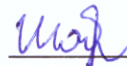


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

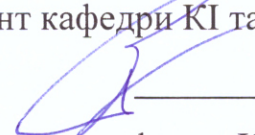
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби моделювання фішингових
сценаріїв для оцінювання ефективності захисту
ПОШТОВИХ СИСТЕМ»

Виконав студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека»

 Олександр ШАБРАНЮК

Керівник доцент кафедри КІ та КБ, к.т.н.

 Олександр ПІРОГ

Рецензент завідувач кафедри КІ та КБ, к.т.н.

 Андрій ЄФІМЕНКО

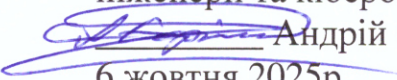
Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
6 жовтня 2025р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Шабранюк Олександр Миколайович

Тема роботи: «Методи та засоби моделювання фішингових сценаріїв для оцінювання ефективності захисту поштових систем»

затверджена Наказом університету від 6 жовтня 2025 р. № 566/с

Термін здачі студентом закінченої роботи 14 грудня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

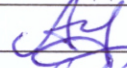
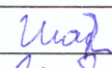
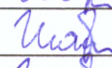
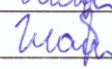
- Розробити структурований сценарій фішингової розсилки;
- Розробити сценарій і послідовність дій для імітації фішингової атаки;
- Скласти план фішингової кампанії для проведення тестування безпеки;
- Здійснити аналіз ефективності механізмів захисту електронних

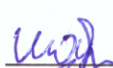
поштових систем.

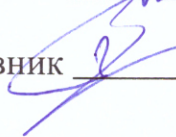
Обладнання та програмне забезпечення:

1. Програмне забезпечення для тестування фішингових атак: Gophish, SEToolkit, King Phisher;
2. Сервери електронної пошти Gmail, hMailServer;
3. Поштовий клієнт Thunderbird.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Шелуха О.О.	 06.10.25	06.10.25 
2	Шелуха О.О.	 06.10.25	06.10.25 
3	Шелуха О.О.	 06.10.25	06.10.25 

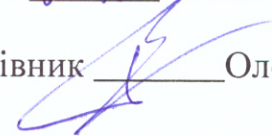
Студент  Олександр ШАБРАНЮК

Керівник  Олександр ПІРОГ

Календарний план

№з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 жовтня	
2	Пошук теоретичної інформації	8 жовтня	
3	Вибір програмного забезпечення	20 жовтня	
4	Розробка плану фішингової атаки	30 жовтня	
5	Проведення фішингової атаки hmailserver	5 листопада	
6	Проведення фішингової атаки Gmail	11 листопада	
7	Проведення аналізу ефективності поштових систем	1 грудня	
8	Оформлення пояснювальної записки	10 грудня	

Студент  Олександр ШАБРАНЮК

Керівник  Олександр ПІРОГ

АНОТАЦІЯ

Метою кваліфікаційної роботи є дослідження механізмів фішингових атак та оцінювання ефективності засобів захисту електронної пошти з метою підвищення рівня інформаційної безпеки користувачів.

У роботі визначено основні загрози, пов'язані з фішингом та соціальною інженерією, а також проаналізовано принципи їх реалізації. Розглянуто основні види фішингових атак, їх характерні ознаки та методи психологічного впливу на користувачів. Особливу увагу приділено практичному моделюванню фішингових розсилок із використанням платформи Gophish.

У межах дослідження було розгорнуто та налаштовано локальний поштовий сервер hMailServer, підключено поштові скриньки до поштового клієнта Thunderbird і проведено тестування фішингових атак у локальному середовищі. Також виконано тестування доставки фішингових повідомлень на поштовий сервіс Gmail з метою аналізу його механізмів захисту, включаючи спам-фільтрацію, перевірку SPF/DKIM/DMARC та відображення попереджувальних повідомлень для користувача. Додатково було продемонстровано можливість блокування фішингових розсилок на рівні локального сервера за допомогою правил фільтрації.

Наведено результати експериментального дослідження, які підтверджують ефективність багаторівневих механізмів захисту сучасних поштових систем та можливість протидії фішинговим атакам як у хмарних сервісах, так і в локальному середовищі.

Дипломна робота має обсяг 119 сторінки, містить 58 рисунків, 2 таблиці, 38 літературних джерел та один додаток.

Ключові слова: фішинг, соціальна інженерія, фішингові атаки, локальний поштовий сервер, поштовий хмарний сервер, поштовий клієнт.

ANNOTATION

The thesis has a volume of 119 pages, contains 38 figures, 2 table, 58 literary sources and one appendix.

The purpose of this qualification work is to study the mechanisms of phishing attacks and to evaluate the effectiveness of email security measures in order to increase the level of users' information security.

The paper identifies the main threats associated with phishing and social engineering and analyzes the principles of their implementation. The main types of phishing attacks, their characteristic features, and methods of psychological influence on users are examined. Special attention is paid to the practical modeling of phishing email campaigns using the Gophish platform.

Within the scope of the study, a local mail server based on hMailServer was deployed and configured, email accounts were connected to the Thunderbird mail client, and phishing attack testing was conducted in a local environment. In addition, phishing email delivery to the Gmail mail service was tested to analyze its security mechanisms, including spam filtering, SPF/DKIM/DMARC verification, and the display of warning messages to the user. Furthermore, the possibility of blocking phishing campaigns at the level of a local mail server using filtering rules was demonstrated.

The results of the experimental study confirm the effectiveness of multi-layered protection mechanisms of modern email systems and demonstrate the ability to counter phishing attacks both in cloud-based services and in local environments.

Keywords: phishing, social engineering, phishing attacks, gmail, hmailserverl, thunderbird.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ОСНОВИ ФІШИНГУ ДЛЯ ОЦІНЮВАННЯ ЗАХИСТУ ПОШТОВИХ СИСТЕМ	10
1.1 Роль кіберзагроз інформаційного простору	10
1.2 Сутність фішингу та його роль у формуванні кіберзагроз.....	12
1.3 Соціально-інженерні техніки: характеристика та оцінка	19
1.4 Правове регулювання боротьби з кіберзлочинністю, що базується на методах соціальної інженерії.	33
Висновки до першого розділу	39
РОЗДІЛ 2 РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ТА ВПРОВАДЖЕННЯ СПОСОБУ АТАКИ	40
2.1 Заходи безпеки проти фішингових атак	40
2.2 Особливості організації та виконання фішингових дій	48
2.3 Методологія підбору атак для пентестування (аналіз факторів впливу)....	53
Висновки до другого розділу	66
РОЗДІЛ 3 АНАЛІЗ ФУНКЦІОНУВАННЯ ТА НАДІЙНОСТІ ПРОГРАМНИХ СИСТЕМ	68
3.1 Конфігурація сценарію атаки та здійснення тестового аналізу	68
3.2 Оцінювання ефективності захисту поштових систем.....	84
Висновки до третього розділу	113
ВИСНОВКИ.....	114
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	116

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

2FA – Двофакторна автентифікація

AOL – American Online

BOA – Bank of America

DKIM – DomainKeys Identified Mail

DMARC – Domain-based Message Authentication, Reporting and Conformance

DNS – Domain Name System

HTML – HyperText Markup Language

HTTP – HyperText Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

IMAP – Internet Message Access Protocol

IP – Internet Protocol address

MFA – Multi-Factor Authentication

SMTP – Simple Mail Transfer Protocol

SPF – Sender Policy Framework

SSH – Secure Shell

SSL – Secure Sockets Layer

URL – Uniform Resource Locator

VoIP – Voice-over-IP

XSS – Cross-Site Scripting

ПЗ – Програмне забезпечення

ВСТУП

Актуальність теми. У сучасному цифровому середовищі електронна пошта залишається одним із ключових засобів комунікації, а також одним з основних векторів реалізації кібератак. Серед різноманітних загроз особливе місце займає фішинг — метод соціальної інженерії, спрямований на введення користувачів в оману з метою отримання конфіденційної інформації, облікових даних або доступу до інформаційних ресурсів. Незважаючи на розвиток технічних засобів захисту, фішингові атаки продовжують еволюціонувати та залишаються актуальною загрозою як для окремих користувачів, так і для організацій.

Актуальність дослідження зумовлена зростанням кількості фішингових розсилок, які використовують підроблені повідомлення від відомих сервісів, зокрема поштових платформ та вебсервісів. Ефективність таких атак значною мірою залежить від рівня захищеності поштових систем та обізнаності користувачів. Тому важливим є практичне дослідження механізмів виявлення і блокування фішингових повідомлень як у хмарних поштових сервісах, так і в локальних поштових середовищах.

Метою кваліфікаційної роботи є дослідження механізмів фішингових атак та оцінювання ефективності засобів захисту електронної пошти на прикладі хмарного сервісу Gmail і локального поштового сервера hMailServer з метою підвищення рівня інформаційної безпеки користувачів.

Для досягнення поставленої мети у роботі визначено такі завдання:

- дослідити теоретичні основи фішингу та соціальної інженерії;
- проаналізувати основні види фішингових атак і методи психологічного впливу;
- розглянути механізми захисту електронної пошти, зокрема SPF, DKIM та DMARC;
- проаналізувати можливості платформи Gophish для моделювання фішингових кампаній;
- налаштувати та протестувати локальний поштовий сервер hMailServer;

- виконати тестування фішингових розсилок у локальному середовищі та на сервісі Gmail;
- дослідити механізми блокування фішингових повідомлень на рівні поштового сервера;

Об’єктом дослідження є процеси забезпечення інформаційної безпеки електронної пошти в умовах фішингових атак.

Предметом дослідження є методи реалізації фішингових атак, механізми їх виявлення та блокування, а також програмні засоби для моделювання фішингових розсилок і захисту електронної пошти.

Методологія роботи. Під час виконання кваліфікаційної роботи використовувалися загальнонаукові та прикладні методи дослідження, зокрема аналіз і синтез, порівняння, узагальнення, систематизація, а також методи експерименту та спостереження. Практична частина роботи базується на експериментальному моделюванні фішингових атак із використанням платформи Gophish та аналізі реакції поштових систем на потенційно небезпечні повідомлення.

Практичне значення одержаних результатів. Практичне значення роботи полягає у демонстрації реальних механізмів виявлення та блокування фішингових розсилок у хмарних і локальних поштових системах.

Отримані результати можуть бути використані під час навчання з інформаційної безпеки, підготовки фахівців з кібербезпеки, а також при проведенні тестувань на проникнення у частині моделювання фішингових атак та оцінювання рівня захищеності електронної пошти.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних літературних джерел та додатку. Основний зміст роботи викладено на 119 сторінках друкованого тексту. Робота містить 2 таблиці та 58 рисунків. Список використаної літератури налічує 38 джерел, що викладені на 4 сторінках.

РОЗДІЛ 1 ОСНОВИ ФІШИНГУ ДЛЯ ОЦІНЮВАННЯ ЗАХИСТУ ПОШТОВИХ СИСТЕМ

1.1 Роль кіберзагроз інформаційного простору

У сучасних умовах розвитку суспільства інформаційний простір набуває дедалі більшої глобалізації та взаємозалежності. Паралельно з активним упровадженням цифрових технологій зростає і кількість, і складність кіберзагроз, що чинять вплив на державні, корпоративні та індивідуальні інформаційні системи. Серед таких загроз особливе місце займає фішинг, який, згідно з аналітичними дослідженнями, продовжує бути одним із головних інструментів кібератак у світі.

Кількість користувачів інтернету та цифрових платформ щороку невинно збільшується, що, у свою чергу, підвищує ризик витоку або компрометації даних. За даними Statista (2024) [\[3\]](#), понад п'ять мільярдів осіб активно користуються мережею Інтернет, роблячи її привабливим середовищем для діяльності кіберзлочинців.

