996 року. У цьому виді шахрайства жертві надсилається електронний лист з проханням надати конфіденційні дані. Наприклад, лист може надійти від імені інтернет-провайдера з проханням повідомити логін і пароль через технічні проблеми. Відомий випадок, коли клієнти одного американського банку отримали повідомлення про велике перерахування на їх рахунок з проханням підтвердити отримання через надане посилання. Багато хто не зміг протистояти жадібності, і кілька тисяч клієнтів стали жертвами фішинг-атаки.

Онлайн фішинг передбачає створення шахраями копій відомих сайтів з дуже схожими доменними іменами і дизайном. Жертва, перебуваючи на такому підробленому сайті, може завантажити вірус під виглядом потрібного файлу або здійснити покупку, передавши свої платіжні дані. Шахраї використовують неуважність користувачів, які підтверджують переведення коштів без перевірки деталей.

Комбінований фішинг об'єднує два попередні види: поштовий і онлайн фішинг. Його поява зумовлена тим, що класичні методи стали менш ефективними, оскільки користувачі стали більш обізнаними в галузі інформаційної безпеки. Фішери створюють підроблений сайт, а потім

відправляють листи з проханням зайти на цей сайт. Це потужний психологічний хід, завдяки якому комбінований фішинг швидко набув поширення.

Справа в тому, що користувачі стали обережнішими щодо невідомих сайтів і рідко вводять свої паролі без вагомої причини. Але в комбінованому фішингу настороженість знімається, оскільки в листі не просять надати конфіденційні дані, а просто перейти на сайт і виконати необхідні дії. Дизайн сайту провокує користувача до певних дій.

Фішери використовують зв'язок з певними подіями для своїх атак. Наприклад, у день народження користувач отримує вітальну листівку від "банку", який пропонує зайти на сайт і отримати $500, введши необхідну інформацію. Інший приклад — після великих терактів або стихійних лих різні організації просять допомогу, і фішери використовують ці події, просячи перейти на підроблений сайт, зареєструватися і перерахувати гроші до фонду допомоги постраждалим.

Фармінг

Більш небезпечним видом шахрайства, ніж фішинг, є фармінг. Останнім часом у мережі використовують таке визначення: «Фармінг (англ. pharming) — це процедура таємного перенаправлення жертви на хибну IP-адресу». Фармінг полягає у зміні DNS-адрес, щоб сторінки, які відвідує користувач, були не оригінальними, а фішинг-сторінками.

Оскільки фармінг автоматично перенаправляє користувачів на фальшиві сайти, він є набагато небезпечнішим за фішинг. Новий метод крадіжки даних не вимагає надсилання листів потенційним жертвам і їх відповіді на них, що робить його більш витонченим і технічно складнішим за фішинг. У випадку фармінгу у користувача практично немає підстав для підозри: ніхто не надсилав листів і не просив заходити на сайт. Користувач самостійно вирішує зайти на сайт банку, але потрапляє на підроблений, а не на оригінальний сайт.[3]

1.4. Види соціальної інженерії

Фішинг – є однією з найпоширеніших форм атак соціальної інженерії. У цьому типі атаки кіберзлочинець надсилає електронний лист або текст, замаскований під легітимний із джерела, якому довіряють. Мета полягає в тому, щоб обманом змусити одержувача надати інформацію або перейти за посиланням. Після цього зловмисник може отримати доступ до даних чи грошей або запустити шкідливе програмне забезпечення на пристрої одержувача.

Розберемо декілька підвидів фішингу:

Цільовий фішинг (spear phishing) – це ще одна цілеспрямована форма фішингу. У цьому типі атаки зловмисник обирає конкретних осіб або організації, адаптуючи повідомлення до типового повідомлення, яке може отримати жертва, і використовуючи назви посад або контакти, які надають йому легітимності. Повідомлення просить одержувачів змінити пароль і перенаправляє їх на сторінку, яка збирає їхні облікові дані.

Вейлінг (whaling) - більш масштабна форма фішингу - націлена на високопоставлених осіб, які мають доступ до більш привілейованих або цінних даних, таких як керівники компаній, фінансові директори (CFO) або урядовці.

SMS-фішинг, смішинг (smishing) поєднує в собі «SMS» і «фішинг», застосовуючи текстові повідомлення для проведення атаки.

Голосовий фішинг, вішинг (vishing) складається з комбінації слів «voice» та «фішинг». У цьому типі атак використовуються телефонні дзвінки для отримання конфіденційних даних цілі. [4]

Фішинг електронною поштою:

- Опис: Зловмисник надсилає електронні листи, що виглядають як офіційні повідомлення від компаній, банків чи інших організацій, із запитом надати конфіденційну інформацію або виконати певні дії.

- Приклад: Листи, що маскуються під повідомлення від банків, з проханням оновити пароль або підтвердити ідентифікаційні дані.

- Мета: Отримання доступу до облікових записів, паролів або інших конфіденційних даних.

Інші види атак:

Watering hole – це метод «водопою», який поєднує в собі соціальну інженерію та хакерство. Зловмисник зламує веб-сайт, який часто відвідують і якому довіряють особи, на яких спрямована атака. Потім зловмисник заражає веб-сайт, якому довіряють, шкідливим програмним забезпеченням або вставляє посилання, на які користувачі переходять під час відвідування веб-сайту. [9]

Бейтінг (baiting) – це різновид соціальної інженерії, коли жертву заманюють до надання конфіденційної інформації або облікових даних, обіцяючи щось цінне безкоштовно. Наприклад, жертва отримує електронного листа, в якому обіцяють подарункову картку, безкоштовне завантаження ігор, музики чи фільмів, якщо вона перейде за посиланням для проходження опитування. Посилання може перенаправляти на підроблену сторінку входу в Office 365, яка перехоплює адресу електронної пошти та пароль і надсилає їх зловмиснику.[10]

Претекстінг (pretexting) – створення певної ситуації, що спонукатиме ціль видати зловмиснику свою чутливу інформацію. За допомогою претексту зловмисник, використовуючи соціальну інженерію, обманює когось, щоб отримати доступ до даних. У повідомленнях, які нібито надходять від колеги, правоохоронних органів або фінансових установ, зловмисник часто просить підтвердити приватну інформацію, нібито для того, щоб працівник або посадова особа могла виконати важливе завдання. [11]

Послуга за послугу (Quid Pro Quo) - це практика соціальної інженерії, коли зловмисник вдає, що пропонує щось в обмін на допомогу жертви. При цьому типі соціальної інженерії зловмисник просить інформацію, щоб надати жертві допомогу, наприклад, у сфері інформаційних технологій (IT). Потім зловмисник використовує цю інформацію, щоб отримати доступ до приватної інформації або встановити шкідливе програмне забезпечення.[12]

«Медова пастка» (honeytrap) – це різновид соціальної інженерії, в якому зловмисники створюють фальшиві профілі у соціальних мережах і на сайтах знайомств з викраденими фото, аби привабити потенційні цілі. Видаючи себе за людину, з якою одержувач може мати стосунки, зловмисник використовує «медову пастку», щоб заманити цільову особу. Імітуючи зацікавленість у стосунках, зловмисник обманом змушує людину поділитися інформацією.

Відлякувальні програми (scareware) - зловмисники використовують програми-лякалки, щоб змусити користувача повірити в те, що його пристрій заражений шкідливим програмним забезпеченням або незаконним контентом. Потім зловмисник пропонує вирішення «проблеми», яке передбачає несвідоме завантаження справжнього шкідливого програмного забезпечення або придбання непотрібних послуг. [13]

Компрометація корпоративної електронної пошти (business e-mail compromise, BEC) – це просунутий вид кібератак, націлений на підприємства та організації. До прикладу, він може включати обман співробітника або керівника для виконання грошового переказу, або ж злам електронної пошти працівника чи управлінця для відправки листів зі шкідливим кодом контактам компанії (клієнтам, постачальникам тощо).

Висновки до розділу 1

Дослідження всебічно аналізує соціальну інженерію в контексті кібербезпеки, підкреслюючи ключову роль людського фактора як найслабшої ланки в інформаційних системах. Історичний аналіз дозволяє порівняти сучасну соціальну інженерію з історичними прикладами маніпуляцій та обману, що демонструє її еволюцію та актуальність.

Визначення сутності та особливостей соціальної інженерії показує її відмінність від традиційних хакерських методів та вказує на її потенційно деструктивний характер. Статистичні дані підтверджують значний вплив атак соціальної інженерії на особисті та корпоративні сектори, що демонструє

реальну загрозу. Розгляд різноманітних сфер застосування соціальної інженерії, включаючи фінансові махінації, крадіжку інформації та цільові атаки на корпоративні таємниці, підкреслює її широкий спектр використання.

Класифікація різних видів атак, таких як фішинг, смішинг, вішинг та інші, допомагає краще зрозуміти різноманітність і складність цієї загрози в сучасному цифровому світі. Це сприяє розробці ефективних заходів протидії.

Таким чином, дослідження забезпечує глибоке розуміння поняття, історії, застосування та видів соціальної інженерії, створюючи міцну основу для подальшого аналізу сценаріїв атак та розробки стратегій їх запобігання.

РОЗДІЛ 2.
АНАЛІЗ СЦЕНАРІЇВ РЕАЛІЗАЦІЇ АТАК НА БАЗІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1. Методи соціального інженерії

З давніх-давен людство використовувало психологічні методи маніпуляції в тій чи іншій формі. Яскравим прикладом цього є "нічні демони" Японії, ніндзя, які майстерно володіли мистецтвом обману та гіпнозу. Ще в Римській імперії цінували людей, які могли ввести співрозмовника в оману, змусивши його повірити в те, чого не існує. Видаючи себе за представників влади, вони за допомогою лестощів, переконливих аргументів або дезінформації вели переговори та вирішували питання не лише особистого, а й державного значення.

У шпигунському середовищі (розвідці) соціальна інженерія завжди була одним із головних інструментів.Наприклад, агенти КДБ СРСР та ЦРУ США, видаючи себе за інших людей, могли викрасти державні таємниці.

Таким чином, протягом всієї історії підтверджується твердження, що найслабшою ланкою будь-якої системи безпеки є людина.

В сучасному розумінні термін "соціальна інженерія" з'явився порівняно недавно. Його автором є Кевін Мітник, який стверджував, що набагато простіше дізнатися пароль людини, ніж зламати всю систему цілком.[11]

Зважаючи на те, що понад 70% випадків порушення інформаційної безпеки пов'язані з людським фактором. К.Мітник запропонував використовувати методи соціальної інженерії для:

• **Збору інформації про об'єкт атаки (розвідка):** вивчення інтересів та особливостей поведінки потенційної жертви, онлайн-спільнот, які вона відвідує, та імен, під якими вона з'являється в Інтернеті. Це може бути досягнуто шляхом спілкування з нею або її оточенням у месенджерах, наприклад ICQ.

