

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

магістр

(ступінь вищої освіти)

на тему Аналіз методів виявлення та протидії фішинговим атакам на веб-ресурси
(назва теми)

Виконав: студент 6 курсу, групи БК-812м

Спеціальності 125 Кібербезпека

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних і комунікаційних мереж

ВАРОВ А.П

(ПРІЗВИЩЕ та ініціали)

Керівник НЕЛАСА Г.В.

(ПРІЗВИЩЕ та ініціали)

Рецензент

(ПРІЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІБтаН

к. ф.-м. н. Андрій КОРОТУН

« _____ » _____ 20__ року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ВАРОВА Антона Павловича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз методів виявлення та протидії фішинговим атакам на веб-ресурси.

Analysis of methods for detecting and countering phishing attacks on web resources.

керівник проєкту роботи к.т.н., доцент НЕЛАСА Ганна Вікторівна,

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

затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 475

2. Строк подання студентом проєкту (роботи) «08» грудня 2023 року

3. Вихідні дані до проєкту (роботи) методи та засоби виявлення та протидії фішинговим атакам на веб-ресурси

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Дослідити теоретичні аспекти аналізу фішингових атак; визначити методи, алгоритми та технології застосування фішингових атак на веб-ресурси; дослідити методи, алгоритми та технології протидії фішинговим атакам на веб-ресурси

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів) 17 рисунків (приклади фішингових атак; інтерфейси фішингового ПЗ; схеми алгоритмів роботи ПЗ; інтерфейси антифішингового ПЗ). Презентація доповіді (підготовлена в Microsoft PowerPoint)

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	прийняв виконане завдання
1-4	Неласа Г. В., доцент кафедри ІБтаН	10.09.23	01.12.21
Нормоконтроль	Корольков Р. Ю., доцент. кафедри ІБтаН		

7. Дата видачі завдання «10» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження	12.09.23 – 21.09.23	
2.	Огляд нормативно-правових актів в сфері захисту	22.09.23 – 07.10.23	
3.	Дослідження методів і засобів фішингових атак	08.10.23 – 20.10.23	
4.	Аналіз застосування фішингових атак на веб-ресурси	21.10.23 – 10.11.23	
5.	Виконання графічної пояснювальної записки	11.11.23 – 03.12.23	
6.	Оформлення матеріалів магістерської роботи	04.12.23 – 10.12.23	

Студент

_____ Антон ВАРОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи)

_____ Ганна НЕЛАСА
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 69 с., 28 рис., 28 джерел.

АНАЛІЗ ФІШИНГОВИХ АТАК, БЕЗПЕКА ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, КІБЕРЗЛОЧИННІСТЬ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ПЕРСОНАЛЬНА ІНФОРМАЦІЯ, СОЦІАЛЬНИЙ ІНЖЕНЕРІНГ, ФІШИНГ

Об'єкт дослідження – фішингові атаки, які спрямовані на веб-ресурси.

Мета роботи – систематизація та аналіз сучасних методів виявлення та протидії фішинговим атакам на веб-ресурсах. Визначення ефективних технологій та стратегій, спроможних забезпечити надійний захист інформації та користувачів в онлайн середовищі.

Методи дослідження – наукова абстракція, аналіз і синтез (для розкриття теоретичних положень), формалізація (для опису вимог щодо захисту інформації в інформаційно-телекомунікаційних системах) порівняння (для оцінки переваг і недоліків методів протидії фішинговим атакам) та методи системного підходу.

У роботі аналізуються сучасні методи виявлення фішингових атак, визначаються їх характеристики та ефективність у різних сценаріях. Розглядаються технології ідентифікації та автентифікації, їх застосування в інформаційно-телекомунікаційних системах, а також вивчається роль нормативно-правового забезпечення у забезпеченні безпеки веб-ресурсів. Робота пропонує комплексний підхід до розгляду проблематики фішингових атак і надає рекомендації з підвищення ефективності заходів захисту.

ABSTRACT

Explanatory note to the master's thesis: 69 p., 28 fig., 28 sources.

ANALYSIS OF PHISHING ATTACKS, INFORMATION SECURITY, CYBER SECURITY, CYBERCRIME, UNAUTHORIZED ACCESS, PERSONAL INFORMATION, SOCIAL ENGINEERING, PHISHING

The object of the research is phishing attacks aimed at web resources.

The purpose of the work is systematization and analysis of modern methods of detecting and countering phishing attacks on web resources. Determination of effective technologies and strategies capable of ensuring reliable protection of information and users in the online environment.

Research methods – scientific abstraction, analysis and synthesis (to reveal theoretical propositions), formalization (to describe the requirements for information protection in information and telecommunication systems), comparison (to assess the advantages and disadvantages of methods of countering phishing attacks), and methods of a system approach.

The work analyzes modern methods of detecting phishing attacks, determines their characteristics and effectiveness in various scenarios. Identification and authentication technologies, their application in information and telecommunication systems are considered, as well as the role of regulatory and legal support in ensuring the security of web resources is studied. The work offers a comprehensive approach to considering the problem of phishing attacks and provides recommendations for increasing the effectiveness of protection measures.

ЗМІСТ

Перелік скорочень.....	7
Вступ	8
1 Теоретичні аспекти аналізу фішингових атак.....	9
1.1 Визначення фішингу та його видів.....	11
1.2 Огляд основних методів фішингу.....	14
1.3 Поглиблений аналіз інструментів та механізмів, що використовуються при фішингових атаках.....	23
1.4 Фішингова атака на практиці.....	32
Висновки до першого розділу.....	40
2 Методи, алгоритми та технології виявлення фішингових атак.....	41
2.1 Аналіз методів виявлення фішингу.....	41
2.1.1 Аналіз характеристик фішингових атак.....	42
2.1.2 Системи виявлення фішингових атак.....	43
2.2 Роль машинного навчання та штучного інтелекту в системах виявлення фішингу.....	44
Висновки до другого розділу.....	47
3 Протидія фішинговим атакам: технологічні та організаційні аспекти.....	48
3.1 Розгляд технологічних методів захисту від фішингу.....	49
3.1.1 Антифішингова система Netcraft.....	50
3.1.2 Антифішингова система SpoofGuard.....	52
3.1.3 Візуалізації бінарних даних та МН у протидії фішингу.....	54
3.2 Аналіз організаційних заходів для запобігання фішинговим атакам.....	58
3.2.1 Інформаційна освіта та навчання.....	59
3.2.2 Розробка плану реагування на інциденти.....	61
Висновки до третього розділу.....	62
Висновки.....	64
Перелік джерел посилань	66

ПЕРЕЛІК СКОРОЧЕНЬ

BM	– віртуальна мережа;
IC	– інформаційна система;
MH	– машинне навчання;
ПЗ	– програмне забезпечення;
CI	– соціальна інженерія;
ARP	– address resolution protocol ‘протокол визначення адрес’;
DFW	– distributed firewall ‘розподілений міжмережевий екран’;
DHCP	– dynamic host configuration protocol ‘протокол динамічної конфігурації вузла’;
DNS	– domain name system ‘ієрархічна розподілена система перетворення імені хоста в IP-адресу’;
HTTPS	– hypertext transfer protocol secure ‘протокол передачі даних’;
HTML	– hypertext markup language ‘мова розмітки гіпертексту’;
IP	– internet protocol address ‘ідентифікатор мережевого рівня’ графічної інформації’;
MAC	– media access control ‘управління доступом до посередників’;
MITM	– man in the middle ‘людина посередині’ інформації’;
SMS	– short message service ‘послуга обміну короткими текстовими повідомленнями в телекомунікаційних мережах’;
SSL	– secure sockets layer ‘рівень захищених сокетів’;
TOFU	– trust on first use ‘режим фільтрації IP-адрес’;
URL	– uniform resource locator ‘уніфікований локатор ресурсів’;
VLAN	– virtual local area network ‘віртуальна локальна комп'ютерна мережа’;
VPN	– virtual private network ‘віртуальна приватна мережа’;
2FA	– two-factor authentication ‘метод додаткового захисту облікового запису’.

ВСТУП

В умовах неперервного розвитку інформаційних технологій та зростаючої значущості веб-ресурсів у сучасному суспільстві питання інформаційної безпеки та захисту від фішингових атак набувають особливого значення. Загроза втрати особистих даних, конфіденційної інформації та безпеки веб-ресурсів стає надто серйозною, вимагаючи детального розгляду та розробки ефективних заходів протидії.

Метою цього дослідження є аналіз сучасних методів виявлення та протидії фішинговим атакам на веб-ресурси, зосереджуючись на розгляді різних технік, інструментів та стратегій, використовуваних зловмисниками для здійснення фішингу. Вивчення цих аспектів дозволить розкрити складність проблематики фішингових атак та розробити практичні рекомендації для підвищення ефективності заходів безпеки.

Зазначена тема не тільки визначає актуальність дослідження, але й визначає його вагомість в контексті сучасних викликів та загроз інформаційної безпеки. Наголос на аналізі різноманітних методів виявлення та стратегій протидії створить необхідну базу для розробки практичних стратегій захисту від фішингу на веб-ресурсах.

В ході роботи над дипломною темою важливо враховувати не лише технічні аспекти захисту від фішингових атак, але й ефективно поєднувати їх із сучасними вимогами нормативно-правового середовища. Отже, дана робота має на меті вирішення важливої проблеми інформаційної безпеки, привертаючи увагу до комплексного підходу до виявлення та протидії фішинговим атакам, що враховує як технічні, так і юридичні аспекти.

1 ТЕОРЕТИЧНІ АСПЕКТИ АНАЛІЗУ ФІШИНГОВИХ АТАК

За останні роки фішингові атаки стали однією з найбільш серйозних загроз в інформаційному просторі. Розгляд теоретичних аспектів цього явища є важливим для розуміння його сутності та механізмів дії.

Однією з основних характеристик фішингових атак є їх витонченість і постійна еволюція. Зловмисники вдосконалюють свої методи, використовуючи нові технології та тактики, щоб обійти традиційні системи захисту. Це створює виклик для розробників безпеки та органів правопорядку, які повинні постійно адаптуватися до зростаючого рівня винахідливості та хитрості атак [13].

Дослідження різних видів фішингових атак є ключовим етапом в аналізі цього явища. Вони можуть включати СІ, де атакуючі використовують психологічні методи для отримання конфіденційної інформації, або технічний фішинг, який базується на використанні шкідливого ПЗ для отримання доступу до системи.

Поняття фішингу також тісно пов'язане з питанням СІ. Атаки використовують маніпуляції та обман для отримання інформації, здебільшого використовуючи довіру або недбалість користувачів. Розуміння цих теоретичних аспектів є критично важливим для розробки ефективних стратегій протидії та захисту від фішингових атак.

Фішинг є видом кібератаки, який спрямований на шахрайське отримання конфіденційних даних від користувачів шляхом підробки веб-сайтів, електронних повідомлень або інших комунікаційних каналів. Зловмисники, виступаючи як відомі та довірені джерела, намагаються обманути користувачів, переконати їх розкрити особисту інформацію, таку як паролі, номери банківських карток, соціальні номери та інші конфіденційні дані.

Фішингові атаки характеризуються наступними особливостями:

- СІ: фішингові атаки використовують методи соціальної маніпуляції, щоб викликати довіру та спонукати користувачів до виконання певних дій, які можуть викрити їх конфіденційну інформацію;

- підробка веб-сайтів: зловмисники створюють фальшиві веб-сайти, які виглядають абсолютно ідентичними до оригінальних, з метою залучення користувачів до введення своїх особистих даних;

- використання електронних повідомлень: фішингові атаки можуть бути здійснені через електронні листи, повідомлення в соціальних мережах або миттєві повідомлення, де зловмисники намагаються переконати користувачів у важливості негайного реагування та надання своїх конфіденційних даних;

- направленість на чутливу інформацію: фішингові атаки спрямовані на отримання важливих особистих даних, таких як паролі, фінансова інформація, дані банківських карток, соціальні номери та інша конфіденційна інформація [13].

Фішингові атаки можуть мати серйозні наслідки для користувачів та організацій. Деякі з найпоширеніших наслідків включають:

- крадіжка особистих даних: зловмисники можуть отримати доступ до особистої інформації користувачів, що може призвести до крадіжки ідентичності, шахрайства або інших злочинів;

- фінансові втрати: шляхом отримання фінансових даних, таких як номери банківських карток або паролі до електронних платіжних систем, зловмисники можуть заволодіти коштами користувачів;

- пошкодження репутації: якщо веб-сайт або організація стають жертвою фішингової атаки, це може призвести до пошкодження репутації та втрати довіри користувачів [14];

1.1 Визначення фішингу та його видів

Незважаючи на те, що Інтернет надає безліч переваг, він також приховує різноманітні загрози кібербезпеки, які використовуються для атак на нічого не підозрюючих користувачів онлайн. Злочинці використовують електронну пошту, голосовий зв'язок, месенджери та соціальні мережі, щоб взаємодіяти з потенційними жертвами.

У зв'язку з асинхронністю, характерною для електронної пошти, зловмисні схеми СІ на її основі стають все більш поширеними інструментами, які використовують кіберзлочинці. Згідно з нещодавньою статистикою, 96% фішингових атак були здійснені через електронну пошту [2]. Враховуючи те, що ці шахрайські електронні листи мають відносно низьку собівартість для зловмисників [3], вони можуть стати причиною суттєвих фінансових ризиків для потенційних жертв.

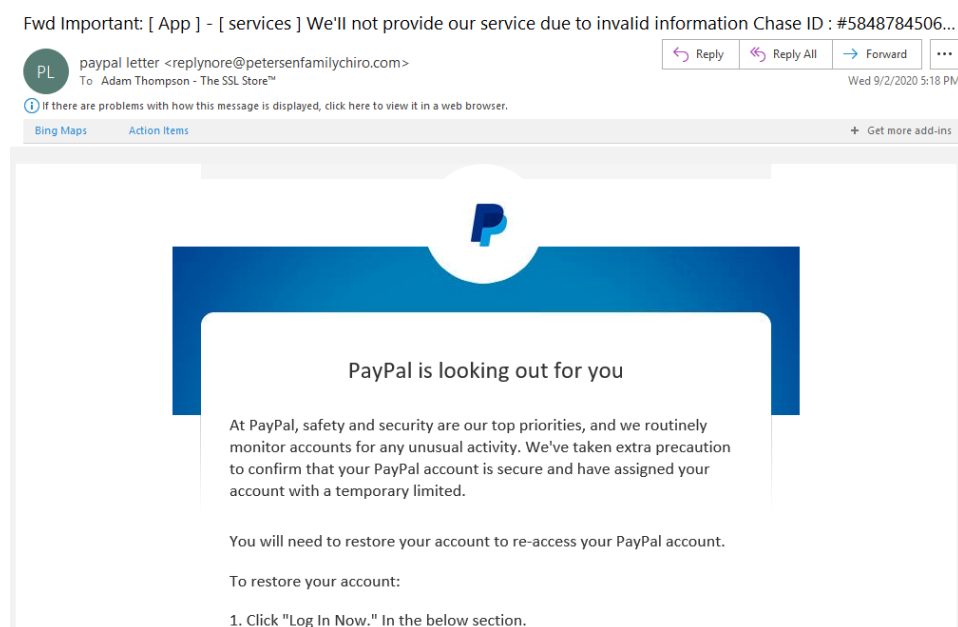


Рисунок 1.1 – приклад фішингового листа, отриманного електронною поштою [4]

Важливо розрізняти основні типи шахрайських електронних листів, такі як сноушунг, оманливий фішинг та цільовий фішинг. Ці види фішингу використовуються зловмисниками для видачі себе за легальні бізнес-організації. Це відкриває їм широкий простір для введення людини у оману задля розкриття своїх персональних даних та фінансової інформації, а також виконання переказу коштів шахраям.

Останнім часом, фішингові атаки набувають нових форм та хитрощів, включаючи використання штучного інтелекту та соціальних інженерних методів для створення більш обманливих та переконливих схем [5]. Відтак, освіта та підвищення кібербезпеки стають ключовими елементами для ефективної протидії цим загрозам.

Окрім того, разом із зростанням популярності таких месенджерів, як Telegram, Signal, WhatsApp, та Viber, зростає і кількість шахрайських схем, які використовуються у них. Лише у Telegram за 2022 рік було зареєстровано 378,496 спроб викрадення аккаунту за допомогою фішингових посилань [6]. Загалом, ці методи за своєю суттю майже нічим не відрізняються від методів, притаманних фішингу через електронну пошту, але вони теж мають свої певні особливості

Фішинг через месенджери використовує хитрі методи з метою залучення уваги та отримання довіри потенційних жертв. Це включає створення профілів відомих осіб чи компаній, а також застосування загадкових сценаріїв, що спонукають користувачів до виконання небезпечних дій.

