ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Михайло БЕЗПРОЗВАННИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
БЕЗПРОЗВАННИЙ Михайло
(прізвище, ім'я)

Керівник д. ф., доцент МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Безпрозванному Михайлу Ігоровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак»
керівник кваліфікаційної роботи Марченко Віталій, д. ф., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
Рішення GoPhish;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту кінцевих точок організації.
2. Аналіз методів та засобів захисту конфіденційної інформації від соціотехнічних атак.
3. Розроблення рекомендацій щодо захисту конфіденційної інформації від на базі GoPhish.
4. Рекомендації щодо застосування методів та програмного забезпечення для захисту конфіденційної інформації від на базі GoPhish.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту конфіденційної інформації	27.02.2024 р.	Викон.
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	05.03.2024 р.	Викон.
3.	Аналіз методів та засобів захисту конфіденційної інформації від на базі GoPhish	15.04.2024 р.	Викон.
4.	Практична реалізація варіанту захисту конфіденційної інформації від на базі GoPhish	15.04.2024 р	Викон.
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту конфіденційної інформації організації.	15.05.2024 р	Викон.
6.	Оформлення результатів дослідження.	16.05.2024 р	Викон.
7.	Підготовка доповіді до захисту.	31.05.2024 р.	Викон. D

Здобувач вищої освіти _____ Михайло БЕЗПРОЗВАННИЙ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача БЕЗПРОЗВАННОГО Михайла

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак»

Актуальність: Соціотехнічні атаки часто використовують психологічні прийоми для отримання доступу до чутливої інформації або систем, оминаючи технічні засоби захисту. Це може призвести до серйозних наслідків, таких як витік конфіденційних даних, фінансові втрати, репутаційні ризики та порушення правового регулювання. Особливо вразливими є організації, співробітники яких не достатньо поінформовані про методи таких атак та не володіють навичками їх розпізнавання.

Вивчення шляхів захисту від соціотехнічних атак та розробка відповідних рекомендацій дозволить створити більш надійні системи безпеки, що включають не тільки технічні, але й організаційні та освітні заходи. Це дослідження сприятиме підвищенню рівня обізнаності співробітників, впровадженню ефективних практик інформаційної безпеки та розвитку культури безпеки в організаціях.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту конфіденційної інформації організації та визначено мету та завдання даного виду забезпечення, а також його складові частини.
2. Досліджено методи та засоби захисту конфіденційної інформації організації на базі GoPhish.
3. Запропоновано варіант системи захисту конфіденційної інформації організації на базі GoPhish та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз змісту захисту кінцевих точок на прикладі конкретної організації.
2. Запропонований порядок застосування методів та засобів захисту кінцевих точок бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач **БЕЗПРОЗВАННИЙ Михайло** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач БЕЗПРОЗВАННИЙ Михайло до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***БЕЗПРОЗВАННИЙ Михайло*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БЕЗПРОЗВАННИЙ Михайло*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Висновок: Кваліфікаційна робота заслуговує оцінку **«відмінно»**, а здобувач **БЕЗПРОЗВАННИЙ Михайло** – присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.'

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БЕЗПРОЗВАННИЙ Михайло** допускається до захисту
даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 53 сторінки, 17 рисунків, 12 джерел.

Об'єкт дослідження – технологія проведення тестових кампаній на основі фреймворку GoPhish.

Предмет дослідження – методи та засоби захисту конфіденційної інформації організації на базі GoPhish.

Мета роботи розробити варіант системи на базі рішення GoPhish та рекомендації щодо застосування методів та засобів захисту конфіденційної інформації організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

GoPhish – це інструмент з відкритим вихідним кодом, який використовується для організації та проведення фішингових кампаній з метою навчання та підвищення обізнаності працівників щодо соціотехнічних атак. Його сфера застосування охоплює декілька ключових напрямків:

В роботі досліджено проблему захисту конфіденційної інформації організації, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів захисту конфіденційної інформації організації. Досліджено методи та засоби захисту конфіденційної інформації організації на базі GoPhish. Визначено призначення, основні функції та склад рішення GoPhish.

На основі досліджень проведених в роботі запропоновано варіант системи на базі GoPhish. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту конфіденційної інформації організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, КІНЦЕВІ ТОЧКИ, ЗАХИСТ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ОРГАНІЗАЦІЇ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Advanced Fee - Авансовий платіжі

Business Email Compromise (BEC) - Компрометація ділової електронної пошти

Botnet – Ботнет

Credit Card Fraud/Check Fraud - Шахрайство з кредитними картками

Crimes Against Children - Злочини проти дітей

Data Breach - Порушення даних

Employment - Працевлаштування

Extortion - Вимагання

Government Impersonation - Видавання себе за державного службовця

Harassment/Stalking – Харасмент, спостереження

Identity Theft – Викрадення Ідентифікації

Investment - Інвестиції

IPR/Copyright and Counterfeit - Незаконна крадіжка та використання чужих ідей, винаходів і творчих

Lottery/Sweepstakes/Inheritance - Лотерея / тоталізатор / спадщина

Malware - Шкідливе програмне забезпечення

Non-Payment/Non-Delivery - Несплата/не доставлений товар

Overpayment – Передплата

Personal Data Breach - Витік персональних даних,

Phishing/Spoofing: - Фішинг/Спуфінг

Ransomware - Програми-вимагачі

Real Estate – Нерухомість

SIM Swap - Підміна SIM-картки

Tech Support - Технічна підтримка

Threats of Violence - Погрози насильством

ВСТУП

Актуальність дослідження. Тема "Дослідження шляхів та розробка рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак" вкрай актуальна в сучасному цифровому світі. Спочатку, коротке пояснення, що таке соціотехнічні атаки - це стратегії, спрямовані на отримання конфіденційної інформації через маніпулювання людським фактором, такими як соціальна інженерія, фішинг, використання маніпулювальних технік, тощо. Ці атаки стають все більш витонченими та складними, і вони можуть призвести до серйозних наслідків для компаній, установ, та індивідуальних користувачів.

З огляду на постійний розвиток технологій та зростання кількості інтернет-підключених пристроїв, включаючи мобільні телефони, планшети, носимі пристрої та хмарні сервіси, обсяг та цінність конфіденційної інформації, що знаходиться в цифровому форматі, постійно зростає. До того ж, важливо відзначити, що зростання кількості користувачів соціальних мереж та інших онлайн-платформ, що створює нові вектори атак та можливості для соціотехнічних атак, також мають бути взяти до уваги, як постійно-прогресуючий ризик. Все це створює ще більшу потребу у розробці ефективних стратегій захисту, оскільки вразливість перед соціотехнічними атаками ставить під загрозу не лише бізнес-структури та урядові організації, а й приватні особи, які часто використовують онлайн-сервіси для зберігання особистої та фінансової інформації, що може призвести до витоку важливих даних, порушення конфіденційності, фінансових втрат, а також завдати шкоди репутації та довірі до організації.

Отже, вивчення та розробка стратегій захисту від соціотехнічних атак стає невід'ємною частиною боротьби з кіберзлочинністю та забезпечення безпеки конфіденційної інформації в цифровому світі. Враховуючи широкий спектр потенційних загроз та ризиків, розвиток ефективних методів захисту від соціотехнічних атак є критично важливим завданням для всіх сфер суспільства і важливою складовою стратегії кібербезпеки в цифрову епоху.

Фішинговий фреймворк GoPhish - це відкрите програмне забезпечення, яке використовується для проведення соціотехнічних атак, зокрема, фішингових кампаній. Цей фреймворк дозволяє користувачам створювати та розгортати фішингові атаки, які спрямовані на отримання конфіденційної інформації, такої як паролі, дані банківських карток та інші особисті дані, шляхом маніпулювання людським фактором.

GoPhish надає можливості створення різноманітних фішингових шаблонів для листів електронної пошти та сторінок веб-сайтів, які виглядають автентично, але насправді призначені для збору особистих даних. Крім того, він забезпечує інструменти для відстеження та аналізу ефективності фішингових кампаній, таких як відкриття листів, кліки по посиланнях та введення конфіденційних даних.

У контексті дослідження шляхів та розробки рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак, GoPhish може відігравати декілька ролей. По-перше Використання GoPhish може допомогти дослідникам та експертам у кібербезпеці аналізувати потенційні загрози, які виникають внаслідок соціотехнічних атак. Вони можуть створювати різноманітні фішингові кампанії за допомогою GoPhish, щоб визначити, наскільки легко атаки можуть бути успішними та які види інформації можуть бути скомпрометовані. По-друге, використання GoPhish дає можливість оцінити ефективність заходів захисту від соціотехнічних атак. Проведення контрольованих фішингових кампаній дозволяє оцінити, як добре підприємство або організація захищені від подібних загроз. По-третє, GoPhish може бути використаний у якості навчального інструменту для підвищення обізнаності персоналу з питань кібербезпеки. Проведення контрольованих фішингових кампаній може допомогти навчити співробітників розпізнавати підозрілі листи та ситуації та реагувати на них належним чином. І нарешті, результати фішингових кампаній, проведених за допомогою GoPhish, можуть слугувати основою для розробки рекомендацій щодо покращення захисту від соціотехнічних атак. Аналізуючи вразливості та недоліки, виявлені під час тестування, дослідники можуть розробити рекомендації щодо поліпшення освіти

користувачів, розробки технічних заходів безпеки та вдосконалення процедур управління ризиками.

Отже, GoPhish може використовуватися як інструмент для проведення досліджень, розробки рекомендацій, навчання та тестування, спрямованих на підвищення захисту від соціотехнічних атак.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження шляхів та розробка рекомендацій щодо захисту конфіденційної інформації від соціотехнічних атак використовуючи інструмент GoPhish.

Об'єкт дослідження – ахист організації або фізичної особи від соц.тех атак

Предмет дослідження – Методи та засоби соц.тех атак, використовуючи інструмент GoPhish

Мета роботи – Дослідження та розуміння загроз, їх аналіз, аналіз методів боротьби з загрозами, розробка рекомендацій на основі власного досвіду, набутого за допомогою інструменту GoPhish.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту від соціально технічних атак, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ВІД СОЦІОТЕХНІЧНИХ АТАК

1.1. Поняття “Соціотехнічна атака”. Аналіз типів та механізмів соц.тех. атак

Згідно з NIST[1] соціальнотехнічна атака визначається як "дії, спрямовані на маніпулювання людьми, щоб вони розкрили конфіденційну інформацію або виконали дії, які ставлять під загрозу безпеку інформаційної системи".