• **Отримання конфіденційної інформації про об'єкт атаки (розвідка) або** інформації, яка цікавить зловмисника, наприклад номерів телефонів потенційної жертви, адреси її реєстрації/проживання, реального імені та прізвища тощо. Це може бути досягнуто шляхом встановлення контакту з нею та/або введення її в оману.

• **Отримання інформації про об'єкт атаки (розвідка),** необхідної для отримання несанкціонованого доступу до системи, наприклад пароля, серії та номера паспорта потенційної жертви та інших відомостей про неї. Це може бути досягнуто шляхом вступу в довіру до обраної жертви.

• **Примушення об'єкта атаки (розвідка) до дій, необхідних зловмиснику**, шляхом нав'язування їй нової моделі поведінки.

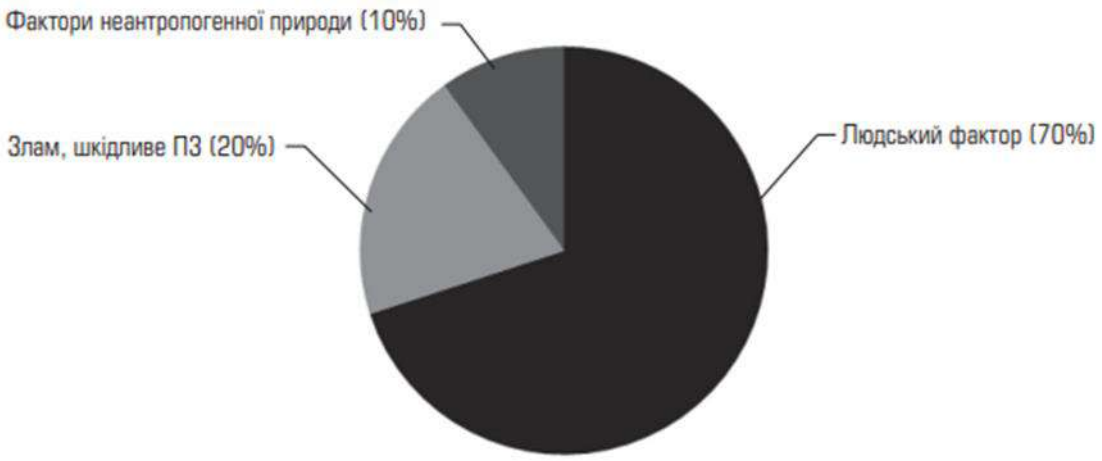


Рисунок 2.1. – Діаграма причинності соціальної інженерії

У цій роботі розглядаються сучасні методи соціальної інженерії (СІ), які використовуються для крадіжки інформації з підприємств. Ці методи ґрунтуються на психологічних факторах, таких як стрес, корисливі інтереси та прагнення до самоствердження, які можуть спонукати співробітників порушувати правила безпеки.

Рисунок 2.2. – Сфери застосування СІ

Групи ризику:

Методи СІ спрямовані на наступні групи осіб:

• **Керівники та начальники відділів:** Ці особи мають доступ до конфіденційної інформації та можуть впливати на інших співробітників.

• **Персонал відділу кадрів, секретарі та особисті помічники:** Ці особи мають доступ до особистої інформації співробітників та можуть використовуватися для її крадіжки.

• **Нові та тимчасові співробітники:** Ці особи можуть бути не знайомі з правилами безпеки або мати до них негативне ставлення.

Методи MCI:

Соціоінженери використовують різні методи для крадіжки інформації, які можна поділити на наступні категорії:

• *За взаємодією з політикою безпеки:* Ці методи можуть використовуватися для обходу або порушення правил безпеки.

• *За ініціалізацією та маніпулюванням:* Ці методи можуть використовуватися для того, щоб змусити співробітників розкрити конфіденційну інформацію або виконати дії, які можуть призвести до витоку інформації.

• *За порушенням характеристик безпеки:* Ці методи можуть використовуватися для того, щоб виявити та експлуатувати слабкі місця в системах безпеки.

• *За реляційними ознаками:* Ці методи можуть використовуватися для того, щоб визначити та атакувати співробітників, які є більш схильними до ризику.

• *За ступенем важкості:* Ці методи можуть варіюватися від простих до складних.

• *За типом джерела:* Ці методи можуть використовувати різні джерела інформації, такі як соціальні мережі,веб-сайти та електронні листи.

• *За типом доступу:* Ці методи можуть використовуватися для отримання доступу до різних типів інформації,таких як паролі, файли та дані.

Використання технічних засобів:

Методи MCI можуть використовуватися як самостійно, так і в поєднанні з технічними засобами, такими як програмні закладки та шпигунські програми.

Типи MCI:

Залежно від того, як вони використовуються щодо політики безпеки, методи СІ можна поділити на два типи:

• Постполітизаційні МСІ: Ці методи використовують недоліки в існуючій політиці безпеки.

• Деполітизаційні МСІ: Ці методи не ґрунтуються на жодних правилах безпеки.

Приклади недоліків політики безпеки:

• Неправильно побудовані правила розмежування доступу

• Використання програмних і апаратних засобів із недостатнім рівнем захисту

• Прорахунки у блокуванні каналів витоку інформації з обмеженим доступом

• Заборона видачі імен та телефонів персоналу джерелу (яке здійснює запит), вірогідно не ідентифікованому. [14]

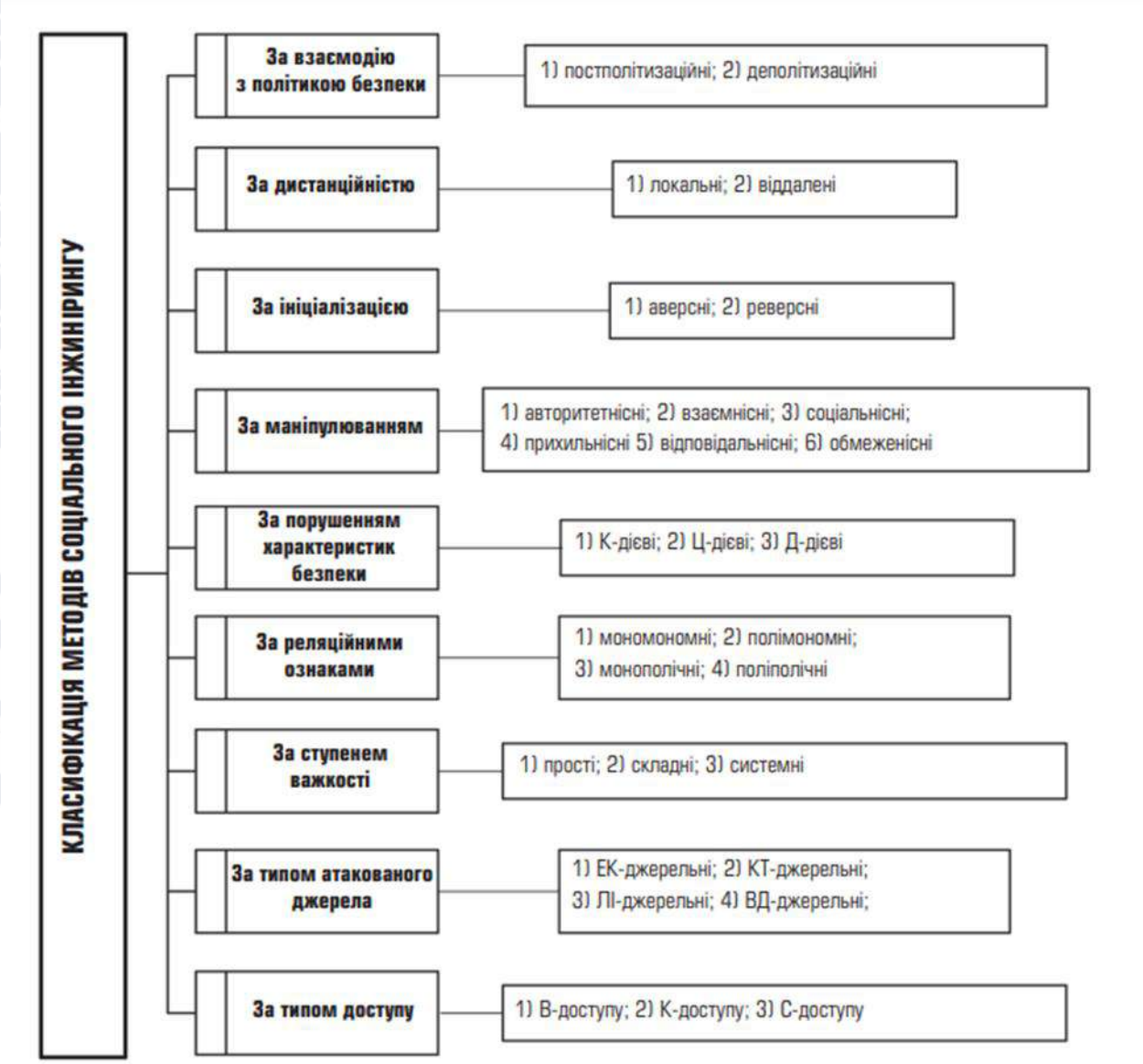


Рисунок 2.3. – Класифікація методів соціального інжинірингу

Деполітизаційні атаки ґрунтуються на помилках і недбальстві, допущених виконавцями під час реалізації заходів з безпеки організації. Це зазвичай пов'язано з людським фактором, що проявляється у разі адміністративної підтримки, коректності виконання захисних функцій та своєчасного реагування на нестандартні ситуації (коли виникають обставини, не описані у політиці безпеки, і працівники реагують на них непередбачувано). Прикладом нестандартної ситуації може бути неправильна реакція персоналу на запит керівництва компанії щодо доступу до секретної інформації.

Залежно від дистанції, соціотехнічні інтервенції (MCI) поділяються на локальні та віддалені. **Локальні MCI** здійснюються через безпосереднє індивідуальне спілкування соціотехніка з жертвою, наприклад, коли соціотехнік представляється як співробітник, постачальник або працівник партнерської компанії та просить про допомогу.

Віддалені MCI поділяються на Т- та МТ-віддалені. Віддалені MCI здійснюються за допомогою засобів комунікації (телефон, факс, електронна пошта, віртуальна комп'ютерна мережа тощо).