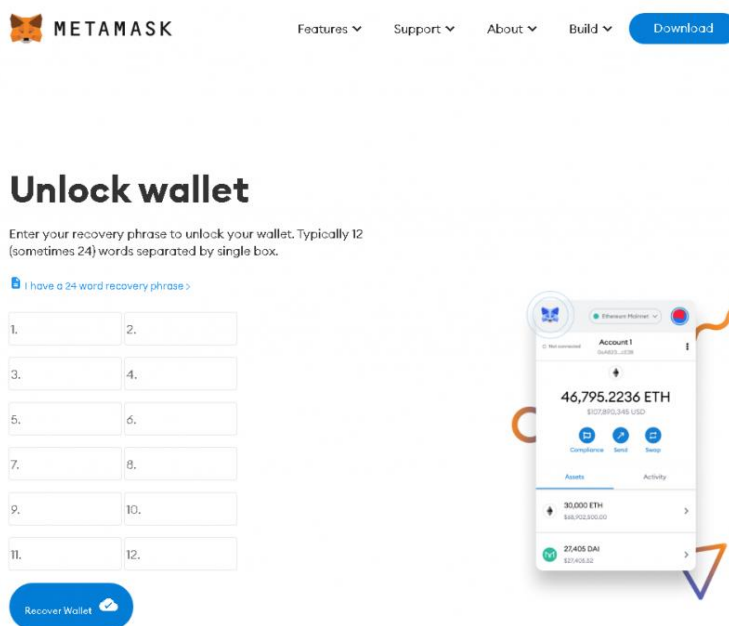


Рисунок 1.2 – Приклад спонукання до виконання небезпечних дій.

Фішери старанно працюють над удосконаленням своїх методів, імітуючи типові юзер-флоу та інтерфейси відомих месенджерів, таких як WhatsApp, Telegram чи Facebook Messenger. Це робить їхні атаки менш підозрілими для користувачів, оскільки вони можуть виглядати як звичайні повідомлення від контактів жертви.

Сутність фішингу через месенджери полягає у використанні СІ для отримання ключових інформаційних даних. Зловмисники часто представляються за друзів, колег чи офіційних представників, використовуючи психологічні та емоційні методи для досягнення своїх цілей.

1.2 Огляд основних методів фішингу та їх характеристики

В основному фішингові атаки поділяються на:

- оманливий фішинг;
- цільовий фішинг;
- вейлінг;
- фармінг;
- смішинг;
- вішинг;
- клонувальний фішинг;
- сноушуінг.



Рисунок 1.3 – Типи фішингових атак

Оманливий фішинг є однією з найпоширеніших та підступних форм фішингових атак, яка спрямована введення користувачів в оману та отримання

їх конфіденційних даних. Цей вид фішингу базується на використанні маніпуляцій та вигаданих сценаріїв для переконання людей поділитися своїми особистими чи фінансовими даними.

Оманливий фішинг часто має форму електронних листів, повідомлень або веб-сайтів, що імітують легітимні джерела, такі як банківські установи, соціальні мережі чи відомі компанії. Атаки цього типу вимагають від атакуючих високого рівня навичок «втирання» у довіру та імітації легітимності для того, щоб атаки виглядали максимально автентично та не викликали підозр.

Однією з загальних тактик оманливого фішингу є використання логотипів та графічних елементів, ідентичних тим, які використовуються справжніми сервісами чи організаціями. Це створює ілюзію надійності та привертає увагу потенційних жертв. Нерідко, атаки цього типу супроводжуються високоякісними текстами та поясненнями, щоб викликати в користувача довіру та переконаність у необхідності негайних дій.

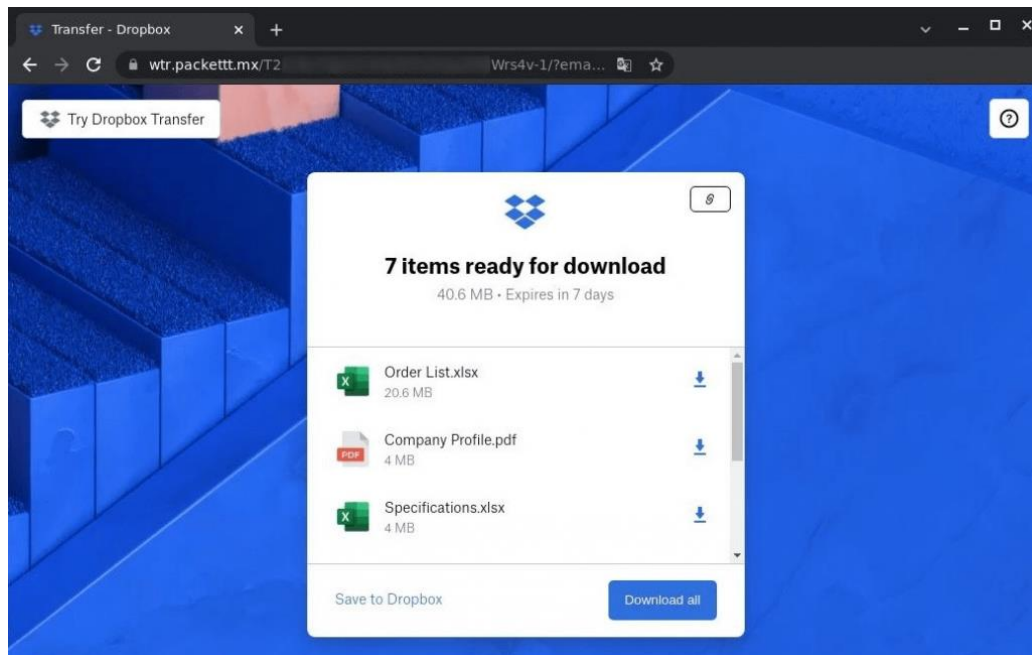


Рисунок 1.4 – Приклад фейкової сторінки сервісу для обміну файлами Dropbox [6]

Цільовий фішинг – це вид фішингу, який спеціально націлений на конкретні організації чи особи з метою отримання конфіденційних даних чи інших цінних ресурсів. Цей вид фішингу відрізняється високим рівнем персоналізації та вивченням потенційних жертв, що робить його особливо стійким до виявлення та протидії.

Цільовий фішинг базується на ретельному вивченні об'єкта атаки. Зловмисники проводять детальний аналіз цільової організації або особи, вивчаючи їхні звички, контакти та специфіку взаємодії. Це дозволяє зловмисникам створювати персоналізовані фішингові повідомлення та/або листи, які виглядають вкрай автентично та не викликають жодних підозр.

Основною частиною цільового фішингу є використання СІ для інтеграції інтригуючих сценаріїв та психологічних маніпуляцій. Ці атаки можуть мати форму електронних листів, які маскуються під повідомлення від колег чи начальства.

Перший етап цільового фішингу – це ретельне збирання інформації. Атакуюча сторона аналізує публічно доступні джерела, соціальні мережі та електронні архіви для отримання повної картини щодо об'єкту атаки. Наступним кроком є створення персоналізованих фішингових повідомлень, які враховують конкретні контексти та інтереси потенційної жертви. Після успішного обману жертви та виклику у неї інтересу, зловмисники намагаються потрапити в систему, в якій знаходиться жертва. Це можуть бути як шкідливе ПЗ, так і СІ або інші методи, що допоможуть зловмисникам отримати доступ до конфіденційних даних.

Зловмисники можуть експлуатувати отриманий доступ для збирання конфіденційної інформації, включаючи логіни, паролі, корпоративні дані та іншу чутливу інформацію. Цей етап спрямовано є головним у досягненні основної мети атаки.

Щоб зменшити ризик виявлення, зловмисники можуть робити певні дії щодо приховання своєї присутності в системі, наприклад маскувати трафік, використовувати проксі-сервера, видалення логів тощо.

Усі ці етапи, що було перелічено вище, формують повний цикл цільового фішингу. Зловмисники постійно вдосконалюють свої методи, щоб залишатися непомітними та максимізувати результати своєї роботи.

Вейлінг представляє собою удосконалену форму цільового фішингу кібератак, спрямовану на впливових посадових осіб та керівників компаній з метою отримання конфіденційної інформації. Цей вид фішингу вирізняється високим рівнем індивідуалізації та використанням вдосконалених технік СІ для максимізації ймовірності успіху.

В контексті вейлінгу використовуються інтригуючі та хитрі прийоми для привертання уваги впливових осіб. Злочинці формують персоналізовані електронні повідомлення (як і у випадку із цільовим фішингом), які маскуються під важливі ділові, або особисті питання, і спонукають жертву виконати певні дії. В рамках вейлінг-атак зловмисники детально аналізують інформацію про обрану ціль, охоплюючи публічні профілі, медійні виступи та корпоративні події. Це дозволяє їм створювати фіктивні сценарії, які максимально відповідають індивідуальним особливостям кожного високопосадовця.

Таким чином, у 2016 році працівники всесвітньо відомої компанії Seagate стали жертвами вейлінгу. У результаті атаки до рук зловмисників потрапила інформація щодо номерів соціального страхування, імен, домашніх адрес, та доходів щонайменше 10000 працівників компанії [7].

Фармінг в контексті кібербезпеки представляє собою вдосконалений вид фішингу, спрямований на використання механізмів довіри користувачів до популярних веб-сайтів та онлайн-платформ. Цей вид атаки включає в себе створення вигляду легітимних веб-ресурсів, які надзвичайно схожі на офіційні, що здатні вводити в оману навіть досвідчених користувачів.

Нвід'ємною частиною фармінгу є використання DNS-спуфінгу та отруєння кешу DNS, які дозволяють атакуючим перенаправляти користувача із справжніх сайтів на фальшиві ресурси, які перебувають під контролем щзловмисників. Це створює можливість для отримання такої конфіденційної

інформації, як особисті дані, різноманітні ідентифікатори та фінансові реквізити. Сучасні фармінг-атаки використовують не тільки технічні засоби, але і соціально-інженерні методи. Зловмисники активно вивчають публічні профілі та діяльність потенційних жертв, щоб створити вигадані сценарії та легенди, які максимально наближені до реальних. Це допомагає підвищити ймовірність того, що користувачі потраплять у пастку, перейшовши на фальшивий ресурс та введучи свої особисті дані.

У 2014 році фінансові інституції США потрапили під фармінгову атаку, в ході якої атакуючі створили фальшивий банківський веб-сайт, надто схожий на офіційний. Користувачі, отримавши спам-листи відмінної від офіційної електронної адреси, переходили на фальшивий сайт і вводили свої банківські дані, що призвело до великих фінансових втрат [8].

Фармінгові атаки часто використовують соціальні мережі. У 2017 році був виявлений великий обман через Facebook, де злоумисники створили фальшиві акаунти відомих брендів і організацій. Користувачі, що були підписані на ці аккаунти, переходили за посиланнями, вказаними у цих профілях, на фальшиві веб-сайти, що призвело до передачі конфіденційної інформації та фінансових ресурсів зловмисникам [9].

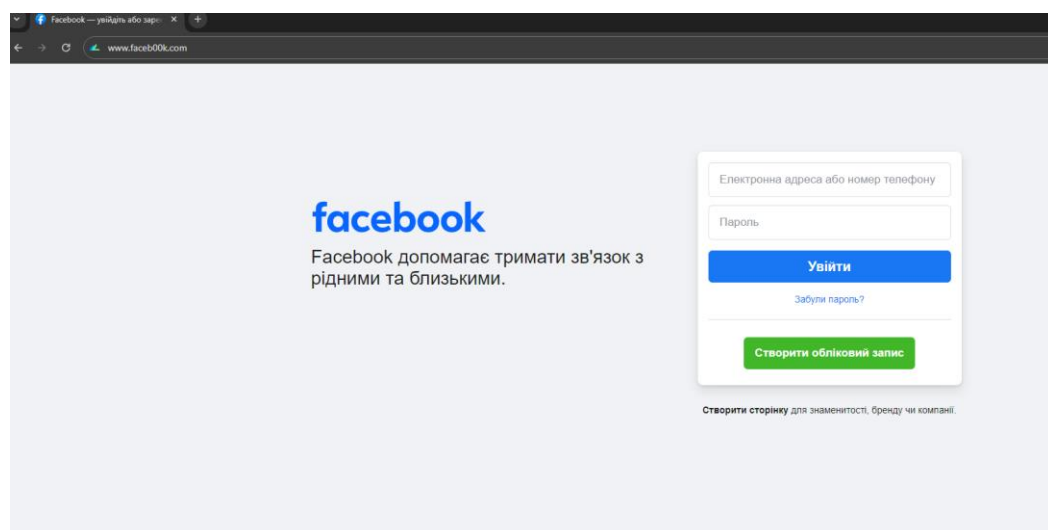


Рисунок 1.5 – Посилання на підроблений веб-сайт (www.faceb00k.com) та інтерфейс на ньому

У поточному 2023 році одна з фармінгових атак була спрямована на користувачів платформи Zimbra із України та Польщі. Зловмисники відправляли листи із вкладеною HTML-сторінкою, у яких повідомлялось про оновлення сервера пошти, проблеми із обліковим записом тощо. Після відкриття HTML-файлу жертва потрапляла на, стилізовану під свою організацію, сторінку авторизації, вводила свої дані, такі як логін та пароль, а HTML-форма у фоновому режимі відправляла цю інформацію на сервер зловмисників [10].

Смішинг – це форма фішингу, що використовує мобільні технології, зокрема, текстові повідомлення (SMS), для здійснення інформаційного або фінансового шахрайства. Цей вид атаки базується на СІ та психологічних методах отримання доступу до особистої інформації та фінансових ресурсів потенційної жертви.

Смішинг використовує технічні прийоми для імітації легітимних повідомлень від компаній чи операторів зв'язку, банківських закладів тощо. Уся суть полягає у відправці фішингових SMS, які маскуються під офіційні повідомленнями від банків, фінансових установ або інших довірених джерел. Зловмисники також можуть користуватися технікою підміни номеру, щоб змінювати відправників повідомлень і підвищувати ймовірність успішного виконання смішингової атаки. Однією з ключових рис смішингу є використання психологічних методів для спонукання жертви до негайних дій. Здійснюючи атаку, зловмисники частіше за все надають інформацію, яка створює враження невідкладності або кризи, викликаючи паніку та бажання жертви негайно реагувати.

Кожного дня фіксується велика кількість смішингових атак, під час яких зловмисники висилають масові текстові повідомлення, маскуючись під фінансові установи та інші довірені джерела. Лише за квітень 2023 року спеціалісти компанії EarthWeb зареєстрували 376,032,773 смішингових SMS на добу [11]. В повідомленнях надається інформація про блокування картки,

спрямована на залякування жертв та перевірку статусу їхніх банківських рахунків через прикріплене у SMS посилання, або номер. Жертви, перейшовши за посиланням, потрапляли на фішингові веб-сайти, де їм пропонувалось авторизуватись у свій банківський акаунт.

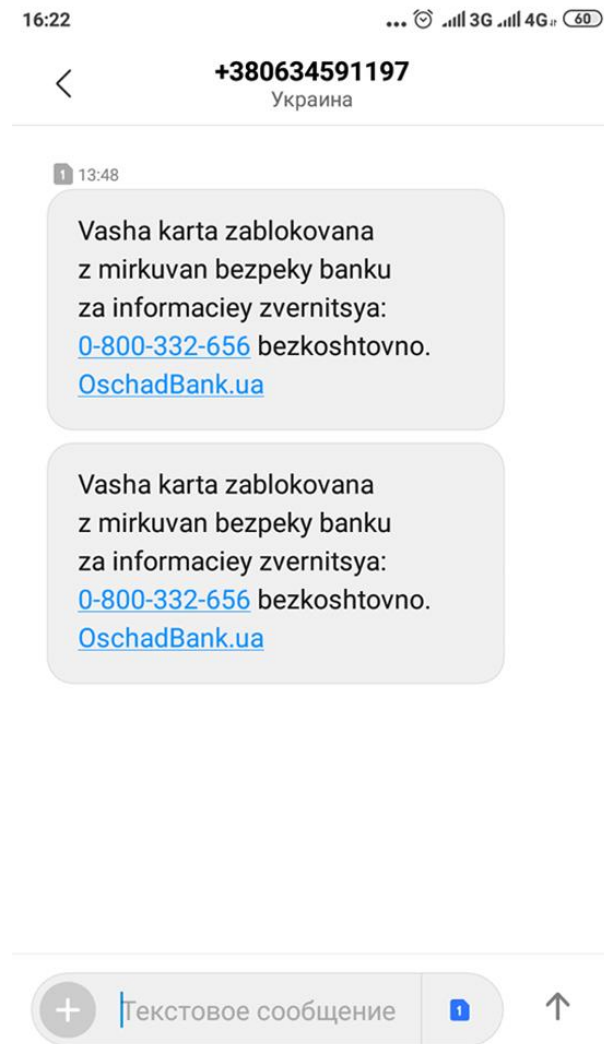


Рисунок 1.6 – Смішингова атака у вигляді SMS від Ощадбанку [12]

Фішинг типу "вішинг" представляє собою вид кібератак, при якому зловмисники використовують голосове спілкування, або голосові записи для реалізації своїх шахрайських задумів. Цей метод атаки, як і всі попередні, ґрунтується на СІ та використовує технологію маніпулювання

психологічними вразливостями жертви з метою отримання доступу до конфіденційної інформації.