NIST описує соціальнотехнічні атаки як "один з найефективніших методів кіберзлочинів", оскільки вони ґрунтуються на природній схильності людей до довіри та співпраці. Зловмисники ретельно планують свої атаки, вивчаючи жертву та використовуючи інформацію про неї, щоб створити персоналізований та переконливий підхід.

NIST[2,і3] виділяє наступні ключові характеристики соціальнотехнічних атак:

- **Використання людських факторів:** Зловмисники використовують психологічні принципи, щоб маніпулювати жертвами, наприклад, соціальний тиск, дефіцит, авторитет, взаємність та любов.
- **Персоналізація:** Атаки ретельно плануються та адаптуються до кожної жертви, щоб максимізувати шанси на успіх.
- **Обман:** Зловмисники часто видають себе за законних осіб або організації, щоб здобути довіру жертви.
- **Маніпуляція:** Зловмисники використовують різні методи, щоб змусити жертву розкрити інформацію або виконати дії, наприклад, погрози, фальшиві почуття терміновості або апеляції до емоцій.

Механізми соціотехнічних атак

Соціотехнічні атаки ґрунтуються на ряді психологічних принципів, щоб маніпулювати жертвами. Ось деякі з найпоширеніших механізмів, які наводять CERT[2]:

- **Соціальний тиск:**

Зловмисники можуть використовувати почуття обов'язку або лояльності жертви, щоб схилити її до розкриття інформації або виконання дій, які вона зазвичай не робила б. Наприклад, зловмисник може видавати себе за технічного фахівця та попросити жертву надати пароль до її комп'ютера, щоб "виправити проблему".

- **Дефіцит:**

Зловмисники можуть використовувати почуття терміновості або страху жертви, щоб змусити її діяти швидко, не думаючи про наслідки. Наприклад, зловмисник може надіслати електронний лист жертві, який виглядає так, ніби він надходить від її банку, і повідомити їй, що її рахунок був скомпрометований. Зловмисник може потім попросити жертву надати свої банківські дані, щоб "захистити" свої кошти.

- **Авторитет:**

Зловмисники можуть видавати себе за авторитетну фігуру, щоб здобути довіру жертви та змусити її виконувати їхні вказівки. Наприклад, зловмисник може видавати себе за поліцейського та попросити жертву надати особисту інформацію.

- **Взаємність:**

Зловмисники можуть запропонувати жертві щось цінне в обмін на розкриття інформації або виконання дій. Наприклад, зловмисник може запропонувати жертві безкоштовний подарунок або знижку на продукт, якщо вона надасть свою адресу електронної пошти.

- **Симпатія:**

Зловмисники можуть використовувати почуття любові або симпатії жертви, щоб маніпулювати нею. Наприклад, зловмисник може створити фейковий профіль у соціальній мережі та подружитися з жертвою. Зловмисник може потім використовувати цю дружбу, щоб отримати доступ до особистої інформації жертви або переконати її виконати дії, які ставлять під загрозу її безпеку.

Типи соціотехнічних атак

Існує дуже багато різних типів соціотехнічних атак, але деякі з найпоширеніших включають:

- **Фішинг:** Зловмисники надсилають електронні листи, текстові повідомлення або повідомлення в соціальних мережах, які виглядають так, ніби вони надходять від законного джерела, наприклад, банку або веб-сайту онлайн-магазинів. Ці повідомлення зазвичай містять посилання або вкладення, які, якщо на них натиснути, можуть перенаправити жертву на підроблений веб-сайт або заразити її комп'ютер шкідливим програмним забезпеченням.
- **Спірнінг:** Зловмисники телефонують жертві, видаючи себе за співробітника банку, служби технічної підтримки або іншої законної організації. Вони можуть попросити жертву надати особисту інформацію, таку як паролі або номери кредитних карток, або завантажити шкідливе програмне забезпечення на свій комп'ютер.
- **Квиткова атака:** Зловмисники кидають на видному місці USB-накопичувач або інший портативний пристрій, який містить шкідливе програмне забезпечення. Жертва, яка знаходить пристрій, може підключити його до свого комп'ютера, щоб переглянути вміст, що призводить до зараження комп'ютера.
- **Атака типу "людина посередині":** Зловмисники перехоплюють зв'язок між двома сторонами, наприклад, між користувачем і веб-сайтом. Вони можуть підслуховувати або змінювати трафік, щоб вкрасти особисту інформацію або заразити комп'ютер жертви шкідливим програмним забезпеченням.

Узагальнюючи, соціотехнічна атака - це складний процес, який поєднує в собі технічні та соціальні елементи з метою надмірного використання довіри людей або недоліків у їх поведінці для досягнення злочинних мет. Для захисту від таких атак важливо поєднувати технічні заходи безпеки з програмами навчання та освіти з метою підвищення обізнаності користувачів та співробітників щодо потенційних загроз і методів захисту. Тим

1.2 Модель зловмисника

Модель зловмисника[5] - це абстрактне або формалізоване описання дій зловмисника, яке відображає його практичні та теоретичні можливості, апріорні знання, час та місце тощо. Її використовують для аналізу ризиків та розробки засобів захисту інформаційних систем.

Загальна модель складається з 6ти етапів:

1. Розвідка (Reconnaissance):

Зловмисник здійснює розвідку, збираючи інформацію про свої цілі та потенційні жертви. Це може включати аналіз соціальних мереж, вивчення публічної інформації про компанії або особистості, а також сканування систем на предмет вразливостей.

2. Формування атаки (Attack Formulation):

На основі зібраної інформації зловмисник розробляє стратегію атаки. Він визначає, які соціальні і технічні методи використовувати для досягнення своїх мет.

3. Експлуатація (Exploitation):

Зловмисник використовує підготовлені атаки для здійснення нападу на ціль. Це може бути відправка фішингових листів, використання шкідливих програм або навіть особистий контакт з жертвою для отримання доступу до систем або інформації.

4. Отримання доступу (Gaining Access):

Після успішного виконання атаки зловмисник намагається отримати доступ до цільових ресурсів або інформації. Це може включати отримання паролів, ключів доступу або навіть встановлення зловмисного програмного забезпечення на цільові системи.

5. Збір інформації (Information Gathering):

Після отримання доступу зловмисник збирає необхідну інформацію з цільових систем або мережі. Це може бути конфіденційна інформація, особисті дані або будь-яка інша цінна інформація для нього.

6. Етап після атаки (Post-Attack):

Після успішної атаки зловмисник займається приховуванням слідів та збиранням поживної інформації для майбутніх атак. Він може також використовувати отриману інформацію для вимагання викупу, продажу на чорному ринку або використання її для злочинних цілей.

Також, треба звернути увагу на альтернативні типи моделей зломисників, наприклад STRIDE

Модель загроз STRIDE - це mnemonic (мнемонічний код), який допомагає визначити та класифікувати потенційні загрози безпеці інформаційних систем. Модель STRIDE є корисною для аналізу безпеки інформаційних систем на етапі проектування, розробки та експлуатації. Вона допомагає розробникам та фахівцям з безпеки виявити потенційні вразливі місця та вжити заходів для їх усунення. STRIDE є абревіатурою від шести основних типів загроз:

- **Spoofing (Видача себе за іншого):** Зловмисник видає себе за законного користувача, систему або службу, щоб отримати доступ до конфіденційної інформації або ресурсів. Наприклад, фішинговий електронний лист може виглядати так, ніби він надходить від банку, щоб змусити жертву розкрити свої банківські реквізити.
- **Tampering (Зміна даних):** Зловмисник змінює дані в інформаційній системі. Це може призвести до неправильних рішенням, фінансових втрат або інших негативних наслідків. Наприклад, зловмисник може змінити суму на банківському рахунку, щоб вкрасти гроші.і
- **Repudiation (Відмова від дій):** Зловмисник заперечує виконання певних дій в системі. Це може ускладнити розслідування інцидентів безпеки та притягнення зловмисників до відповідальності. Наприклад, зловмисник може стверджувати, що його комп'ютер був зламаний, щоб уникнути звинувачень у кібератраці.
- **Information Disclosure (Розкриття інформації):** Зловмисник отримує несанкціонований доступ до конфіденційної інформації. Це може включати особисті дані, фінансову інформацію, комерційні секрети тощо. Наприклад, зловмисник може зламати веб-сайт і вкрасти номери кредитних карток клієнтів.

- **Denial of Service (Відмова в обслуговуванні):** Зловмисник перевантажує інформаційну систему трафіком або іншими способами робить її недоступною для законних користувачів. Це може призвести до фінансових втрат, втрати продуктивності та інших негативних наслідків. Наприклад, зловмисник може здійснити DDoS-атаку (атака типу "відмова в обслуговуванні"), щоб зробити веб-сайт недоступним для відвідувачів.

Elevation of Privilege (Підвищення прав доступу): Зловмисник отримує більш високий рівень доступу до інформаційної системи, ніж йому дозволено. Це дозволяє зловмиснику виконувати дії, які він не повинен робити, наприклад, видаляти файли або встановлювати шкідливе програмне забезпечення. Наприклад, зловмисник може використовувати експлойт для отримання прав адміністратора на комп'ютері.

1.3 Статистика та потенційні наслідки соціотехнічних атак

Загальна статистика, яка може бути знайдена у дослідженнях та звітах організацій з кібербезпеки, показує, що соціотехнічні атаки стають все більш поширеними і складними. Зокрема, фішингові/спуфінгові атаки залишаються найпоширенішим видом соціотехнічних атак, але з кожним наступним роком, динаміка кількості інцидентів, все ж таки, іде на спад. Чого не можна сказати про деякі інші типи соціотехнічних атак, наприклад: Extortion(Вимагання), BEC((Business Email Compromise) - Компрометація ділової електронної пошти), Tech support (тип шахрайства, під час якого зловмисники видають себе за представників легальної служби технічної підтримки) та інше, чиї показники тільки зростають з кожним роком.