Відповідно до Verizon Data Breach Investigations Report (2024) [\[2\]](#), понад 80% кібератак розпочинаються із застосування соціальної інженерії, зокрема фішингу, що свідчить про його ключову роль у загальній структурі кіберзагроз. Крім того, у звіті ENISA Threat Landscape (2024) [\[1\]](#) зазначається, що фішингові кампанії стають дедалі складнішими та використовують нові цифрові канали — електронну пошту, месенджери й соціальні мережі — для досягнення максимальної ефективності.

Крім безпосереднього впливу на безпеку даних, фішинг суттєво формує загальний ландшафт кіберзагроз, оскільки є стартовою точкою для більшості складних атак, таких як компрометація облікових записів, розповсюдження шкідливого програмного забезпечення чи атак типу «ланцюгового зламу».

У звіті INTERPOL Global Crime Trend Report (2024) [\[4\]](#) зазначено, що фішинг є основним інструментом початкового проникнення у 60% кіберінцидентів, зареєстрованих у різних регіонах світу. Це свідчить про його

системний вплив на глобальну кібербезпеку та актуальність проблеми у масштабах усього інформаційного простору.

Крім того, зростання фішингової активності сприяє поширенню недовіри до цифрових сервісів і державних електронних платформ. Згідно з аналітичним оглядом World Economic Forum Global Risks Report (2024) [\[5\]](#), кіберінциденти, пов'язані з фішингом, належать до п'ятірки найнебезпечніших глобальних ризиків у сфері цифрової економіки. Такі атаки не лише завдають фінансових збитків, а й підривають довіру громадян до процесів цифровізації, що є критичним для сталого розвитку інформаційного суспільства.

Фішинг виконує подвійну роль у сучасному інформаційному середовищі: з одного боку, він виступає безпосередньою загрозою для конфіденційності та безпеки даних, а з іншого — впливає на стратегічні аспекти формування політики кіберзахисту, визначаючи пріоритети національної та міжнародної безпеки в цифровій сфері.

В умовах цифрової трансформації державного управління, бізнесу та освіти проблема фішингу набуває не лише технічного, а й соціального виміру. Користувачі часто стають найвразливішою ланкою в системі кіберзахисту, адже навіть найсучасніші технологічні засоби безпеки не можуть гарантувати повного захисту без належного рівня цифрової грамотності. Саме тому важливим аспектом протидії фішингу є розвиток культури інформаційної безпеки, підвищення обізнаності громадян та навчання розпізнаванню ознак фішингових атак.

На державному рівні боротьба з фішингом вимагає комплексного підходу — від удосконалення законодавчої бази до впровадження національних програм кіберосвіти. Європейське агентство з мережевої та інформаційної безпеки (ENISA) у своїх рекомендаціях 2024 року наголошує, що ефективна протидія фішинговим кампаніям можлива лише за умови співпраці між урядовими структурами, приватним сектором і користувачами. Це дозволяє не лише мінімізувати наслідки атак, але й підвищити загальну стійкість інформаційного простору до нових кіберзагроз.

Таким чином, роль фішингу у формуванні кіберзагроз є комплексною — він одночасно виступає каталізатором нових типів атак і індикатором вразливості цифрового суспільства. Розуміння цих процесів створює передумови для розробки більш ефективних стратегій кіберзахисту, що поєднують технологічні, організаційні та освітні заходи.

1.2 Сутність фішингу та його роль у формуванні кіберзагроз

Фішинг — це різновид кібершахрайства, суть якого полягає у незаконному отриманні персональних або фінансових даних користувачів шляхом обману. Сам термін походить від англійського слова ***phishing***, що утворене від *fishing* — «риболовля». Аналогія доволі показова: зловмисник, подібно до рибалки, «закидає вудку» у вигляді оманливого повідомлення чи посилання, сподіваючись, що користувач «клоне» на наживку.



Рис 1.1 – Фішинг

На практиці це відбувається так: шахрай створює фальшиву вебсторінку, яка майже повністю копіює дизайн легітимного сайту банку, державної установи або популярного онлайн-сервісу. Потім потенційній жертві надсилається повідомлення із закликом виконати певну дію — наприклад, підтвердити акаунт, оновити пароль чи перевірити платіж. Для цього користувача спонукають перейти за посиланням, де він сам вводить власні конфіденційні дані, фактично передаючи їх кіберзлочинцю.

Фішингові кампанії сьогодні є не просто інструментом викрадення паролів — вони стають стартовою фазою складних багаторівневих атак (наприклад, ransomware, BEC або шкідливого програмного забезпечення). За даними Verizon

Data Breach Investigations Report 2024 [\[7\]](#) , у понад 80% кіберінцидентів фішинг є початковим вектором проникнення.

Одна з ключових причин стійкості фішингу — його висока ефективність: зловмисники експлуатують усталені психологічні схильності людей. Найчастіше використовуються такі поведінкові тригери:

- авторитетний вплив — повідомлення, що нібито надходять від банків, роботодавців чи державних установ, викликають автоматичну довіру та швидку реакцію;
- ефект терміновості — маніпуляції через нібито критичні ситуації (компрометація акаунта, затримка доставки, обмеженість пропозиції) стимулюють імпульсивні дії;
- спонукання до взаємодопомоги — сценарії, де повідомлення видаються від імені колег або знайомих, розраховують на готовність допомогти;
- цікавість і допитливість — привабливі заголовки та несподівані вкладення («рахунок», «звіт», «оголошення») часто провокують користувачів відкрити матеріали без належної перевірки.

Крім цього, сучасні технології значно полегшують реалізацію фішингових схем: поширення мобільних пристроїв із невеликими екранами та швидкою поведінкою користувачів зменшує увагу до деталей і збільшує ймовірність помилок. Сучасні кампанії також почали застосовувати інструменти автоматизації та штучного інтелекту для генерації персоналізованих, багатомовних і технічно переконливих повідомлень, що ще більше підвищує їхню ефективність.

Сутність фішингу полягає у використанні соціальної інженерії — впливу на психологію жертви для того, щоб вона добровільно надала доступ до своїх персональних або фінансових даних. Зазвичай такі атаки реалізуються через підроблені електронні листи, вебсторінки, SMS чи повідомлення у соціальних мережах.

Через те, що фішинг базується насамперед на методах соціальної інженерії, важливо розуміти механізми, якими зловмисники експлуатують особливості людської психології. Наприклад, вони апелюють до довіри, користуються

почуттям терміновості або співчуття, щоб змусити людину вчинити неочікувані дії — розкрити секретну інформацію або виконати кроки, що відкривають доступ до системи. Тому ефективний захист від фішингу починається з усвідомлення того, які саме психологічні прийоми застосовуються під час атаки.

Нижче наведені типові сценарії інтернет-фішингу, викладені у вигляді прикладів:

- Підроблені електронні листи з вимогою підтвердити облікові дані. Жертві надходить повідомлення, яке імітує лист від банку або сервісу, з проханням ввести логін і пароль на сторінці, що зовні схожа на офіційну.
- Шахрайські інтернет-аукціони та фальшиві оголошення. Зловмисники розміщують оголошення про продаж товарів або створюють “аукціонні” сторінки, але оплата направляється на підконтрольний їм сайт або реквізити.
- Підставні благодійні кампанії. Шахрайські організації просять пожертви під приводом надзвичайних ситуацій або благодійних ініціатив — це особливо дієво у періоди криз.
- Фальшиві інтернет-магазини або вигідні пропозиції. Створюються копії магазинів або лендінги з надто привабливими знижками; при оформленні замовлення користувач вводить дані платіжної карти, які потрапляють до злочинців.
- Клон-повідомлення (clone phishing). Копіюється раніше надіслане легітимне повідомлення, але посилання або вкладення замінюються на шкідливі.
- Таргетовані атаки (spear phishing). Повідомлення підготовлені з урахуванням конкретної інформації про особу або організацію, що значно підвищує їхню правдоподібність.
- Використання рекламних мереж і шкідливих файлів. Атаки можуть поширюватися через шкідливі банери, підроблені додатки або заражені вкладення.

Технічні прийоми, якими підсилюють ці схеми, також еволюціонують: шахраї застосовують підроблені сертифікати HTTPS, маніпулюють URL-адресами (homograph-атаки, typosquatting), використовують редиректи та тимчасові домени, щоби зробити підробки більш правдоподібними. Ускладненням є й те, що нині фішингові кампанії комбінують кілька каналів (електронна пошта → SMS → соціальні мережі), що ускладнює їх виявлення.

Розуміння типових сценаріїв і технік — ключовий елемент протидії: воно дозволяє не лише впроваджувати технічні бар'єри, а й формувати поведінкові політики (навчання користувачів, моделювання атак, протоколи реагування), які значно знижують успішність шахрайських кампаній.

Оскільки фішинг значною мірою спирається на прийоми соціальної інженерії, захист від таких атак вимагає розуміння того, які психологічні механізми використовують зловмисники — як вони апелюють до довіри, страху чи відчуття терміновості, щоб змусити людину вчинити небажані або імпульсивні дії.

Соціальна інженерія — це методика впливу на людей, яка використовується окремими зловмисниками або організованими групами для маніпулювання поведінкою жертв з метою отримання конфіденційної інформації або змусити їх виконати дії, що підривають безпеку. На відміну від технічних атак, соціальна інженерія орієнтується передусім на психологічні чинники — довіру, страх, поспіх чи цікавість — а не на експлуатацію вразливостей програмного забезпечення.

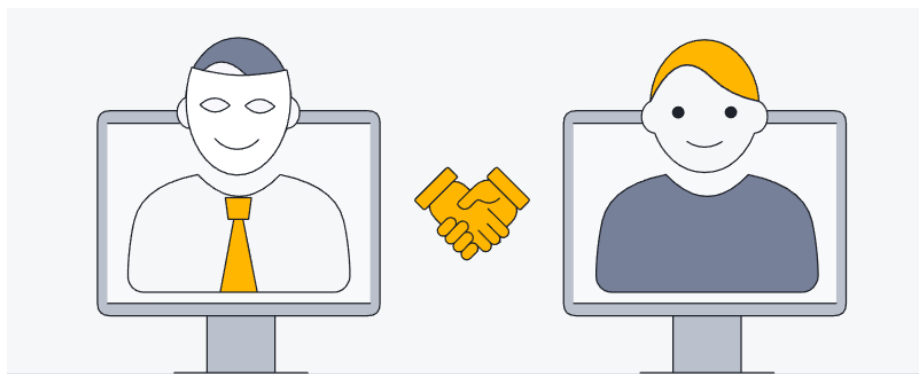


Рис 1.2 – Соціальна інженерія

Успішна соціально-інженерна атака зазвичай починається з ретельного збору відкритої інформації про потенційну жертву або групу жертв. Зловмисники використовують публічні джерела — насамперед профілі в соціальних мережах, списки підписок, публікації та контакти — щоб зібрати електронні адреси, дані про вподобання, довірені бренди і імена знайомих чи колег. На підставі цієї розвідки формується персоналізована «наживка»: повідомлення, яке здається автентичним і має високу правдоподібність у очах отримувача.

На етапі контакту нападники навмисне апелюють до емоційних тригерів — цікавості, страху чи відчуття терміновості — щоб послабити критичне мислення та підвищити ймовірність бажаної реакції. Підсилюючи емоційний фон підручними засобами (офіційна стилістика, логотипи, часова обмеженість пропозиції), вони роблять повідомлення більш переконливим і змушують людину діяти імпульсивно — перейти за посиланням, відкрити вкладення або ввести конфіденційні дані.

Класичний приклад такого підходу — розсилка псевдо-лотерейних сповіщень до користувачів, які беруть участь в онлайн-іграх: повідомлення імітує офіційне звернення (підроблений логотип, відповідна стилістика) і закликає «терміново підтвердити» дані для отримання виграшу. Насправді мета кампанії — не вручити приз, а заволодіти особистою інформацією, яку можна використати для несанкціонованого доступу або продати на чорному ринку.

Ефективність фішингових атак багато в чому визначається не технічними хитрощами, а вмінням маніпулювати людською психологією: збір OSINT, ретельна персоналізація повідомлення і цілеспрямоване підбурювання емоцій — ось основні складові успіху зловмисника. Саме тому захист від таких схем повинен поєднувати технічні контрзаходи з підвищенням пильності та навчанням користувачів.