Вішингові атаки найчастіше застосовують технології голосового синтезу та обробки мови для створення автентичних аудіозаписів, що імітують голоси авторитетних осіб, представників впливових організацій, та зірок. Вішинговою атакою може бути дзвінок із банку, урядової установи, компанії, у якій працює жертва тощо. Основою вішингу є використання психологічних прийомів для створення ситуацій тиску та невідкладності. Здійснюючи атаку, зловмисники можуть використовувати емоційні важелі, що спонукають жертву до негайних дій, таких як розкриття особистої інформації чи виконання фінансових транзакцій.

У останні роки вішинг став особливо небезпечним через те, що зловмисники удосконалюють техніки маніпулювання голосом та адаптують їх до сучасних технологічних досягнень. Спостерігається тенденція використання інтелектуальних систем, що надає атакам ще більшу автентичність та переконливість.

Яскравим прикладом вішингу можна назвати вже традиційну злочинну схему «мамо, я збив(ла) людину». Зловмисники дзвонять до людей, представляючись їхніми родичами, найчастіше – донькою або сином, та кажуть, що він/вона збили людину і тепер, щоб уникнути проблем із законом, потрібно терміново перевести певну суму грошей на банківський рахунок. Будучи у стресовому та панічному стані, родичі найчастіше не встигають навіть замислитись та перевірити правдивість цієї інформації, згодом відправляючи кошти зловмисникам [15].

Фішинг методом клонування листа електронної пошти є винахідливою та ефективною стратегією кібератак, де зловмисники використовують клон офіційної електронної пошти для отримання особистої інформації від користувачів. Цей метод атаки базується на підміні легітимних електронних листів, що призводить до великого ризику для конфіденційності та безпеки особистої інформації.

Зловмисники, які обирають клонування фішингу, спочатку викрадають оригінальний електронний лист з папки «Вхідні» жертви. Після цього вони створюють точну копію цього листа, залишаючи лише URL-адресу в повідомленні зміненою на свою. Основною метою цієї атаки є створення вигляду справжності листа для того, щоб увести жертву у оману. Зловмисники вдосконалюють технічні навички для створення ідеальних клонів електронних листів, включаючи логотипи, структуру та інші елементи, щоб забезпечити максимальну правдоподібність. Особливо небезпечною особливістю цього методу фішингу є здатність зловмисників маскувати фішингову URL-адресу під легітимну, що створює ілюзію безпеки для потенційної жертви.

Клонування листа електронної пошти створює серйозні ризики для безпеки інформації користувачів. Потрапляючи на підроблений веб-сайт через клонований електронний лист, користувачі можуть ненавмисно передати зловмисникам свою конфіденційну інформацію, яка потім може бути використана у різноманітних шахрайських схемах.

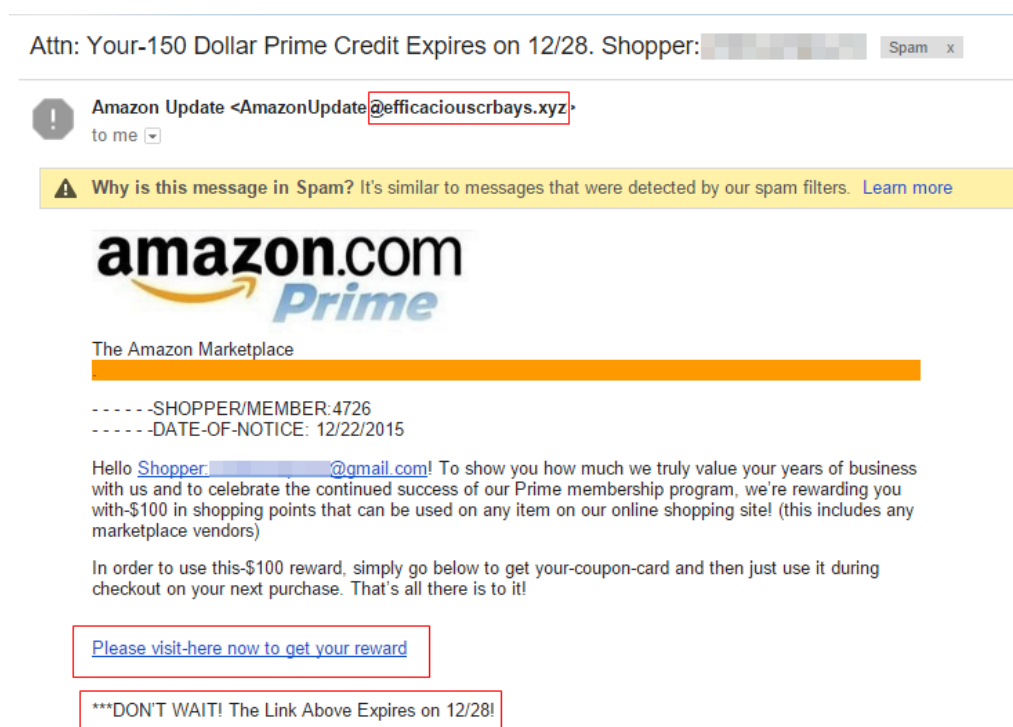


Рисунок 1.7 – Клонований лист з електронної пошти із фішинговим посиланням [18]

Сноушуїнг (Snowshoeing) – це метод розсилки фішингового спаму, в якому використовується не одна, а кілька IP-адрес. Назва цього виду спаму походить від снігоступів, що говорить про їх здатність розподіляти вагу на велику площу, подібно до того, як снігоступи допомагають людині рухатися по снігу без провалювання у нього [16].

Сноушуїнг важко виявити, оскільки цей метод використовує не одну, а кілька IP-адрес для відправлення великої кількості фішингових спам-листів. Завдяки цьому атака виглядає так, наче електронні листи надходять із різних джерел, ускладнюючи завдання фільтрації та блокування такого спаму.

Спамери, які використовують сноушуїнг, активно маневрують, змінюючи IP-адреси, щоб уникнути свого виявлення та блокування спам-листами. Такий вид фішингового спаму зазвичай важко взяти під контроль, оскільки традиційні методи боротьби, по типу сортування за відправником, або складання блок-листів, можуть бути менш ефективними у випадку розсилки спама з кількох джерел.

Метою використання зловмисниками методики сноушуїнгу збільшується навантаження на електронні пошти жертв та зростає вірогідність отримання спаму користувачами, а значить і переходу потенційних жертв по фішинговим посиланням. Цей вид атаки висуває вимоги до розробників систем фільтрації спаму та вимагає постійного удосконалення методів його виявлення та блокування подібних атак.

1.3 Поглиблений аналіз інструментів та механізмів, що використовуються при фішингових атаках

Основою усіх фішингових атак є атака на найбільш вразливу ланку сучасної системи безпеки – на людину. Розрізнення оригінальної веб-адреси

банку від фішингової копії не завжди є тривіальним завданням для потенційної жертви, оскільки адреси, подібні до `mybank.account.com` чи `account.mybank.com`, можуть бути легко переплутані. Зловмисники також використовують те, що в деяких шрифтах маленька буква "i" і велика "L" виглядають ідентично ($I = l$), різницю між буквою "O" і цифрою "0" теж мало хто зможе помітити без певних навичок. Ці прийоми дозволяють обдурити людей, надсилаючи їм електронні листи з посиланнями, які ведуть на фейкові версії популярних веб-ресурсів.

Зловмисники володіють різноманітним арсеналом інструментів, включаючи підміну локальних IP-адрес за допомогою внесення змін до файлу `hosts` в ОС Windows. Вони також вдаються до фармінгу, що передбачає таємне перенаправлення жертви на хибну IP-адресу. Додатковою стратегією є підміна веб-сторінки локально за допомогою вірусу трояну, який може додавати додаткові поля (наприклад, для введення номера кредитної картки) на зображеній браузером сторінці.

Фішери, прагнучи досягти якомога швидше результату, маскують свої атаки під найпопулярніші сервіси, такі як аукціони, платіжні системи та великі банки, розраховуючи на те, що людина, яка випадково отримає деяку кількість спам-листів має обліковий запис в одному з цих сервісів.

Фішингові атаки у сучасному кіберпросторі визначаються використанням ряду важливих інструментів та механізмів, спрямованих на отримання конфіденційної інформації. Один із основних методів полягає у створенні фальшивих веб-сайтів, що імітують офіційні ресурси банків чи компаній. Це включає точне клонування дизайну та URL-адрес оригіналу, створюючи враження легітимності. Зловмисники також вдало використовують фішингові листи, які завдяки СІ набувають вигляду переконливих повідомлень від банків чи популярних сервісів. Ці електронні листи спрямовані на отримання особистих даних від потенційних жертв, видаючи себе за легітимні повідомлення.

Технічні аспекти фішингових атак включають в себе використання IP-адрес та інших технічних засобів для приховування слідів зловмисників. Це може включати використання VPN, проксі-серверів та інших інструментів для уникнення виявлення їх справжнього місцезнаходження. Загалом, VPN та проксі використовуються зловмисниками з цілого ряду різних причин:

- анонімність та прихованість IP-адреси: використання VPN дозволяє зловмисникам приховати свою справжню IP-адресу, замінюючи її на IP-адресу VPN-сервера. Це робить їх більш захищеними до виявлення та відслідковування;
- обхід географічних блокувань: VPN може допомагати обійти географічні обмеження залежно від регіону для доступу до ресурсів або інформації, які за рядом певних причин може бути важко отримати з їх справжнього місцезнаходження;
- захист трафіку: використання VPN дозволяє шифрувати і захищати передані дані між зловмисником і сервером. Це допомагає уникнути перехоплення і аналізу трафіку, забезпечуючи більш високий рівень конфіденційності;
- створення ілюзії легітимності: зловмисники можуть використовувати VPN для встановлення таких обставин, ніби їх трафік йде через звичайні комерційні мережі, маскуючи справжній регіон або конкретну мережу та підмережу;
- обхід блокувань та фільтрації: VPN дозволяє обійти різноманітні технічні обмеження та системи фільтрації, які можуть бути встановлені на рівні мережі [17].

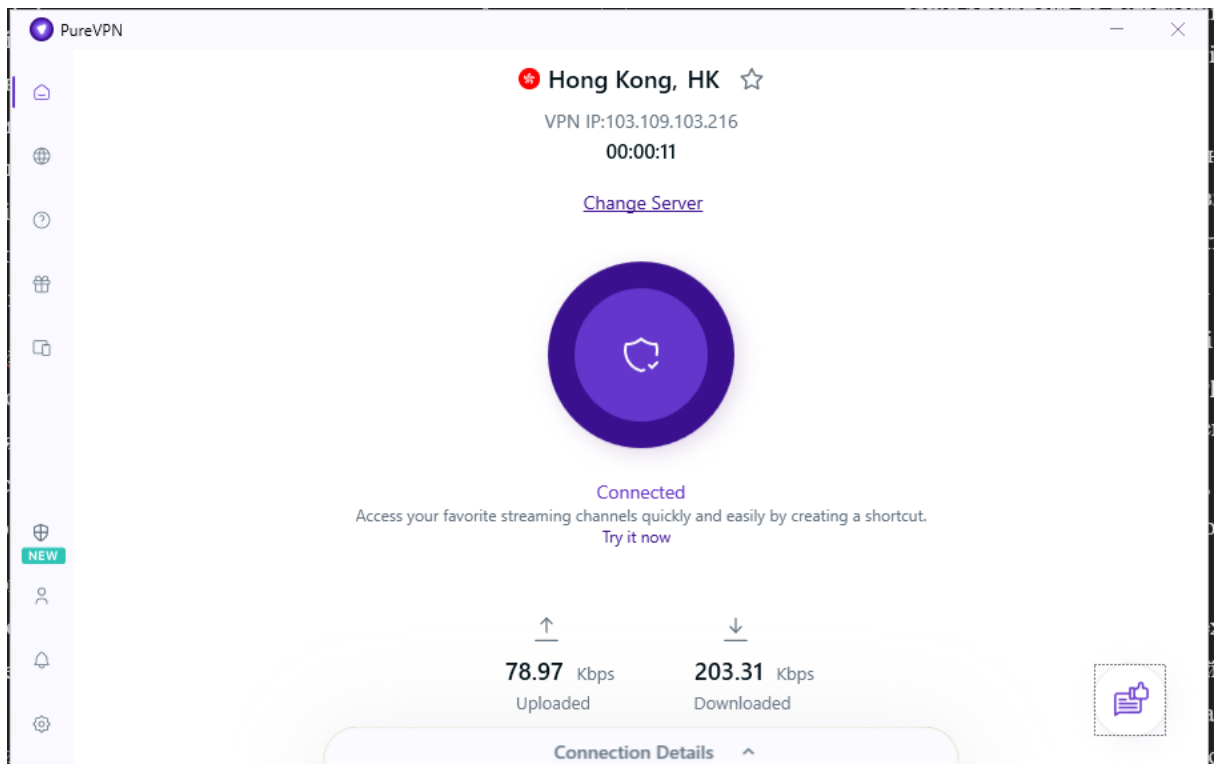


Рисунок 1.8 – Інтерфейс програми PureVPN. Трафік з комп’ютера йде через сервер у Гонг-Конгу

Зловмисники можуть використовувати підміну DNS (Domain Name System) для фішингових атак шляхом впровадження неправильних або підроблених DNS-записів, що вказують на фішинговий сайт, замість оригінального. Цей вид атаки дозволяє їм спрямовувати користувачів на підроблені веб-сайти, де можуть проводитися фішингові операції.

DNS spoofing

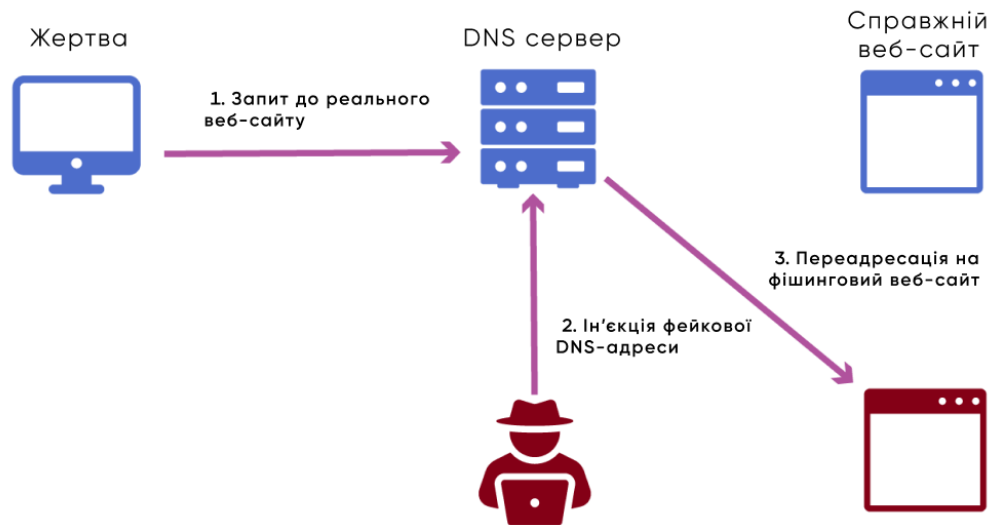


Рисунок 1.9 – Схема процесу підміни DNS-адреси зловмисниками

Основні методи використання підміни адреси DNS для фішингу:

- DNS Spoofing (імітація DNS): зловмисники можуть втручатися в мережевий трафік і відправляти фальшиві DNS-відповіді на запити користувачів. Це може бути виконано шляхом впровадження фальшивих DNS-відповідей в локальний DNS-кеш або через Man-in-the-Middle (MitM) атаку;
- DNS Cache Poisoning (отруєння кеша DNS): зловмисники можуть спробувати засмічення кеша DNS, додаючи фальшиві DNS-записи в кеш DNS-серверів. Це призводить до того, що навіть легітимні DNS-запити перенаправляються на фішинговий сайт;
- використання фішингових DNS-серверів: зловмисники можуть створювати фішингові DNS-сервери, які відповідають на запити користувачів і направляють їх на підроблені веб-сайти;

– СІ для зміни DNS-налаштувань: зловмисники можуть використовувати методи СІ для переконання користувачів вручну змінити налаштування DNS на власні, які будуть вести на фішинговий сервер.

Соціальна інженерія у контексті фішингових атак відіграє ключову маніпулятивну роль, замість використання технічних вразливостей. Цей підхід направлений на створення сценаріїв, які змушують людей розкривати конфіденційну інформацію чи виконувати небезпечні дії, керуючись власними емоціями та відчуттями у моменті.