Але все ж таки, в загальному, кількість кейсів стає меншою з кожним роком. (рис. 1.1)

LAST-THREE-YEAR COMPLAINT COUNT COMPARISON

By Complaint Count			Trend from previous Year		
Crime Type	*2023*		*2022*		*2021*
Advanced Fee	8,045	▼	11,264	▲	11,034	▼
BEC	21,489	▼	21,832	▲	19,954	▲
Botnet	540	▼	568		N/A	
Confidence Fraud/Romance	17,823	▼	19,021	▼	24,299	▲
Credit Card/Check Fraud	13,718	▼	22,985	▲	16,750	▼
Crimes Against Children	2,361	▼	2,587	▲	2,167	▼
Data Breach	3,727	▲	2,795	▲	1,287	▼
Employment	15,443	▲	14,946	▼	15,253	▼
Extortion	48,223	▲	39,416	▲	39,360	▼
Government Impersonation	14,190	▲	11,554	▲	11,335	▼
Harassment/Stalking	9,587	▼	11,779		N/A	
Identity Theft	19,778	▼	27,922	▼	51,629	▲
Investment	39,570	▲	30,529	▲	20,561	▲
IPR/Copyright and Counterfeit	1,498	▼	2,183	▼	4,270	▲
Lottery/Sweepstakes/Inheritance	4,168	▼	5,650	▼	5,991	▼
Malware	659	▼	762	▼	810	▼
Non-Payment/Non-Delivery	50,523	▼	51,679	▼	82,478	▼
Other	8,808	▼	9,966	▼	12,346	▲
Overpayment	4,144	▼	6,183	▲	6,108	▼
Personal Data Breach	55,851	▼	58,859	▲	51,829	▲
Phishing/Spoofing	298,878	▼	321,136	▼	342,494	▲
Ransomware	2,825	▲	2,385	▼	3,729	▲
Real Estate	9,521	▼	11,727	▲	11,578	▼
SIM Swap	1,075	▼	2,026		N/A	
Tech Support	37,560	▲	32,538	▲	23,903	▲
Threats of Violence	1,697	▼	2,224		N/A	

Рис. 1.1 Статистика ФБР[6]: типи порушень та кількості випадків за три останні роки

У приклад в цій роботі використовуються статистика скарг до ФБР за три роки: 2021, 2022, та 2023, для наглядного відображення спаду або прогресії випадків та збитків від того чи іншого типу атаки. (рис. 1.1, 1.2) та Діаграма відношення скарг та сбитків на вікові групи людей з, так званим, “кроком” в 10 років. (рис. 1.3)

LAST-THREE-YEAR COMPLAINT LOSS COMPARISON

By Complaint Loss			▼ ▲ = Trend from previous Year
Crime Type	*2023*	*2022*	*2021*
Advanced Fee	$134,516,577 ▲	$104,325,444 ▲	$98,694,137 ▲
BEC	$2,946,830,270 ▲	$2,742,354,049 ▲	$2,395,953,296 ▲
Botnet	$22,422,708 ▲	$17,099,378 ▲	N/A
Confidence Fraud/Romance	$652,544,805 ▼	$735,882,192 ▼	$956,039,739 ▲
Credit Card/Check Fraud	$173,627,614 ▼	264,148,905 ▲	$172,998,385 ▲
Crimes Against Children	$2,031,485 ▲	$577,464 ▲	$198,950 ▼
Data Breach	$534,397,222 ▲	$459,321,859 ▲	$151,568,225 ▲
Employment	$70,234,079 ▲	$52,204,269 ▲	$47,231,023 ▼
Extortion	$74,821,835 ▲	$54,335,128 ▼	$60,577,741 ▼
Government Impersonation	$394,050,518 ▲	$240,553,091 ▲	$142,643,253 ▲
Harassment/Stalking	$9,677,332 ▲	$5,621,402	N/A
Identity Theft	$126,203,809 ▼	189,205,793 ▼	$278,267,918 ▲
Investment	$4,570,275,683 ▲	$3,311,742,206 ▲	$1,455,943,193 ▲
IPR/Copyright and Counterfeit	$7,555,329 ▲	$4,591,177 ▼	$16,365,011 ▲
Lottery/Sweepstakes/Inheritance	$94,502,836 ▲	$83,602,376 ▲	$71,289,089 ▲
Malware	$1,213,317 ▼	$9,326,482 ▲	$5,596,889 ▼
Non-Payment/Non-Delivery	$309,648,416 ▲	$281,770,073 ▼	$337,493,071 ▲
Other	$240,053,059 ▲	$117,686,789 ▲	$75,837,524 ▼
Overpayment	$27,955,195 ▼	$38,335,772 ▲	$33,407,671 ▼
Personal Data Breach	$744,219,879 ▲	$742,438,136 ▲	$517,021,289 ▲
Phishing/Spoofing	$18,728,550 ▼	$160,015,411 ▲	$126,383,513 ▼
Ransomware	$59,641,384 ▲	$34,353,237 ▼	$49,207,908 ▲
Real Estate	$145,243,348 ▼	$396,932,821 ▲	$350,328,166 ▲
SIM Swap	$48,798,103 ▼	$72,652,571	N/A
Tech Support	$924,512,658 ▲	$806,551,993 ▲	$347,657,432 ▲
Threats of Violence	$13,531,178 ▲	$4,972,099	N/A

Рис 1.2 Статистика ФБР: типи порушень та збитки від них (у валюті Американський долар) за три останні роки

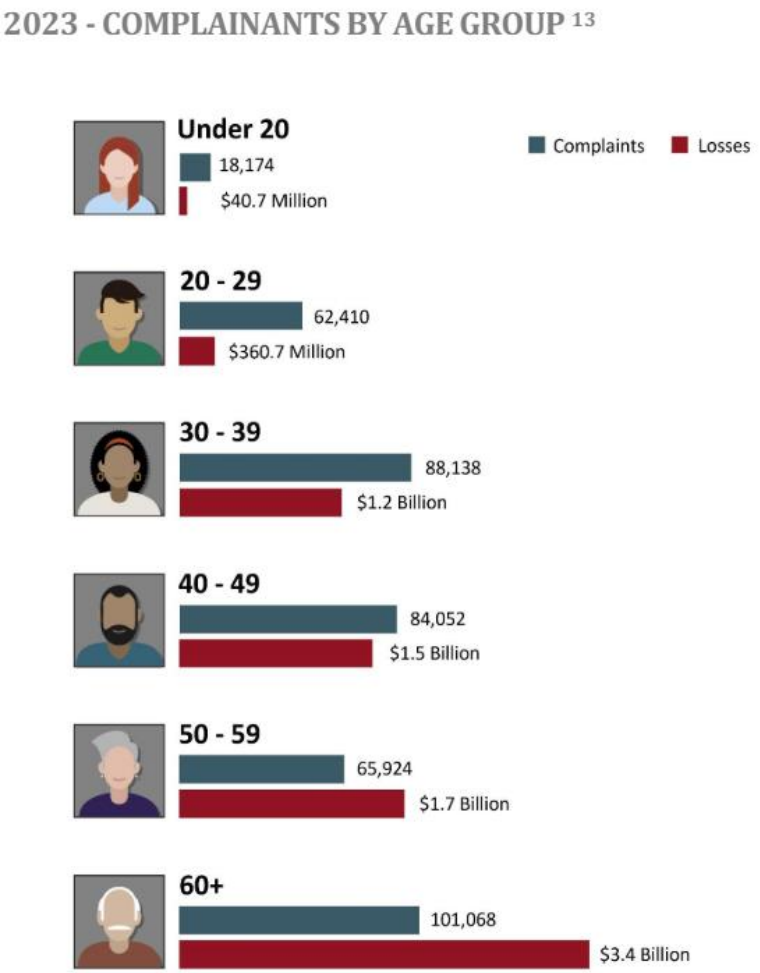

Рис. 1.3 – Діаграма скарг та збитків на вікові групи людей (Статистика Verizon) [7]

Проаналізувавши всі наведені статистики, можна зробити висновок, що соціотехнічні атаки з кожним роком стають більш таргетованими та складними. За графіками ми бачимо, що найбільші збитки завдаються атаками типу BEC, Investment та Tech Support. Перераховані методи шахрайства потребують дуже високого рівня підготовки, обладнання, розвідних даних про жертву, комунікативних та переконуючих психологічних здібностей та часу на підготовку та проведення злочину. Хоча самих інцидентів не так багато, в середньому, у зловмисника виходить нанести збитків на 137132$ за один інцидент (BEC), 115498$ на один інцидент (Investment) та 24614$ на один інцидент (Tech Support). На жаль, кількісні та середні показники, з роками, лише ростуть, але треба відмітити, що типи злочинів, в яких, средні показники збитків на кількість інцидентів були низькими у порівнянні з топовими

позиціями у списку, у 2023 році стрімко почали деградувати. Найнагляднішій приклад – Фішинг

За останній рік кількість інцидентів знизилась майше на 40 тис., що у відсотковому значенні дорівнює всього 7 %, але середній показник збитку на інцидент впав з 498$ на інцидент до 63$ на інцидент. Різниця складає майже 88%. Сукупність цих фактів свідчить про зміну рентабельності на ринку кіберзлочинності, і про ускладнення методів соціотехнічих атак. Не дивлячись на ресурсні затрати, зловмисники проводять все більше і більше складних типів атак, що свідчить про їх рентабельність, та актуальність на сьогодні.

Також, діаграма скарг на інциденти кіберзлочинів та збитків на вікові групи людей свідчить про те, що злодії націлені на більш старшу групу населення, що свідчить про падаючий рівень кіберосвідченності з віком. Це робить старших людей найпріорітетнішою ціллю кібершахраїв.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ВІД СОЦІОТЕХНІЧНИХ АТАК

2.1 Проведення аналізу типових сценаріїв атак

Проведення аналізу типових сценаріїв атак передбачає вивчення та аналіз широкого спектру соціально-інженерних атак з метою виявлення загальних шаблонів та характеристик, які їх об'єднують. Цей процес включає в себе розгляд різноманітних методів, таких як фішинг, інженерія довіри та інші, що використовуються зловмисниками для отримання доступу до конфіденційної інформації або виконання шкідливих дій. Це дозволяє виявити основні стратегії та прийоми, які використовуються зловмисниками, а також ідентифікувати потенційні вразливості, які можуть бути використані для реалізації атак. На основі цього аналізу можна розробити ефективні заходи захисту та превентивні стратегії для запобігання подібним інцидентам у майбутньому.

Спочатку розглянемо фішингові атаки. Типовий сценарій атаки складається приблизно з 5 кроків, а саме:

1. Зловмисник створює підроблений веб-сайт або електронний лист:

- Веб-сайт: Зловмисник може створити веб-сайт, який імітує легітимний веб-сайт, наприклад, сайт банку, онлайн-магазину або соціальної мережі. Цей веб-сайт буде мати схожий дизайн та макет, як і легітимний сайт, щоб обдурити жертв, змушуючи їх повірити, що вони знаходяться на справжньому сайті.
- Електронний лист: Зловмисник може створити електронний лист, який імітує легітимний електронний лист від відомої компанії або організації. Цей електронний лист буде містити логотип компанії, правильне форматування та інші деталі, щоб виглядати переконливо.