Т-віддалені MCI використовують телефон для проведення соціотехнічних атак. Атакувальник, вдаючи з себе іншу особу, може отримати потрібну інформацію, якщо вдається переконати жертву (це особливо дієво у великих корпораціях, де важко знати всіх співробітників). Соціотехніки приділяють особливу увагу створенню психологічного середовища для атаки, намагаючись переконати жертву у своїй довіреності за допомогою маскарадингових технологій.[15]

МТ-віддалені MCI базуються на використанні мережних технологій, таких як електронна пошта, віруси та інше шкідливе ПЗ, інтернет-ресурси. Наприклад, жертві може бути надіслано запит від імені керівництва щодо надання місячного звіту на запропоновану електронну адресу. Інший приклад - відправлення електронного листа з вірусом або шкідливим ПЗ, або посилання на

заражений інтернет-ресурс. Жертва може, не підозрюючи нічого поганого, зареєструватися або увійти на фальшивий сайт, залишаючи свої дані, які будуть використані соціотехніком для подальших атак.

За *ознаками порушень характеристик безпеки*, методи соціальної інженерії (MCI) поділяються на К-, Ц- та Д-дієві.

К-дієві методи спрямовані на порушення конфіденційності. Наприклад, соціотехнік може отримати конфіденційну інформацію, незважаючи на заборону доступу до неї. [16]

Рекомендації щодо захисту від К-дієвих атак:

1. Бухгалтери, секретарі та інший рядовий персонал не повинні мати повноважень на встановлення будь-якого програмного забезпечення на своїх робочих місцях.
2. У разі виявлення несправностей у комп'ютерах або мережі дії користувачів мають бути чітко регламентовані.
3. Кожна організація має впроваджувати чітку ієрархічну модель видання наказів (директор → керівник відділу → працівник) та суворі правила щодо роботи з цінними документами.

Ц-дієві методи спрямовані на порушення цілісності інформації. Наприклад, соціотехнік може замінити блоки коду нового програмного продукту.

Рекомендації щодо захисту від Ц-дієвих атак:

1. Не можна встановлювати програмне забезпечення з ненадійних джерел.
2. Неприпустимо вводити авторизаційні дані без підтвердження надійності ресурсу чи програмного забезпечення.
3. Для робочих і особистих потреб слід використовувати дві різні електронні адреси. При найменшій підозрі на інцидент необхідно змінити пароль до електронної пошти.

Д-дієві методи спрямовані на порушення доступності інформації. Наприклад, можна досягти відмови мережевого сервера, скориставшись ідентифікатором та паролем адміністратора безпеки.

Рекомендації щодо захисту від Д-дієвих атак:

1. У разі будь-яких неочікуваних змін у складі обслуговуючого персоналу слід перевірити їх легітимність, звернувшись до відповідної компанії.
2. Після технічного обслуговування необхідно пересвідчитись, що роботоздатність пошкодженої системи відновлено, і уважно стежити за роботою працівника з технічного обслуговування.
3. Переконатись у легальності встановлюваного оновлення.

Атаки, що порушують різні характеристики безпеки, належать до комбінованого типу, тобто КЦД-дії, що порушують конфіденційність, цілісність і доступність інформації.

За реляційними ознаками МСІ поділяються на моно- і полімономні, моно- і поліполічні.

Мономономні МСІ передбачають атаку одного атакувальника на одного атакованого. Наприклад, дзвінок із запитом щодо отримання потрібної інформації.

Полімономні МСІ передбачають участь двох чи більше атакувальників проти одного атакованого. Наприклад, відправлення електронної пошти від кількох соціотехніків на адресу однієї особи з метою переконати її відкрити інтернет-ресурс і завантажити шкідливе ПЗ.

Монополічні МСІ спрямовані від одного атакувальника на двох чи більше атакованих. Наприклад, соціотехнік може телефонувати різним особам для отримання потрібних йому даних.

Поліполічні МСІ поєднують полімономні та монополічні технології, тобто атака реалізується від двох чи більше атакувальників до двох чи більше атакованих. Це дозволяє швидше отримати потрібну інформацію від кількох осіб.

За ступенем складності методи соціальної інженерії (МСІ) поділяються на прості, складні та системні.

Прості МСІ реалізуються в кілька кроків. Наприклад, щоб дізнатися імена працівників певного відділу на підприємстві, соціотехнік може скористатися наявними інформаційними ресурсами компанії, такими як веб-сайт. Знайшовши номер телефону служби підтримки і зателефонувавши туди, він може отримати потрібну інформацію.

Складні МСІ передбачають комбінування простих алгоритмів для отримання необхідної інформації. Наприклад, для отримання паролів користувачів зловмисник спочатку визначає, чиї паролі йому потрібні, встановлює імена цих осіб, знаходить відповідні джерела інформації і намагається отримати паролі відомими способами.

Системні МСІ реалізуються згідно зі складними алгоритмами, що включають розгалужені, зворотні зв'язки та циклічні процеси. Це використовується для отримання інформації, яку неможливо здобути іншим шляхом, наприклад, коди нових продуктів програмного забезпечення або доступ до серверів систем безпеки.

За типом атакованого джерела МСІ поділяються на ЕК-, ЛГ-, КН- і ВП-джерельні, залежно від рівня поінформованості атакованого.

ЕК-джерельні атаки розраховані на експертів, чиї професійні знання та контакти забезпечують високу ерудицію у питанні, яке цікавить соціотехніка. Експерт може не лише надати базову інформацію, а й вказати на інші джерела.

ЛГ-джерельні атаки орієнтуються на легковажних осіб, здатних ненавмисно розголосити доступну їм інформацію. Проте такі джерела можуть надавати неточну або навіть навмисну дезінформацію.

КН-джерельні атаки спрямовані на контактерів, які мають або мали зв'язок з об'єктом атаки (особою, групою осіб, організацією). Це можуть бути випадкові ділові партнери, родичі або знайомі, працівники сервісу тощо. Контактери можуть не лише надавати інформацію, а й сприяти у наближенні до об'єкта атаки.

ВП-джерельні атаки використовують випадкових індивідів, які не розглядаються як потенційні інформатори, але є носіями важливої інформації.

Через випадковість взаємодії та непередбачуваність їх поведінки, соціотехніки не покладаються на такі джерела, хоча й намагаються використовувати їх повною мірою.

Якщо під час атаки задіяні різні типи джерел, вона належить до комбінованого типу. Наприклад, ЕККН-джерельна атака пов'язана з експертом та контактером.

За типом доступу до інформації методи поділяються на В-, К- та С-доступ.

Методи В-доступу стосуються інформації з відкритих джерел (друковані видання, інтернет-ресурси, засоби масової інформації, бази даних служби підтримки тощо).

Методи К-доступу зорієнтовані на конфіденційну інформацію, доступ до якої контролюється певними особами (імена, номери телефонів, поштові адреси, посади тощо).

Методи С-доступу мають на меті отримання інформації з грифом секретності, доступ до якої мають лише довірені особи (секретні коди, новітні розробки, секретні матеріали тощо).

Комбіновані методи нападу використовують різні типи доступу до інформації. Наприклад, ВК-доступ спрямований на отримання як відкритої, так і конфіденційної інформації.

З огляду на сказане, кібератаки з використанням соціальної інженерії можна поділити на три категорії за такими ознаками:

1. Засоби здійснення — використання телефону, електронної пошти, інтернету, звичайної пошти або особистої харизми під час зустрічі.
2. Рівень стосунків з об'єктом розвідки — офіційний, товариський чи дружній.
3. Ступінь доступу об'єкта до інформаційно-комунікаційних систем — високий (адміністратор), середній (начальник), низький (користувач).

Таким чином, соціотехнік має у своєму розпорядженні безліч методів для:

- пошуку інформації у відкритих джерелах,
- отримання паролів або кодів доступу до потрібної системи,
- надсилання шкідливого ПЗ або вірусу троянця потенційній жертві,

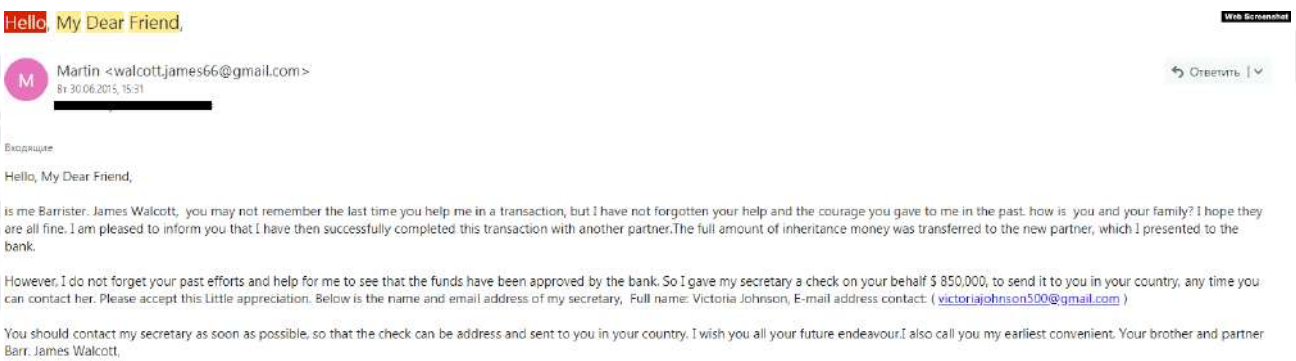
- використання вмісту сміттєвих контейнерів компанії як джерела інформації,
- відвідування компанії під виглядом клієнта, співробітника постачальника, представника партнерської компанії або законодавчого органу,
- проникнення в компанію під виглядом нового керівника, співробітника, представника обслуговуючого персоналу, знайомого чи родича,
- здійснення псевдопомилкових дзвінків до компанії або її співробітників,
- встановлення персональних стосунків зі співробітниками компанії,
- працевлаштування у компанію — потенційну жертву атаки. [5].

2.2. Практичні приклади соціальної інженерії

Дуже поширеним різновидом соціальної інженерії також є надсилання електронних листів, у яких особу повідомляють про отримання спадщини чи дружнього переказу грошей. Зазвичай лист звертається до адресата за прізвищем і містить детальну історію для привернення його уваги.

Такі листи містять довгі історії з багатьма деталями, що мають додати ситуації правдоподібності. Коли людина виходить на зв’язок, у неї просять надати дані для підтвердження особи й прискорення процесу. Таким чином зловмисники можуть просто обікрасти жертву.

Наприклад, текст одного з таких листів має такий вигляд:



Hello, My Dear Friend,

Web Screenshot

M Martin <walcott.james66@gmail.com>
Вт 30.06.2015, 15:31

Ответить

Входящие

Hello, My Dear Friend,

is me Barrister. James Walcott, you may not remember the last time you help me in a transaction, but I have not forgotten your help and the courage you gave to me in the past. how is you and your family? I hope they are all fine. I am pleased to inform you that I have then successfully completed this transaction with another partner.The full amount of inheritance money was transferred to the new partner, which I presented to the bank.