Під час таких атак нападник часто видає себе за довірену особу або офіційну інстанцію, щоб викликати довіру та змусити жертву добровільно надати потрібні відомості. У своїй практиці зловмисники застосовують різні прийоми —

імітацію реальних листів або дзвінків, переконливі легенди, соціальний тиск або емоційні тригери — щоб отримати цінну інформацію, наприклад:

- паролі та облікові дані;
- банківські реквізити та фінансову інформацію;
- дані доступу до корпоративних систем і мереж.

Атаки соціальної інженерії можуть мати різні форми й ступінь складності, але їхня спільна риса — експлуатація людських слабких місць. Стратегія полягає не в складних алгоритмах чи експлойтах, а в тому, щоб змусити людину зробити те, що вигідно злочинцю: відкрити доступ, переслати документи або виконати фінансовий платіж. Саме тому боротьба з цим видом загроз потребує не лише технічних засобів захисту, а й підвищення цифрової грамотності та критичного мислення користувачів.

Phishing



Spear phishing



Baiting



Рис 1.3 – Приклади соціальної інженерії

Зловмисники розсилають підроблені електронні листи, повідомлення чи посилання на сайти, що зовнішньо нагадують офіційні ресурси. Мета — обдурити отримувача, щоб він перейшов за посиланням і видав конфіденційну інформацію (наприклад, паролі, дані банківських карток або інші персональні відомості).

- (clone phishing). Це варіант фішингу, коли шахраї створюють майже ідентичну копію раніше легітимного повідомлення — замінюючи в ньому справжні посилання на шкідливі. На відміну від масових розсилок, клон-фішинг може бути досить переконливим, бо повторює структуру і оформлення оригіналу.
- (spearphishing). Схожий на звичайний фішинг, але значно більш прицільний: повідомлення підлаштовують під конкретну людину або організацію, використовуючи персональні дані жертви для підвищення правдоподібності та шансу на успіх.

- (baiting). Шахраї пропонують привабливу «наживку» — наприклад, безкоштовну програму, медіафайл або вигідну пропозицію — в обмін на особисті дані або доступ до системи. Така «підмога» може містити заражені файли або вести на шкідливі сайти, що компрометують пристрій жертви.

Методи соціальної інженерії різноманітні, проте серед найпоширеніших виділяють такі прийоми: імітація авторитетних осіб, створення відчуття терміновості, апеляція до співчуття та активне використання соціальних мереж для збору персональних даних. Уся ця сукупність тактик спрямована на психологічний тиск на людину з метою змусити її зробити помилковий крок — розкрити конфіденційну інформацію або виконати дію, що загрожує безпеці.

Також однією з базових тактик є видавання себе за іншу особу: зловмисник може видаватися колегою, співробітником служби підтримки або представником знайомої організації, щоб заслужити довіру жертви й отримати доступ до потрібних відомостей. Використовуючи природну схильність довіряти знайомим голосам чи обличчям, нападник значно підвищує ймовірність того, що людина добровільно повідомить паролі, коди доступу чи іншу чутливу інформацію.

У мережі функціонує безліч шахрайських схем фішингу, у яких соціальна інженерія поєднується з технічними засобами для крадіжки приватної інформації користувачів. Зібрані персональні дані зловмисники застосовують по-різному: розсилають спам та цільові повідомлення через електронну пошту або соціальні мережі, перепродають відомості на чорних ринках або використовують їх для несанкціонованого доступу до акаунтів.

Часто ініціатором збору даних є підроблені ресурси, що зовні імітують знайомі сайти: копіюється дизайн, структура сторінки та навіть адресний рядок, тож на перший погляд така сторінка може видатися офіційною. Жертви приваблюються привабливими пропозиціями — знижками, акціями або «обмеженими» розпродажами — і за інерцією вводять платіжні реквізити або інші конфіденційні відомості. У підсумку покупець втрачає гроші й не отримує товар,

а його дані потрапляють до рук шахраїв, що масштабує наслідки фішингової атаки.

Отже, було розглянуто ключові теоретичні положення щодо фішингу та соціальної інженерії й окреслено типові стадії проведення соціально-інженерних атак. Виявлено, що найпоширеніші інтернет-схеми фішингу включають: масові розсилки шахрайських листів (спам) із підробленими запитами, організацію фіктивних інтернет-аукціонів, створення фальшивих благодійних ініціатив, роботу підробних інтернет-магазинів, використання спливаючих вікон, а також розміщення шкідливих посилань у листах або коментарях на вебсторінках.

1.3 Соціально-інженерні техніки: характеристика та оцінка

Фішингові атаки можуть реалізовуватися через різні канали — електронні листи, SMS-повідомлення, телефонні дзвінки або шляхом підміни вебадрес і перенаправлень на підроблені ресурси. Кожна кампанія включає декілька етапів і технік, спрямованих на те, щоб дістатися до цільового користувача та змусити його виконати небажану дію.

Найпоширеніші типи фішингу:

- Spear-phishing — цілеспрямовані, персоналізовані атаки на конкретних осіб або групи;
- Vishing (voice-phishing) — шахрайські телефонні дзвінки, що імітують представників банків, служб чи колег;
- Pharming — перенаправлення користувачів на підроблені сайти через маніпуляції з DNS або хости;
- Whaling — таргетовані атаки на керівний склад або ключових співробітників організації;
- Clone phishing — відтворення раніше легітимного листа з підміною посилань або вкладень на шкідливі;
- Smishing (SMS-phishing) — фішинг через текстові повідомлення.

Щодня принаймні одна людина стикається з якоюсь формою фішингу, часто навіть не підозрюючи про ризик стати жертвою.

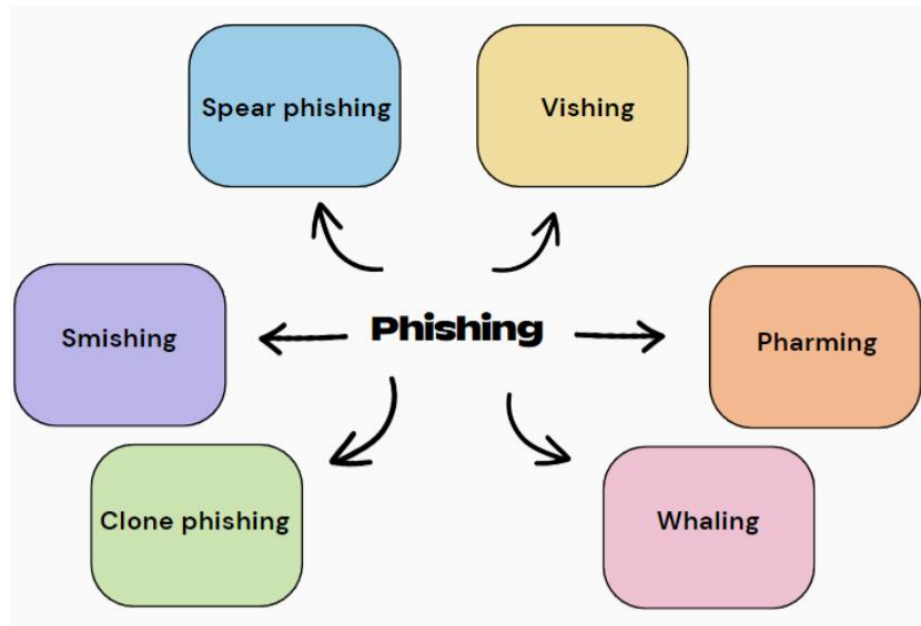


Рис 1.4 – Соціально-інженерні техніки фішингу

Vishing — це різновид фішингу, що реалізується через голосовий зв'язок: шахраї телефонують жертвам і за допомогою обману змушують їх розкрити конфіденційну інформацію. Такі атаки ґрунтуються на попередньому зборі даних про ціль — відомості про оточення, поведінку та особисті звички використовуються для підвищення правдоподібності вимог шахрая. Часто зловмисники ретельно видають себе за знайомих осіб або офіційних представників, що дозволяє їм викликати довіру й отримувати потрібні відомості.

Для масового проведення вішингу зловмисники застосовують технології VoIP, які дають змогу здійснювати велику кількість дзвінків одночасно та координовано. Мета таких операцій — здебільшого отримання платіжних реквізитів, даних облікових записів та інших чутливих відомостей. Сьогодні шахраї вміло збирають демографічні та ідентифікаційні дані (ім'я, вік, стать тощо), щоб сформувати реалістичні профілі жертв і підвищити шанси успіху атаки.

Аналітичні звіти вказують на помітне зростання вішингу: відповідні дослідження фіксують п'ятикратне збільшення кількості таких інцидентів у період від початку 2021 року до першого кварталу 2022 року, що свідчить про підвищену ефективність цього вектора атак (за даними Agari та PhishLabs).

На відміну від класичного фішингу, де жертва здебільшого пасивно переходить за підробленим посиланням, у вішингу від неї вимагається активна участь — усне підтвердження даних або їх озвучення. Через це атака потребує більш індивідуального підходу: шахрай особисто зв'язується з обраною особою, іноді застосовуючи заздалегідь зібрану інформацію, тож для успішного проведення таких операцій не обов'язково володіти складними технічними навичками.

Окремий підвид — **spear-vishing** — передбачає таргетований підхід: нападник готує дзвінок, маючи достовірні відомості про конкретну людину (наприклад, ім'я, адресу чи фрагменти паролів), і на їх основі веде розмову з метою отримати доступ до фінансових чи других конфіденційних ресурсів. Саме через високий ступінь персоналізації такі атаки можуть бути особливо руйнівними для жертв та організацій.

У своїй базовій формі атака типу вішинг спрямована на те, щоб створити у жертви відчуття довіри через телефонний дзвінок, під час якого шахрай використовує заздалегідь зібрану з відкритих джерел інформацію про людину чи організацію. Це можуть бути знайдені онлайн імена співробітників, номери телефонів, робочі електронні адреси та інші дрібні деталі, що роблять історію правдоподібною. Наприклад: «Я щойно говорив із Карен Сміт із бухгалтерського відділу, і вона повідомила...».

Хоча цей метод заснований на старих прийомах психологічного впливу, він продовжує успішно працювати, і багато людей знову й знову стають жертвами таких маніпуляцій.

Можна подумати: «Мене так не обдурять». Але на практиці сучасні атаки вішингу можуть бути дуже ретельно спланованими, технічно складними та вражаюче переконливими.

Злочинці, які застосовують вішинг, часто маскуються під довірені джерела — банки, кредитні установи, державні органи або відомі компанії — шляхом підміни ідентифікатора абонента (caller ID spoofing) або ретельної підготовки образу «представника». Така імпровізація підвищує правдоподібність дзвінка й

штовхає адресата до імпульсивної реакції: надати персональні дані, підтвердити платіж або виконати іншу дію, яка відкриває доступ до ресурсів.

Схеми вішингу часто комбінують кілька каналів — наприклад, спочатку надходить електронний лист із проханням зателефонувати на вказаний номер, після чого відбувається голосовий контакт. У розмові зловмисники використовують прийоми соціальної інженерії: встановлюють довірливий тон, посиляються на «терміновість», вигадують формальні підстави й апелюють до емоцій, аби добитися від жертви розкриття конфіденційної інформації. Стратегія може включати імовірні сценарії — повідомлення про «виграш», «перевірку рахунку», «підозрілу транзакцію» тощо.

Часті цілі вішингу — люди похилого віку, нові працівники та співробітники, що регулярно взаємодіють із зовнішніми абонентами: ці групи більш вразливі через менший досвід у сфері кібербезпеки або через характер їхніх робочих обов'язків. Особливо небезпечні таргетовані форми атаки — *spear-vishing* — коли телефонний контакт будується на попередньо зібраних персональних даних жертви (ім'я, посада, відомості про родину чи фінанси), що значно підвищує ймовірність успіху.