2. Зловмисник надсилає електронний лист або розміщує рекламу на веб-сайті:

- Електронний лист: Зловмисник може надіслати цей електронний лист тисячам або мільйонам людей, сподіваючись, що деякі з них відкриють його, клікнуть на посилання в ньому або завантажать вкладення.

- Реклама: Зловмисник може розмістити рекламу на веб-сайтах, які часто відвідують люди, яких він хоче атакувати. Ця реклама може містити посилання на підроблений веб-сайт.

3. Жертва відкриває електронний лист, клікає на посилання або завантажує вкладення:

- Електронний лист: Якщо жертва відкриває електронний лист і клікає на посилання в ньому, вона буде перенаправлена на підроблений веб-сайт.
- Вкладення: Якщо жертва завантажує вкладення, воно може містити шкідливе програмне забезпечення, яке може заразити комп'ютер жертви.

4. Жертва вводить свою конфіденційну інформацію на підробленому веб-сайті:

- Підроблений веб-сайт: На підробленому веб-сайті жертві буде запропоновано ввести свою конфіденційну інформацію, таку як пароль, номер кредитної картки або номер соціального страхування, тощо.
- Зловмисний доступ: Коли жертва вводить свою інформацію, зловмисник може її перехопити та використовувати для крадіжки особистих даних, фінансових коштів або вчинення інших злочинів.

5. Жертва не усвідомлює, що стала жертвою:

- Необізнаність: Жертва може не усвідомлювати, що стала жертвою фішингової атаки, доки не з'ясується, що її особисті дані або гроші були вкрадені.

У даній роботі будуть наведені декілька прикладів інцидентів у великих компаніях, на основі яких в подальшому будуть розроблені рекомендації щодо заходів захисту від подібних кібер-злочинів. Першочергово наведемо приклад типового Фішингу, а саме атаку 2022 року, спрямовану на працівників Google[9], яка призвела **до витоку даних 300 000 користувачів**. Зловмисники використали досить винахідливий метод, щоб здійснити атаку. Вони надсилали електронні листи, які виглядали так, ніби вони надходять від Google Cloud, провідного хмарного сервісу від Google, з проханням оновити інформацію про безпеку. У відправлених листах містилися посилання, які, якщо їх відкрити, перенаправляли жертв на підроблений веб-сайт Google Cloud. Цей сайт був створений з метою

виглядати як офіційний, але насправді збирати особисті дані користувачів. Зловмисники, які стояли за атакою, отримали доступ до імен користувачів, їх паролів та інших особистих даних. Ця атака відбулася на фоні загального зростання фішингу як одного з найпоширеніших методів кіберзлочинності. Зловмисники намагаються використати соціальні та технічні способи маніпуляції, щоб перехопити конфіденційну інформацію або отримати доступ до захищених систем. У цьому конкретному випадку, вони використали довіру до Google та його послуг, а також створили реалістичну імітацію офіційного веб-сайту, щоб здійснити успішну атаку. Цей інцидент є наглядним прикладом типової фішингової атаки. Дана атака була здійснена суто за сценарієм наведеним вище.

Другим прикладом наводимо спуфінгову атаку телефоном, також відому як вішинг. Спуфінг телефоном – більш таргетований та ресурсозатратний тип атак. Зловмисник видає себе за іншу, авторитетну для жертви, особу і має підтримувати контакт з жертвою (в чаті або на телефонній лінії) аж до досягнення своїх цілей. Через це змінюється типовий алгоритм дій зловмисника.

Типовий сценарій спуфінгових атак виглядає приблизно так:

1. Зловмисник збирає інформацію про жертву:

- Соціальні мережі: Зловмисник може шукати інформацію про жертву в соціальних мережах, наприклад, її ім'я, місце роботи, посаду, номер телефону та адресу електронної пошти.
- Інші джерела: Зловмисник може використовувати інші джерела інформації про жертву, такі як веб-сайти компаній, публічні записи або навіть темну мережу.

2. Зловмисник готує телефонний дзвінок:

- Персоналізація: Зловмисник використовує зібрану інформацію, щоб персоналізувати телефонний дзвінок. Він може звертатися до жертви по імені, знати про її посаду або навіть згадувати про нещодавні проекти, над якими вона працювала.
- Встановлення довіри: Зловмисник може видавати себе за представника законного джерела, наприклад, співробітника банку, IT-відділу компанії або державної установи.

3. Зловмисник телефонує жертві:

- Впевнений тон: Зловмисник буде говорити впевнено та професійно, щоб змусити жертву повірити йому.
- Терміновість: Зловмисник може створити відчуття терміновості, стверджуючи, що з рахунком жертви виникла проблема, її комп'ютер заражений шкідливим програмним забезпеченням або їй загрожує шахрайство.
- Маніпуляції: Зловмисник може використовувати різні методи маніпуляції, щоб змусити жертву виконати його вказівки. Він може тиснути на неї, лякати або навіть апелювати до її емоцій.

4. Жертва розкриває конфіденційну інформацію або виконує інструкції зловмисника:

- Паролі: Зловмисник може попросити жертву розкрити свої паролі до банківських рахунків, електронної пошти або інших онлайн-аккаунтів.
- Віддалений доступ: Зловмисник може попросити жертву надати йому віддалений доступ до свого комп'ютера, щоб він міг "вирішити проблему".
- Перекази коштів: Зловмисник може попросити жертву переказати йому гроші під приводом вирішення проблеми з рахунком або оплати послуг.

5. Жертва не усвідомлює, що стала жертвою:

- Необізнаність: Жертва може не усвідомлювати, що стала жертвою спуфінгової атаки, доки не з'ясується, що її особисті дані або гроші були вкрадені.

Як приклад вдалої атаки, розглянутого типу, візьмемо атаку на Німецький Commerzbank[8].

У 2021 році відбулася серйозна спуфінгова атака, спрямована на співробітників німецького банку Commerzbank, яка призвела до витоку 40 мільйонів євро. Зловмисники використали підступний метод, щоб здійснити атаку, видаючи себе за співробітників IT-відділу банку.

Атака розпочалася з того, що зловмисники дзвонили співробітникам банку із номерів, які здалися легітимними, і представлялися як члени IT-відділу. Під виглядом необхідності технічного обслуговування або віддаленого доступу до комп'ютерів, зловмисники переконували співробітників у необхідності надати їм

віддалений доступ до своїх робочих систем. Жертви, намагаючись допомогти службі підтримки, надавали зловмисникам доступ до своїх комп'ютерів. Після цього злочинці могли отримати контроль над системами банку та здійснювати операції з переказу коштів. Згідно з повідомленням Commerzbank, ця атака призвела до втрати банком 40 мільйонів євро. Цей випадок повністю відповідає сценарію наведеному вище.

2.2 Аналіз соціальних інженерних технік

Аналіз соціальних інженерних технік передбачає вивчення та класифікацію різноманітних методів, які використовуються зловмисниками для маніпулювання людьми з метою отримання несанкціонованого доступу до інформації або ресурсів. Для аналізу цих технік можна провести їх класифікацію за різними критеріями, такі як: метод маніпуляції, канал(метод) комунікації з жертвою, цільова аудиторія та використані ресурси.

За каналом зв’язку зловмисників дуже легко класифікувати. Найпопулярнішим методом зв’язку з жертвою є найбільш комфортний, для самої жертви, канал комунікації, тобто пошта, телефонний зв’язок або соціальні мережі. Але є і виключення, наприклад особистий контакт, або через посередника, в приклад можна навести підкинуті носії з шкідливим ПЗ, прохання передати інформацію особисто, побуджуючу жертву на дії, авторитетну для жертви персону, тощо. Деяких своїх цілей зловмисники досягають транслюючи вібро-акустичні сигнали в середовище жертви, наприклад постійний високочастотний звук з невідомого для жертви джерела, який змусить жертву рано чи пізно покинути середовище в якому знаходяться цікаві для зловмисника девайси для подальшого фізичного втручання самого зловмисника.

Цільова аудиторія соціально-інженерних атак може бути різноманітною і залежить від конкретних цілей зловмисників. Ось деякі типи цільової аудиторії, класифіковані за характером: Співробітники компаній (Employees): Зловмисники можуть спрямовувати атаки на співробітників компаній з метою отримання

доступу до конфіденційної інформації, фінансових даних або внутрішніх систем. Клієнти банків та фінансових установ (Bank and Financial Institution Customers): Зловмисники можуть вибирати цільовою аудиторією клієнтів банків та фінансових установ з метою викрасти фінансові дані, паролі або особисту інформацію. Адміністратори систем та IT-персонал (System Administrators and IT Personnel): Зловмисники можуть атакувати адміністраторів систем та IT-персонал з метою отримання доступу до критичних систем або мереж. Публічні посадовці (Public Officials): Зловмисники можуть спрямовувати атаки на публічних посадовців з метою отримання конфіденційної інформації, маніпулювання рішеннями або здійснення інших впливових дій. Вікова група: зловмисники можуть націлено шукати людей з певної вікової групи, використовуючи статистику як на Рис 1.3, знаючи, що на досягнення власних цілей, ресурсів буде витрачено набагато менше, якщо при виборі жертви з однаково-достатнім для задач зловмисника, рівнем доступу до цільової системи, буде вибрана людина з правильної вікової групи.

Цільова аудиторія може бути дуже різноманітною і залежить від мети та характеру конкретної атаки. Зрозуміння потенційної цільової аудиторії допомагає в розробці стратегій захисту та превентивних заходів.

За методом маніпуляції соціальні інженери використовують різні прийоми для отримання несанкціонованого доступу до інформації або ресурсів. Ось кілька найпопулярніших загальних типів маніпуляції, які можна виділити:

1. Психологічний тиск: Цей метод передбачає використання емоційного або психологічного тиску на жертву. Одна з провідних методик телефонних спуферів. Наприклад, соціальний інженер може створювати загрози або підказувати про можливі негативні наслідки у разі відмови від виконання певних дій, наприклад зробити зеркальну транзакцію, щоб повернути вже забрану суму, психологічно давити жертву видаючи себе за високопосадовця силових або керуючих органів влади, погрожувати наслідками від неіснуючого ПЗ на девайсі жертви, видаючи себе за агента технічної служби авторитетної організації, тощо

2. Підроблення авторитету: Зловмисники можуть виглядати або видавати себе за осіб з високим рівнем авторитету або впливу, щоб переконати жертву в

необхідності виконання певних вимог і своєї правоти. Ця техніка популярна майже серед усіх соціотехнічних злодіїв. До цієї техніки можна віднести як і підробку сайтів, електронних пошт, аккаунтів в соціальних мережах, так і видання себе в чаті чи по телефону за дерслужбовця, агента банку, співробітника чи близького жертви, тощо. Зазвичай жертва, під впливом авторітету зловмисника чи його продукту сама іде на зустріч зловмиснику та своїми руками робить все для досягнення його цілей, навіть не піддаючись психологічному тиску з боку атакуючої сторони.