However, I do not forget your past efforts and help for me to see that the funds have been approved by the bank. So I gave my secretary a check on your behalf $ 850,000, to send it to you in your country, any time you can contact her. Please accept this Little appreciation. Below is the name and email address of my secretary, Full name: Victoria Johnson, E-mail address contact: (victoriajohnson500@gmail.com)

You should contact my secretary as soon as possible, so that the check can be address and sent to you in your country. I wish you all your future endeavour.I also call you my earliest convenient. Your brother and partner Barr. James Walcott,

Переклад листа (з рис. 2.4)

Привіт, мій любий друже,

Я адвокат Джеймс Волкотт. Можливо, ти не пам'ятаєш останній раз, коли ти допоміг мені в транзакції, але я не забув твою допомогу і мужність, яку ти надав мені в минулому. Як ти та твоя сім'я? Я сподіваюся, що в них все добре. Я радий тобі повідомити, що я тоді успішно завершив цю транзакцію з іншим партнером. Повна сума спадкових грошей була передана новому партнерові…

Але я не забув і про твої минулі зусилля й допомогу мені в тому, що кошти були схвалені банком. Тому я дав своєму секретареві чек на твоє ім'я на суму 850 тисяч доларів, щоб відправити його тобі в твою країну, в будь-який час, коли ти з нею зв'яжешся. Будь ласка, прийми цю маленьку винагороду. Нижче вказано ім'я та адресу електронної пошти мого секретаря, повне ім'я: Вікторія Джонсон, адреса електронної пошти: (victoriajohnson500@gmail.com)

Тобі треба зв'язатися з моїм секретарем якомога швидше, щоб чек був проадресований і відправлений у вашу країну. Бажаю успіхів у всіх твоїх справах. Я також можу тобі зателефонувати, коли зручно.

Твій брат і партнер

Адвокат Джеймс Волкотт

Рисунок 2.4. – Фішинговий дружній лист

Часто власники гаджетів Apple отримують електронні листи, в яких служба підтримки компанії начебто повідомляє їх про здійснення платежів із їхніх карток – чи то купівля музичного альбому, застосунків тощо.

Так людина отримує «рахунок від Apple». Електронний лист, на перший погляд, маає досить реалістичний вигляд – клієнта сповіщають про зняття 40 доларів за внутрішні покупки в застосунку.

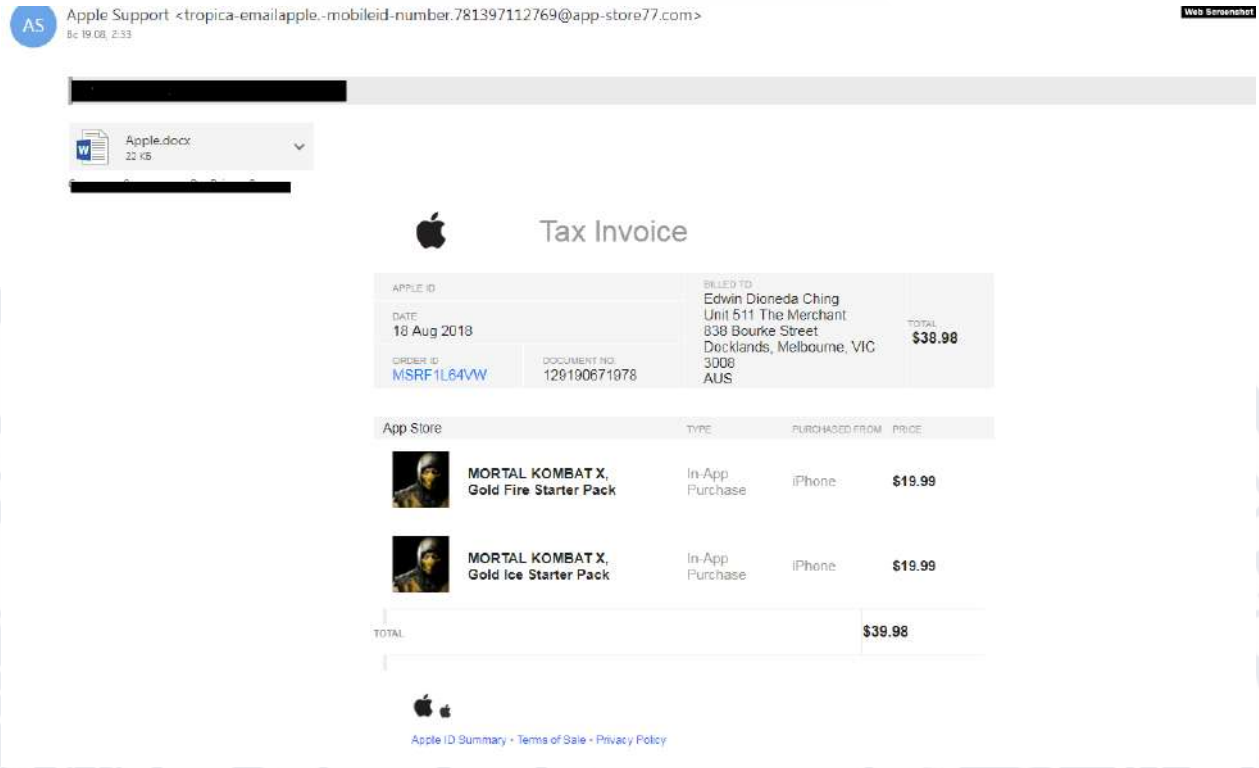


Рисунок 2.5. – Приклад фішинг-повідомлення

Приклад фішинг-повідомлення, надісланого начебто від імені технічної підтримки компанії Apple. Електронний лист є начебто рахунком за сплату послуг усередині застосунку. Щоб розібратися, людина має відкрити вкладений додаток.

Зазвичай люди стурбовані таким несанкціонованим зняттям коштів і переходять за посиланням, щоб швидше вирішити проблему. Відправник і сам, розуміючи це, може порадити в листі ознайомитися з деталями платежу або ж скасувати його, відкривши додаток або посилання.

Проте якщо вивчити електронний лист як слід, можна помітити, що навіть сама електронна адреса має неправдоподібний вигляд. У даному випадку: **tropica-emailapple.-mobileid-number.781397112769@app-store77.com**.

Часто зловмисники можуть зробити дуже знайомий для жертви інтерфейс, наприклад, Фейсбуку. [6]

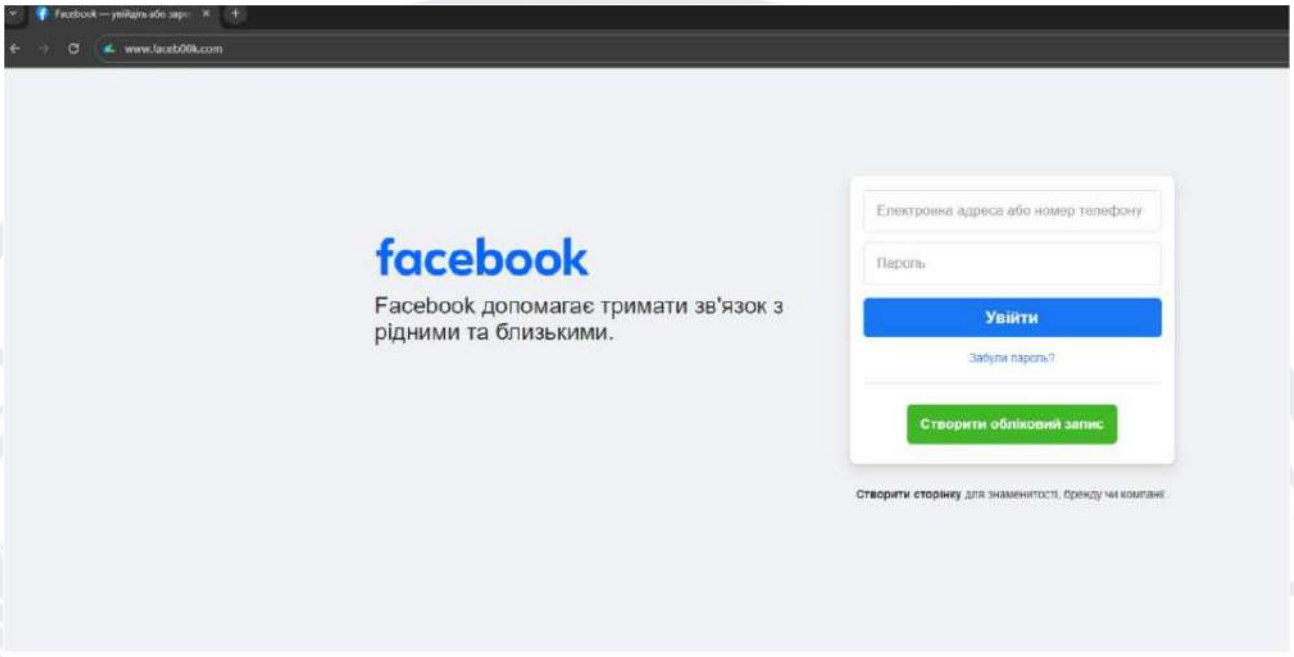


Рисунок 2.6. – Приклад фішинг сайту.

Користувач нічого не підозрюючи проходить авторизацію, вписуючи логін та пароль. Проте, якщо звернути увагу, можна побачити, що сайт **www.faceb00k.com** не є справжнім. Таким чином зловмисник отримує потрібні данні для входу на обліковий запис.

Смішинг (SMS-фішинг)

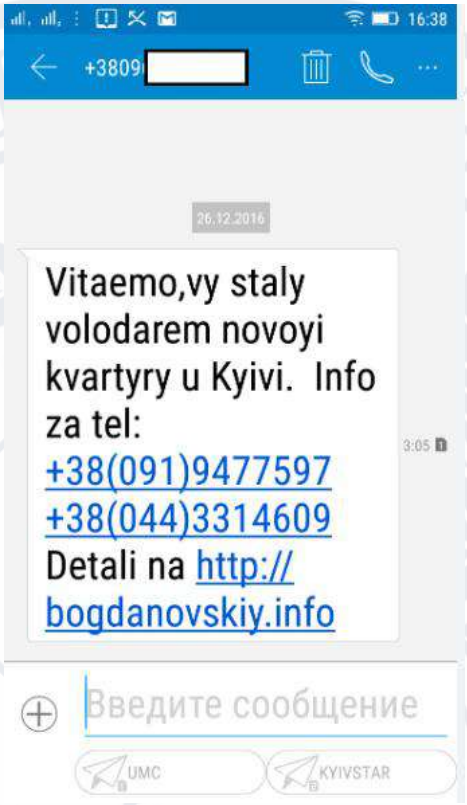


Рисунок 2.7. – Приклад смішингу

Давайте розглянемо практичний приклад перехоплення данних для входу в особистий аккаунт Telegram. Для цього зловмиснику знадобиться додаток “Termux” на пристрої з ОС Android. Termux – це додаток, що реалізує Linux-подібне середовище, взаємодія з яким відбувається за допомогою консолі без необхідності мати root-права на пристрої. Як інструмент злодій може використовувати KingFish3. За його допомогою можна створити фішингову сторінку авторизації найпопулярніших соціальних мереж та месенджерів, а також одразу отримати на неї посилання

Створивши фішингове посилання та замаскувавши його, зловмисник надсилає його жертві. В додаток потрібно придумати причину, за якої жертва відкриє це посилання.