Фішери намагаються створити ілюзію безпечності та правдоподібності атак, імітуючи повідомлення від банків, урядових установ чи інших довірених джерел. Елементи емоційного впливу, такі як страх, цікавість або невідкладність, використовуються для того, щоб змусити жертв реагувати швидко та недбало, не переймаючись власною безпекою.

Важливою частиною соціальної інженерії є вивчення потенційної жертви (у одиничному випадку) та цільової аудиторії (у масовому), включаючи аналіз соціальних мереж та збір персональних даних із загальнодоступних джерел. Зловмисники використовують цю інформацію для створення персоналізованих атак, максимально маскуючись під щось конкретне.

Окрім того, зловмисники можуть вигадувати різні причини для атаки, такі як використання емейлів від імітованих служб підтримки, що намагаються отримати конфіденційну інформацію. Уся суть СІ полягає у тому, щоб максимально втертися у довіру до жертви, у підсумку змушуючи її виконувати майже будь-які, необхідні зловмисникам дії, без обговорення.

Одним, із популярних у зловмисників інструменту фішингу, є фреймворк GetGorphish. Це відкрите ПЗ, яке використовується для проведення тестів на проникнення у систему та навчання персоналу з питань кібербезпеки. Його основна мета полягає в імітації фішингових атак, щоб визначити рівень свідомості та готовності співробітників та користувачів реагувати на потенційно можливі фішингові сценарії. Але, тим не менш, це не заважає

нечистим на руку людям використовувати цей фреймворк у своїх злочинних цілях.

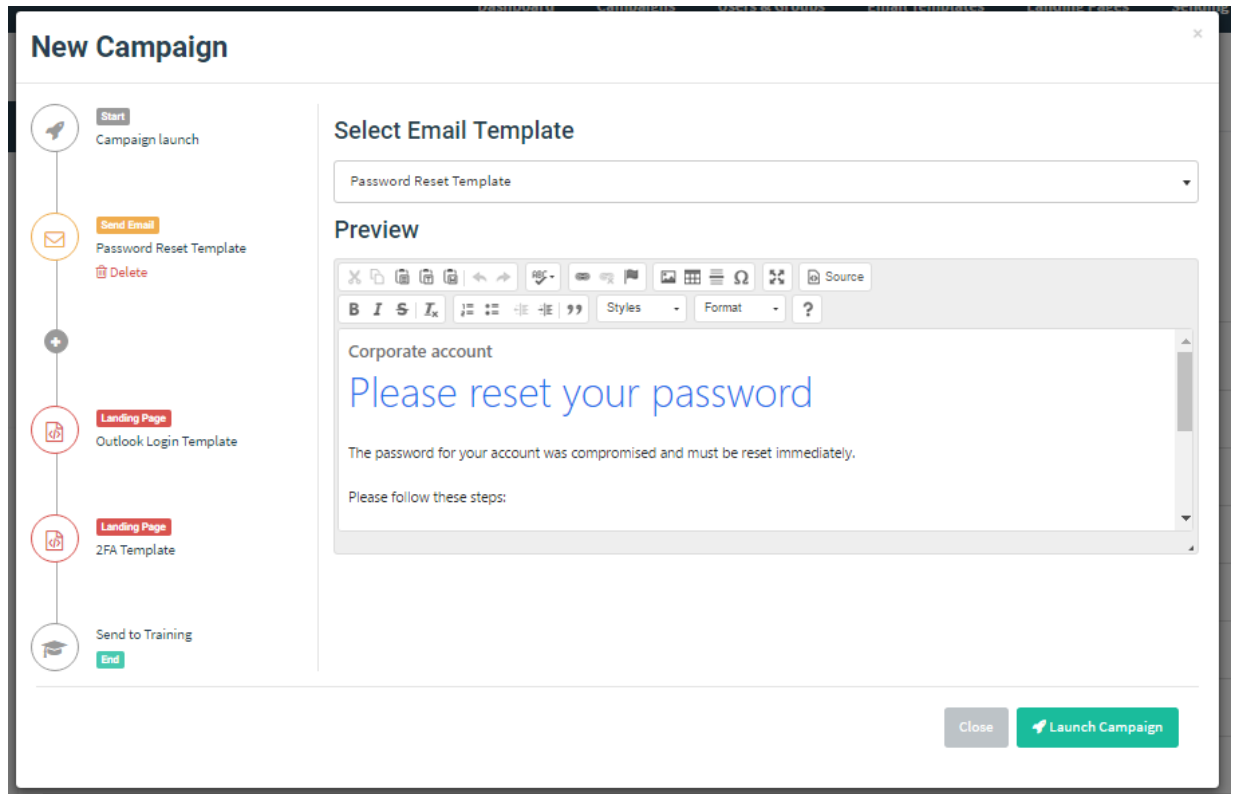


Рисунок 1.10 – Інтерфейс створення фішингового листа у фреймворку GetGophish [19]

GetGophish пропонує користувачам інтуїтивно зрозумілий інтерфейс для створення та впровадження фішингових кампаній. Основні механізми роботи включають в себе наступні етапи:

- створення кампанії: користувачі можуть створювати фішингові кампанії, вибираючи різноманітні сценарії та методики атак. Це може включати електронні листи, веб-сторінки, опитування та інші інструменти;
- налаштування параметрів: GetGophish дозволяє налаштовувати різні параметри атак, такі як вміст листа, ім'я відправника, домени та інші аспекти, що роблять атаку більш схожою на справжній контент;

- відправлення фішингових листів: після налаштування кампанії користувач може запустити відправку фішингових листів за вказаними адресами. Фреймворк може відстежувати дії жертв на цих листах;
- аналіз результатів: після завершення кампанії або певного етапу, GetGophish збирає та аналізує дані щодо того, які та як користувачі взаємодіяли з фішинговими листами, введенням інформації на фейкових сторінках і т.д;
- навчання та звітність: за допомогою зібраних даних, GetGophish надає можливості для навчання персоналу з кібербезпеки та генерації звітів для оцінки результатів виконаної кампанії.

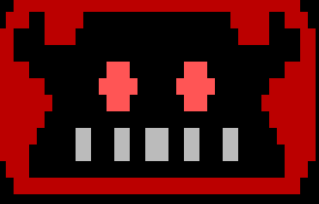
Зловмисники використовують GetGophish у шкідливих цілях, створюючи дуже реалістичні фішингові сайти, листи, тощо. Вони імітують відомі компанії, використовують СІ та отримують великі об'єми інформації від некомпетентних користувачів ПК. GetGophish, в контексті кіберзлочинів, став дуже серйозним інструментом, який максимізує можливості злочинців та підвищує ефективність фішингових атак.

Іншим прикладом ПЗ для фішингу є Evilginx 3.0. Це фреймворк атаки типу MITM, який використовується для фішингу облікових даних разом із файлами cookie поточного сеансу, що, у свою чергу, дозволяє обійти захист двофакторної автентифікації. Цей інструмент є наступником Evilginx, випущеного в 2017 році, який використовував спеціальну версію HTTP-сервера nginx, щоб забезпечити атаку типу MITM, щоб діяти як проксі-сервер між браузером і фішинговим веб-сайтом. Поточна версія повністю написана на мові програмування GO як окрема програма, яка реалізує власні HTTP та DNS сервера, що робить її надзвичайно простою у налаштуванні та використанні [20].

```

root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

```



```

no nginx - pure evil
by Kuba Gretzky (@mrgretzky) version 2.0.0

```

```

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [inf] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-almost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [inf] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

```

id	phishlet	username	password	tokens	remote ip	time
19	google			none		2018-05-28 08:23

```

[08:24:22] [inf] [0] Username: [redacted@gmail.com]
[08:24:29] [inf] [0] Password: [redacted]
[08:24:41] [inf] [0] all authorization tokens intercepted!
[08:24:41] [inf] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

```

id	phishlet	username	password	tokens	remote ip	time
19	google	[redacted@gmail.com]	[redacted]	captured		2018-05-28 08:24

Рисунок 1.11 – Інтерфейс фреймворку Evilginx 3.0 [20]

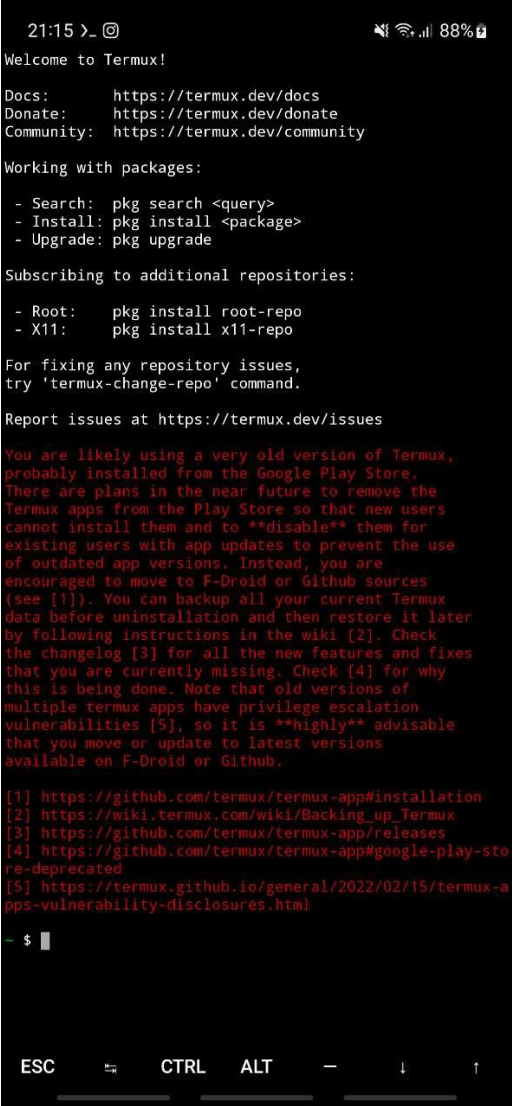
Однією з ключових функцій Evilginx 3.0 є перехоплення та аналіз куків (cookies) сесій користувачів. Ці файли, зазвичай, містять інформацію про автентифікацію, що надає зловмисникам можливість отримати несанкціонований доступ до облікових записів користувачів.

Ще однією важливою особливістю є здатність Evilginx 3.0 впізнавати та обходити заходи двофакторної аутентифікації (2FA). Використовуючи розуміння принципів роботи різних методів 2FA, фреймворк може атакувати навіть ті облікові записи, які додатково захищені. Також, за допомогою Evilginx 3.0 зловмисники можуть створювати фальшиві фішингові веб-сторінки, які точно копіюють сторінки авторизацій веб-сайтів.

Зручність Evilginx 3.0 полягає в тому, що за допомогою цього інструменту можна автоматизувати багато етапів атаки, що значно полегшує життя кібер-злочинцям і підвищує ефективність їхніх атак.

1.4 Фішингова атака на практиці

Уявімо, що мені, як зловмиснику необхідно вкрати поточну сесію користувача у месенджері Telegram. Комп'ютера у мене із собою немає, зате є додаток “Termux” на пристрої з ОС Android. Termux – це додаток, що реалізує Linux-подібне середовище, взаємодія з яким відбувається за допомогою консолі без необхідності мати root-права на пристрої.



```
21:15 ~_@
Welcome to Termux!

Docs:      https://termux.dev/docs
Donate:    https://termux.dev/donate
Community: https://termux.dev/community

Working with packages:
- Search:  pkg search <query>
- Install: pkg install <package>
- Upgrade: pkg upgrade

Subscribing to additional repositories:
- Root:    pkg install root-repo
- X11:     pkg install x11-repo

For fixing any repository issues,
try 'termux-change-repo' command.

Report issues at https://termux.dev/issues

You are likely using a very old version of Termux,
probably installed from the Google Play Store.
There are plans in the near future to remove the
Termux apps from the Play Store so that new users
cannot install them and to disable them for
existing users with app updates to prevent the use
of outdated app versions. Instead, you are
encouraged to move to F-Droid or Github sources
(see [1]). You can backup all your current Termux
data before uninstallation and then restore it later
by following instructions in the wiki [2]. Check
the changelog [3] for all the new features and fixes
that you are currently missing. Check [4] for why
this is being done. Note that old versions of
multiple termux apps have privilege escalation
vulnerabilities [5], so it is highly advisable
that you move or update to latest versions
available on F-Droid or Github.

[1] https://github.com/termux/termux-app#installation
[2] https://wiki.termux.com/wiki/Backing_up_Termux
[3] https://github.com/termux/termux-app/releases
[4] https://github.com/termux/termux-app#google-play-store-deprecated
[5] https://termux.github.io/general/2022/02/15/termux-apps-vulnerability-disclosures.html

~ $
```

Рисунок 1.12 – Інтерфейс додатку Termux

Використовувати я буду інструмент KingFish3. За його допомогою можна створити фішингову сторінку авторизації найпопулярніших соціальних мереж та месенджерів, а також одразу отримати на неї посилання. Але спочатку треба встановити всі необхідні для цього пакети.

```

19:30 100% 74%
science Release
404 Not Found
Get:6 https://grimler.se/termux-packages-24 stable/main
aarch64 Packages [497 kB]
Reading package lists... Done
E: The repository 'https://dl.bintray.com/grimler/game-p
ackages-24 games Release' does not have a Release file.
N: Metadata integrity can't be verified, repository is d
isabled now.
N: Possible cause: repository is under maintenance or do
wn (wrong sources.list URL?).
E: The repository 'https://dl.bintray.com/grimler/scienc
e-packages-24 science Release' does not have a Release f
ile.
N: Metadata integrity can't be verified, repository is d
isabled now.
N: Possible cause: repository is under maintenance or do
wn (wrong sources.list URL?).
$ pkg install python
Checking availability of current mirror: ok
Reading package lists... Done
Building dependency tree... Done
The following additional packages will be installed:
  clang gdbm glib libandroid-posix-semaphore
  libcompiler-rt libexpat libffi libllvm libsqlite
  libxml2 lld llvm make ncurses ncurses-ui-libs
  ndk-sysroot pcre2 pkg-config python-ensurepip-wheels
  python-pip resolv-conf zstd
Suggested packages:
  python-tkinter
The following NEW packages will be installed:
  clang gdbm glib libandroid-posix-semaphore
  libcompiler-rt libexpat libffi libllvm libsqlite
  libxml2 lld llvm make ncurses-ui-libs ndk-sysroot
  pcre2 pkg-config python python-ensurepip-wheels
  python-pip resolv-conf zstd
The following packages will be upgraded:
  ncurses
1 upgraded, 22 newly installed, 0 to remove and 52 not u
pgraded.
Need to get 101 MB of archives.
After this operation, 628 MB of additional disk space wi
ll be used.
Do you want to continue? [Y/n] y
Get:1 https://grimler.se/termux-packages-24 stable/main
aarch64 ncurses aarch64 6.4.20231001-3 [524 kB]
Get:2 https://grimler.se/termux-packages-24 stable/main
aarch64 libffi aarch64 3.4.4-1 [30.9 kB]
Get:3 https://grimler.se/termux-packages-24 stable/main
aarch64 libxml2 aarch64 2.12.2 [539 kB]
Get:4 https://grimler.se/termux-packages-24 stable/main
aarch64 zstd aarch64 1.5.5-1 [328 kB]
Get:5 https://grimler.se/termux-packages-24 stable/main
aarch64 libllvm aarch64 17.0.6 [25.1 MB]
13% [5 libllvm 11.2 MB/25.1 MB 45%] 206 kB/s 7min 8s
ESC CTRL ALT — ↓ ↑

```

Рисунок 1.13 – Процес встановлення пакетів у Termux

Запускаю KingFish3 та обираю необхідну мені соцмережу, або месенджер. Цього разу це буде Telegram.

```

-<|====[Social]=====|>-|
-<|SOCIAL|>-|
-<|=====|>-|
-<|====[Master]=====|>-|

Starting...

::[New Social Fish]::
What to attack?
[*][1] - ICQ
[*][2] - ok.ru
[*][3] - Ozon
[*][4] - WhatsApp
[*][5] - Telegram
[*][6] - Vk
[*][7] - Instagram
[*][8] - Other
::[GPS Fish]::
[*][9] - Pokemon GO!
[*][10] - IG Search account [For mobile]
::[Network]::
[*][11] - WI-FI Admin Cp
[*][12] - WI-FI Password
::[Other]::
[*][13] - Password in head

|-[>>>]: █

```

Рисунок 1.14 – Вікно вибору мети атаки у KingFish3

Обираю у меню пункт «Telegram», вводимо номер порту, до якого жертва буде під'єднуватися, та прописую посилання веб-сторінки, на яку буде перенаправлено жертву після того, як вона введе усю необхідну мені інформацію.

```

[*][6] - Vk
[*][7] - Instagram
[*][8] - Other
::[GPS Fish]::
[*][9] - Pokemon GO!
[*][10] - IG Search account [For mobile]
::[Network]::
[*][11] - WI-FI Admin Cp
[*][12] - WI-FI Password
::[Other]::
[*][13] - Password in head

|-[>>>]: 5
[Enter port]: 8080
[Location URL]: https://google.com

```

Рисунок 1.15 – Введення початкових параметрів у KingFish3

Програма видає мені посилання у моїй локальній мережі на порт 8080. За допомогою вже іншого інструменту NGrok створюю SSH-тунель до моєї локальної мережі. Для того, щоб мене не змогли ідентифікувати, використовую віртуальну машину з віддаленим доступом та встановленим на неї Termux-ом. Також не забуваю про використання платного VPN.