3. Маніпулювання соціальними нормами: Соціальні інженери можуть використовувати норми та очікування, щоб змусити людей діяти певним чином. Наприклад, створюючи ситуації, коли виконання певних дій здається соціально прийнятним або навіть очікуваним. Наприклад фейкові відгуки на самостворенних сайтах-підробках, що побуджує, так званий “стадний інстинкт” або діпфейк відео, голосові повідомлення, фото, скани тексту від руки з підписом, тощо від авторитетних для жертви авторів, що викликає в жертви довіру. Також, зловмисники, які працюють за цією схемою, часто прибігають до соціального ізоляціонізму, переконуючи жертву, що все її оточення вже виконало дії, які потрібні зловмисникам. До маніпулючання соціальними нормами, можно віднести довготривалу інфільтрацію, тобто поступове завоювання довіри жертви через тривалі взаємодії, щоб переконати співробітників виконати фінансові перекази або надати конфіденційну інформацію. Цей процес необмежений по часу і може продовжуватись роками, це залежить тільки від поставлених цілей шахраїв.

4. Створення штучних невідомостей: Соціальні інженери можуть використовувати вигадані ситуації або створювати невідомості, щоб збудити певні емоції або примусити жертву виконати певні дії.

Після упішнього первинного контакту с жертвою і отримання доступу до системи, чи завантаження свого ПЗ до системи жертви, зловмисників можна класифікувати за технічними методами подальшого отримання даних без відома і усвідомлення самої жертви. Найпопулярніші методи отримання інформації наведені нижче.

Кейлогінг – це метод реєстрації натискань клавіш на клавіатурі для отримання конфіденційної інформації, такої як паролі, номери кредитних карток або особисті повідомлення. Зловмисники можуть застосовувати як програмні, так і апаратні типи кейлогерів. **Програмні кейлогери**: Інстальовані на комп'ютер у вигляді шкідливого програмного забезпечення. Вони можуть приховуватися в системі і працювати у фоновому режимі, записуючи всі натискання клавіш. **Апаратні кейлогери**: Фізичні пристрої, що підключаються між клавіатурою і комп'ютером або вбудовуються у саму клавіатуру. Також між зловмисників популярний метод скрінскрейпінгу це метод зчитування інформації, яка відображається на екрані комп'ютера. Це може бути виконано за допомогою програмного забезпечення або зовнішнього пристрою, приєднаного до девайсу жертви, що знімає скріншоти або читає інформацію з екрану і зберігає її, або передає в прямому режимі на носії зловмисника. Третім популярним методом здобування конфіденційної інформації жертви є перехоплення пакетів. Несанкціонование отримання інформації цим методом здійснюється за допомогою перехоплення одиниць даних, що передаються між пристроями в межах мережі, тобто мережевих пакетів. Після втручанна в мережеве середовище жертви злочинне ПЗ чи девайс починає захоплювати, аналізувати і зберігати мережеві пакети, в яких можуть міститись паролі, облікові дані, електронні листи та інші передані дані.

2.3 Тестування та порівняння ефективності методів та засобів захисту

Регулярне проведення тестової кампанії в межах організації вкрай необхідно для виявлення слабких місць в існуючих системах безпеки та оцінки, наскільки ефективно ці системи можуть захистити від реальних загроз. Тестування дає можливість оцінити ефективність існуючих заходів безпеки, таких як політики, процедури, технічні засоби та підготовка персоналу. Допомагає виявити слабкі ланки серед співробіників та навчити їх розпізнавати та реагувати на соціотехнічні

атаки. Результати тестування дають змогу впроваджувати зміни та покращення в заходах безпеки для підвищення захисту від майбутніх атак.

Періодичне тестування заходів безпеки, особливо стосовно соціальних інженерних атак, є критично важливим для підтримання надійного захисту інформації та ресурсів організації. Періодичність тестування систем захисту від соціальних інженерних атак залежить від низки факторів, таких як розмір організації, рівень ризику, галузь, у якій вона працює, та швидкість змін в інформаційних системах і загрозах. Базове тестування безпеки варто проводити щонайменше раз на рік. Це дозволяє виявляти нові вразливості, які могли з’явитися за рік, та забезпечувати підтримання загального рівня безпеки. Для організацій з високим рівнем ризику, таких як фінансові установи або медичні заклади, рекомендується проводити тестування частіше – наприклад, раз на квартал. Це допомагає оперативно виявляти нові загрози та адаптувати захисні заходи. Також тестування має проводитися після будь-яких значних змін в інформаційних системах, наприклад, після впровадження нових програмних або апаратних засобів, змін у політиках безпеки, чи після реорганізації структури компанії. Якщо організація зазнала атаки або стався інцидент безпеки, необхідно провести додаткове позапланове тестування після усунення наслідків. Це допоможе оцінити ефективність виправлень та запобігти повторенню інциденту. Проводити регулярні тренування та навчання співробітників з моделюванням соціальних інженерних атак слід кілька разів на рік, щоб підтримувати високий рівень обізнаності та готовності.

Для оптимізації процесу тестування компанії проводять його за певним алгоритмом. В приклад алгоритму візьмемо компанію "TechSolutions".

Мета: Оцінка ефективності заходів безпеки та підвищення обізнаності співробітників про соціальні інженерні атаки.
Алгоритм проведення:

1. Планування:
   - Визначення мети: Оцінити готовність співробітників до фішингових атак.

- Оцінка ризиків: Аналіз останніх інцидентів та виявлення потенційних загроз.
- Розробка плану: Визначення і засекречення дати проведення фішингової симуляції, відповідальних осіб та критеріїв оцінки.

2. Підготовка:

- Збір інформації: Аналіз поточних політик безпеки та рівня обізнаності співробітників.
- Вибір методів: Розробка сценарію фішингової атаки, який включає підроблений лист від "IT-відділу" з проханням змінити пароль.
- Підготовка матеріалів: Створення фішингових листів та підробленої веб-сторінки для збору даних.

3. Проведення тестування:

- Реалізація сценарію: Розсилка фішингових листів всім співробітникам.
- Збір даних: Фіксація кількості співробітників, які відкрили лист, перейшли за посиланням та ввели свої дані.

4. Аналіз результатів:

- Оцінка вразливостей: Аналіз отриманих даних та визначення відсотка співробітників, які потрапили на фішинг.
- Звітність: Підготовка звіту з результатами тестування та рекомендаціями щодо покращення.

5. Впровадження покращень:

- Корекційні дії: Оновлення політик безпеки, впровадження нових заходів захисту.
- Оновлення навчальних програм: Коригування програм навчання для підвищення обізнаності співробітників.

6. Навчання та тренування співробітників:

- Проведення тренінгів: Організація тренінгів для співробітників з розпізнавання фішингових атак та правильної поведінки у разі їх виявлення.
- Оцінка ефективності: Періодичне тестування обізнаності співробітників.

7. Постійний моніторинг та вдосконалення:

- Регулярний моніторинг: Постійний аналіз нових загроз та вдосконалення заходів безпеки.
- Аналіз тенденцій: Відстеження тенденцій у сфері кібербезпеки та адаптація до них.

Комплекс інструментів, які використовуються, для проведення тесових соціотехнічних атак:

1) GoPhish - це відкритий інструмент для проведення фішингових симуляцій, який дозволяє організаціям перевіряти свої заходи безпеки та навчати співробітників розпізнавати фішингові атаки. Він надає простий у використанні інтерфейс для створення та управління фішинговими кампаніями.

Основні можливості GoPhish – це Простий інтерфейс для створення та налаштування фішингових кампаній, Можливість імпортувати списки цільових співробітників, Інструменти для створення та редагування шаблонів фішингових листів та можливість використовувать власні шаблони, або створювати їх х нуля. GoPhish дає нам дуже багато інформації на аналіз після проведенні кампанії, наприклад: Реальний час відстеження відкриттів листів, переходів за посиланнями та введення даних на фішингових сторінках та детальні звіти з аналітикою результатів кампаній. З переваг, можна виділити те, що GoPhish надає можливість створення та хостингу підроблених веб-сторінок для збору даних та використання SSL для шифрування трафіку.

2) KnowBe4 - це потужна платформа для навчання співробітників кібербезпеці та проведення фішингових симуляцій. Вона допомагає організаціям виявляти вразливості, підвищувати обізнаність персоналу та знижувати ризики, пов'язані з соціально-інженерними атаками.

Основні можливості KnowBe4: Простий інтерфейс для створення та управління фішинговими кампаніями. Велика бібліотека шаблонів фішингових листів та підроблених веб-сторінок. Автоматизація розсилки та відстеження результатів. Широкий спектр навчальних матеріалів для персоналу, включаючи відеоуроки, інтерактивні модулі та курси. Персоналізовані навчальні плани на основі результатів фішингових тестів. Регулярні оновлення контенту для

відповідності актуальним загрозам. Реальний час відстеження дій співробітників: відкриття листів, переходи за посиланнями, введення даних. Детальні звіти з аналітикою результатів кампаній та навчання. Інструменти для оцінки ризиків та побудови звітів для керівництва. Можливість інтеграції з системами управління безпекою та існуючими процесами кібербезпеки. Підтримка API для автоматизації та розширення функціоналу.

3) PhishMe, зараз відомий як **Cofense**, - це спеціалізована платформа, що надає інструменти для проведення фішингових симуляцій і навчання співробітників, допомагаючи організаціям захищатися від соціально-інженерних атак. Платформа спрямована на підвищення обізнаності персоналу про кіберзагрози та зниження ризику успішних фішингових атак. Основні можливості PhishMe (Cofense): Простий у використанні інтерфейс для створення та управління фішинговими кампаніями. Велика бібліотека шаблонів фішингових листів і підроблених веб-сторінок. Можливість кастомізації листів та сторінок для реалістичнішого вигляду. Інтерактивні навчальні модулі та відеоуроки, що навчають співробітників розпізнавати фішингові атаки. Автоматизоване навчання на основі результатів фішингових тестів. Відстеження поведінки співробітників під час фішингових симуляцій: відкриття листів, переходи за посиланнями, введення даних. Детальні звіти з аналітикою результатів кампаній та рекомендаціями щодо покращення. Платформа підтримує інтеграцію з існуючими системами кібербезпеки та управління ризиками. API для автоматизації та розширення функціоналу.