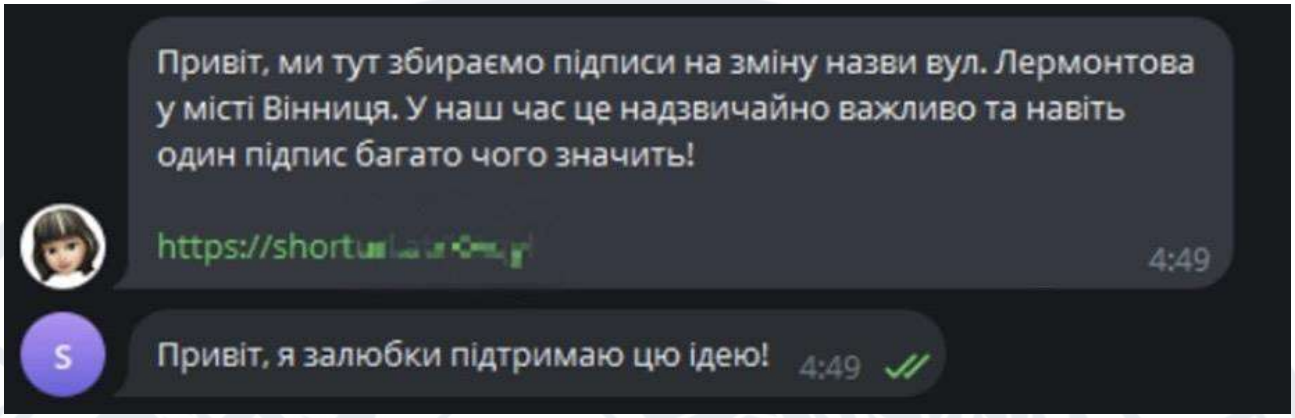


Рисунок 2.8. – Повідомлення з фішинговим посиланням

Перейшовши за посиланням жертва бачить схожий до звичного інтерфейс авторизації у обліковий запис Telegram. Незважаючи, на схожість дизайну, сайт є несправжнім і служить лише для того, аби жертва ввела свої данні, а зловмисник їх перехопив.

Рисунок 2.9. – Інтерфейс фішингового сайту під виглядом Telegram

Для авторизації у аккаунт є два етапи. Номер телефону та код підтвердження (2FA). Після того як жертва вводить номер телефону, зловмисник отримує його у KingFish3.

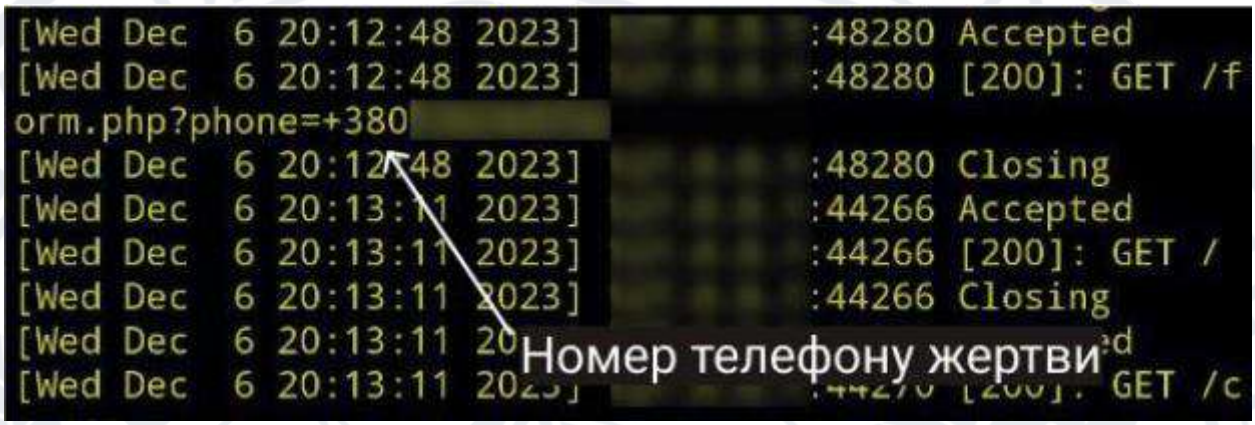


Рисунок 2.10. – Номер телефону жертви у KingFish3

Після введення номеру телефону відкривається наступна сторінка із запитом кодом двофакторної аутентифікації.

Рисунок 2.10. – Інтерфейс введення 2FA

Одночасно з цим зловмисник авторизується в Telegram за допомогою номеру телефону жертви.

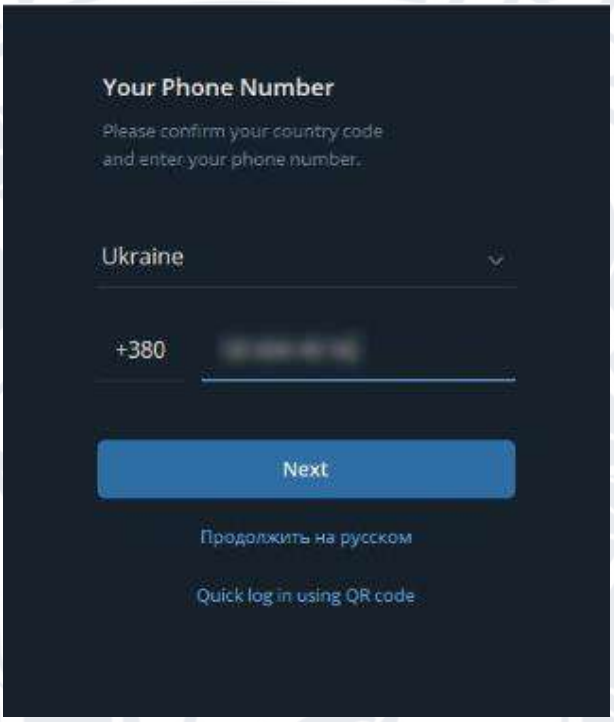


Рисунок 2.11. – Введення номеру телефону жертви у Telegram

Код 2FA жертва отримає, після того, як зловмисник натисне кнопку “Next”. Його вона так само, як і номер телефону введе на фішинговому сайті у поле вводу.

Рисунок 2.12. – КОД 2FA у KingFish3

Цей код зловмисник вводить у Telegram та отримує доступ до облікового запису жертви.

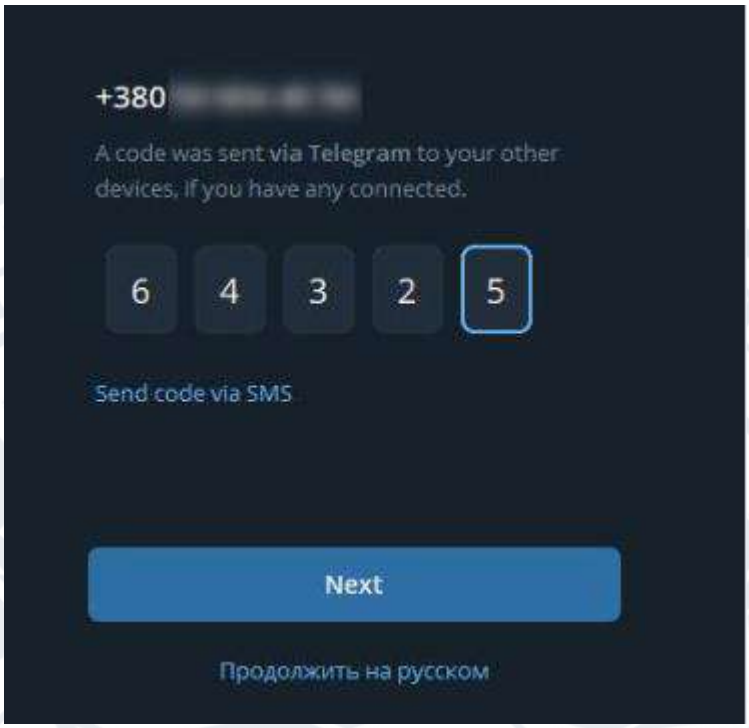


Рисунок 2.13. – Введення коду 2FA

Отримавши доступ таким чином, зловмисник має усі особисті листування та багато іншої особистої інформації жертви. Її він може використовувати в подальших корисливих цілях.

2.3. Методи запобігання та протидії соціальної інженерії

У рамках соціоінженерного підходу вразливості людини розглядаються як її слабкості, потреби, пристрасті та захоплення. Маніпулювання цими аспектами дозволяє отримати несанкціонований доступ до інформації. Це призводить до нових моделей поведінки та створення умов, що сприяють реалізації загроз безпеці інформації, знижуючи ефективність систем захисту (див., наприклад, рис. 2.14). До таких форм маніпулювання належать шахрайство, обман, афери, інтриги, містифікації та провокації. Кожна з цих форм маніпулювання вимагає ретельного планування, організації та контролю.

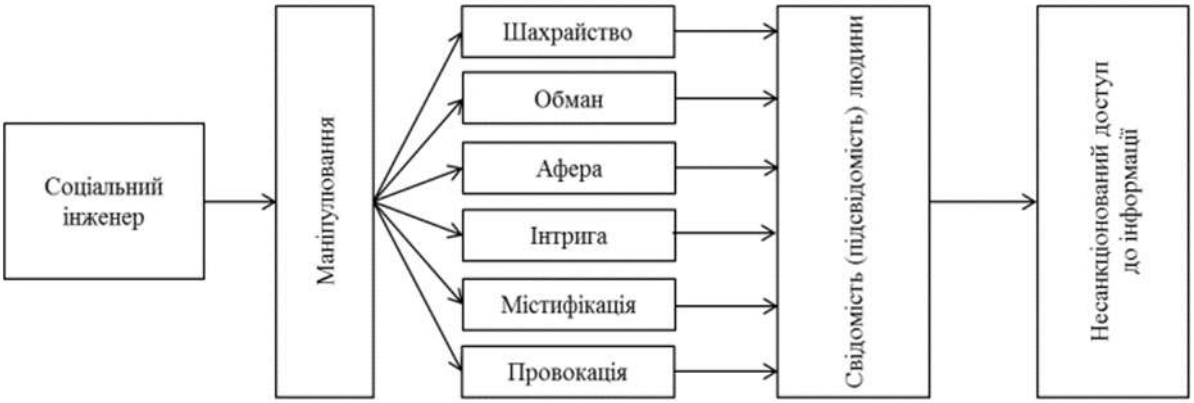


Рисунок. 2.14. – Соціоінженерний підхід

Згідно з рис. 2.14, соціоінженерний підхід передбачає цілеспрямований вплив на свідомість людини, здійснюваний проти її волі, але за її згодою. Цей вплив дозволяє керувати поведінкою керівництва, адміністраторів та користувачів через їхні слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан. Маніпулювання цими уразливостями виражається у формах, таких як шахрайство, обман, афери, інтриги, містифікації та провокації. Використання кожної з цих форм маніпулювання потребує ретельного планування, організації та контролю. Форми маніпуляцій змінюються залежно від типу атак соціальної інженерії, таких як:

1. **Фішінг (Phishing)** – масове розсилання електронних листів для виманювання персональних даних.