Посилання має наступний вигляд:

A terminal window with a black background. The word "Forwarding" is on the left in a light green font. To its right, the URL "https://[redacted].ngrok.io" is displayed in a light blue font. The redacted part is a series of blue and white squares.

Рисунок 1.16 – Посилання на створену фішингову сторінку

Під замазаною частиною адреса у форматі «a2b2-1-11-111-111», де на місці цифри «1» стоять випадкові цифри. Така адреса не викликає довіри зовсім, а й навпаки – може стати причиною підозри. Тому отриману адресу я проганяю через сервіс для скорочення посилань. Останнім часом подібними сервісами користується все більше і більше людей, тому нове посилання не повинно викликати підозр.

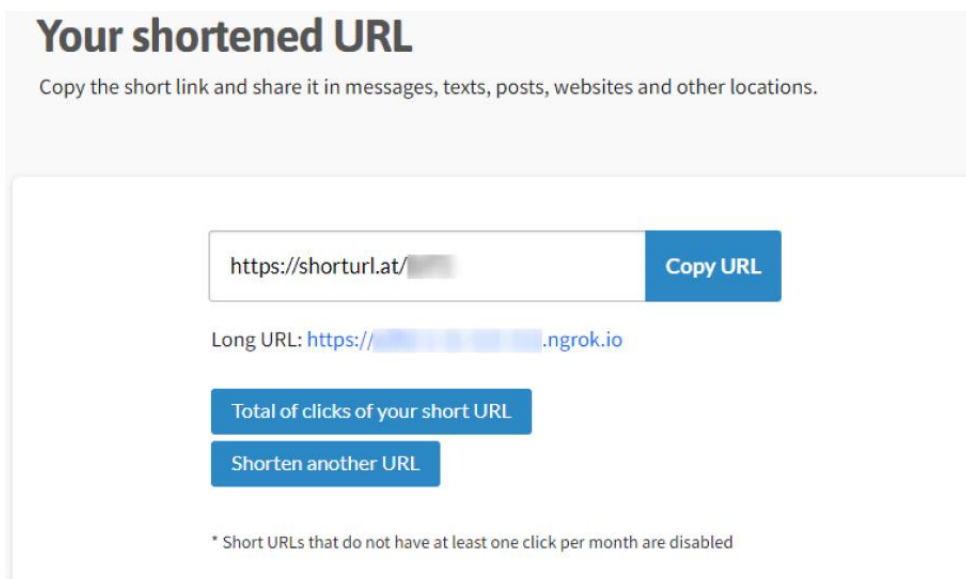


Рисунок 1.17 – Скорочення посилання на фішингову сторінку

Тепер це посилання можна відправляти жертві. Для того, щоб вона перейшла за ним, потрібно вигадати правдоподібний привід.

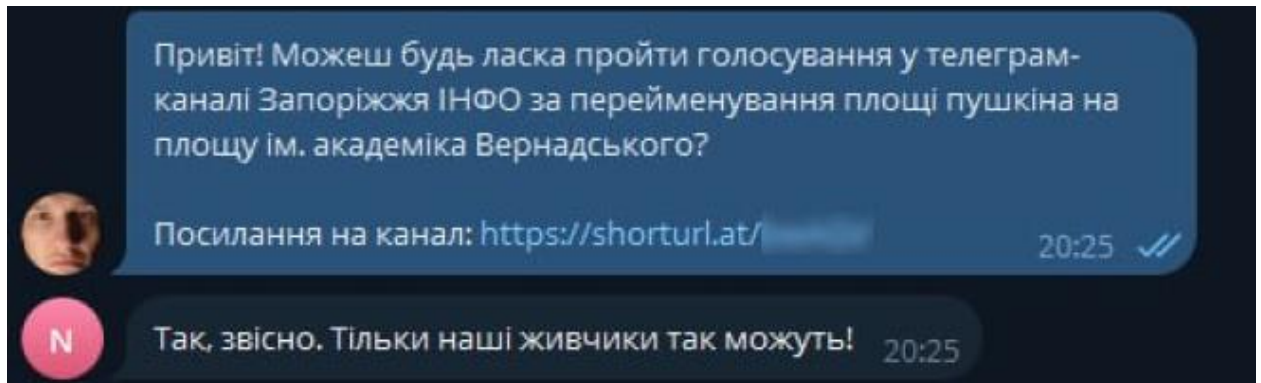


Рисунок 1.18 – Повідомлення-приманка для жертви

Після переходу по посиланню жертва бачить сторінку авторизації у Telegram із відповідним дизайном:



Рисунок 1.19 – Фішингова сторінка авторизації

Для того, щоб авторизуватись у Telegram, жертва повинна ввести номер свого мобільного телефону, до якого прив'язаний акаунт у месенджері. Після того, як жертва введе свій номер, я побачу його у логах KingFish3.

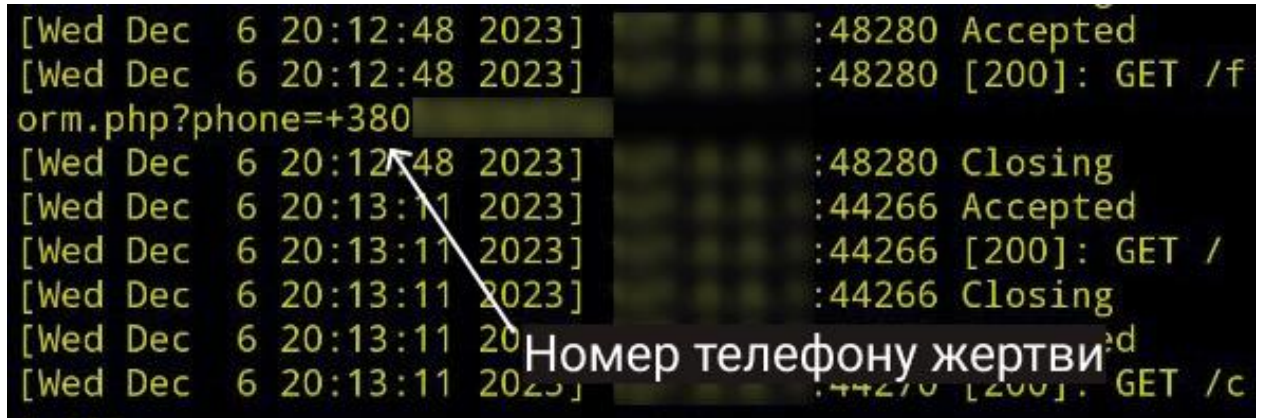


Рисунок 1.20 – Номер мобільного телефону жертви у логах

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

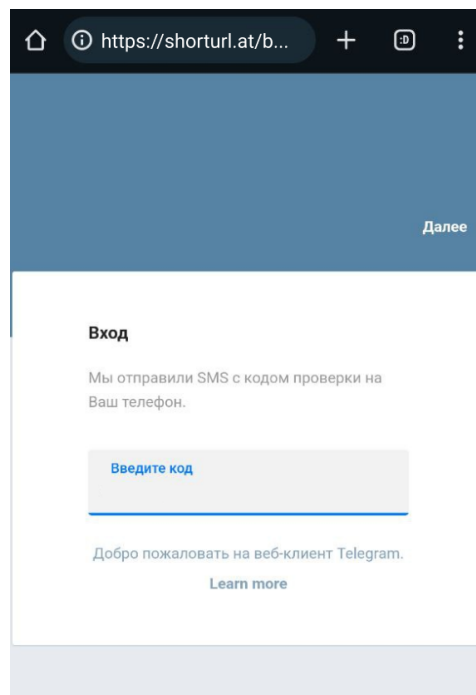


Рисунок 1.21 – Фішингова сторінка аутентифікації

У той самий час я, як зломисник, проходжу авторизацію у Telegram за допомогою номеру мобільного телефону жертви:

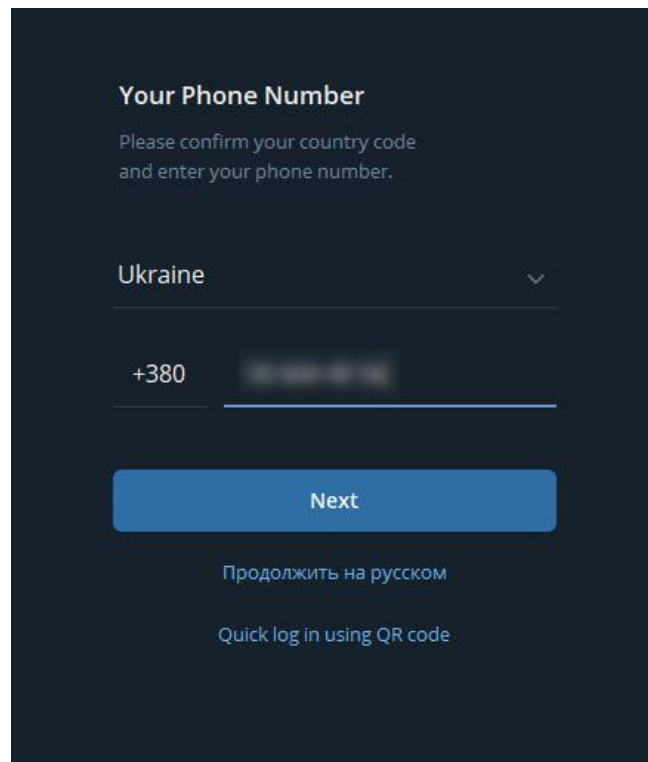


Рисунок 1.22 – Проходження авторизації у Telegram

Натиснувши кнопку «Next», Telegram відправить жертві на її мобільний номер код двофакторної аутентифікації, який вона введе у поле на фішинговій сторінці, яка показана на рисунку 1.15. Цей код буде показано у логах KingFish3 так само, як і мобільний номер до цього.

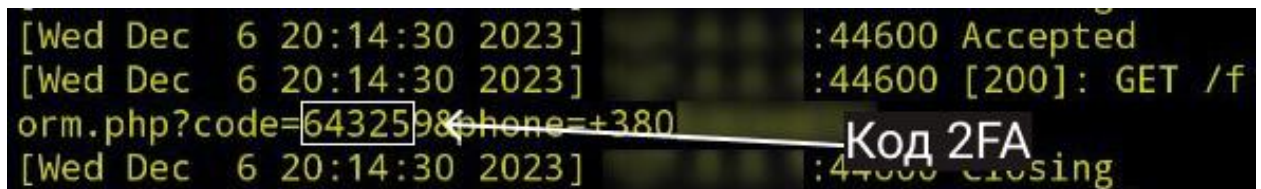


Рисунок 1.23 – Код двофакторної аутентифікації жертви у логах

Отриманий код я вводжу у відповідне поле у месенджері:

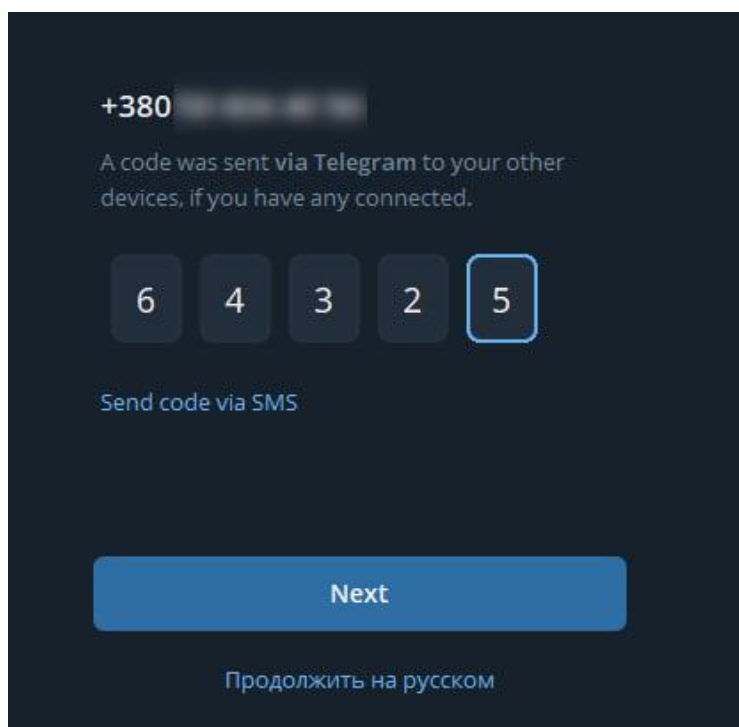


Рисунок 1.24 – Введення коду 2FA

Авторизація та аутентифікація пройдені. Я у особистому профілі жертви в Telegram:

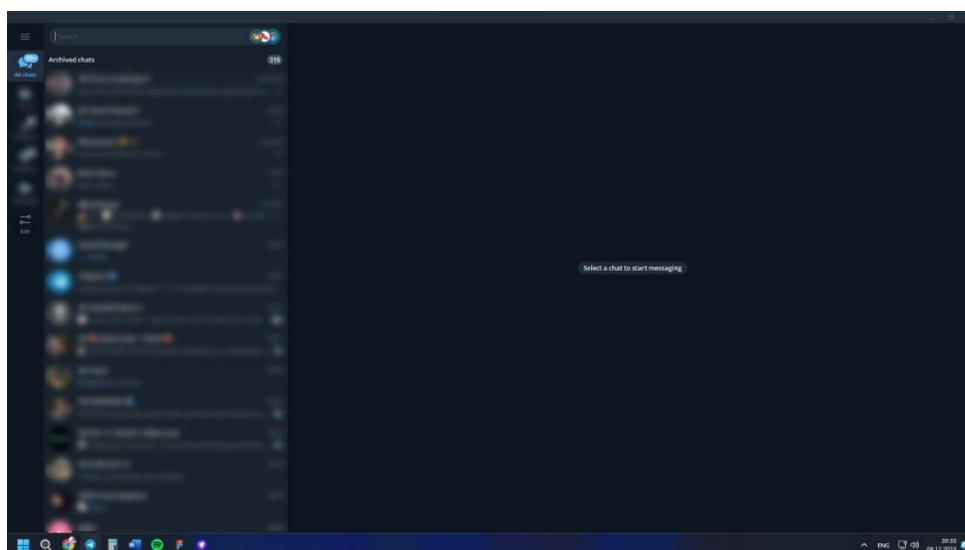


Рисунок 1.25 – Вікно месенджеру Telegram

Після введення коду 2FA у поле на фішинговій веб-сторінці жертву перенаправило на сайт Google, тому що я вказав його у налаштуваннях KingFish3.

Звичайно, з часом жертва може зрозуміти, що саме сталося та зайти перевірити список активних сесій у месенджері, але на той момент я, скоріш за все, вже встигну отримати всю необхідну мені інформацію.

Висновки до першого розділу

Цей розділ присвячений поглибленому аналізу фішингу та його різновидів, розглянутих в контексті основних методів та інструментів, які використовуються при виконанні фішингових атак. Ознайомлення із інформацією, наявною в цьому розділі, є дуже важливим для розуміння сутності всіх процесів та механізмів такого виду кіберзлочинності, як фішинг.

Спершу, було докладно проаналізовано визначення поняття фішингу та виділено основні його види. Визначено, що фішинг майже цілковито базується на соціально-інженерних методах, які є рушійною силою у техніках обману та маніпуляцій.

Було розглянуто різноманітні методи фішингу, такі як спам-пошта, фармінг, вішинг, смішинг, тощо. Глибокий аналіз виявив, що фішингові атаки можуть набувати різної форми та використовувати різноманітні соціально-інженерні методи для досягнення мети зловмисників.

Основною частиною розділу став докладний аналіз інструментів та механізмів, що використовуються зловмисниками для виконання фішингових атак. Зокрема, висвітлений Evilginx 3.0, який відрізняється високою ефективністю у втручанні в автентифікаційні процеси та уникненні заходів безпеки.

На основі проведеного аналізу можна зробити висновок, що фішинг є серйозною загрозою для кібербезпеки, особливо через різноманітність методів та інструментів, що можуть бути застосовані для цього виду атак. Знання сутності цього явища та його механізмів є ключовим фактором для ефективного протистояння фішинговим атакам.

2 МЕТОДИ, АЛГОРИТМИ ТА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК

Фішинг, завдяки своїй соціально-інженерній природі, ускладнює завдання по виявленню атаки для захисників інформаційної безпеки. Кожен новий метод атаки стає справжнім викликом для сучасних систем виявлення, оскільки зловмисники використовують інноваційні технології та алгоритми, щоб оминати численні захисні бар'єри.