4) Social-Engineer Toolkit (SET) - це потужний набір інструментів для проведення соціально-інженерних тестів і оцінки безпеки. Розроблений спеціально для тестувальників на проникнення та професіоналів з кібербезпеки, SET надає можливість створювати реалістичні соціально-інженерні атаки, щоб оцінити вразливості організації та підвищити обізнаність співробітників. Основні можливості Social-Engineer Toolkit: Можливість створювати фішингові листи з шкідливими вкладеннями або посиланнями. Налаштування підроблених веб-сторінок для збору облікових даних. Цільові фішингові атаки, спрямовані на

конкретних осіб або групи в організації. Використання індивідуальних підходів для підвищення ймовірності успішної атаки. Створення шкідливих USB-накопичувачів, які автоматично виконують атаки при підключенні до комп'ютера. Розповсюдження шкідливих програм через USB. Налаштування серверів для проведення атак у реальному часі. Використання різних модулів для тестування безпеки мережі. Генерація шкідливих QR-кодів, які перенаправляють користувачів на фішингові веб-сайти. Використання QR-кодів для зараження мобільних пристроїв.

Проведення регулярних симуляцій атак за допомогою цих інструментів є критично важливим для підготовки співробітників до реальних загроз. Результати тестувань дозволяють виявляти слабкі місця в системах безпеки, впроваджувати необхідні зміни та покращення, а також підвищувати загальний рівень кіберзахисту організації.

Періодичне тестування та навчання співробітників сприяє створенню культури безпеки в організації, де кожен усвідомлює важливість кібербезпеки та знає, як діяти у разі виявлення потенційної загрози. Це не тільки допомагає захистити організацію від соціально-інженерних атак, але й підвищує загальну стійкість до різноманітних кіберзагроз.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ВІД СОЦІОТЕХНІЧНИХ АТАК

3.1 Реалізація фішингово фреймворку GoPhish

1. **Встановлення та налаштування GoPhish**

Завантаження GoPhish: Перейдіть на офіційний сайт GoPhish (https://getgophish.com) та завантажте останню версію для вашої операційної системи.

Інсталяція: Розпакуйте завантажений архів та запустіть виконавчий файл. Для Windows це буде gophish.exe, для Linux та Mac - відповідний бінарний файл. Після запуску .exe файлу,в терміналі треба буде знайти посилання на ресурс та тимчасовий пароль (рис. 3.1)

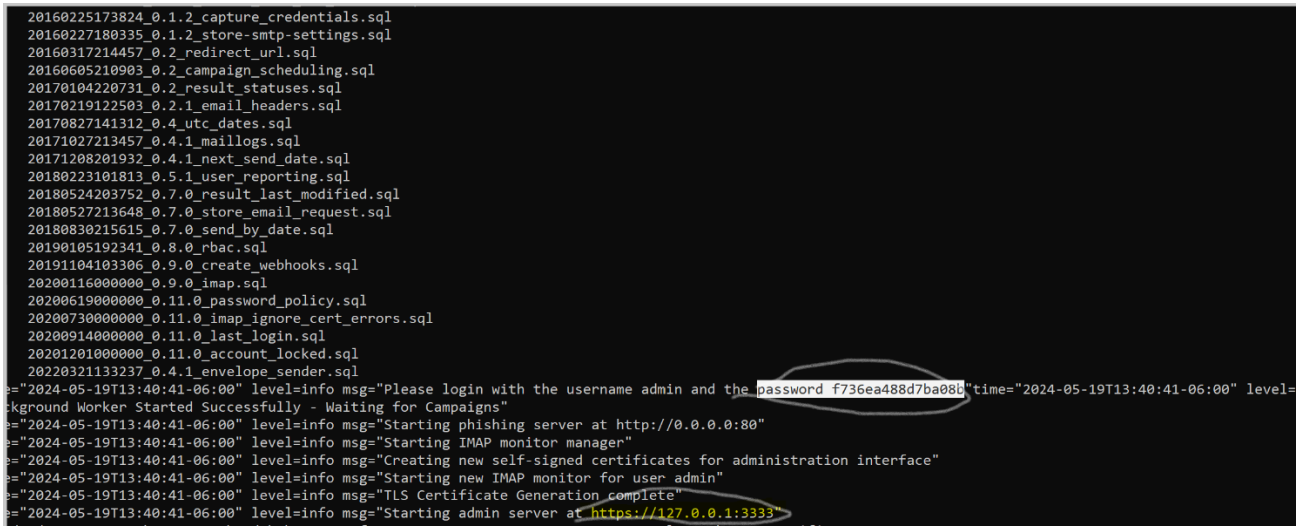

Рис 3.1 Термінал .exe файлу

Після переходу за посиланням придумайте пароль та продублюйте його.

Створення фішингової кампанії

Налаштування серверу відправки: Додайте сервер відправки електронної пошти у розділі Sending Profiles. Це може бути SMTP сервер вашої організації або сторонній сервіс, такий як Gmail або SendGrid (рис. 3.2)

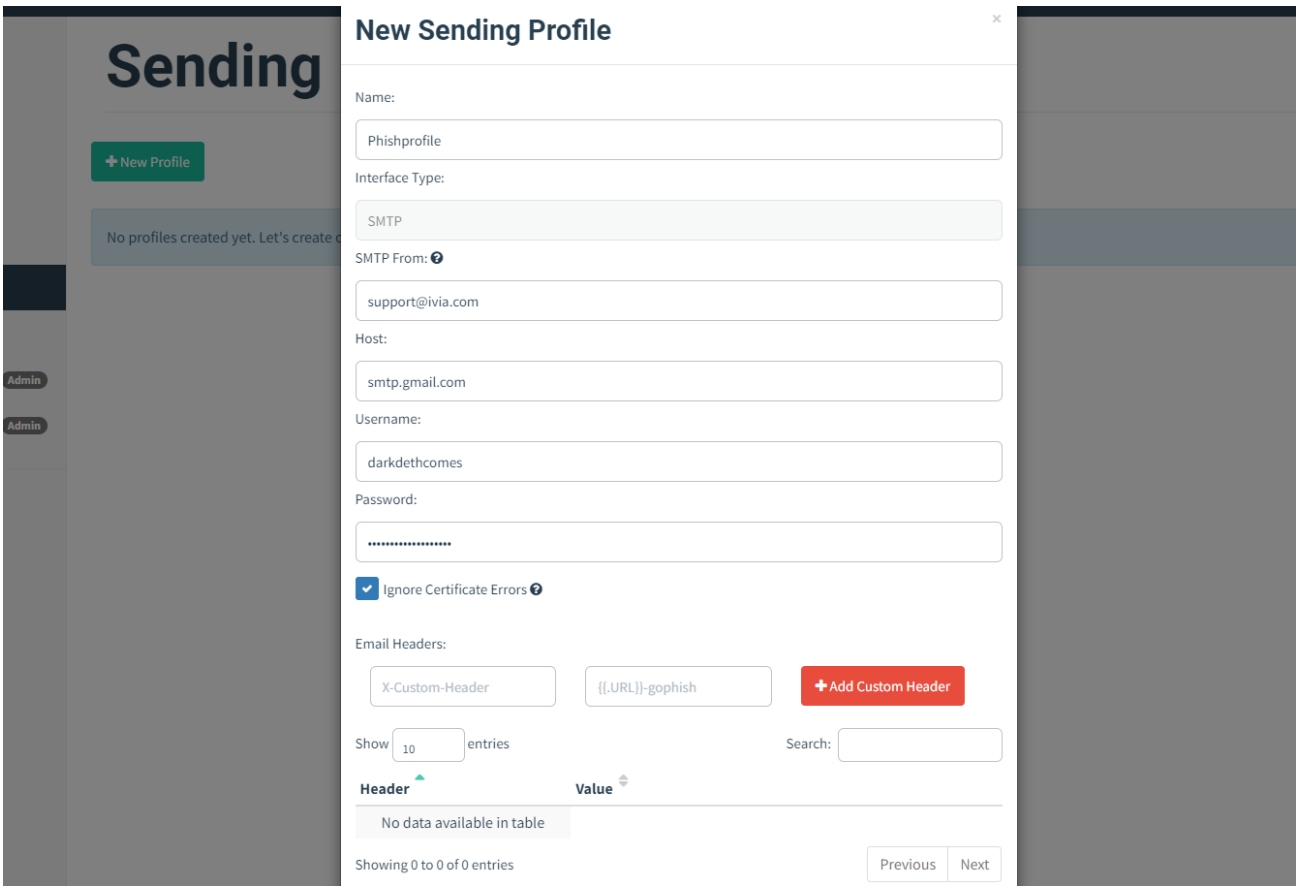

Рис. 3.2 Налаштування профілю відправнка

Після вдалого налаштування на вказану вами пошту має прийти лист “ Default Email from Gophish ” (рис. 3.3)

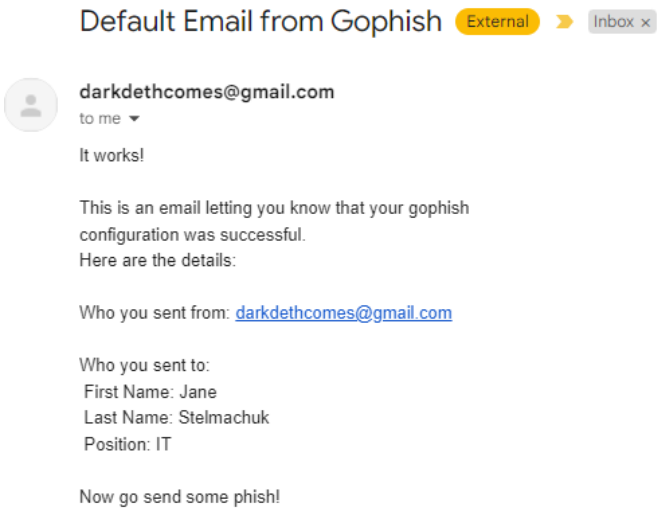

Рис 3.3 Тестовий лист

Після цього переходимо до вкладки групи та додаємо всі пошти, яким ми хочемо надіслати фішинговий лист. Я додав туди всіх диспетчерів зі своєї логістичної компанії для подальшого їх тестування (рис. 3.4)