2. **Фармінг (Pharming)** – перенаправлення користувачів на шахрайські сайти для отримання їхніх логінів та паролів.

3. **Претекстінг (Pretexting)** – отримання інформації або спонукання до дій через створення фіктивних ситуацій.

4. **Смішінг (Smishing)** – отримання інформації через масове розсилання SMS з посиланнями на веб-ресурси.

5. **Вішінг (Vishing)**– отримання інформації шляхом входження в довіру під час розмови через IP-телефон.

6. **Спір фішінг (Spear Phishing)** – надсилання електронних листів конкретним адресатам.

7. **Вейлінг (Whaling)–** надсилання електронних листів представникам керівництва організацій.

Отже, отримання несанкціонованого доступу до інформації за допомогою фішингу, фармінгу, смішінгу, вішінгу, спір фішингу та вейлінгу здійснюється через такі маніпулятивні впливи, як шахрайство та обман (див., наприклад, табл. 1). У той час, як створення фіктивних ситуацій при прітекстінгу базується на аферах, інтригах, містифікаціях та провокаціях.

Таблиця 2.1. – Різновиди соціоінженерних атак та їх характеристика

№ п/п	Різновид соціоінженерної атаки	Шахрайство	Обман	Афера	Інтрига	Містифікація	Провокація
1.	Фішинг	+	+	-	-	-	-
2.	Фармінг	+	+	-	-	-	-
3.	Претекстінг	+	+	+	+	+	+
4.	Смішинг	+	+	-	-	-	-
5.	Вішинг	+	+	-	-	-	-
6.	Спір фішинг	+	+	-	-	-	-
7.	Вейлінг	+	+	-	-	-	-

Тому при оцінюванні захищеності інформації в комп’ютерних системах за соціоінженерним підходом слід враховувати форми маніпулятивного впливу. Методи соціальної інженерії імітують дії зловмисників проти персоналу організації. Соціальні інженери використовують контактну інформацію, отриману з публічних джерел, наприклад, прізвища, імена та посади користувачів, для визначення вразливостей і реалізації загроз.

Основою використання методів соціальної інженерії є [2]:

- особливості, що впливають на людську свідомість;
- цільова аудиторія або поле діяльності;

- некомпетентність аудиторії в певних термінах і предметних областях у сфері інформаційної безпеки;
- нестійкість психологічних властивостей особистості, яка характеризується поведінковими стереотипами. Ці особливості можна використовувати для маніпулювання через основні потреби, слабкості, бажання та ідеали.

Більшість соціальних інженерів діє за однаковими або подібними шаблонами, що призводить до схожих сценаріїв атак. Вивчення їхніх методів дозволяє виокремити такі рівні взаємодії з об'єктом впливу, як домінування, маніпулювання, суперництво та партнерство.

Усі методи соціальної інженерії можна поділити на дві групи:

Віддалена соціальна інженерія реалізується засобами сучасних телекомунікацій шляхом використання:

Телефонного зв'язку

Соціальний інженер може залишатися анонімним і водночас мати прямий контакт з об'єктом впливу. Це важливо, оскільки безпосередній контакт не дає співрозмовнику часу на обмірковування поведінки у ймовірних ситуаціях. Вирішувати необхідно швидко, під тиском соціального інженера. Під час телефонної розмови відбувається обмін лише звуковою інформацією, тому велике значення має інтонація і голос співрозмовника. Ці характеристики підбираються відповідно до моделі поведінки соціального інженера для отримання інформації про об'єкт впливу, наприклад:

а) *Начальник* – людина, яка звикла віддавати команди, цінує свій час і досягає поставленої мети. Манера розмови жорстка, нетерпляча, впевнена в собі і зверхня до рядового персоналу. Тон показує, що проблема, з якою звернулися, є дрібницею, яку треба вирішити якомога швидше. Жодних прохань – тільки вимоги і вказівки. На недовірливі репліки – допустиме незадоволення і залякування співрозмовника.

b) *Секретар*– дівчина (здебільшого) з приємним голосом. Її завдання – виконати конкретне доручення начальника, не відволікаючись на умовності. Вона володіє інформацією про начальника та його справи, у своїй мові користується фактами, які складно перевірити. Характер розмови м'який, з легким фліртуванням (якщо співрозмовник – чоловік). Реакція на небажання співпрацювати – бурхливе розчарування і скарга на реакцію начальства.

c) *Технічний співробітник* – працівник організації, який має поблажливе, але дружелюбне ставлення до клієнтів. Його мета – усунути несправність, використовуючи специфічні терміни для демонстрації компетентності. На відмову співпрацювати реагує здивуванням, оскільки співпраця вигідна для клієнта. Залякування важкими наслідками є допустимим.

d*) Користувач* – працівник, що виконує свої обов'язки і наляканий виникненням неочікуваної проблеми. Мотивований швидко вирішити всі проблеми і повернутися до своєї роботи. Він не розуміє характеру проблеми, зацікавлений лише в її вирішенні. Характер спілкування – показати безнадійність свого положення і готовність віддатися у руки спеціаліста.

Глобальна мережа Інтернет

Найпоширенішими способами реалізації методів соціальної інженерії через Інтернет є:

a) проведення соціальної інженерії через електронне листування;

b) використання систем обміну повідомленнями (Skype, Viber);

c) соціальна інженерія на форумах, чатах та блогах.

Особистий контакт

Це найскладніший і найнебезпечніший метод соціальної інженерії. Окрім вимог до сценарію спілкування і моделі поведінки, соціальний інженер повинен приділяти увагу своїй зовнішності та манерам у безпосередньому спілкуванні. Для правильного візуального сприйняття потрібно ретельно підібрати:

a) колір одягу та взуття;

b) манери та жести під час спілкування;

c) положення в просторі відносно співрозмовника.

Також при використанні методів соціальної інженерії необхідно визначити слабкості співрозмовника за голосом або зовнішністю, щоб використовувати їх для досягнення мети. Основні слабкості людини, які разом з правильно підібраною поведінкою і сценарієм розмови дозволяють досягти бажаного результату, включають:

a) довірливість;

b) страх;

c) жадібність;

d) відкритість;

e) зверхність;

f) милосердя.

Основні причини впливу на об’єкт соціальної інженерії можуть бути такі:

a) почуття гідності;

b) прагнення до успіху;

c) матеріальна вигода.

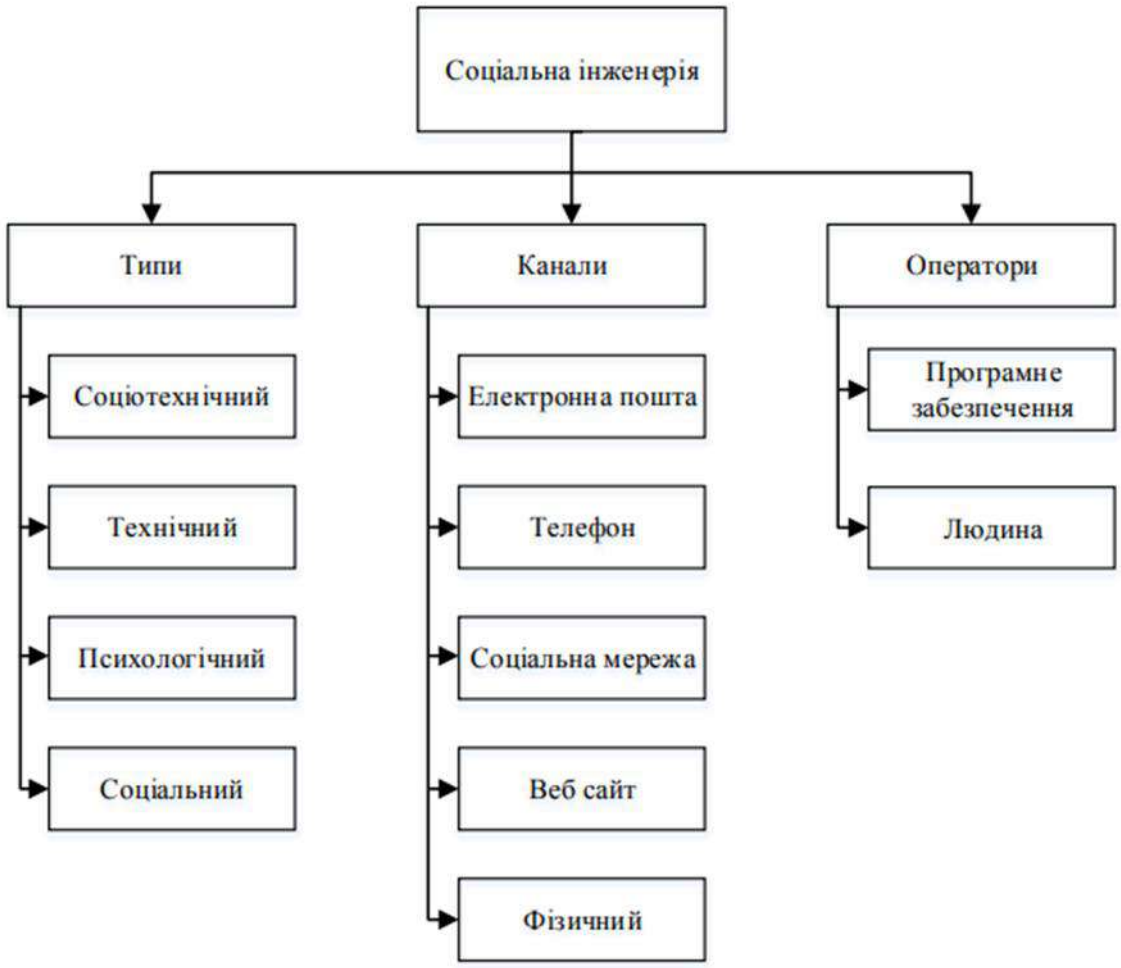


Рисунок 2.15. – Схема типів, каналів та операторів соц. інженерії

З огляду на сутність соціоінженерного підходу, форми маніпулятивного впливу та методи соціальної інженерії, виокремлюються такі напрями її протидії, як тестування на проникнення та моделювання дій об'єкта і суб'єкта соціоінженерного впливу.