Технічні інструменти, які використовують зловмисники у вішингу, охоплюють: VoIP-сервіси для масової розсилки дзвінків, wardialing для пошуку активних номерів, підробку ідентифікатора абонента (caller ID spoofing), пошук інформації в смітті (dumpster diving) та класичні методи соціальної інженерії. Поєднання цих технік дає змогу атакувати як окремих осіб, так і великі корпоративні цілі.

Захист від вішингу повинен бути багаторівневим. Технічні заходи включають впровадження систем автентифікації дзвінків (наприклад, стандарти для перевірки ідентичності виклику), використання рішень для фільтрації підозрілих дзвінків та посилення безпеки електронної пошти, щоб зменшити кількість «тригерних» повідомлень. Важливим є також встановлення політик щодо обробки конфіденційної інформації по телефону, наприклад заборона

передавати платіжні дані голосом, та технічні обмеження — прив'язка критичних операцій до підтвердження через захищені канали.

Не менш значущими є організаційні заходи: регулярні тренінги з розпізнавання телефонного шахрайства, практичні вправи зі службою підтримки, чіткі процедури ескалації підозрілих викликів і наявність швидкої лінії для повідомлень про потенційні інциденти. Для категорій співробітників, які найбільше піддаються ризику, доцільно розробити додаткові інструкції та контрольні чек-листи.

Також організаціям слід впроваджувати механізми оперативного реагування: ведення журналів дзвінків, аналіз індикаторів компрометації та алгоритми миттєвого припинення підозрілих сесій. Юридичний супровід і співпраця з операторами зв'язку допомагають відстежувати джерела атак, блокувати їх та зменшувати наслідки для постраждалих користувачів.

Отже, ефективний захист від вішингу базується на поєднанні технічних рішень, чітких організаційних процесів і постійного навчання персоналу. Лише така комплексна стратегія дозволяє мінімізувати ризики несанкціонованого розкриття даних, фінансових втрат і шкоди репутації.

Pharming – цей метод ґрунтується на маніпулюванні слабкими місцями DNS-серверів, які відповідають за перетворення доменних назв у відповідні IP-адреси. Зловмисники можуть використовувати різні техніки — наприклад, підміну DNS-кешу — щоб змінити IP-адресу, що асоціюється з певним доменом. У результаті користувач, намагаючись відкрити справжній вебресурс, непомітно для себе опиняється на підробленій сторінці, ретельно сконструйованій нападником і максимально схожій на оригінал.

На підроблених сторінках користувачі часто несвідомо вводять свої логіни, паролі, платіжні дані чи іншу приватну інформацію, будучи впевненими, що перебувають на справжньому вебресурсі. Усі ці відомості одразу перехоплюються зловмисником, після чого можуть бути використані для крадіжки особи, несанкціонованого доступу до фінансів або проведення інших шахрайських дій.

Фармінг вважається особливо небезпечним, оскільки фальшиві сайти здебільшого майже точно копіюють зовнішній вигляд оригіналу. Через це користувачеві складно помітити відмінності в адресному рядку чи у позначках безпечного з'єднання HTTPS. У результаті пересічний користувач часто навіть не підозрює, що потрапив на шкідливу сторінку. Регулярне оновлення програм, уважність до будь-яких незвичних запитів та обережність під час введення конфіденційних даних значно підвищують захист від таких атак.

Фармінгові атаки ґрунтуються на непомітному перенаправленні користувачів із легітимних сайтів на сфальсифіковані ресурси, що досягається шляхом зміни параметрів DNS. У такій ситуації людина може й не здогадуватися, що потрапила на підробку, і власноруч передати зловмисникам свої облікові дані, фінансову інформацію чи інші конфіденційні відомості. Надалі ці дані використовуються для викрадення особистості, доступу до рахунків або різного виду фінансових махінацій.

Одним із механізмів здійснення фармінгу є встановлення на пристрій жертви шкідливого програмного забезпечення. Воно непомітно втручається в процес перенаправлення інтернет-запитів і автоматично перекидає користувача на підроблені сторінки навіть тоді, коли адреса вебсайту введена абсолютно правильно. Яскравим прикладом подібного інциденту став випадок із компанією CheckFree: кіберзлочинці отримали доступ до адміністративного акаунта через майданчик Network Solutions і протягом кількох годин керували перенаправленням офіційного домену на шахрайський сайт. Ця подія поставила під загрозу інформацію більш ніж п'яти мільйонів клієнтів та продемонструвала, наскільки крихкою може бути система захисту онлайн-переказів.

Крім крадіжки даних, фармінг нерідко сприяє подальшому розповсюдженню шкідливих програм. Переходячи на фальшивий сайт, користувач може несвідомо завантажити додаткове ПЗ, здатне змінювати системні налаштування, викрадати файли або заражати комп'ютер через приховані скрипти. Особливо небезпечним є різновид «drive-by pharming»: зловмисники застосовують JavaScript, аплети та інші вебтехнології для атак на

домашні маршрутизатори й ПК. Такі дії можуть спричинити зависання системи, неконтрольовані перенаправлення, захоплення браузера, DoS та DDoS-атаки, а також появу нав'язливих спливаючих елементів.

Варто враховувати, що фармінг суттєво підриває довіру користувачів до Інтернету як до безпечного середовища для здійснення онлайн-транзакцій. Для його успішної реалізації необов'язково заражати пристрій користувача — іноді достатньо скомпрометувати мережеві служби. Яскравим прикладом є отруєння DNS-кешу, коли зловмисники підміняють IP-адреси на DNS-сервері, змушуючи користувачів автоматично переходити на підроблені ресурси. До того ж вразливості в системі цифрових сертифікатів (PKI) можуть дозволити хакерам отримати фальшивий сертифікат, який браузер сприйме як легітимний, що створює можливість повністю замаскувати шкідливий сайт під офіційний.

Фармінгові атаки нерідко поєднуються з фішингом, шкідливим програмним забезпеченням і атаками «людина посередині» (MITM), що значно підсилює їхню результативність. Наприклад, фішингові листи можуть слугувати інструментом для викрадення облікових даних, які згодом застосовують для компрометації DNS-системи — як це сталося під час відомого інциденту з CheckFree.

Щоб продемонструвати, як саме можуть проявлятися фармінгові атаки на практиці, доцільно розглянути кілька реальних інцидентів.

- Масштабна атака на банківський сектор (2007 р.).
У 2007 році було зафіксовано одну з найбільших фармінгових кампаній, унаслідок якої постраждали понад 50 фінансових установ у США, Європі та Азії. Зловмисники використовували комбінацію шкідливого програмного забезпечення та підміни DNS-записів, створюючи точні копії офіційних вебсторінок банків і перенаправляючи на них клієнтів. Це дозволило їм отримувати конфіденційні дані користувачів без їхнього відома.
- Атака в Бразилії із використанням фішингу та фармінгу (2015 р.).
У 2015 році кіберзлочинці розсилали фішингові листи абонентам найбільшої телекомунікаційної компанії Бразилії. У вкладених

посиланнях містилося шкідливе ПЗ, яке після встановлення змінювало DNS-конфігурації домашніх маршрутизаторів жертв. Це призводило до автоматичного перенаправлення користувачів на підроблені ресурси, навіть коли вони вводили правильні адреси.

- Інцидент із волонтерами у Венесуелі (2019 р.). У 2019 році група хакерів атакувала онлайн-платформи волонтерської організації у Венесуелі. Користувачів непомітно скеровували на фальшивий вебсайт, де збиралися їхні особисті дані. Ця атака продемонструвала, наскільки легко кіберзлочинці можуть перехоплювати інформацію, використовуючи методи фармінгу в поєднанні з соціальною інженерією.

Соціальна інженерія також має ключове значення у здійсненні фармінгових атак: зловмисники маніпулюють користувачами, змушуючи їх переходити за шкідливими посиланнями або розкривати конфіденційну інформацію. Усе це створює сприятливі умови для отруєння DNS та перенаправлення користувачів на підроблені ресурси.

Види фармінгових атак.

- Локальний фармінг. У цьому випадку зловмисники націлюються безпосередньо на пристрій користувача. Вони інфікують систему шкідливим програмним забезпеченням, яке змінює файл *hosts* або інші мережеві налаштування, перенаправляючи запити з реальних сайтів на шахрайські копії. Зараження зазвичай відбувається через небезпечні завантаження, вірусні вкладення в електронних листах або експлуатацію вразливостей програм.
- Фармінг через DNS-сервери (DNS poisoning). Цей вид атаки спрямований на сервери DNS. Якщо кіберзлочинцям вдається їх скомпрометувати, то весь вебтрафік, що проходить через такий сервер, автоматично спрямовується на підроблені вебресурси. Оскільки DNS обслуговує багатьох користувачів, наслідки можуть бути масштабними й торкнутися значної кількості людей одночасно.

Отже, Фармінг є однією з найнебезпечніших форм кіберзлочинності, оскільки дозволяє зловмисникам непомітно перенаправляти користувачів на підроблені вебсайти та викрадати їхні конфіденційні дані без будь-яких явних ознак атаки. Маніпуляції з DNS, зараження пристроїв шкідливим ПЗ та поєднання з фішингом і соціальною інженерією роблять такі атаки надзвичайно ефективними й масовими. Для протидії фармінгу важливо підтримувати актуальність програмного забезпечення, перевіряти налаштування мережі, використовувати захищені канали зв'язку та бути уважним під час введення особистих даних. Саме обізнаність і цифрова грамотність є ключем до мінімізації ризиків.

Whaling – фішингової атаки належить до найскладніших, оскільки його ціллю стають керівники високого рівня або ж зловмисники видають себе за таких осіб, щоб ввести в оману інших працівників. Найтиповіші сценарії включають пряму атаку на генерального директора або створення фальшивої комунікації від його імені з метою впливу на ключові підрозділи компанії — фінансових директорів, бухгалтерію, служби безпеки чи осіб, відповідальних за комунікації.

Під час «Whaling» кіберзлочинці застосовують складні прийоми соціальної інженерії, враховуючи, що керівники організацій зазвичай користуються сучасними засобами захисту від фішингових загроз. Виявити таких зловмисників доволі непросто, адже вони ретельно приховують своє цифрове походження та використовують методи, які ускладнюють встановлення їхньої особи та місцезнаходження.

Оскільки керівники високого рівня добре усвідомлюють ризики фішингових атак, зловмисники змушені застосовувати різні тактики, щоб підвищити ефективність своїх «китобійних» кампаній. Наприклад, вони можуть вивчати профіль керівника у LinkedIn, щоб надати своїм повідомленням індивідуалізований та правдоподібний характер. Саме загроза витоку інформації є однією з причин, чому іноді радять обмежувати використання LinkedIn або бути вкрай обережним із даними, які там публікуються.

Хакер, який планує атаку цього типу, може також ознайомлюватися з професійною термінологією певної галузі, аби виглядати максимально переконливо, або маніпулювати емоціями жертви, пропонуючи нібито перспективну ділову пропозицію. Після завершення етапу збору інформації зловмисники переходять до застосування конкретних векторів атаки, характерних для фішингу, спрямованого на керівників.

Мета атаки значно ширша, ніж проста крадіжка інформації. Головним завданням зловмисників є вплив на керівників таким чином, щоб вони самі санкціонували великі фінансові операції або розкривали критично важливі відомості.

Приклад ситуації: Фінансовий директор отримує нібито терміновий лист від генерального директора, який перебуває у відрядженні за кордоном. У повідомленні йдеться про необхідність негайного переказу коштів для завершення «таємної угоди щодо придбання» та окремо підкреслюється вимога зберегти все в строгій конфіденційності.

Лист здається цілком достовірним: у ньому згадується реальна інформація про поїздку керівника та посилання на недавні обговорення ради директорів. Такий рівень деталізації створює переконливу ілюзію справжнього службового запиту. Якщо компанія не має чітких перевірочних процедур, фінансовий директор може виконати переказ, що в підсумку спричинить серйозні фінансові збитки.