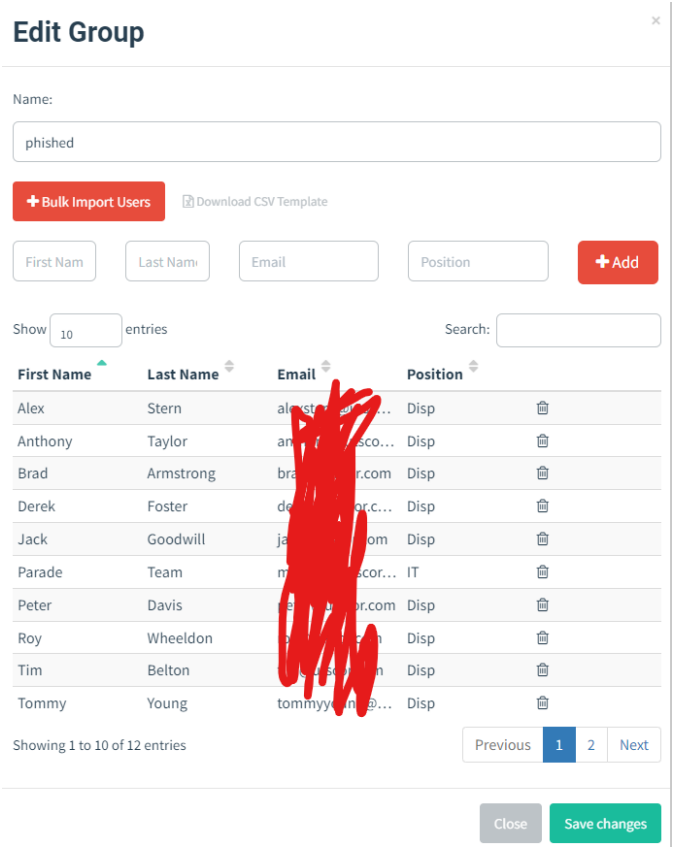

Рис. 3.4 – налаштування груп жертв

Далі треба перейти до розділу Landing Page та імпортувати сайт для імітації. В моєму випадку це був лоадборд Parade, до якого є доступ майже у всіх диспетчерів мого відділу (рис. 3.5)

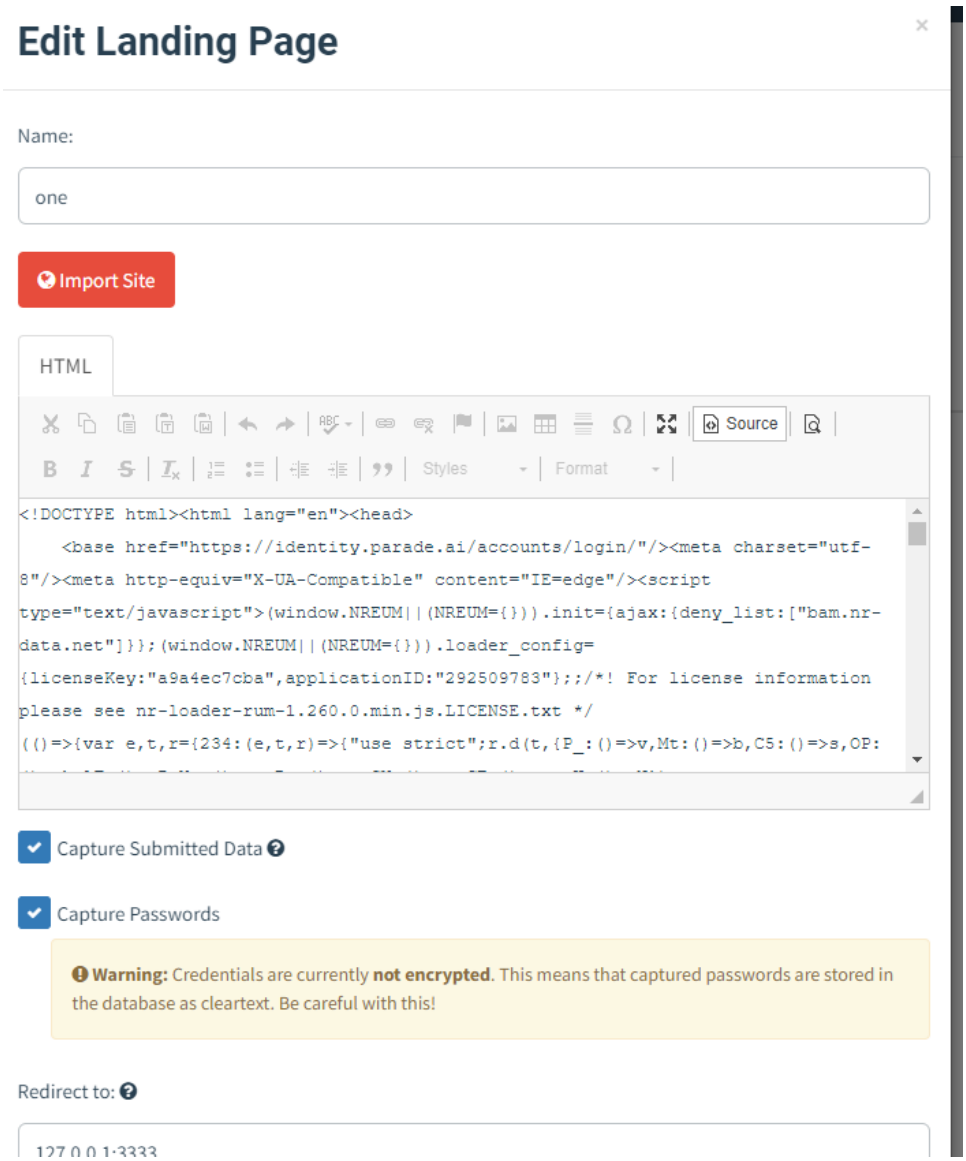

Рис 3.5 Налаштування Landing page

Після треба перейти до налаштуваввння листового темплейту та створити лист, який отримає жертва. (рис. 3.6)

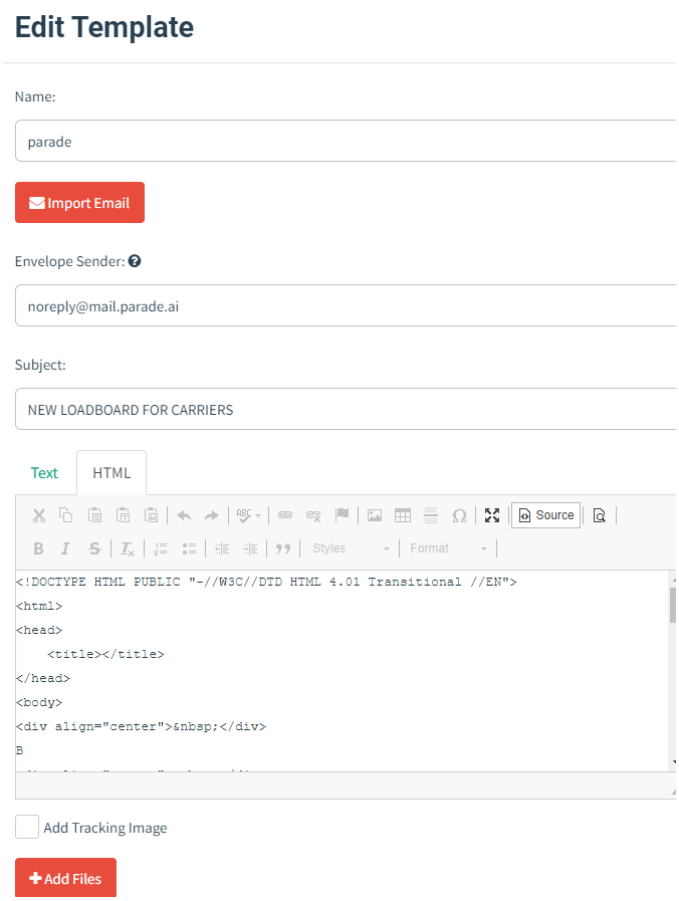

Рис. 3.6 Налаштування темплейту листа

На кінець – розгортання самої кампанії. У вкладці Campaign створюємо та налаштовуємо кампанію під себе, використовуючи темплейти з 3х минулих кроків. (рис. 3.7)

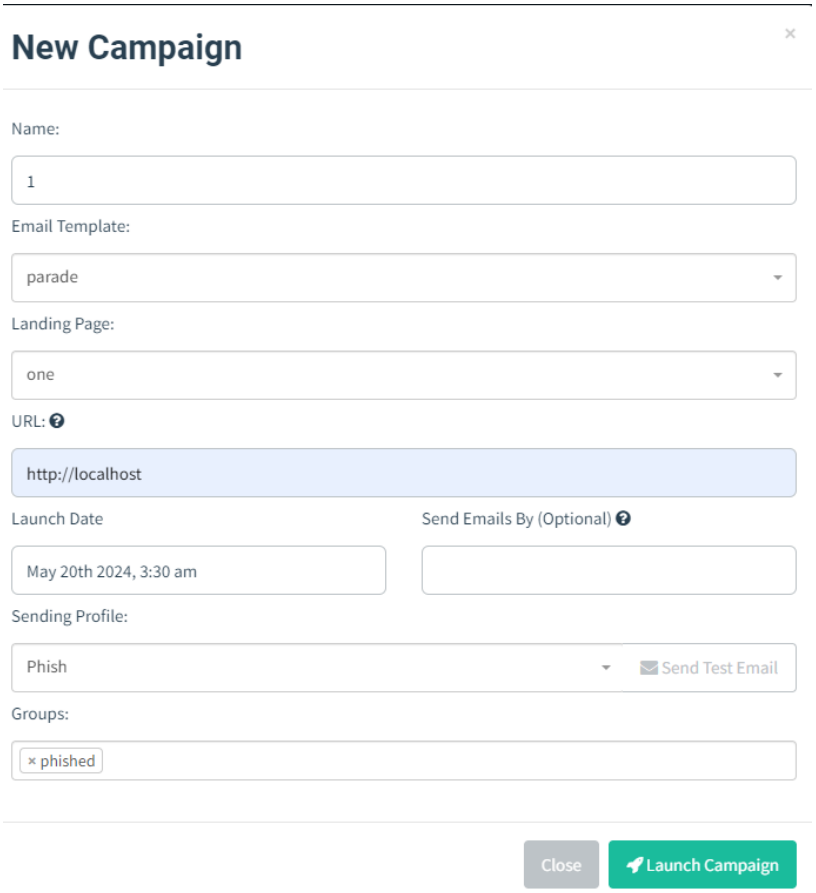

Рис. 3.7 Налаштування розгортання кампанії

Кампанія була розгорнута в межах диспетчерських відділів логістичної компанії UT-Service з ціллю зібрати дані від лоадборду Parade для подальшої обробки інформації, яка зберігається на платформі. До тестування було залучено 15 людей, віковою групою 20-33 років, 2 з яких – керівники відділів (рис. 3.8). За результатами, з 15ти відправлених листів було відкрито лише 2, дані для авторизації ввів тільки один користувач, що свідчить про високий рівень обізнаності персоналу. Не зважаючи на те, що лише дві людини з 15 відкрило листа, дані для авторизації, яка ввела одна з них, були правильними, тобто атаку можна вважати успішною.