Тестування на проникнення за соціоінженерним підходом орієнтоване на автоматизацію створення і реалізації векторів атак (див., наприклад, рис. 2.16, 2.17). Для цього використовується інструментальний засіб соціального інженера (Social-Engineer Toolkit, SET). Він забезпечує практичну правдоподібність атак соціальної інженерії. Ключовим фактором є правильне налаштування та використання цього інструменту. SET постачається як окремий комплекс або як компонент Kali Linux, з можливістю внесення змін до конфігураційного файлу, що дозволяє розширювати його можливості.

Перевагами цього методу є, по-перше, автоматизація процесу протидії соціальній інженерії; по-друге, правдоподібність векторів атак. Однак одним із основних недоліків є необхідність високої кваліфікованості користувача.

Рисунок 2.16. Меню інструментального засобу SET

Рисунок 2.17. Меню соціоінженерних атак інструментального засобу SET

Метод моделювання дій об’єкта та суб’єкта соціоінженерного впливу зосереджується на виокремленні двох ключових ролей – нападника та захисника (див., наприклад, рис. 2.18). Нападник намагається здійснити соціоінженерний вплив, тоді як захисник прагне цьому протидіяти. Наступний крок полягає у використанні соціальної інженерії нападником для тестування здатності захисника протидіяти. Якщо захисник виявляється більш ефективним у протистоянні, ролі змінюються на основі результатів цього порівняння.

Перевагою цього методу є можливість чітко визначити ролі нападника і захисника. Однак його ефективність значною мірою залежить від наявних

шаблонів атак соціальної інженерії, що впливає на здатність запобігати їх реалізації.

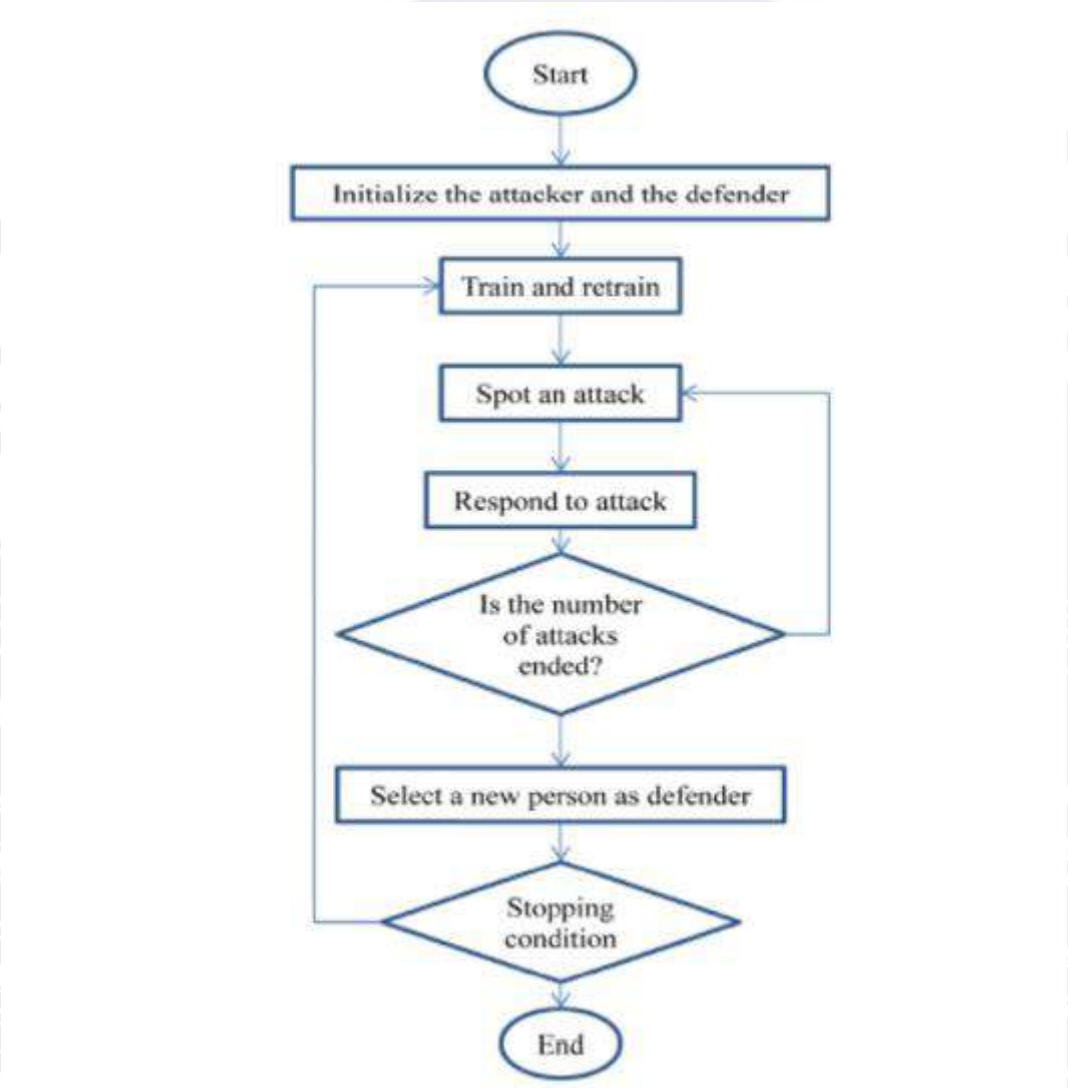


Рисунок 2.18 – Схема використання оптимізатора соціальної інженерії

Метод виявлення і повідомлення про атаки соціальної інженерії людиною. Цей метод реалізовано за допомогою інструменту *Cogni-Sense.* Для виявлення та повідомлення про атаки соціальної інженерії достатньо одного повідомлення від користувача. Такий підхід залучає працівників організації не лише для профілактики, наприклад, через кібергігієну, але й для активного інформування про загрози кібербезпеці .

Перевага цього методу полягає в активній участі користувачів у забезпеченні кібербезпеки. Водночас існує ризик, що окремий користувач може приховати інформацію про атаку, доки об'єктом не стане інший користувач.

Метод протидії використанню соціальної інженерії за SEDF (Social Engineering Defensive Framework). Основні етапи застосування цього методу включають:

- визначення соціоінженерного впливу;
- оцінку можливостей протидії;
- навчання персоналу;
- упорядкування існуючих технологій та політики.

Перевагами цього методу є можливість адаптації до потреб організації та незалежність етапів його застосування. Недоліком є залежність від досвіду експерта, залученого до навчання персоналу. [7]

Висновки до розділу 2

Розглянуто різні методи соціальної інженерії, що використовуються кіберзлочинцями для крадіжки інформації, з акцентом на як класичних, так і сучасних підходах, що базуються на психологічних факторах та людських уразливостях. Виокремлено групи ризику, типи методів за їх впливом на безпеку, використанням технічних засобів, рівнем складності та джерелами інформації. Детально проаналізовано принципи атак, що базуються на людських помилках та недбальстві, з описом нестандартних ситуацій, які можуть бути використані соціотехніками. Рекомендації щодо захисту включають комплексний підхід до протидії різним типам атак.

Практичні приклади атак соціальної інженерії, такі як фішинг, смішинг, фармінг та методи "медової пастки", показали їх ефективність у реальних умовах. Методи запобігання та протидії, такі як тестування на проникнення, моделювання дій та використання інструментів Social-Engineer Toolkit (SET) та Cogni-Sense, підкреслюють важливість психологічної підготовки користувачів. Підвищення обізнаності та навчання для розпізнавання соціальних атак є ключовими для захисту.

РОЗДІЛ 3
НАУКОВЕ ДОСЛІДЖЕННЯ РІВНЯ ЗНАНЬ

3.1. Створення тесту

Метою дослідження є - провести наукове дослідження та перевірити обізнаність пересічного користувача інтернету у сфері соціальної інженерії.

Для цього я зібрав 10 людей різного віку, статі, роду занять тощо. Мій науковий експеримент заключатиметься у перевірці початкових знань та аналізу данних, які отримали (учасники не знатимуть результати тесту). Після чого учасники пройдуть невеличкий урок по соціальній інженерії та методам боротьби з нею. Усі матеріали будуть взяті з пунктів 1 та 2. Після чого вони ще раз пройдуть тест і ми поглянемо чи змінили учасники свої відповіді.

Це дослідження дасть розуміння наскільки обізнанними є пересічні користувачі інтернету, покаже групу людей, яка краще впорається з завданнями та перевірить інформацію зібрану у цій бакалаврській роботі. Важливо, що інформація у моїй роботі повинна бути не лише корисною, а і доступною, адже більшість наших учасників, всього лише звичайні користувачі інтернету без глибоких знань у цій галузі.

Тестування виглядатиме таким чином(правильні відповіді виділено жирним):

1.Що таке соціальна інженерія у контексті інформаційної безпеки?

A) Використання спеціального програмного забезпечення для злому паролів

B) Психологічні маніпуляції з метою отримання конфіденційної інформації

C) Захист даних за допомогою криптографії

D) Процес відновлення даних після кібератаки

2.Який метод найчастіше використовується для протидії атакам соціальної інженерії?

A) Регулярне оновлення операційної системи

B) Навчання працівників розпізнаванню та реагуванню на соціальні інженерні атаки

C) Встановлення додаткових брандмауерів

D) Використання тільки однієї складної комбінації пароля для всіх облікових записів

3. Що з варіантів НЕ є ознакою соціальної інженерії?

A) Почуття терміновості

B) Незвична адреса відправника

C) Запит на конфіденційну інформацію

D)Попередження антивіруса про можливі загрози

4. Яка з наступних порад допоможе захиститися від фішинг-атак?

A) Використання простих паролів для всіх облікових записів

B) Ігнорування всіх електронних листів

C) Перевірка відправника і змісту повідомлення перед тим, як натискати на посилання або відкривати вкладення

D) Завантаження програмного забезпечення тільки з неперевірених джерел

5. Який з наведених методів є прикладом соціальної інженерії?

A) Брутфорс-атака

B) Фішинг

C) Використання антивірусного програмного забезпечення

D)Шифрування даних

6. На що вказує літера «s» у префіксі «https»?

A) На те, що з'єднання безпечне і зашифроване

B) На те, що з'єднання не є безпечним

C) На те, що з'єднання небезпечне і заблоковане

D)На те, що сайт має pop-up рекламу

7. Вішинг — це:

A) Різновид фішингу, який здійснюється через телефон

B) Вид фішингового електронного листа

C) Вид шкідливого програмного забезпечення

D) Програмний комплекс для захисту від фішингових атак

8. Чому атаки з використанням прийомів соціальної інженерії до сьогодні залишаються одним із найефективніших методів атак?

A) Вони дешеві в проведенні

B) Незважаючи на відносну простоту в здійсненні, вони відрізняються високою ефективністю

C) Соціальна інженерія атакує не операційну систему та не програмне забезпечення, а їхнього користувача, який найчастіше є найвразливішим

D) Усе перераховане вище

9. Яка з наступних дій є прикладом використання методу «honeytrap»?