Whaling атаки базуються на використанні авторитету та довіри, якими володіють керівники або інші впливові особи в компанії. Зловмисники видають себе за таких осіб, щоб ввести співробітників в оману та змусити їх виконати шкідливі дії. Нижче наведено кілька реальних інцидентів:

- Mattel Inc. У 2015 році фінансовий директор компанії, що виробляє іграшки, отримав електронний лист, який виглядав як офіційне повідомлення від генерального директора. У листі містилось прохання перерахувати 3 мільйони доларів китайському постачальнику. Переказ було виконано, але пізніше керівництво з'ясувало, що це була

добре спланована «китобійна» атака. На щастя, після втручання влади компанії вдалося повернути гроші.

- Ubiquity Networks Inc. Того ж року кіберзлочинці, видавши себе за керівника компанії, обманули фінансовий департамент технологічної фірми. У результаті шахраям вдалося отримати 46,7 мільйона доларів через фіктивних контрагентів. Пізніше компанія повернула лише трохи більше 8 мільйонів.
- Leonі AG. У 2016 році німецький виробник кабельної продукції став жертвою складної схеми соціальної інженерії. Зловмисники, видаючи себе за топменеджерів компанії, переконали співробітників здійснити низку фінансових переказів. Загальні втрати перевищили 43 мільйони доларів.
- Неназвана енергетична компанія (Велика Британія) Британська енергетична компанія постраждала від особливо витонченої атаки, в якій зловмисники використали аудіодоріжку, згенеровану штучним інтелектом. Керівник отримав телефонний дзвінок, що звучав як голос генерального директора материнської компанії з Німеччини, з вимогою термінового переказу коштів. Після виконання переказу нападники зателефонували ще кілька разів, що врешті-решт викликало підозру у керівника і спонукало його звернутися до влади.

Організації повинні активно підвищувати рівень навчання співробітників, впроваджувати надійні системи захисту та забезпечувати швидке повідомлення про інциденти, щоб запобігти успіху кібершахраїв. Це включає постійне підвищення обізнаності персоналу з питань кібербезпеки, регулярний аудит захисних систем і своєчасне реагування на підозрілі дії. Наявність ефективних інструментів і процедур для виявлення та блокування атак дозволяє компаніям зберегти конфіденційність даних, фінансову стабільність і репутацію.

Smishing - це форма соціальної інженерії, коли атакувальники надсилають жертвам шахрайські SMS-повідомлення, прагнучи змусити їх надати логін-

пароль, відкрити доступ до систем, розкрити важливу інформацію або завантажити шкідливе програмне забезпечення. Хоч smishing і визначається саме як атака через текстові повідомлення, її механіка може змінюватися залежно від конкретної ситуації.

Для звичайних користувачів така атака часто виглядає як SMS нібито від банку чи представників певної організації, у яких зловмисники намагаються змусити людину перейти за фішинговим посиланням або передати конфіденційні дані.

У компаніях smishing може здійснюватися складніше й мати більш серйозні наслідки. Наприклад, у випадку з Twilio хакери використали довірений канал — месенджер Signal — і представилися співробітниками внутрішнього IT-відділу. Створивши ілюзію довіри, вони змогли отримати доступ до службових облікових записів і переконати працівників відкривати шкідливі посилання чи розголошувати внутрішню інформацію.

Smishing відрізняється від класичного фішингу лише каналом доставки — замість електронних листів використовуються SMS-повідомлення. Попри це, більшість типових прийомів і маніпуляцій, властивих фішинговим атакам, зберігаються, тому smishing часто розглядають як одну з підкатегорій фішингу. Обидва типи атак ґрунтуються на принципах соціальної інженерії та мають спільну мету — схилити користувача до передачі доступу або конфіденційних даних. Водночас смішинг не слід плутати з вішингом: у випадку вішингу зловмисники застосовують телефонні дзвінки. Саме таким способом було здійснено атаку з використанням програм-вимагачів на MGM Resorts улітку 2023 року.

Зловмисники часто поєднують смішинг із різними прийомами соціальної інженерії, щоб підвищити успішність атаки. Наприклад, вони можуть спершу зателефонувати жертві, представившись офіційною установою чи компанією, та отримати від неї певні персональні дані. Зібрану інформацію потім використовують у подальшому SMS-повідомленні, роблячи його вигляд максимально правдоподібним.

Щоб повідомлення виглядало ще більш реалістично, атакувальники часто використовують загальнодоступні відомості — ім'я, адресу чи інші деталі про людину. Завдяки цьому текст виглядає індивідуалізованим, а отже, викликає менше сумнівів і збільшує ймовірність того, що жертва виконає вказівки.

У більшості випадків у таких SMS міститься посилання, яке веде на фальшивий сайт або спричиняє встановлення шкідливого програмного забезпечення. Після переходу за посиланням пристрій користувача може бути заражений: шкідливе ПЗ збирає особисті дані або непомітно передає їх на сервер, що контролюється зловмисником.

Кіберзлочинці застосовують різні тактики, щоб їхні smishing повідомлення виглядали переконливо та спонукали отримувача діяти негайно. Основні психологічні механізми, на яких ґрунтуються такі атаки, — це створення довіри, відчуття терміновості та інтересу. Завдяки цьому зловмисники змушують людину розкрити конфіденційну інформацію або виконати небезпечні дії, зокрема перейти за шкідливими посиланнями.

До найбільш поширених прийомів smishing належать:

- Підроблення особи. Нападники часто видають себе за представників банків, популярних сервісів чи державних установ. Повідомлення оформлюються так, щоб максимально повторювати стиль легітимних організацій: включають логотипи, характерні фрази та правдоподібні контакти. Це створює враження справжності та спонукає людину виконувати вказівки.
- Виклик страху або терміновості. Шахраї можуть повідомляти про вигадані проблеми: підозрілі дії в акаунті, ризик блокування або інші критичні ситуації, які «потрібно негайно усунути». Таке психологічне тиснення змушує користувачів поспішати й діяти необдуманно.
- Спокусливі пропозиції. Часто надсилаються повідомлення про виграш, знижки, подарункові карти чи «ексклюзивні» можливості. У смс зазначається, що пропозиція діє обмежений час, що підштовхує людину перейти за посиланням або надати особисті дані, щоб «не втратити шанс».

- Фальшиві повідомлення про доставку. Особливо актуальні в періоди підвищеної кількості замовлень. Людині можуть надіслати SMS про нібито затримку або прибуття посилки та запропонувати перейти за посиланням для уточнення інформації. Оскільки багато користувачів дійсно чекають доставку, такі повідомлення здаються правдивими й часто вводять в оману.

У зв'язку з постійним поширенням смартфонів прогнозується збільшення як частоти, так і складності смішинг-атак. Тому важливо регулярно оновлювати свої знання про ці загрози, щоб вчасно розпізнавати ризики. Крім того, корисно отримувати від мобільних операторів періодичні сповіщення щодо випадків SMS-фішингу, адже це допомагає запобігати можливим інцидентам у майбутньому.

Clone phishing – це метод шахрайства, при якому кіберзлочинець видає себе за відомий бренд або організацію та надсилає електронні листи чи повідомлення від імені цього бренду. Основна мета таких атак — обманом змусити жертву перейти за шкідливим посиланням, що може призвести до зараження пристрою шкідливим програмним забезпеченням, викрадення облікових даних або інших конфіденційних відомостей. На відміну від традиційного фішингу, фішинг-клон більш персоналізований: злочинці детально вивчають своїх жертв і створюють максимально правдоподібні листи чи підроблені вебсайти, що значно підвищує ймовірність успішної атаки.

Ці атаки становлять серйозну загрозу як для окремих користувачів, так і для організацій, оскільки можуть призводити до фінансових втрат, компрометації корпоративних даних, втрати довіри та репутаційної шкоди. Для ефективного захисту від фішинг-клонів важливо поєднувати технічні заходи безпеки (антивірусне програмне забезпечення, фільтри спаму, багаторівнева аутентифікація) з навчанням користувачів розпізнавати підозрілі повідомлення та контролем мережевої активності.

Крім фішинг-клонів, сучасні кіберзлочинці активно застосовують різні методи соціальної інженерії — Spearphishing, Vishing, Pharming, Whaling і Smishing. Всі ці методи дозволяють отримувати особисту інформацію, здійснювати фінансові махінації, впливати на поведінку користувачів і завдавати

шкоди організаціям. Розуміння принципів їхньої роботи та впровадження комплексних превентивних заходів є ключовим для забезпечення безпеки, захисту приватних даних і фінансових ресурсів у цифровому середовищі.

1.4 Правове регулювання боротьби з кіберзлочинністю, що базується на методах соціальної інженерії

У правовій системі України кібербезпека визначається як сукупність заходів і стан захищеності, що гарантують безпечне функціонування людини, суспільства та держави в умовах активного використання інформаційних технологій. Її основна мета — забезпечити безперервний розвиток цифрового середовища, захист комунікаційних систем та своєчасне реагування на будь-які загрози, що можуть поставити під сумнів національну безпеку в кіберпросторі.

Перша група кіберзлочинів охоплює діяння, спрямовані на порушення конфіденційності, цілісності та доступності комп'ютерної інформації й ІТ-інфраструктури. До них відносять незаконне проникнення в комп'ютерні системи, навмисне втручання в роботу програм або даних, їх спотворення, блокування, пошкодження чи приховування. Також до цієї категорії належить розробка та поширення шкідливих програм і технічних засобів, що можуть бути використані для здійснення таких правопорушень.

Другу групу складають злочини, у яких комп'ютерні технології застосовуються як інструмент для завдання матеріальної шкоди або отримання неправомірної вигоди. Це може бути маніпулювання даними з корисливою метою, видалення чи фальсифікація інформації, а також вплив на роботу комп'ютерних систем з метою обману, шахрайства чи посягання на майнові права фізичних або юридичних осіб.

Попри значну кількість відкритих кримінальних проваджень, Департамент кіберполіції не оприлюднює деталізованих відомостей про результати проведених розслідувань. У звітності [\[29\]](#) згадується лише про встановлення приблизно 800 осіб, причетних до кіберзлочинів, однак немає жодної інформації щодо кількості повідомлень про підозру, обвинувальних актів чи винесених вироків. Таким

чином, залишається невідомим, скільки з цих осіб фактично притягнуто до кримінальної відповідальності та на якому етапі перебувають відповідні провадження.

Розслідування кіберзлочинів в Україні здійснюється переважно за такими статтями Кримінального кодексу України [\[29\]](#):

- ст.176 — порушення авторських і суміжних прав;
- ст.190 — шахрайство;
- ст.361 — несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, мереж чи засобів електрозв'язку;
- ст.361-1 — створення, розповсюдження або збут шкідливих програмних чи технічних засобів;
- ст.361-2 — незаконне розповсюдження або продаж інформації з обмеженим доступом, що зберігається в комп'ютерних системах або мережах;
- ст.362 — викрадення, привласнення чи вимагання комп'ютерної інформації, у тому числі шляхом шахрайства або зловживання службовим становищем;
- ст.363 — порушення правил експлуатації автоматизованих систем;
- ст.363-1 — створення перешкод у роботі комп'ютерних систем або мереж шляхом масового розповсюдження електронних повідомлень.

Єдиний державний реєстр судових рішень містить значний масив інформації щодо вироків та інших судових актів у справах про кіберзлочини. У реєстрі також можна знайти ухвали слідчих суддів у кримінальних провадженнях, що перебувають на різних стадіях розгляду, що дає змогу простежувати динаміку та особливості судової практики у сфері протидії кіберзлочинності. Дані цього реєстру демонструють, що в Україні ведеться планомірна та систематична робота з протидії кіберзлочинності.

Важливим результатом діяльності Ради Європи стала Конвенція про кіберзлочинність, прийнята 23 листопада 2001 року в Будапешті. Цей документ має значну історичну вагу й посідає провідне місце серед нормативно-правових

актів, що регулюють правові відносини у сфері глобальних комп'ютерних мереж, залишаючись унікальним міжнародним актом такого масштабу [30]. Конвенція є всебічним документом, який містить норми, що впливають на різні правові сфери — кримінальне, кримінально-процесуальне, авторське, цивільне та інформаційне право. Вона побудована на основних принципах міжнародного права, таких як повага до прав людини, співробітництво між державами та сумлінне виконання міжнародних зобов'язань.