Розгляд алгоритмів та технологій виявлення фішингових атак виявляється критичним у забезпеченні надійності та безпеки в інтернет-середовищі. В даному розділі буде розглянуто сучасні методи, що застосовуються для виявлення фішингу, і їх потенційний вплив на підвищення рівня як особистої кібербезпеки, так і корпоративної.

2.1 Аналіз методів виявлення фішингу

Ефективні методи виявлення фішингу включають в себе детальний аналіз характеристик атак, таких як доменні імена, SSL-сертифікати, контент веб-сторінок та структура отриманих електронних листів. Спеціалізовані алгоритми аналізу таких параметрів дозволяють виявляти відмінності від легітимних ресурсів.

Також важливим аспектом виявлення фішингу є постійний моніторинг веб-ресурсів. Активне відстеження нових доменних імен, реєстрація яких може бути пов'язана із підготовкою до фішингових атак, дозволяє оперативно реагувати та блокувати шахрайські сайти.

Окрім того, не треба забувати і про візуальний метод виявлення фішингових ресурсів. Суть метода закладена у його назві – аналіз зовнішнього

вигляду веб-ресурсів веб-адреси (URL), листів, додатків тощо. За допомогою цього методу можна перевірювати дизайни, логотипи, кольорові палітри та загальні структури веб-контенту для виявлення невідповідностей або імітації оригінальних брендів. Розрізнення та ідентифікація візуальних елементів дозволяє швидко впізнати потенційно шахрайські ресурси та зменшити ризик витоку інформації.

2.1.1 Аналіз характеристик фішингових атак

Однією з ключових сфер у сучасному виявленні фішингових атак є ретельний аналіз їхніх характеристик. Це включає в себе систематичне дослідження різних аспектів атак, таких як:

- аналіз доменних імен: фішери нерідко використовують схожі на легітимні доменні імена для створення маскувального ефекту. Важливо вивчати реєстрацію нових доменів, виявляти схожість з вже існуючими та аналізувати їхню історію для вчасного виявлення підозрілих ресурсів;
- SSL-сертифікати: легітимні веб-сайти використовують захищені SSL-з'єднання. Фішингові атаки можуть використовувати самопідписані або шахрайські сертифікати. Аналіз SSL-сертифікатів є необхідним для виявлення підозрілих змін та вирізнення легітимних від фішингових з'єднань;
- контент веб-сторінок вивчення змісту веб-сайтів важливо для розпізнавання фішингу. Фішери можуть використовувати імітацію дизайну та логотипів легітимних брендів. Аналіз контенту допомагає виявити відмінності та невідповідності, що є ознаками фішингових спроб;
- структура електронних листів: фішингові атаки часто включають надсилання електронних листів, що імітують комунікацію від легітимних джерел. Детальний аналіз заголовків, мови та структури може розкрити аномалії, що свідчать про фішинг.

2.1.2 Системи виявлення фішингових атак

У постійно зростаючому цифровому середовищі, де фішингові атаки стають все більш вдосконаленими, важливою стає роль систем виявлення фішингових атак. Компанії та організації активно впроваджують різноманітні інструменти для реактивного та превентивного виявлення шахрайських дій, спрямованих на фішинг, зокрема використовуючи такі системи як Netcraft, та SpoofGuard.

Netcraft відзначається своєю високою ефективністю у виявленні фішингових атак, використовуючи різноманітні технічні методи та системи виявлення. Однією з ключових характеристик їхнього підходу є використання технології постійного аналізу веб-ресурсів для створення бази даних, що дозволяє швидко виявляти та блокувати нові фішингові сайти. Здатність Netcraft в реальному часі взаємодіяти з інтернет-середовищем забезпечує користувачам надійний захист у віртуальному просторі.

SpoofGuard, зі своїм акцентом на аналіз поведінки користувачів, використовує підходи машинного навчання для виявлення фішингових атак. Система аналізує великі обсяги даних про поведінку користувачів, враховуючи їхні звички відносно відкривання листів, відвідування веб-сайтів і взаємодії з контентом. Такий комплексний аналіз дозволяє SpoofGuard ефективно визначати неправомірні дії та вчасно попереджати користувачів.

EarthLink відзначається високою ефективністю у фільтрації спаму та виявленні фішингових повідомлень через застосування алгоритмів, що базуються на сигнатурах. Система активно моніторить вхідні повідомлення на наявність характерних рис фішингу, таких як підроблені URL-адреси чи спроби виманити конфіденційні дані. EarthLink також робить акцент на оновленнях сигнатур, забезпечуючи постійну актуальність та ефективність системи виявлення.

Архітектура VMware NSX SpoofGuard відслідковує ARP-адреси відносно IP-адрес і реагує на їхні зміни. У випадку несподіваної зміни IP-адреси до ARP-адреси, система автоматично блокує доступ. VMware NSX SpoofGuard дозволяє конфігурувати окремі мережі і надає адміністраторам можливість розробляти політику щодо визначених IP-адрес.

SpoofGuard функціонує в кількох режимах, де можливі різні параметри:

- режим TOFU (Trust On First Use) автоматично довіряє призначенню IP при його першому використанні. Цей режим ґрунтується на довірі до першої IP-адреси, яку повідомляє диспетчер NSX.
- Ручний режим передбачає перевірку та затвердження всіх призначень IP-адрес перед їх використанням. Адміністратор вручну визначає набір IP-адрес, які потрібно затвердити, при цьому весь інший трафік блокується за замовчуванням.
- У середовищах з використанням DHCP не рекомендується використовувати режим "TOFU", оскільки IP-адреси тут динамічні і можуть змінюватися. TOFU не застосовується, оскільки довіряє лише першій використаній віртуальною машиною IP-адресі.

2.2 Роль машинного навчання та штучного інтелекту в системах виявлення фішингу

Традиційні методи виявлення фішингу, такі як фільтрація спаму та аналіз сигнатур, часто не можуть ефективно розпізнавати фішингові атаки через зростання їхньої складності. Машинне навчання та штучний інтелект відкривають новий підхід до виявлення фішингу, використовуючи аналіз різних ознак, таких як:

- структура електронного листа або повідомлення;
- вміст електронного листа або повідомлення;

- URL-адреса посилання або вкладення;
- поведінка користувача.

МН здатне виявляти фішингові атаки, аналізуючи великі обсяги даних, що включають як фішингові, так і невідомі електронні листи та повідомлення. Штучний інтелект може аналізувати складні ознаки, такі як поведінка користувача.

Переваги підходів до використання МН та ШІ для виявлення фішингу:

- точність та ефективність. МН та ШІ можуть бути більш точними у виявленні фішингу, ніж традиційні методи, такі як фільтрація спаму та аналіз сигнатур. Це тому, що машинне навчання може навчитися розпізнавати фішингові атаки, аналізуючи великі набори даних (датасети), що містять як фішингові, так і нефішингові електронні листи та повідомлення;

- гнучкість. МН та ШІ можуть бути більш гнучкими у виявленні фішингу, ніж традиційні методи. Це тому, що машинне навчання може адаптуватися до нових типів фішингових атак, або навіть бути підготовленим до них заздалегідь.

Недоліки підходів до використання машинного навчання та штучного інтелекту для виявлення фішингу:

- складність. Розробка та впровадження систем виявлення фішингу на основі МН та ШІ може бути складним і дорогим процесом;

- точність. Навіть найкращі системи виявлення фішингу на основі машинного навчання та штучного інтелекту все ще можуть помилятися.

- неадекватна поведінка користувача. Якщо користувачі не будуть дотримуватися правил безпеки, вони все одно можуть стати жертвами фішингу, навіть якщо система виявлення фішингу на основі ШІ працює правильно.

В цілому, підходи до використання машинного навчання та штучного інтелекту для виявлення фішингу мають потенціал для революції у цій галузі. Ці технології можуть допомогти організаціям і користувачам краще захищатися від фішингових атак.

В контексті стрімкого зростання складності та вдосконалення фішингових атак МН та ШІ виявляються потужними інструментами, спрямованими на аналіз різноманітних аспектів, за якими можна визначити фішинг. Давайте ознайомимось детальніше із тим, в яких саме аспектах вказані технології можуть виявити свою ефективність:

- аналіз структури електронного листа або повідомлення. Машинне навчання може використовуватися для виявлення фішингу, аналізуючи структуру електронного листа або повідомлення. Наприклад, фішингові електронні листи часто містять помилки в граматиці або орфографії. Вони також можуть містити посилання або вкладення, які не відповідають темі електронного листа;

- аналіз вмісту електронного листа або повідомлення. ШІ може також використовуватися для виявлення фішингу, аналізуючи вміст електронного листа або повідомлення. Наприклад, фішингові електронні листи часто містять заклики до дії, такі як "негайно натисніть тут" або "введіть свої особисті дані". Вони також можуть містити залякування або загрози;

- аналіз URL-адреси посилання або вкладення. МН може аналізувати URL-адресу посилання або вкладення, які прикріплені до електронного листа. Наприклад, фішингові URL-адреси часто містять помилки або не відповідають домену, який вони нібито представляють;

- аналіз поведінки користувача. ШІ може використовуватися для аналізу поведінки користувача, щоб виявити фішингові атаки. Наприклад, якщо користувач часто бездумно відкриває електронні листи з категорії спаму, або переходить за випадковими посиланнями у мережі Інтернет то це може бути ознакою того, що він є потенційною жертвою фішингу.

Висновки до другого розділу

У розділі "Методи, алгоритми та технології виявлення фішингових атак" була розглянута поточна актуальність застосування різноманітних підходів для боротьби із зростаючою складністю та вдосконаленням фішингових атак. Традиційні методи, такі як фільтрація спаму, аналіз сигнатур, та інше, стають менш ефективними, оскільки атаки стають більш витонченими. В цьому контексті машинне навчання та штучний інтелект виглядають дуже перспективними інструментами для виявлення фішингу, оскільки вони здатні аналізувати різноманітні аспекти, такі як структуру електронного листа, вміст повідомлення, URL-адреси, вкладені файли та поведінку користувача.

Використання МН для аналізу великих обсягів даних, що містять як фішингові, так і нефішингові електронні листи, дозволяє створювати моделі для ефективного розпізнавання фішингових атак. ІІІ, в свою чергу, використовується для аналізу більш складних ознак, таких як поведінка користувача.

Особливу увагу слід звернути на інструменти та технології, такі як SpoofGuard та системи виявлення фішингу від Netcraft, які використовують комбінацію статистичного аналізу та технології фільтрації трафіку для ефективного захисту від фішингових атак.

Підсумовуючи, можна стверджувати, що впровадження МН та ІІІ у сферу виявлення фішингових атак може стати революцією у боротьбі з цим видом кіберзлочинності.

3 ПРОТИДІЯ ФІШИНГОВИМ АТАКАМ: ТЕХНОЛОГІЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

Фішери постійно шукають нові точки проникнення у технологічному забезпеченні. Цей аспект визнається як ключовий у контексті порушення цілісності інформаційної безпеки як організацій, так і приватних осіб. Питання про роль цього аспекту в сучасній безпековій моделі комп'ютерних систем є настільки важливим, тому що фішингові атаки успішно застосовуються й дотепер, оминаючи усі технологічні бар'єри, скеровуючи свої потужності на застарілі або неефективні веб-браузери, антивірусні програми, та брандмауери. Зловмисники використовують велику кількість різних платформ по типу соцмереж, месенджерів, сервісів електронної пошти тощо для привертання уваги потенційних жертв. Налаштування антифішингових систем та брандмауерів є загальноприйнятим стандартом для більшості організацій, але їх ефективність визначається лише актуальністю оновлень баз даних, які можуть не тільки не встигати, а й навіть суттєво відставати від актуальних трендів у зловмисників.

Набуття та підтримання високого рівня кібербезпеки на підприємстві обов'язково пов'язані з розумінням та навчанням персоналу, особливо тих, хто відповідає за управління та адміністрування ІС. Однією з ключових складових є рекрутинг та навчання компетентного персоналу з питань кібербезпеки для ефективної протидії фішинговим атакам. Менеджери та адміністратори повинні володіти не лише технічними знаннями, а й навичками виявлення та запобігання фішинговим загрозам. Навчання персоналу повинно охоплювати такі аспекти, як визначення підозрілих повідомлень у електронній пошті, розпізнавання фішингових веб-сайтів та важливість безпекових процедур при роботі з певною інформацією. Забезпечення кібербезпеки також включає в себе перевірку кандидатів під час рекрутингу, аналіз їхнього рівня кіберграмотності та ступінь свідомості щодо потенційних кіберзагроз.

Людський фактор є ключовим аспектом в захисті від фішингових атак і визначається рівнем усвідомленості та особливостями поведінки користувачів. Відповідною освітою та регулярними тренуваннями можна в значній мірі знизити ризики, пов'язані зі схильністю до фішингу.

Фішингові атаки також можуть використовувати тактику "соціального інженерінгу в реальному світі". Наприклад, атакуючий може виглядати як співробітник офісу, кур'єр або представник компанії з технічної підтримки, щоб отримати доступ до необхідних йому приміщень, по типу серверних, або задля того, щоб впливати на жертву особисто.

Для мінімізації ризиків від людського фактору необхідно акцентувати увагу на освіті персоналу, проводити тренінги з виявлення фішингового контенту та регулярно нагадувати про правила безпеки в мережі. Особиста відповідальність та бережливість при користуванні мережею Інтернет є важливими елементами зниження ймовірності успіху фішингових атак.

3.1 Розгляд технологічних методів захисту від фішингу

Алгоритми захисту від фішингу вбудовані в будь-яке програмне забезпечення чи систему, яка призначена для протидії фішинговим атакам [24]. Розробка таких систем набуває популярності, особливо через значне зростання кількості фішингових атак у всьому світі. Фішинг є ефективним завдяки обману людини, та гарантує те, що жертва не здогадається про напад до того, як стане вже занадто пізно. Ефективність алгоритмів полягає в їх здатності виявляти атаку в процесі її виконання. ШІ та технології МН внесли вагомий внесок у успіх алгоритмів захисту від фішингу [24]. Ці технології спроможні виявляти фішинг завдяки тому, що машинне навчання приблизно відтворює алгоритми мислення людей. Здатність до навчання гарантує, що системи зможуть освоювати нову інформацію та виявляти фішингові атаки швидше та ще до того, як вони почнуть

діяти. Використання технології ШІ для запобігання фішингу демонструє високу ефективність. Однією з ключових переваг використання штучного інтелекту для виявлення фішингових атак є його висока швидкість і ефективність. Більшість систем захисту в останні роки використовують штучний інтелект через його велику чутливість. За останні кілька років ця технологія досягла вражаючих результатів, що свідчить про її високий потенціал у сфері алгоритмів захисту від фішингу.

3.1.1 Антифішингова система Netcraft

Netcraft, одна з провідних компаній у цій сфері, пропонує інноваційні рішення для виявлення фішингових атак через моніторинг та аналіз великого обсягу інтернет-ресурсів. Їх технології базуються на великій базі даних та використанні аналітики для виявлення аномалій та підозрілих патернів веб-ресурсів.

Одним із ключових аспектів підходу системи Netcraft є активне виявлення фішингових веб-сайтів та інших шахрайських ресурсів. Netcraft використовує сучасні методи аналізу веб-ресурсів, включаючи регулярні сканування та моніторинг доменних імен. Їхні інструменти здатні реагувати на нові загрози та швидко виявляти та блокувати фішингові ресурси після їхнього виявлення. Компанія також активно вивчає соціальні мережі та інші онлайн-канали для виявлення спроб фішингових атак, використовуючи аналіз поведінки користувачів та інші аспекти СІ. Особливу увагу приділяється розробці інтегрованих інструментів для захисту користувачів електронної пошти та браузерів від фішингових атак. Це включає в себе фільтрацію та виявлення шкідливих листів, а також убезпечення браузерів від небезпечних веб-сайтів.

chromewebstore.google.com

Site Report

Risk Rating: 7

Country:	US	Site rank:	NA
First seen:	July 2023	Host:	Google LLC
PFS:	✓	SSLv3:	Not supported

Disable protection for this site ☐

Report malicious URL:

The URL of the site: ✓

Add a reason ☐

Your email address (to receive updates): ✓

netcraft

Рисунок 3.1 – Інтерфейс веб-додатку системи Netcraft

Завдяки комплексному підходу, за заявою Netcraft, їх система кожного дня аналізує більше 5 мільйонів підозрілих веб-посилань, усього заблоковано 190 мільйонів спроб скоєння фішингу, і більше 20 мільйонів переривань злочинних дій [21].