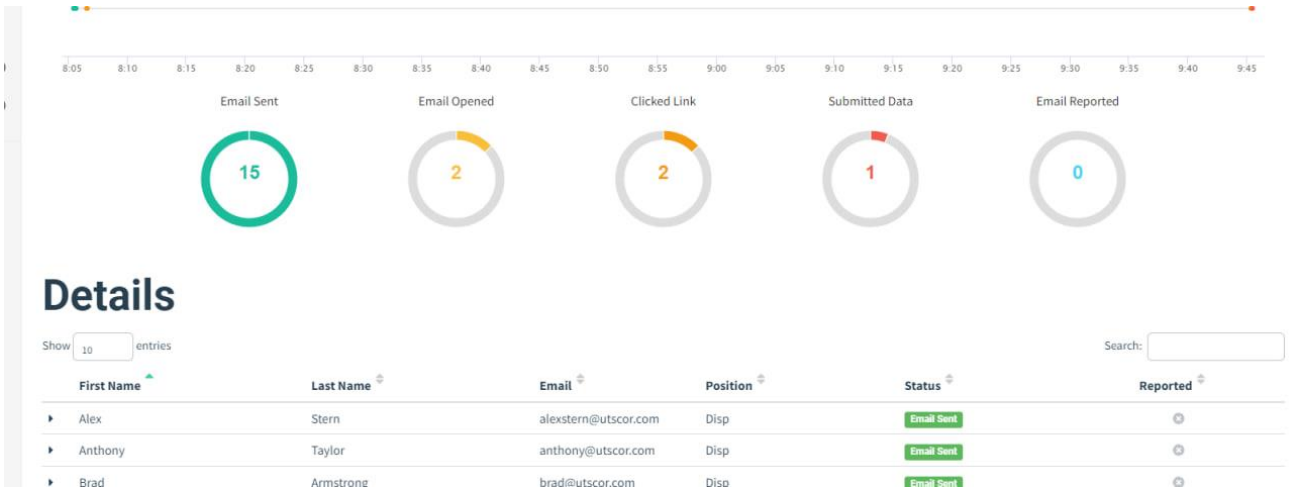

Рис. 3.8. Результати розгорнутої кампанії

Висновок кампанії

Результати тестової кампанії показують, що більшість співробітників дотримується обережності при взаємодії з електронною поштою. Однак той факт, що один з них ввів правильні дані для авторизації, підкреслює необхідність постійного навчання та впровадження технічних заходів для захисту. Реалізація вищенаведених рекомендацій допоможе значно підвищити рівень інформаційної безпеки у вашій компанії.

3.2 Рекомендації щодо захисту конфіденційної інформації від соціотехнічних атак на основі фреймворку GoPhish

На основі аналізу результатів тестової кампанії за допомогою GoPhish, розробимо конкретні рекомендації для підвищення рівня захисту конфіденційної інформації в компанії.

Підвищення обізнаності співробітників
Навчання та тренінги

- **Регулярні тренінги:** Проводьте щоквартальні тренінги з кібербезпеки для всіх співробітників, особливо звертайте увагу на тих, хто провалив тестову кампанію. Тренінги мають включати реальні приклади фішингових атак і практичні поради щодо їх розпізнавання.

- **Орієнтація на нових співробітників**: Включіть кібербезпеку в програму орієнтації нових співробітників.
- **Реалістичні сценарії**: Використовуйте реалістичні фішингові листи для імітації атак під час тренінгів.

Комунікація та інформування

- **Розсилка інформаційних бюлетенів**: Регулярно надсилайте співробітникам бюлетені з інформацією про останні загрози та порадами щодо захисту.
- **Візуальні матеріали:** Розміщуйте постери та брошури в офісі, які нагадують про ознаки фішингових атак.

Інтерактивні заходи

- **Вікторини та опитування**: Організовуйте вікторини та опитування після тренінгів для перевірки засвоєних знань.
- **Рольові ігри**: Проводьте рольові ігри, де співробітники мають реагувати на симульовані фішингові атаки.

Технічні заходи

Антифішингові фільтри

- **Інсталяція та налаштування**: Встановіть та налаштуйте сучасні антифішингові фільтри на поштових серверах.
- **Додаткові модулі**: Використовуйте модулі безпеки для офісних програм, таких як Microsoft Defender для Office 365.

Багатофакторна автентифікація (MFA)

- **Впровадження MFA**: Застосуйте багатофакторну автентифікацію для всіх важливих систем і сервісів компанії.
- **Обов’язковість**: Забезпечте обов’язкове використання MFA для всіх співробітників, особливо для керівників.

Регулярні оновлення

- **Оновлення програмного забезпечення**: Регулярно оновлюйте всі системи та програмне забезпечення для усунення відомих вразливостей.

- **Патч-менеджмент**: Впровадьте систему патч-менеджменту для автоматичного застосування оновлень.

Постійне вдосконалення та тестування

Регулярні фішингові кампанії

- **Періодичність:** Проводьте регулярні фішингові кампанії для перевірки обізнаності співробітників. Наприклад, щоквартально.
- **Аналіз результатів**: Аналізуйте результати кожної кампанії та надавайте зворотний зв’язок співробітникам.

Оцінка ризиків

- **Постійний моніторинг:** Ведіть постійний моніторинг ризиків та вразливостей в компанії.
- **Оновлення політик:** Регулярно переглядайте та оновлюйте політики безпеки.

Культура безпеки

Заохочення співробітників

- **Визнання та винагороди**: Впровадьте систему визнання та винагороди для співробітників, які активно допомагають виявляти загрози.
- **Конкурси та нагороди:** Організовуйте конкурси з кібербезпеки та нагороджуйте переможців.

Зворотний зв’язок

- **Звітування про інциденти**: Заохочуйте співробітників звітувати про підозрілі листи та інциденти. Створіть просту та зрозумілу процедуру звітування.
- **Система звітування:** Впровадьте інтуїтивно зрозумілу систему звітування про інциденти.

Співпраця з фахівцями безпеки

Зовнішні аудити

- **Регулярні аудити:** Проводьте регулярні зовнішні аудити безпеки та тестування на проникнення.
- **Аудит безпеки:** Щорічний зовнішній аудит для оцінки поточного рівня захисту.ш

Консультації

- **Залучення експертів**: Співпрацюйте з експертами з кібербезпеки для постійного вдосконалення систем захисту.
- **Тренінги від експертів:** Залучайте експертів для проведення спеціалізованих тренінгів та консультацій.

Реалізація вищезазначених рекомендацій на основі фреймворку GoPhish допоможе значно компанії значно підвищити рівень захисту від соціотехнічних атак. Регулярне навчання, технічні заходи, постійне тестування та культура безпеки створять надійну систему захисту конфіденційної інформації.

ВИСНОВКИ

У даному дослідженні ми розглянули проблему забезпечення захисту конфіденційної інформації від соціотехнічних атак, детально проаналізували типи та механізми таких атак, а також вивчили методи та засоби їх запобігання. Соціотехнічні атаки є складними, багатофакторними загрозами, що спрямовані на маніпулювання людьми для отримання несанкціонованого доступу до конфіденційної інформації. Зловмисники, які здійснюють соціотехнічні атаки, можуть мати різні мотиви та ресурси, починаючи від окремих хакерів і закінчуючи організованими групами. Соціотехнічні атаки мають значний вплив на організації, спричиняючи фінансові втрати, компрометацію даних та шкоду репутації.

Вивчення різноманітних випадків соціально-інженерних атак виявило загальні шаблони та методи, що використовуються зловмисниками. Було розроблено класифікацію технік маніпулювання, таких як фішинг, вішинг, смішинг та інші. Проведення симуляцій атак дозволило оцінити ефективність існуючих заходів безпеки та виявити їхні слабкі місця.

Реалізація фішингового фреймворку GoPhish включала встановлення та налаштування фреймворку для організації та проведення фішингових кампаній. Використання GoPhish для моніторингу та аналізу результатів кампаній дозволяє швидко виявляти атаки та реагувати на них. На основі цього було розроблено конкретні заходи для підвищення рівня обізнаності співробітників, впровадження технічних рішень та створення культури безпеки в організації.

Проведений аналіз та дослідження показали, що соціотехнічні атаки є серйозною загрозою для конфіденційної інформації будь-якої організації. Використання фреймворку GoPhish для тестування та навчання співробітників є ефективним методом підвищення рівня захисту від таких атак. Розроблені рекомендації, що базуються на результатах фішингових кампаній, включають навчання співробітників, впровадження технічних заходів безпеки та формування культури інформаційної безпеки, що разом створює комплексну систему захисту від соціотехнічних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST URL: https://www.nist.gov/cybersecurity (дата звернення: 26.11.2023).

2. NIST Cybersecurity Framework (CSF) URL: https://www.nist.gov/cyberframework (дата звернення: 26.11.2023).

3. NIST Computer Security Incident Response Center (CSIRC) URL: **https://csrc.nist.gov/**

(Accessed December 3, 2023).

4. NIST National Initiative for Cybersecurity Education (NICE) URL: **https://www.nist.gov/itl/applied-cybersecurity/nice** (дата звернення: 26.11.2023).

5 і (CERT) URL: **https://www.sei.cmu.edu/about/divisions/cert/** (дата звернення: 26.11.2023).

6. Статистика ФБР URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (дата звернення: 28.11.2023).

7. Статистика Verizon URL: https://www.verizon.com/business/resources/reports/dbir/

(дата звернення: 26.11.2023).

8. Атака на Commerzbank URL: https://www.commerzbank.de/konten-zahlungsverkehr/wissen/sicherheit-onlinebanking/phishing/ (дата звернення: 26.11.2023).

9. Атака на Google URL: https://www.theverge.com/cyber-security

(дата звернення: 26.11.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)