Прийняття Конвенції [32] стало значущим кроком на шляху до створення міжнародних правових механізмів боротьби з кіберзлочинністю та забезпечення кібербезпеки, оскільки вона сприяє налагодженню співпраці між країнами й гарантує захист прав громадян у цифровому середовищі. У своїй основі документ визначає три ключові напрями дій: уніфікацію національних норм, що встановлюють відповідальність за кіберзлочини; дослідження й удосконалення процедур їх розслідування в міжнародних комп'ютерних мережах; а також створення швидкої та ефективної системи міжнародного співробітництва в боротьбі з кіберзлочинністю.

Положення Конвенції [32] спрямовані на врегулювання трьох основних напрямів:

- Уніфікація підходів до кримінально-правової кваліфікації правопорушень, пов'язаних із використанням комп'ютерної інформації, що дає можливість створити узгоджену міжнародну систему оцінювання таких злочинів.
- Стандартизація кримінально-процесуальних механізмів у різних країнах для забезпечення результативного збирання доказової інформації під час розслідування кіберзлочинних діянь.
- Посилення міжнародної взаємодії в рамках кримінального провадження, що дозволяє отримувати докази щодо злочинів, учинених поза межами держави.

Україна також приєдналася до Конвенції про кіберзлочинність, ратифікувавши її відповідним законом. У документі зазначено, що держава приймає її положення із певними застереженнями та спеціальними заявами. Зокрема, Україна залишає за собою право не впроваджувати положення статті 6,

пункту 1 Конвенції, які передбачають кримінальну відповідальність за створення, придбання або передачу іншим особам спеціальних пристроїв чи програмного забезпечення, призначених для вчинення комп'ютерних злочинів.

Крім того, держава не бере на себе зобов'язання повністю застосовувати статтю 9 щодо криміналізації умисного незаконного отримання дитячої порнографії через комп'ютерні системи або зберігання відповідних матеріалів на цифрових носіях чи в інформаційних системах.

Закон «Про основні засади забезпечення кібербезпеки України» визначає ключові правові та організаційні механізми, спрямовані на захист життєво важливих інтересів громадян, суспільства та держави у кіберпросторі. Документ окреслює головні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також регламентує розподіл повноважень між державними органами, підприємствами, установами, організаціями та громадянами. Крім того, він встановлює принципи координації їхньої діяльності задля забезпечення ефективного функціонування системи кібербезпеки.

Стаття 3. Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки становлять Конституція України, закони, що визначають основи національної безпеки, а також стратегічні документи внутрішньої та зовнішньої політики у сфері електронних інформаційних технологій. Важливе значення мають законодавчі акти, що регулюють захист державних інформаційних ресурсів та інформації, встановлюють вимоги щодо безпеки, а також міжнародні документи, зокрема Конвенція про кіберзлочинність та інші міжнародні угоди, обов'язковість яких затверджена Верховною Радою України. До цієї правової бази також належать акти Кабінету Міністрів та інші нормативно-правові документи, прийняті для реалізації законодавчих положень України.
2. У випадку, якщо міжнародним договором України, ратифікованим Верховною Радою, передбачено норми, що відрізняються від положень цього Закону, застосовуються положення міжнародного договору.

Закони про захист персональних даних [\[34\]](#) відіграють важливу роль у забезпеченні конфіденційності та приватності громадян у цифровому середовищі. Вони визначають права та обов'язки щодо обробки особистої інформації, регулюють діяльність організацій і компаній у цьому напрямі. Законодавство відповідає міжнародним стандартам, враховує динамічний розвиток технологій та змінні потреби суспільства щодо захисту персональних даних, особливо в онлайн-середовищі.

Стаття 1. Обсяг дії Закону

Цей Закон регулює правовідносини, що виникають у процесі захисту персональних даних під час їх обробки. Водночас його положення не поширюються на діяльність, пов'язану зі створенням та обробкою баз персональних даних у наступних випадках:

- фізичною особою – виключно для особистих, сімейних чи побутових цілей;
- журналістом – у межах виконання професійних обов'язків та службових завдань;
- творчим працівником – у рамках професійної або художньої діяльності.

Стаття 3. Законодавча база у сфері захисту персональних даних

Система правових норм щодо захисту персональних даних включає Конституцію України, цей Закон, інші законодавчі та підзаконні акти, а також міжнародні договори України, обов'язковість яких затверджена Верховною Радою.

Стаття 4. Суб'єкти правовідносин у сфері персональних даних

1. Суб'єктами у цій сфері є:

- власник персональних даних;
- володілець бази персональних даних;
- розпорядник бази персональних даних;
- третя особа;
- уповноважений державний орган із питань захисту персональних даних;
- інші державні та місцеві органи, які здійснюють контроль і забезпечення прав на захист персональних даних.

2. Статус володільця або розпорядника бази персональних даних можуть мати: підприємства, установи та організації будь-якої форми власності; органи державної влади та місцевого самоврядування; фізичні особи-підприємці, які обробляють персональні дані відповідно до чинного законодавства.

Ефективність кібербезпеки значною мірою залежить від того, наскільки чіткими, актуальними та дієвими є закони та нормативні акти в цій сфері. Не менш важливим є підвищення обізнаності громадян щодо методів соціальної інженерії та навчання їх розпізнавати потенційні загрози в Інтернеті. Лише комплексна взаємодія законодавства, технічних заходів та освітніх ініціатив дозволяє ефективно протистояти кіберзлочинам, що експлуатують людський фактор, і забезпечити безпечне функціонування цифрового простору.

В українському правовому полі кібербезпека розглядається як ключовий механізм захисту життєво важливих інтересів людини, громадянина, суспільства та держави у сфері інформаційних технологій. Вона охоплює забезпечення стабільного розвитку інформаційного суспільства та цифрового комунікативного середовища, а також своєчасне виявлення, запобігання та нейтралізацію загроз, що можуть негативно впливати на національну безпеку в кіберпросторі.

Крім того, законодавство України у сфері кібербезпеки регламентує питання надійності та стійкості інформаційної інфраструктури, що забезпечує життєдіяльність критично важливих секторів, таких як енергетика, транспорт, охорона здоров'я та інші ключові галузі.

Не менш важливою складовою є законодавство про захист персональних даних, яке гарантує конфіденційність та приватність громадян у цифровому середовищі. Воно визначає права та обов'язки щодо обробки персональної інформації та регламентує діяльність організацій і компаній у цьому контексті.

Законодавство про персональні дані має відповідати міжнародним стандартам та нормам, враховувати стрімкий розвиток технологій і змінні потреби суспільства у забезпеченні захисту особистої інформації, особливо в онлайн-середовищі.

Висновки до першого розділу

У сучасному цифровому світі дослідження проблеми кіберзлочинності, зокрема фішингу та соціальної інженерії, набуває особливої актуальності. Такі загрози становлять значну небезпеку як для окремих користувачів, так і для організацій та підприємств. Вивчення теоретичних аспектів фішингу та методів соціально-інженерного шахрайства дозволяє глибше зрозуміти їхню природу, принципи дії та ключові особливості.

Отримані результати підкреслюють необхідність комплексного підходу до протидії цим загрозам. Він включає не лише застосування технічних засобів захисту, але й розвиток законодавчих норм, освітніх програм і підвищення обізнаності користувачів. Різноманітність і складність методів соціальної інженерії — Spearphishing, Vishing, Pharming, Whaling та Smishing — свідчить про високий рівень ризику, з яким стикаються користувачі у цифровому середовищі. Ці техніки дають змогу зловмисникам отримувати конфіденційну інформацію, проводити фінансові махінації та здійснювати інші шахрайські дії, що підкреслює важливість уважності та обережності в мережі.

Дослідження також вказує на значущість нормативно-правового регулювання у формуванні ефективних стратегій боротьби з кіберзлочинністю на основі соціальної інженерії. Це передбачає створення дієвих правових механізмів для притягнення до відповідальності осіб, які вчиняють такі злочини, а також налагодження міжнародної співпраці правоохоронних органів.

Отже, успішна протидія фішингу та соціально-інженерному шахрайству потребує системного підходу та координації дій усіх зацікавлених сторін — державних органів, бізнесу та суспільства.

РОЗДІЛ 2 РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ТА ВПРОВАДЖЕННЯ СПОСОБУ АТАКИ

2.1 Заходи безпеки проти фішингових атак

Питання інформаційної безпеки стосується організацій незалежно від їхнього масштабу чи галузі. Водночас у масовій свідомості кібератаки часто асоціюються з гучними інцидентами, що стають предметом медійної уваги або художніх сюжетів. У реальних умовах більшість загроз розвивається значно менш помітно: серйозні порушення безпеки нерідко починаються з простих фішингових повідомлень, які залишаються без належної уваги.

Багатоцільові кібератаки, як правило, мають поетапний характер і використовують слабкі місця, виявлені на початкових стадіях проникнення. Саме тому фішинг продовжує бути одним із найзручніших і водночас найрезультативніших інструментів для зловмисників, оскільки дозволяє обійти технічні засоби захисту через маніпуляцію людським фактором.

Подальший розвиток технологій штучного інтелекту, здатних генерувати правдоподібні тексти й імітувати стиль реальних відправників, істотно ускладнює розпізнавання фішингових повідомлень. У таких умовах особливого значення набуває уважне ставлення до електронної кореспонденції, особливо якщо вона надходить від невідомих або нетипових джерел. Аналіз змісту листів і перевірка потенційно підозрілих елементів залишаються дієвими заходами зниження ризику успішних атак.



Рис 2.1 – Методики ідентифікації фішингових атак

Однією з найбільш поширених ознак фішингових повідомлень є нетипова або змінена адреса електронної пошти відправника. Зловмисники часто імітують домени відомих організацій, замінюючи окремі символи або додаючи незначні відхилення, які складно помітити з першого погляду. Навіть мінімальна різниця в написанні адреси може свідчити про спробу обману.

Важливим сигналом ризику також є форма звернення в листі. Повідомлення, що містять загальні фрази без персоналізації, можуть вказувати на масову розсилку шахрайського характеру, оскільки офіційні компанії зазвичай використовують іменні звернення та індивідуальний підхід до комунікації.

Варто враховувати, що жодні навчальні заходи, включно з імітаціями фішингових кампаній, не здатні повністю усунути людський фактор. Очікування, що співробітники детально перевірятимуть кожне отримане повідомлення, є малореалістичним і може негативно вплинути на робочі процеси, адже електронна пошта та вебпосилання залишаються невід'ємною частиною повсякденної діяльності.

Проведення фішингових симуляцій також потребує обережного підходу з правової точки зору. Оскільки повністю уникнути помилок неможливо, застосування санкцій до користувачів за взаємодію з тестовими повідомленнями

може створювати конфліктні ситуації. Саме тому перед впровадженням таких заходів доцільно залучати кадрові та юридичні підрозділи для узгодження правил і процедур навчання.

Практика показує, що орієнтація на покарання не сприяє підвищенню рівня безпеки. Люди можуть припускатися помилок з різних причин, зокрема через психологічний тиск або надмірне навантаження, і страх відповідальності не усуває цих чинників.

Крім того, надмірно жорсткий підхід до симуляцій може негативно вплинути на довіру між персоналом і службами інформаційної безпеки. У разі побоювання негативних наслідків співробітники схильні приховувати інциденти замість того, щоб повідомляти про них. Значно ефективнішою є модель, у якій формується відкрита культура кібербезпеки, що заохочує своєчасне інформування про підозрілі повідомлення та сприяє ранньому виявленню загроз.

Антифішинговий захист слід розглядати як сукупність організаційних і технічних заходів, спрямованих на протидію шахрайським атакам у різних середовищах — електронній пошті, мобільних додатках і спеціалізованих сценаріях, таких як спід-фішинг чи атаки на керівництво організацій. Основним завданням таких рішень є запобігання несанкціонованому доступу до облікових даних і фінансової інформації, а також зменшення ризиків фінансових втрат.