A) Відправлення спам-повідомлення з вірусом

B) Створення фейкового облікового запису на соціальній мережі для збору інформації

C) Перевірка паролів на складність

D)Використання VPN для захисту від кібератак

10. Що з перерахованого нижче на вашу думку, є найціннішим для хакера при плануванні фішингової атаки на підприємство, державну структуру?

A) Фізична адреса головного офісу

B) Години роботи офісу

C) Інформація щодо контрагентів, партнерів, підрядників

D) Ім’я керівника

3.2. Підрахунок результатів та їх аналіз

Для підрахування результатів, я створив таблицю, в яку впишу усіх учасників та їх вік. У таблиці видно буде результати по кожному з завдань.

У цій таблиці будуть вказані правильні чи неправильні відповіді учасників на першому тесті.

Таблиця 3.1. – Результат першого тестування

12.03.2024	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	n/10
Дарина (21)	+	-	-	+	+	+	-	+	-	+	6/10
Володимир (19)	-	+	+	+	-	-	-	-	-	+	4/10
Сергій(20)	+	+	+	+	+	+	+	+	-	+	9/10
Данило(21)	+	+	+	+	+	+	-	+	-	+	8/10
Ганна(47)	-	+	-	+	+	-	-	+	-	+	5/10
Іван(78)	-	-	+	+	+	-	-	-	-	-	3/10
Тетяна (76)	+	-	-	+	+	-	-	-	-	-	3/10
Дмитро(22)	-	-	-	+	+	+	-	+	-	+	5/10
Андрій(16)	+	-	+	+	+	-	-	-	-	-	4/10
Василь(26)	+	-	+	+	+	+	-	+	-	+	7/10

Отже, отримавши результати ми бачимо, що люди які навчаються абопрацюютьу галузі ІТ – мають кращі результати.

Загалом середній бал наших учасників 5,4/10. Поглянемо на те, як він зміниться після короткого екскурсу.

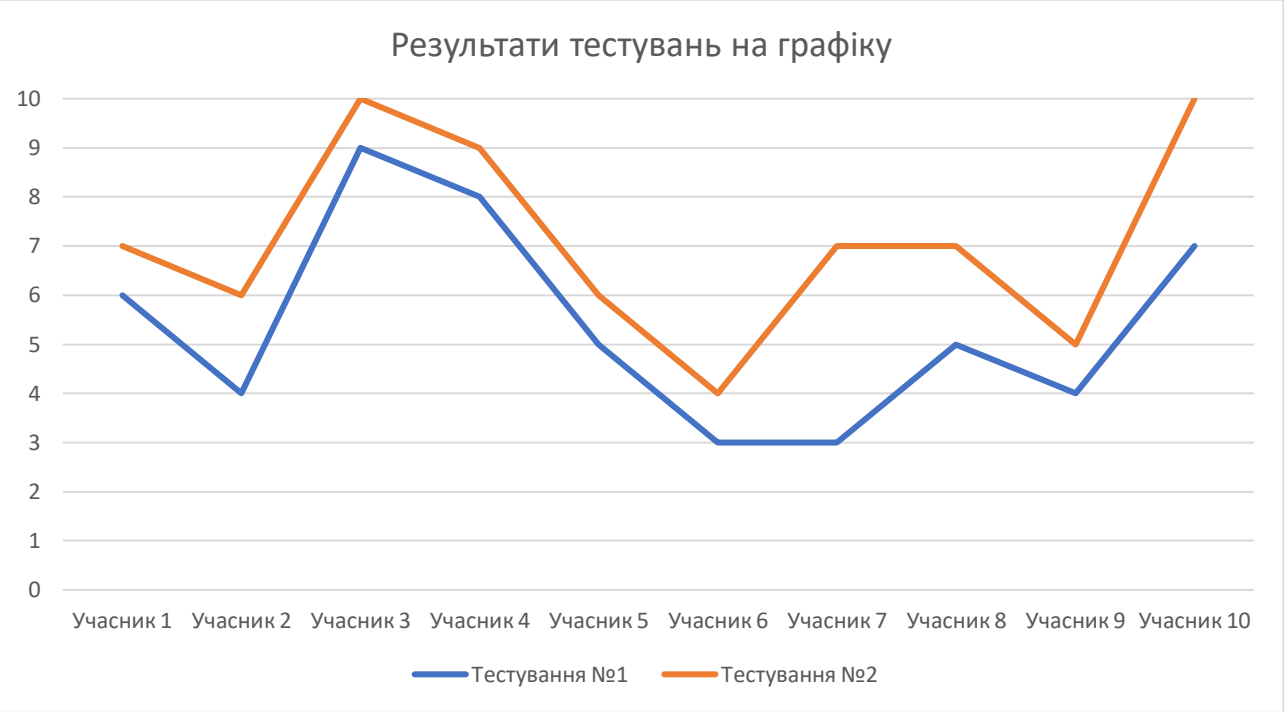
Таблиця 3.2. – Результати другого тестування

28.04.2024	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	n/10
Дарина (21)	+	+	-	+	+	+	-	+	-	+	7/10
Володимир (19)	+	+	+	+	-	-	-	-	+	+	6/10
Сергій (20)	+	+	+	+	+	+	+	+	+	+	10/10
Данило(21)	+	+	+	+	+	+	-	+	+	+	9/10
Ганна(47)	+	-	+	+	+	-	-	+	-	+	6/10
Іван(78)	+	-	-	+	+	-	-	+	-	-	4/10
Тетяна (76)	+	+	-	+	-	+	-	+	+	+	7/10
Дмитро(22)	+	+	-	+	+	+	-	+	-	+	7/10
Андрій(16)	+	-	+	+	+	-	-	-	-	+	5/10
Василь(26)	+	+	+	+	+	+	+	+	+	+	10/10

Аналізуючи другу таблицю, можемо впевненно сказати, що всі учасники перевершили свої попередні результати. На цей раз середній бал досягнув 7,1/10. Такий результат можна вважати чудовим покращенням у рівні знань учасників нашого дослідження.

Для того щоб побачити це детальніше я зображу це на графіку.

Графік 3.1 – Результати тестувань



Як бачимо на графіку усі учасники дізнались щось нове та покращили свої результати хочаб на 1 правильну відповідь, хоча не обійшлось і без неправильних виправлень.

ВИСНОВКИ

У цій бакалаврській роботі я провів тестування рівня знань пересічного користувача інтернету. У результаті тестування, я виявив, що більшість користувачів є легкою ціллю для зловмисників. Тому я надав інформацію щодо соціальної інженерії та методи боротьби з нею. Усі учасники пройшовши невеличкий курс підготовки значно підвищили свої знання у цій сфері. Суспільна необізнаність у сфері соціальної інженерії є важливою проблемою, яка потребує уваги.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Гангал А. В., Волошина Н. М. Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали II всеукр. наук.-практ. конф., Київ, 25 грудня 2022 р / Київ-Одеса, 2022. – 108с.
2. Семенюк А. В. Використання методів машинного навчання та штучного інтелекту для захисту від влпиву соціальної інженерії при кібератаках. Матеріали LIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 20-22 березня 2024 р. Електрон. текст. дані. 2024.
3. Оліферук А.О. Дипломна робота на тему “Моделі соціальної інженерії в умовах захисту персональних даних”. КПІ імені Ігоря Сікорського Фізико-технічний інститут”, Київ, 2 червня 2021 р.
4. Holland S.. 12 Types of Social Engineering Attacks to Look Out For.12/12/2022 URL:https://www.copado.com/resources/blog/12-types-of-social-engineering-attacks-to-look-out-for
5. Бурячок В.Л., Толубко В. Б., Хорошко В. О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник, Київ ДУТ 2015 — 288с.
6. Савчук Т. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. Радіо Свобода, 30 серпня 2018 р. URL:https://www.radiosvoboda.org/a/socialnainzhenerijashaxrajstvo/29460139.html
7. Цуркан О., Герасимов Р., Крук О. Методи протидії використанню соціальної інженерії. P-ISSN 2411-1031. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13)
8. Shivam Lohani. Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 5 лютого 2019, URL: https://ssrn.com/abstract=3329391
9. Kevin D. Mit, Nick William L. Simon. The art of deception, controlling the Human Element of Security. Texas, 577 p.

10. Arif KOYUN, Ehssan Al Janabi - Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 2458-9403 Vol. 4 Issue 6, June – 2017
11. Snyder C. – “Handling Human Hacking, Creating a Comprehensive Defensive Strategy Against Modern Social Engineering”. A Senior Thesis, (Spring 2015), 33p.
12. A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang and H. N. Thakur, "Social Engineering Incidents and Preventions," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2023, pp. 0494-0498, doi:10.1109/CCWC57344.2023.10099202.
13. Aun Y. - "Social Engineering Attack Classifications on Social Media Using Deep Learning," Comput. Mater. Contin., vol. 74, no. 3, pp. 4917-4931. 2023
14. R. Salama, F. Al-Turjman, S. Bhatla and S. P. Yadav, "Social engineering attack types and prevention techniques- A survey," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 817-820, doi: 10.1109/CICTN57981.2023.10140957.
15. Bullée J, Montoya L, Junger M, Pieter H. Hartel - Telephone-based social engineeringattacks:An experiment testing the success andtime decay of an intervention. Conference: Singapore Cyber Security R&D Conference, January 2016, pp. 107-114 doi:10.3233/978-1-61499-617-0-107
16. Massimino, B., Gray, J. V., & Lan, Y. On the Inattention to Digital Confidentiality in Operations and Supply Chain Research. Production and Operations Management, Volume 27, Issue 8 August 1 2018. 27(8), pp. 1492-1515.
17. Alksnis G., J. Purins. Security Evaluation of Wireless Network Access Points – Riga, January 2017. – С. 38–45. DOI:10.1515/acss-2017-0005
18. Laptiev, S. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Електронне фахове наукове

видання «Кібербезпека: освіта, наука, техніка» Київ (30.06.2022) Т. 4, с. 45-62. doi: 10.28925/2663-4023.2022.16.4562

19. Погребняк І. В. Прикладні соціально-комунікаційні технології у 71 т. Київ 2021. Т. 32 с. 273-277. УДК 007: 304: 001
20. Говда М. Соціальна інженерія як інформаціна зброя в ході російсько-української війни. Матеріали IV Міжнародна науково-практична конференція Київ, 27 вересня 2023 року. с. 150-152.
21. Kilavo, H., J. Mselle, L., I. Rais, R., & Mrutu, S. I. Reverse Social Engineering to Counter Social Engineering in Mobile Money Theft: A Tanzanian Context. Journal of Applied Security Research, 31 January 2022 546–558p.