Сам комплексний підхід полягає у 5 пунктах:

- моніторинг доменів та серверів: Netcraft має велику базу даних, яка регулярно оновлюється шляхом сканування й аналізу великої кількості доменів та серверів. Цей моніторинг дозволяє виявляти нові, раніше невідомі фішингові ресурси;
- аналітика відкритого тексту: антифішингові інструменти Netcraft використовують аналітику відкритого тексту для виявлення специфічних ключових слів, патернів та ознак, що характеризують фішингові сайти. Цей аналіз полегшує виявлення спроб маніпулювання текстом, що може вказувати на шахрайські схеми;

- моніторинг SSL-сертифікатів: Netcraft слідкує за видачею та використанням SSL-сертифікатів, оскільки фішери часто використовують шифрування для створення ілюзії оригінальності. Відстеження сертифікатів дозволяє вчасно виявляти та блокувати підроблені SSL-сертифікати;
- система оцінювання довіри: Netcraft використовує систему оцінювання довіри для визначення рівня довіри до конкретних доменів та веб-ресурсів. Вона аналізує різні фактори, такі як час існування домену, історія атак, тощо, для прийняття вірного рішення.
- міжнародний сервіс перевірки сайтів: Netcraft здійснює перевірку сайтів через глобальну мережу веб-ресурсів, які були додані, як «підозрілі».

3.1.2 Антифішингова система SpoofGuard

SpoofGuard – це інструмент, призначений для запобігання зміни віртуальними машинами у вашій мережі їхньої існуючої IP-адреси. У випадку, якщо IP-адреса віртуальної машини не відповідає IP-адресі на відповідному логічному порту та зв'язаному з ним адресом комутатора в SpoofGuard, віртуальний мережевий інтерфейс машини повністю блокує доступ до мережі. SpoofGuard може бути налаштований на рівні порту чи комутатора. Причин для використання SpoofGuard у вашій мережі:

- запобігання тому, щоб ВМ зловмисника приймала IP-адресу існуючої ВМ у вашій мережі;
- забезпечення того, що IP-адреси віртуальних машин не можуть бути змінені без безпосереднього втручання адміністратора – у деяких віртуальних середовищах бажано, щоб ВМ не могли змінювати свої IP-адреси без належного контролю. SpoofGuard допомагає забезпечити це, гарантуючи, що власник віртуальної машини не може просто так змінити IP-адресу та продовжувати працювати без перешкод;

– гарантія того, що правила розподіленого брандмауера (DFW) не будуть ненавмисно (або навмисно) обійдені – для правил DFW, створених з використанням IP-списків як джерел, завжди існує можливість того, що віртуальна машина може підробити свою IP-адресу в заголовку пакета, тим самим обійшовши правила.

Конфігурація SpoofGuard NSX охоплює наступне:

- MAC SpoofGuard – аутентифікує MAC-адресу пакета;
- IP SpoofGuard – аутентифікує MAC- та IP-адреси пакета;
- інспекція динамічного протоколу розпізнавання адрес (ARP), тобто SpoofGuard ARP та Gratuitous ARP (GARP), та перевірка SpoofGuard Neighbor Discovery (ND) виконуються на основі співставлення джерела MAC-адреси, джерела IP-адреси та джерела IP-MAC-пари адрес в корисному навантаженні ARP/GARP/ND.

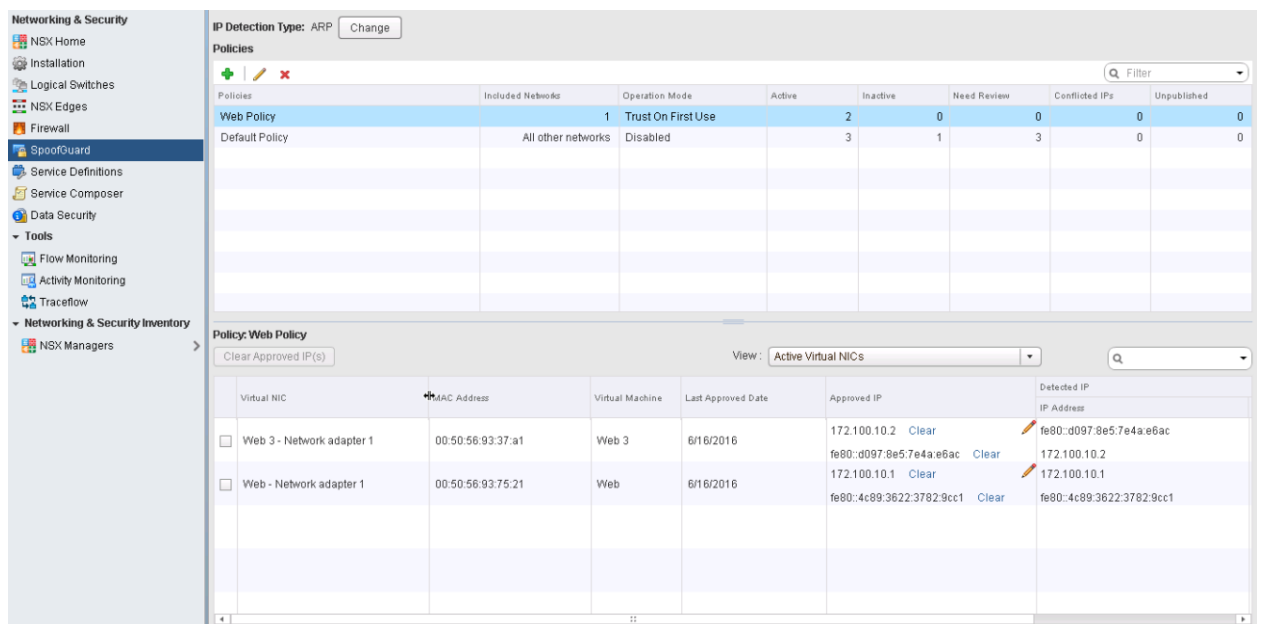


Рисунок 3.2 – Інтерфейс антифішингової системи SpoofGuard [23]

На рівні порту список дозволених MAC/VLAN/IP надається через властивість порту під назвою Address Bindings. Коли віртуальна машина надсилає запит, він блокується у випадку якщо її IP/MAC/VLAN не відповідає

властивостям IP/MAC/VLAN порту. Портовий SpoofGuard аутентифікує трафік, тобто перевіряє, чи відповідають прийняті пакети заданій конфігурації.

На рівні комутатора список дозволених MAC/VLAN/IP так само, як і у випадку з портом, надається через властивість Address Binding. Це, зазвичай, діапазон/підмережа, які дозволяються для комутатора і задачею SpoofGuard є авторизація трафіку на рівні комутатора. Для надходження до комутатора, трафік повинен бути схвалений портовим та комутаторним фільтрами SpoofGuard. Активація чи деактивація портового та комутаторного фільтрів SpoofGuard може бути виконана за допомогою профілю перемикачів [22].

3.1.3 Візуалізації бінарних даних та МН у протидії фішингу

Візуалізація бінарних даних та використання МН представляють собою потужний інструментарій у боротьбі з фішинговими атаками. Виявлення та аналіз бінарних даних, що характеризують фішинг, може бути значно полегшено завдяки використанню методів візуалізації. Ця стратегія дозволяє зрозуміти внутрішню структуру даних та виявляти відмінності, що вказують на потенційні загрози. Машинне навчання, зокрема, використовуючи алгоритми класифікації та кластеризації, дозволяє навчити систему розпізнавати патерни фішингових атак.

Цей метод пропонує новий підхід, який є автоматизованим процесом виявлення фішингових веб-ресурсів без подальшої взаємодії з користувачами, що дозволяє швидше та точніше визначати фішингові сайти. Експерименти показали високий рівень точності цього підходу [25]. Використання МН та обробки зображень для аналізу підозрілих сайтів дозволяє користувачам швидше зрозуміти потенційні загрози та оцінити вірогідність фішингової атаки у даний момент часу. Основна суть методу полягає в цілковитій

автоматизації виявлення фішингових веб-ресурсів та контенту, що на ~95% зменшує шанси зловмисників на вдалу фішингову атаку [25].

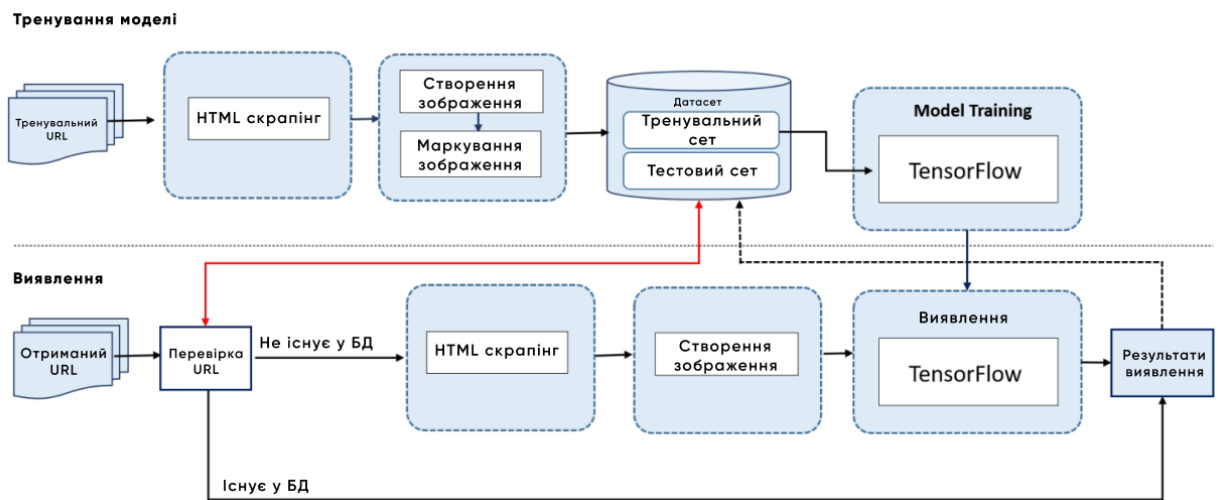


Рисунок 3.1 – Алгоритм виявлення фішингової веб-сторінки

Представлена система складається з двох ключових етапів: етапу навчання та етапу виявлення. Під час першого етапу створюються зразки та визначається топологічна структура машинного навчання TensorFlow. На другому етапі, етапі виявлення, URL-адреси перевіряються на наявність зразків у базі даних для подальшої класифікації. Цей підхід заснований на візуалізації скопійованих файлів HTML у вигляді 2D-зображень, які подаються на обробку TensorFlow. Алгоритм аналізує їх, використовуючи навчальні модулі, для розрізнення оригінальних та фішингових веб-сайтів.

URL-адреси, які пройшли через систему, реєструються в базі даних, і кожна нова URL-адреса, подана системою користувача, перевіряється на предмет дублікатів. Це допомагає підвищити ефективність системи, уникнувши повторного процесу створення бінарного зображення, на що витрачається час та потужності. Якщо подана URL-адреса відсутня в базі даних, система автоматично витягує HTML-код з відповідного веб-ресурсу і зберігає його у форматі бінарного рядка. Після отримання та збереження вихідного коду веб-сайту відповідний бінарний файл передається в модуль

створення зображень, де використовується метод візуалізації BinVis для перетворення бінарних файлів у 2D-зображення. Далі створені зображення проходять аналіз за допомогою нейронної мережі TensorFlow для проведення класифікації.

Після отримання та збереження системою коду веб-ресурсу, вона направляє цей код в BinVis для створення RGB-зображення. BinVis – це інструмент візуалізації бінарних даних, який конвертує файл бінарного типу у візуальний формат, найчастіше JPEG або PNG. Цей інструмент вибирає окремі символи з рядка, сформованого на попередньому етапі, конвертує їх у бінарний вид і далі перетворює на значення RGB. BinVis розподіляє різні символи ASCII за кольорами, таким чином:

- синій – друковані символи ASCII;
- зелений – контрольні символи;
- червоний – розширені символи ASCII;
- чорний і білий – нульовий символ і пробіли.

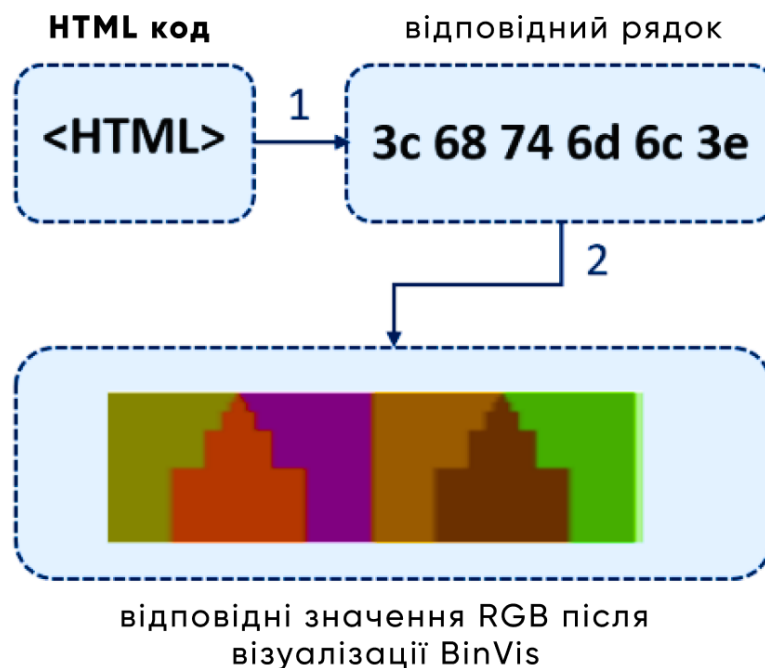


Рисунок 3.2 – Алгоритм процесу генерації зображення

Система МН TensorFlow аналізує та класифікує зображення від Binvis на основі свої алгоритмів широкого навчання. Завдяки адаптивності TensorFlow системи МН використовувалися в різних галузях інформатики, зокрема для пошуку інформації, обробки географічних зображень, робототехніки, комп'ютерного зору тощо [26]. У порівнянні з іншими аналогічними моделями, ця більше підходить для аналізу потенційних фішингових сторінок завдяки видатним можливостям розпізнавання зображень. Нейромережа досить добре визначає відмінності між фотографіями, навіть ті, які людське око не здатне помітити. TensorFlow виконує класифікацію, використовуючи вхідні дані зображення, згенеровані на попередніх етапах. Для перенавчання з метою прискорення роботи системи використовується нейронна мережа MobileNet [27].

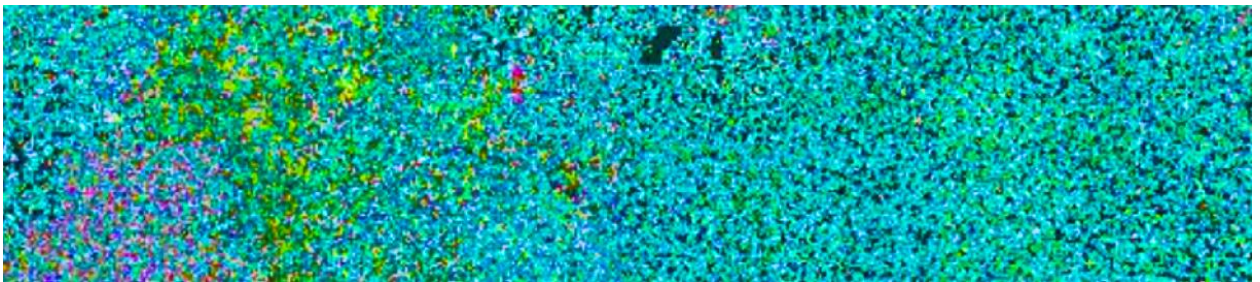


Рисунок 3.3 – Конвертоване зображення оригінальної сторінки авторизації соцмережі Facebook

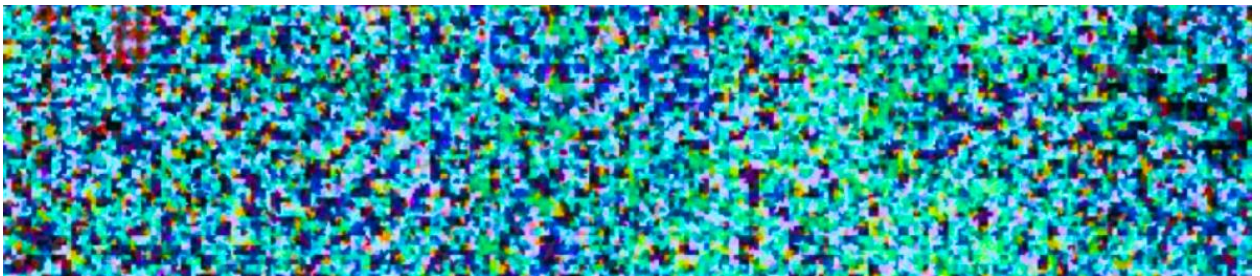


Рисунок 3.4 – конвертоване зображення фішингової сторінки авторизації соцмережі Facebook

Загальні результати показаного методу показані на малюнку досягнули загальної точності виявлення у 94,16%, що є високим показником і задовольняє необхідну точність у реальних ситуаціях. Коефіцієнтом точності класифікації у 95,83% також є досить хорошим показником, демонструючи сильну загальну довіру до процесу розпізнавання образів. Такий показник точності виявлення фішингу вважається поважним і позитивним результатом.