Сучасні автоматизовані системи антифішингу забезпечують оперативне виявлення та нейтралізацію загроз, використовуючи алгоритми аналізу поведінки й машинного навчання. Вони здатні адаптуватися до нових методів атак, забезпечуючи постійно актуальний рівень захисту без необхідності ручного втручання.

Фільтрація електронної кореспонденції виступає базовим елементом захисної інфраструктури. Кожне повідомлення проходить автоматичну перевірку на наявність шкідливих вкладень, підозрілих посилань або маніпулятивних текстових шаблонів. Раннє блокування таких листів запобігає їх доставці користувачам і суттєво знижує ймовірність інцидентів безпеки.

Додатковим рівнем захисту є безперервний моніторинг вебадрес, який дозволяє своєчасно виявляти й блокувати доступ до фальшивих або небезпечних ресурсів. Аналітичні механізми таких систем здатні ідентифікувати аномальні домени та оманливі піддомени, а також підтримують обмін індикаторами компрометації між різними організаціями, формуючи колективний захист від нових загроз.

Завдяки використанню моделей машинного навчання, навчених на великих обсягах легітимних і шахрайських даних, сучасні антифішингові рішення постійно вдосконалюють точність виявлення атак. Безперервний аналіз інформації в режимі реального часу дозволяє відокремлювати безпечний трафік від шкідливого та створює більш стійке й надійне цифрове середовище.

Незважаючи на важливу роль автоматизованих систем безпеки та штучного інтелекту, аналітики SOC залишаються ключовими фахівцями для підтримки високого рівня кібербезпеки в організації. Щоб бути готовими до потенційних атак, організації можуть залучати співробітників до навчальних заходів з протидії фішингу, включаючи:

- Моделювання фішингових атак: проведення симуляційних атак дозволяє оцінити рівень обізнаності та реакції персоналу, швидше виявляти слабкі місця та підвищувати здатність співробітників розпізнавати фішингові спроби.
- Індивідуальні навчальні програми: розробка курсів з урахуванням специфіки робочого середовища та використання реальних прикладів із галузі допомагає навчити співробітників ефективним практикам захисту від фішингу та підвищує стійкість до атак.
- Демонстрація реальних випадків: показ конкретних прикладів фішингових атак, таких як шахрайські кампанії на зразок Okatarus, дає можливість співробітникам побачити реальні сценарії та навчитися розпізнавати ознаки шахрайства.
- Обізнаність щодо мобільного фішингу: включення курсів, що висвітлюють загрози для мобільних пристроїв, зокрема SMS-фішинг

(смішинг), допомагає персоналу вчасно ідентифікувати та уникати таких атак.

- Удосконалення механізмів звітності: автоматизовані системи повідомлень про загрози та навчання співробітників ефективним методам обробки інцидентів дозволяють оперативніше реагувати на інциденти та коригувати стратегію для запобігання майбутнім атакам.

Також Існує кілька дієвих методів захисту від фішингових атак. Серед них – перевірка достовірності доменів, виявлення спроб видачі себе за іншу особу та маркування потенційно підозрілого вмісту в електронних листах. На корпоративному рівні відомі компанії, такі як PhishLabs, IronScales та PhishMe, активно розробляють рішення для захисту організацій від фішингу, мінімізуючи ризики стати жертвою шахраїв.

Хоча шкідливе програмне забезпечення часто поширюється через електронну пошту, воно також може скористатися вразливостями мережі, зокрема через застаріле програмне забезпечення. Тому для користувачів і організацій важливо регулярно оновлювати антивірусні та системні програми, щоб підтримувати високий рівень захисту.



Рис 2.2 – Захисти від фішингових атак

Шифрування даних є критично важливим елементом безпекової стратегії. Воно робить конфіденційну інформацію недоступною для кіберзлочинців, значно

ускладнюючи їхні спроби отримати доступ до системи або зменшуючи ймовірність успішної атаки.

Багатофакторна автентифікація (MFA) забезпечує додатковий рівень захисту, вимагаючи проходження кількох етапів перевірки перед отриманням доступу до конфіденційної інформації. Такий підхід значно підвищує безпеку, оскільки один лише пароль більше не є єдиним бар'єром.

Використання технології DMARC допомагає перевіряти справжність електронних листів на основі домену відправника. Система формує звіти та контролює відповідність вхідних листів базі довірених відправників. Якщо лист не відповідає записам у базі, адміністратор безпеки отримує сповіщення, що дозволяє своєчасно реагувати на потенційні фішингові атаки.

Підвищення рівня цифрової грамотності працівників залишається одним із ключових інструментів протидії атакам соціальної інженерії. Навчальні заняття, що включають імітацію фішингових інцидентів, дозволяють персоналу відпрацьовувати практичні навички розпізнавання підозрілих дій і формують здатність швидко реагувати на спроби маніпуляцій. Завдяки таким вправам компанія отримує можливість оцінити вразливі зони та визначити рівень готовності співробітників до реальних загроз.

Важливою складовою системи захисту є багатофакторна аутентифікація (MFA) та інші сучасні засоби управління доступом — IAM, SSO або рольове розмежування прав. Вони значно ускладнюють проникнення сторонніх осіб у внутрішні системи. Рішення класу EDR забезпечують виявлення та блокування шкідливих програм, а удосконалені системи фільтрації електронної пошти мінімізують кількість листів, що можуть становити фішингову загрозу. Окремим елементом захисту є політики правильного використання соціальних мереж, адже вони зменшують ризик використання приватних даних співробітників зловмисниками.

Встановлення чіткої моделі доступу до інформаційних ресурсів дозволяє контролювати переміщення конфіденційних відомостей і уникнути їх несанкціонованого розголошення. Використання спеціальних інструментів для

зберігання паролів сприяє відмові від небезпечних практик, таких як запис чутливих даних у незахищених форматах.

Також важливою є наявність внутрішніх документів, які регламентують порядок дій у ситуаціях, коли сторонні особи чи організації запитують конфіденційну інформацію. Подібні політики повинні містити вимоги до перевірки особи, правила обміну даними та відповідальність за порушення процедур. Ознайомлення персоналу з такими документами забезпечує однакове розуміння правил і мінімізує ризик випадкових витоків.

Для зміцнення кіберзахисту доцільно впроваджувати додаткові заходи:

- Регулярні аудити та аналіз ризиків. Постійний перегляд технічних рішень, політик та процесів дозволяє виявляти нові вразливості й коригувати заходи безпеки з урахуванням змін у середовищі загроз.
- Формування та тестування планів реагування на інциденти. Чіткі процедури дій у разі кібератаки забезпечують швидке усунення наслідків, відновлення роботи систем та подальший розбір інциденту для покращення майбутніх заходів захисту.
- Взаємодія з галузевими спільнотами та іншими організаціями. Обмін інформацією про нові техніки атак та ефективні методи протидії дозволяє оперативно адаптувати власні механізми безпеки.
- Залучення незалежних фахівців. Зовнішні експерти здатні провести глибокі перевірки безпеки, навчити персонал та надати рекомендації щодо усунення недоліків, які можуть бути непомітні для внутрішніх команд.

Попри важливість технічних засобів, ефективна боротьба з соціальною інженерією неможлива без формування усвідомленого ставлення до безпеки всередині організації. Лише коли кожен співробітник розуміє власну роль у захисті даних, компанія може надійно протистояти атакам. В умовах постійного оновлення тактик кіберзлочинців організації повинні залишатися гнучкими та готовими швидко вдосконалювати свої підходи.

Всеохоплюючий підхід до захисту від фішингових атак полягає в інтеграції технологічних засобів із організаційними, процедурними та культурними змінами. Безпека має бути невіддільною частиною щоденної роботи компанії, а відповідальність за неї — колективною.

У корпоративному середовищі систематичне навчання співробітників щодо кіберзагроз, зокрема фішингу, має вирішальне значення. Таке навчання повинно регулярно оновлюватися, щоб враховувати появу нових технік атак. Основними інструментами захисту виступають поінформованість персоналу та здатність критично оцінювати підозрілі повідомлення.

Для індивідуальних користувачів важливим аспектом протидії фішинговим атакам є ознайомленість із сучасними методами шахрайства та підвищена уважність під час взаємодії з невідомими контактами або сумнівними листами.

Дотримання цих підходів дозволяє значно зменшити ризик потрапляння під фішингові атаки та сприяє формуванню більш захищеного цифрового простору.

Отже, фішингові атаки залишаються однією з найпоширеніших і найнебезпечніших загроз у сучасному цифровому просторі. Кіберзлочинці активно застосовують прийоми соціальної інженерії, щоб отримати доступ до конфіденційних даних користувачів та здійснити фінансові чи інформаційні шахрайства.

Для мінімізації ризиків необхідно впроваджувати комплексні заходи кіберзахисту, серед яких особливе значення мають такі:

- Підвищення обізнаності користувачів. Регулярне навчання допомагає людям розпізнавати підозрілі повідомлення, уникати маніпуляцій та формувати навички безпечної поведінки в інтернеті.
- Використання сучасних антивірусних рішень. Надійне програмне забезпечення для захисту від шкідливих програм може завадити запуску небезпечних файлів і виявити ознаки фішингу ще до того, як користувач взаємодіє з ними.
- Перевірка отриманих матеріалів. Будь-які посилання та вкладення з електронних листів слід відкривати лише після впевненості в їхній

безпеки, особливо якщо повідомлення надійшло з невідомих або нетипових адрес.

- Застосування багатофакторної автентифікації. Додаткові етапи підтвердження входу роблять компрометацію облікового запису значно складнішою, навіть якщо пароль потрапив до рук шахраїв.
- Підтримання актуальності програмного забезпечення. Своєчасні оновлення систем та додатків ліквідують вразливості, якими можуть скористатися зловмисники для організації атак.

Найефективніший підхід — це поєднання всіх зазначених методів, адже саме багаторівневий захист забезпечує найвищу стійкість до фішингових загроз.

2.2 Особливості організації та виконання фішингових дій

Різноманіття фішингових методів значною мірою визначається специфікою регіону, у якому працює організація, та особливостями галузі, до якої вона належить. Від цих чинників залежить як спосіб побудови атаки, так і вибір інструментів, що використовують кіберзлочинці. Для них надзвичайно важливо адаптувати підхід під конкретне середовище — саме гнучкість і вміння враховувати локальні нюанси роблять такі атаки більш переконливими та результативними.

У свою чергу, розуміння цих відмінностей дозволяє організаціям формувати більш точні захисні стратегії. Чітке усвідомлення того, як у певному секторі проявляються фішингові техніки, допомагає створювати дієві превентивні заходи та мінімізувати ризики. Це стосується і загальних тенденцій, і специфічних характеристик, наприклад: рівня цифрової зрілості організації, особливостей професійного середовища, регіонального інформаційного фону чи навіть сезонних коливань у діяльності певних компаній.

До важливих аспектів, які визначають ефективність фішингових кампаній у різних напрямках діяльності, належать: використання спеціалізованої термінології, знання структури взаємодії між учасниками галузі, орієнтація на актуальні події, а також врахування професійних звичок працівників. Такі

фактори дають змогу зловмисникам створити максимально правдоподібні повідомлення, які складно відрізнити від легітимних.

Самі сценарії фішингових атак можуть бути різноманітними — від масових електронних листів до точкових атак, спрямованих на конкретних працівників. До найбільш поширених методів належать надсилання сфальсифікованих e-mail, створення підроблених вебресурсів, розповсюдження шкідливих посилань у соціальних мережах, використання месенджерів для швидкої доставки фішингових повідомлень та застосування SMS-фішингу.

Окреме місце займає соціальна інженерія, яка фактично є «психологічним ядром» більшості фішингових схем. Вона базується на маніпулюванні емоціями людини, її довірою, страхами або почуттям терміновості. Завдяки цьому зловмисники отримують доступ до конфіденційних даних навіть без складних технічних інструментів.