3.2 Аналіз організаційних заходів для запобігання фішинговим атакам

У сучасному бізнес-середовищі вирішення проблеми фішингових атак вимагає комплексного підходу, впроваджуючи такі організаційні заходи для ефективного запобігання і виявлення подібних загроз:

- інформаційна освіта та навчання: однією з ключових стратегій є введення програм інформаційної освіти для персоналу. Ці програми повинні охоплювати різні аспекти кібербезпеки, включаючи розпізнавання фішингових атак, використання складних паролів та управління конфіденційністю. Регулярне навчання персоналу дозволяє підтримувати актуальність їхніх знань та покращувати реакцію на нові загрози;

- впровадження політик безпеки: організації повинні ретельно визначити та впровадити строгі політики безпеки, що стосуються доступу до конфіденційної інформації. Це включає в себе обмеження доступу до специфічних даних лише для необхідних працівників, встановлення прозорих правил використання електронної пошти та інших комунікаційних каналів;

- використання антивірусних та антифішингових програм: організації повинні інвестувати в сучасне програмне забезпечення, яке виявляє та блокує фішингові атаки. Антивіруси та антифішингові програми, оновлювані регулярно, забезпечують ефективний захист від нових загроз та виявляють підозрілі дії персоналу;

- моніторинг та аудит безпеки: важливо реалізувати системи моніторингу та аудиту безпеки для виявлення невідповідностей в практиках безпеки та подій, що можуть вказувати на фішингові атаки. Ці системи дозволяють оперативно реагувати на інциденти та вживати заходів для їхнього усунення;
- захист персональних даних: організації повинні ретельно керувати та захищати персональні дані своїх співробітників та клієнтів. Це включає в себе шифрування даних, безпечне зберігання та обмін інформацією, а також встановлення строгих правил доступу;
- розробка плану реагування на інциденти: вироблення детального плану реагування на інциденти допомагає ефективно впоратися з фішинговими атаками у випадку їхнього виявлення. Цей план може включати в себе ізоляцію компрометованих систем, залучення експертів з кібербезпеки та сповіщення відповідних сторін;
- створення культури безпеки: формування культури безпеки в організації є важливим аспектом протидії фішинговим атакам. Залучення персоналу до активної участі у забезпеченні безпеки та встановлення внутрішньої свідомості стосовно кіберзагроз допомагає підвищити рівень відповідальності та уваги до безпеки даних.

3.2.1 Інформаційна освіта та навчання

З усіх вище перелічених заходів потрібно виділити саме інформаційну освіту та навчання, тому що вони є ключовим елементом стратегії забезпечення кібербезпеки на підприємстві. Цей підхід передбачає систематичне навчання персоналу з питань кіберзагроз, зокрема фішингових атак.

Складові інформаційної освіти:

- розпізнавання фішингових атак: співробітникам надається конкретна інформація про різновиди фішингу, його характеристики та методи виявлення. Навчання включає в себе аналіз характерних рис лукавих повідомлень, електронних листів та посилань;
- соціальна інженерія та психологія атак: освіта охоплює аспекти соціальної інженерії, що допомагає персоналу розуміти, як атаки можуть використовувати психологічні та соціальні методи вводу в оману;
- створення та управління безпечними паролями: навчання забезпечує розуміння важливості сильних паролів та навчає правилам їх створення і регулярної зміни.

Методи проведення навчання:

- онлайн курси та вебінари: застосування сучасних засобів, таких як онлайн платформи та вебінари, дозволяє забезпечити доступні та ефективні заняття для персоналу;
- симуляції фішингових атак: проведення симуляцій допомагає практикувати отримані знання у реальному часі, створюючи сценарії, аналогічні реальним фішинговим загрозам;
- постійні оновлення матеріалів: освітні матеріали повинні постійно оновлюватися, враховуючи нові тренди в кіберзлочинності та зміни в методах атак.

Переваги інформаційної освіти:

- підвищення обізнаності персоналу: зростання рівня знань сприяє свідомому виявленню та униканню потенційно небезпечних ситуацій;
- зменшення ризику успішних атак: навчаний персонал стає менш вразливим перед фішинговими атаками, зменшуючи ризик витоку конфіденційної інформації;
- видимий внесок у загальний рівень кібербезпеки: інформаційна освіта стає частиною загальної культури безпеки на підприємстві, викликаючи позитивні зміни в поведінці персоналу.

3.2.2 Розробка плану реагування на інциденти

Ретельна розробка плану реагування на інциденти є важливим етапом в забезпеченні безпеки організації в умовах зростаючих фішингових загроз. План повинен бути чітко продуманим та повинен враховувати специфіку діяльності конкретного підприємства, або потреб людини:

- визначення загроз і слабких місць: перший крок у розробці плану – аналіз типових фішингових інцидентів, які можуть виникнути під час ведення діяльності. Врахування відомих публічних прикладів та ідентифікація потенційних слабких місць в інфраструктурі та ПЗ дозволяє створити більш ефективні заходи захисту;

- формування команди для реагування: розробники плану повинні визначити ключових членів команди для реагування на подібні інциденти. Ними можуть бути представники з різних відділів, таких як ІТ, відділу безпеки, комунікації та юридичного відділу. Децентралізація команди допомагає більш повно та збалансовано реагувати на інциденти;

- встановлення критеріїв серйозності: необхідно визначити критерії, за якими буде визначатися серйозність інциденту. Це може включати в себе потенційні втрати даних, вплив на функціонування компанії, можливий фінансовий збиток, удар по репутації тощо. Це допоможе розставити пріоритети по реагуванню та вжити необхідні заходи;

- розробка комунікаційного плану: комунікація важлива в управлінні будь-яким інцидентом. План повинен визначати процедури інформування зацікавлених сторін, включаючи внутрішній персонал, клієнтів, партнерів та органи регулювання. Комунікаційний план повинен також враховувати способи збереження репутації підприємства під час інциденту;

- сценарії та тренування: план реагування повинен містити сценарії для різних типів інцидентів, а також провідні практики для ефективної

взаємодії у команді. Регулярні тренування та симуляції інцидентів дозволяють персоналу реагувати швидко та ефективно на реальні загрози;

- оновлення та аналіз: план повинен постійно оновлюватися, враховуючи актуальні загрози та вдосконалення технологій кіберзагроз. Після кожного інциденту важливо провести аналіз для ідентифікації можливих модифікацій та корекцій, як у плані реагування, так і в усій системі безпеки загалом;

- співпраця з експертами: план повинен включати механізми для швидкого залучення зовнішніх незалежних експертів з кібербезпеки у випадках складних або непередбачених інцидентів. Співпраця з фахівцями може значно полегшити виявлення та вирішення проблем.

Висновки до третього розділу

Ефективність комплексного підходу до боротьби з фішингом визначається успішним поєднанням різноманітних методів та технологій, про які йшлося в цьому розділі. Застосування алгоритмів захисту, які використовують ШІ, грає ключову роль у виявленні фішингових атак. МН, зосереджене на аналізі поведінки користувачів та структури електронних повідомлень, дозволяє розпізнавати добре замасковані фішингові схеми.

Паралельно із використанням технологічних рішень, тривале та професійне навчання персоналу стає важливим елементом у захисті від фішингу. Освічені менеджери та адміністратори здатні виявляти підозрілі ситуації та вчасно реагувати на можливі загрози. Навчання сприяє створенню свідомого підходу до кібербезпеки та усвідомленню ризиків, пов'язаних з фішинговими атаками.

Комплексний підхід також передбачає використання антифішингових систем, зокрема SpoofGuard, яка детально відстежує трафік у мережі. За

допомогою SpoofGuard можна контролювати адреси та блокувати доступ у випадках, коли відбуваються непередбачені зміни у адресації. Ця система дозволяє адміністраторам гнучко налаштовувати правила та надає ефективний механізм захисту від різноманітних фішингових сценаріїв.

Урахування людського фактору також є важливою складовою комплексного підходу. Свідомість персоналу щодо методів фішингу та навички розпізнавання підозрілих ресурсів можуть бути вирішальними у запобіганні фішингових атак. Регулярне навчання та інформаційні кампанії, спрямовані на підвищення кібергігієни серед персоналу, можуть значно підвищити рівень, як особистої захищеності, так і захищеності підприємства в цілому.

Тому роблю висновок, що синергія технологічних рішень, компетентного навчання персоналу та використання спеціалізованих антифішингових систем утворює надійний комплексний підхід, який забезпечує максимально ефективний захист від фішингових атак.

ВИСНОВКИ

У ході мого дослідження у рамках дипломної роботи, присвяченої систематизації та аналізу сучасних методів виявлення та протидії фішинговим атакам на веб-ресурсах, я детально розглянув різноманітні підходи до захисту від фішингу, зокрема використання алгоритмів, технологій ШІ, навчання персоналу та спеціалізовані антифішингові системи, такі як SpoofGuard та Netcraft.

Порівнювати усі вище розглянуті методи не бачу сенсу, тому що кожен з них доповнює один одного, утворюючи дуже потужну систему захисту від фішингу. Алгоритми на базі штучного інтелекту виявляють фішингові атаки завдяки здатності аналізувати великі обсяги даних та виявляти аномалії у поведінці користувачів. Технології МН сприяють ранньому виявленню атак та адаптації до нових схем фішингу. Навчання персоналу важливе для створення свідомого підходу до кібербезпеки та розпізнавання підозрілих ситуацій. Антифішингові системи, як SpoofGuard та Netcraft, акцентують увагу на відстеженні трафіку у мережі. Ефективність комплексного підходу виявилася високою через повну взаємодію трьох різних методів. Поєднання алгоритмів ШІ, технологій МН, навчання персоналу та використання антифішингових систем створило повноцінну систему, що забезпечує ефективний захист від фішингових атак на веб-ресурси.

Один із ключових висновків, який можна зробити, полягає в тому, що немає універсального методу виявлення та захисту від фішингу. Різноманітність та стійкість сучасних фішингових атак вимагає поєднання різних інструментів та підходів. Алгоритми на базі штучного інтелекту та машинного навчання, хоча і виявляються ефективними, не можуть функціонувати відокремлено від інших заходів безпеки. Навчання персоналу виходить на перше місце у контексті створення культури кібербезпеки в

організації. Свідомість співробітників стосовно потенційних загроз і їх здатність розпізнавати фішингові схеми є дуже важливим фактором.

Основною метою моєї дипломної роботи було визначення ефективних технологій та стратегій, які забезпечують надійний захист інформації та користувачів в онлайн середовищі. Я впевнений, що досягнуті результати відповідають цій меті, а висновки та рекомендації стануть корисними як для вчених, так і для практиків у галузі кібербезпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. The Use Of Psychology In Phishing Attacks (2023). Packetlabs. URL: <https://www.packetlabs.net/posts/psychology-of-phishing-attacks/> (дата звернення: 26.09.2023)
2. 2021 Data Breach Investigations Report (2021). DBIR. URL: https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report (дата звернення: 20.08.2023)
3. APWG: Phishing Activity Trends Report Q3 2022. Computer Fraud & Security. 2022. Т. 2022, № 3. С. 4. URL: [https://doi.org/10.1016/s1361-3723\(19\)30025-9](https://doi.org/10.1016/s1361-3723(19)30025-9) (дата звернення: 01.11.2023).
4. Phishing Email Examples — The Best & Worst. Re-Hashed. URL: <https://www.thesslstore.com/blog/phishing-email-examples-the-best-worst/> (дата звернення: 12.11.2023)
5. A Systematic Review on Deep-Learning-Based Phishing Email Detection. Kutub Thakur, Md Liakat Ali, Muath A. Obaidat, Abu Kamruzzaman. URL: <https://www.mdpi.com/2079-9292/12/21/4545> (дата звернення: 28.09.2023)
6. Spam and phishing in 2022. Kaspersky. URL: <https://securelist.com/spam-phishing-scam-report-2022/108692/> (дата звернення: 17.10.2023)
7. Seagate Employee Tax Forms Stolen in Phishing Attack. Securityweek. URL: <https://www.securityweek.com/seagate-employee-tax-forms-stolen-phishing-attack/> (дата звернення: 22.11.2023)
8. Bank Hackers Steal Millions via Malware. The New York Times. URL: <https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html> (дата звернення: 14.11.2023)

9. Dangerous "like-farming" scam returns to Facebook. Here's what you need to know. CBS News. URL: <https://www.cbsnews.com/news/dangerous-like-farming-scam-returns-to-facebook-heres-what-you-need-to-know/>

(дата звернення: 27.11.2023)

10. Нова фішинг-атака на користувачів України та Польщі: хто під прицілом. ESET. URL: <https://www.eset.com/ua/about/newsroom/press-releases/malware/nova-fishynh-ataka-na-korystuvachiv-ukrayiny-ta-polshchi-khto-pid-prytsilom/> (дата звернення: 01.10.2023)

11. 13+ Smishing statistics in 2023 (SMS phishing attacks). ErathWeb. URL: <https://earthweb.com/smishing-statistics/> (дата звернення: 05.11.2023)

12. "Картка заблокована": клієнти Ощадбанку отримують SMS від аферистів. InternetUA. URL: <https://internetua.com/-karta-zablokirovana-klienty-osxadbanka-polucsauat-sms-ot-aferistov> (дата звернення: 29.11.2023)

13. What Is Phishing? Phishing.org. URL: <https://www.phishing.org/what-is-phishing> (дата звернення: 09.11.2023)

14. Large-scale automatic classification of phishing pages. C. Whittaker. URL: <https://research.google.com/pubs/archive/35580.pdf> (дата звернення: 10.11.2023)

15. 'Мамо, я збила людину': як у Києві аферисти виманили у жінки мільйон гривень. Informator.ua. URL: <https://kiev.informator.ua/uk/mama-ya-sbila-cheloveka-kak-kieve-aferisty-vymanili-u-zhenshhiny-million-griven> (дата звернення: 27.11.2023)

16. The Major Types of Phishing Attacks & How to Identify Them: The Definitive Guide. WeSecureApp. URL: <https://wesecureapp.com/blog/the-major-types-of-phishing-attacks-how-to-identify-them-the-definitive-guide/> (дата звернення: 29.11.2023)

17. Does VPN Protect You From Phishing Attacks? Tickethold. URL: <https://www.ticktechold.com/does-vpn-protect-you-from-phishing/> (дата звернення: 28.11.2023)

18. Sniff-Phish: A novel framework for resource intensive computation in cloud to detect email scam. ResearchGate. URL:

https://www.researchgate.net/figure/Sniff-Phish-in-context-menu-Starting-to-analyze-an-email-hyperlink-embed-in-an-image_fig4_331969789

(дата звернення: 16.11.2023)

19. Where Gophish is Going in 2019. Getgophish. URL: <https://getgophish.com/blog/post/2019-01-06-gophish-in-2019/> (дата звернення: 30.11.2023)

20. kgretzky/evilginx2. Github. URL: <https://github.com/kgretzky/evilginx2> (дата звернення: 20.11.2023)

21. Defeating cyber attacks with unmatched scale and effectiveness. Netcraft. URL: <https://www.netcraft.com/> (дата звернення: 10.11.2023)

22. Understanding SpoofGuard. VM Ware Docs. URL: <https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-2E331082-1D1C-4B51-BB5A-A909BC> (дата звернення: 22.11.2023)

23. Understanding SpoofGuard. VM Ware Docs. URL: <https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-2E331082-1D1C-4B51-BB5A-A909BCD5FED0.html> (дата звернення: 26.10.2023)

24. Monitoring VMware NSX SpoofGuard with REST API and Perl. VM Ware. URL: <https://blogs.vmware.com/networkvirtualization/2016/06/monitoring-vmware-nsx-spoofguard-rest-api-perl.html/> (дата звернення: 24.11.2023)

25. Detecting Phishing SMS Based on Multiple Correlation Algorithms. Gunikhan Sonowal. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7604914/> (дата звернення: 15.11.2023)

26. A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning / L. Barlow та ін. 2020 IEEE World Congress on Services (SERVICES), м. Beijing, China, 18–23 жовт. 2020 р. 2020. URL: <https://doi.org/10.1109/services48979.2020.00046> (дата звернення: 29.11.2023)

27. TensorFlow : Large-Scale Machine Learning on Heterogeneous Distributed Systems. Eugene Brevdo. URL:

https://www.researchgate.net/publication/319770252_TensorFlow_Large-Scale_Machine_Learning_on_Heterogeneous_Distributed_Systems

(дата звернення: 26.11.2023)

28. MobileNets: Open-Source Models for Efficient On-Device Vision. Andrew G. Howard. URL: <https://blog.research.google/2017/06/mobilenets-open-source-models-for.html> (дата звернення: 10.11.2023)