Вивчення наслідків кібератак вказує на те, що підприємства у переважній більшості секторів можуть понести суттєві фінансові втрати внаслідок успішної фішингової кампанії. У Таблиці 1.1 представлено узагальнену оцінку потенційного збитку, проте слід пам'ятати, що реальні показники завжди залежать від індивідуальних обставин та рівня захисту конкретної організації.

Таблиця 1.1

Потенційна шкода відфішингових атак для деяких галузей

Сфера діяльності	Потенційна вигода для атакуючого
Фінансовий сектор	Висока. Становлять один із найпривабливіших напрямків для атак, оскільки шахраї можуть отримати доступ до значних коштів, клієнтських рахунків та внутрішніх фінанс.

Медична сфера	Висока. Медичні дані мають високу цінність на чорному ринку, адже їх можна використовувати для різноманітних шахрайських схем, включно з вимаганням, страховим обманом або навіть цілеспрямованою дискредитацією конкретних осіб.
ІТ –індустрія	Висока. Зловмисники, отримавши доступ до внутрішніх технічних матеріалів, можуть впливати на розробку програмного забезпечення, отримувати інформацію про вразливості або викрадати інтелектуальну власність. Це створює загрозу не лише окремим компаніям, а й їхнім клієнтам.
Електронна комерція та роздрібна торгівля	Висока. Є привабливими для фішингових схем через велику кількість фінансових транзакцій. Здобувши облікові записи покупців, зловмисники можуть використовувати їх у власних цілях або продавати викрадені дані на спеціалізованих підпільних майданчиках.
Соціальні мережі та медіа	Висока. Компрометація акаунтів може мати значні наслідки — від поширення фейкової інформації до маніпуляцій громадською думкою й нанесення фінансової шкоди користувачам та брендам.

Криптовалютитаблокчейн	Висока. Виступають одним із найризикованіших напрямків, оскільки доступ до криптовалютних гаманців дозволяє миттєво й безповоротно вивести значні суми, що робить цей сектор надзвичайно привабливим для кіберзлочинців
Логістика транспорт	Середня. Рівень вигоди для атакуючих дещо нижчий, однак важлива інсайдерська інформація про маршрути, відправлення чи внутрішню інфраструктуру може використовуватися у конкурентній боротьбі або схемах крадіжок вантажів.

Дослідження сучасної динаміки фішингових загроз показує, що напрями діяльності зловмисників постійно трансформуються відповідно до змін у цифровому середовищі. Основними цілями таких атак і надалі залишаються банківські та фінансові організації, оскільки вони оперують високою концентрацією чутливих даних і забезпечують прямий доступ до грошових активів. Водночас платформи електронної комерції та поштові сервіси поступово демонструють вищий рівень стійкості до класичних фішингових методів, що свідчить про впровадження більш ефективних механізмів захисту та контролю.

Характер фішингових кампаній суттєво відрізняється залежно від типу цільової аудиторії. У межах організацій такі атаки зазвичай мають складнішу структуру, враховують внутрішні бізнес-процеси та взаємодію між підрозділами. Вони можуть бути спрямовані як на окремих працівників, так і на групи користувачів, що потребує комплексних заходів безпеки. Для індивідуальних користувачів загрози часто мають менш організований характер, проте рівень

ризик залишається значним, особливо за відсутності базових засобів кіберзахисту.

Корпоративне середовище характеризується обробкою великих масивів інформації, зокрема внутрішніх даних компаній, а також відомостей про клієнтів і партнерів. Значна кількість співробітників і тісна взаємопов'язаність робочих процесів підвищують імовірність інцидентів, оскільки помилка одного користувача може мати масштабні наслідки для всієї інфраструктури.

Приватні особи зазвичай мають обмежені можливості для впровадження складних рішень безпеки, що робить їх привабливою ціллю для фішингових атак. Водночас рівень обізнаності відіграє ключову роль: використання антивірусного програмного забезпечення, складних паролів і багатофакторної автентифікації суттєво знижує ризик компрометації облікових записів і втрати персональних даних.

Підготовка фішингових кампаній передбачає ретельне планування, яке включає визначення часових меж, послідовності дій, необхідних інструментів і методів впливу. Зловмисники застосовують підроблені електронні повідомлення, імітовані вебресурси та прийоми соціальної інженерії, поєднуючи технічні засоби зі психологічним тиском для досягнення бажаного результату.

Висока здатність атакувальників адаптуватися до поведінки користувачів і змін у захисних механізмах підкреслює потребу в постійному вдосконаленні підходів до кібербезпеки. Сучасні фішингові загрози стають дедалі складнішими завдяки використанню нових технологій і витончених методів соціальної інженерії.

Таким чином, ефективний захист як організацій, так і окремих користувачів можливий лише за умови поєднання технічних рішень із систематичним навчанням, підвищенням рівня цифрової грамотності та впровадженням актуальних інструментів кіберзахисту. Комплексний підхід дозволяє знизити ризики, забезпечити збереження конфіденційних даних і сформувати більш безпечний інформаційний простір.

2.3 Методологія підбору атак для пентестування (аналіз факторів впливу)

Опанування прийомів і технічних засобів, якими користуються шахраї у фішингових кампаніях, є ключовий елемент побудови надійної системи захисту інформації. Оскільки такі атаки становлять реальну і постійну загрозу для організацій і звичайних користувачів, організаціям слід одночасно посилювати технічні механізми захисту та інвестувати в підготовку персоналу.

Практична підготовка передбачає ознайомлення з реальними сценаріями — вміння аналізувати підозрілі заголовки та адреси відправників, оцінювати легітимність URL-адрес і зберігати обережність щодо вкладень. До технічних контрзаходів належать налаштування фільтрації пошти, впровадження SPF/DKIM/DMARC, використання багатфакторної автентифікації та інструментів для безпечного аналізу вкладень або посилань (sandboxing, URL-сканери). Такі інструменти зменшують ймовірність успішного проникнення через людський фактор.

Окремо слід підкреслити роль навчання: імітаційні фішингові кампанії, регулярні тренінги та алгоритми дій у випадку виявлення підозрілих повідомлень формують у працівників практичні навички і покращують реакцію організації на інциденти. Поєднання технічних заходів з культурою кібергігієни створює послідовний захисний шар, що значно знижує ризики та підвищує стійкість до інтернет-загроз.

Social-Engineer Toolkit (SEToolkit) — це спеціалізований фреймворк з відкритим вихідним кодом, створений Дейвом Кеннеді для середовища Linux. Його основне призначення — проведення тестування на проникнення (пентесту), сфокусованого саме на методах соціальної інженерії та фішингу. Цей інструмент дозволяє моделювати складні вектори атак, спрямовані на маніпулювання поведінкою та впливом на людей. Інструмент широко відомий у спільноті пентестерів — його демонстрували на провідних конференціях і активно підтримують у відкритому репозиторії. Завдяки гнучкій архітектурі SET дозволяє дослідникам оцінити рівень людського і технічного захисту організації, ідентифікувати слабкі місця в процесах і відпрацьовувати заходи реагування.

Водночас важливо підкреслити етичне обмеження: застосовувати SET слід лише в законному та узгодженому контексті (за згодою власника інфраструктури або в рамках контрактного пентесту). Ненадане використання таких інструментів карається законом і підриває професійні стандарти.



Рис 2.4 – (SEToolkit)

Окрім цього, Social-Engineer Toolkit (SET) є потужною платформою для імітації спрямованих атак, яка надає широкий функціонал для формування фішингових кампаній, копіювання вебсайтів, вбудовування потенційно небезпечних фрагментів коду та реалізації інших сценаріїв, що застосовуються під час перевірки стійкості інформаційних систем і мереж до загроз.

Розробка SET стала закономірною реакцією на швидкі зміни у сфері кібербезпеки, де прийоми соціальної інженерії відіграють дедалі важливішу роль і постійно еволюціонують. В основі соціальної інженерії лежить маніпулювання психологічними чинниками людини — такими як довірливість, тривожність, цікавість або поспіх — з метою спонукання до рішень, що можуть призвести до порушення безпеки або витоку чутливої інформації.

У таких умовах ключове призначення SET полягає у наданні гнучкого та багатофункціонального набору засобів, за допомогою яких спеціалісти з

інформаційної безпеки можуть моделювати різні типи соціально-інженерних впливів, оцінювати їхню ефективність та розробляти більш дієві методи захисту.

Переваги:

- Функціональна універсальність. Social-Engineer Toolkit охоплює широкий спектр інструментів для імітації соціально-інженерних впливів: створення фішингових повідомлень, відтворення копій вебсайтів, впровадження потенційно небезпечних елементів та інших технік, що дозволяє максимально наблизити тестування до реальних сценаріїв атак у межах пентесту.
- Доступність вихідного коду. Завдяки відкритій архітектурі користувачі мають можливість аналізувати принципи роботи SET, адаптувати його функціонал під власні потреби та інтегрувати інструмент у спеціалізовані середовища безпеки.
- Постійний розвиток і підтримка спільнотою. Активна участь користувачів і розробників забезпечує регулярні оновлення, усунення вразливостей і розширення можливостей, а також обмін практичним досвідом між фахівцями з кібербезпеки.

Недоліки:

- Високий поріг входу. Робота з SET потребує глибокого розуміння принципів інформаційної безпеки та психологічних аспектів соціальної інженерії; за відсутності належної підготовки результати тестування можуть бути некоректними або неправильно витлумаченими.
- Обмеження з боку захисних систем. Окремі механізми, реалізовані в SET, можуть бути зафіксовані засобами моніторингу та захисту (IDS/IPS, антифішингові та антиспам-системи), що ускладнює проведення повноцінної оцінки загроз.
- Можливість неправомірного використання. Через потужний функціонал інструмент може бути застосований не за призначенням, що створює серйозні правові та етичні ризики у разі відсутності належного контролю.

Практичний аспект використання: Застосування SET має здійснюватися виключно в межах чітко визначених умов тестування, із зафіксованим обсягом робіт та обов’язковою згодою власника інформаційних систем. Важливими є також документовані процедури реагування на інциденти та заходи зі зниження ризиків для третіх сторін.

Загалом SET вирізняється стабільною підтримкою та активною екосистемою користувачів, що позитивно впливає на його актуальність і ефективність. Водночас складність інструмента може становити труднощі для спеціалістів без достатнього досвіду, а можливість виявлення дій під час тестування обмежує застосування окремих сценаріїв.

Таким чином, використання Social-Engineer Toolkit потребує зваженого підходу, дотримання законодавчих та етичних норм, а також попереднього аналізу потенційних переваг і ризиків у контексті завдань пентестування.

Ще одним варто згадати **King Phisher** — спеціалізоване програмне рішення для імітації фішингових кампаній, орієнтоване як на оцінювання рівня захищеності організацій, так і на підвищення обізнаності співробітників. Завдяки гнучкій модульній побудові платформа забезпечує детальне керування змістом електронних повідомлень і параметрами серверної частини, що дає змогу створювати правдоподібні сценарії взаємодії користувачів із потенційно небезпечним контентом.



Рис 2.5 – King Phisher

Функціональні можливості King Phisher дозволяють реалізовувати різні типи фішингових симуляцій — від простих навчальних розсилок до складніших моделей, у межах яких користувачі можуть бути перенаправлені на імітовані вебсторінки для аналізу поведінки та реакцій на загрози.

Як проєкт із відкритим вихідним кодом, інструмент вирізняється високим рівнем адаптивності: він підтримує паралельне проведення кількох незалежних кампаній із різними завданнями, а також масштабування під значну кількість отримувачів. Це дозволяє гнучко налаштовувати як вміст повідомлень, так і цільові сторінки, підвищуючи реалістичність тестування та ефективність навчальних програм.

Згідно з офіційними матеріалами, King Phisher також надає можливості збору статистики та аналітики, зокрема фіксацію фактів відкриття листів і взаємодії з ними. Отримані дані використовуються для оцінки результативності проведених кампаній і подальшого вдосконалення заходів із підвищення рівня інформаційної безпеки.

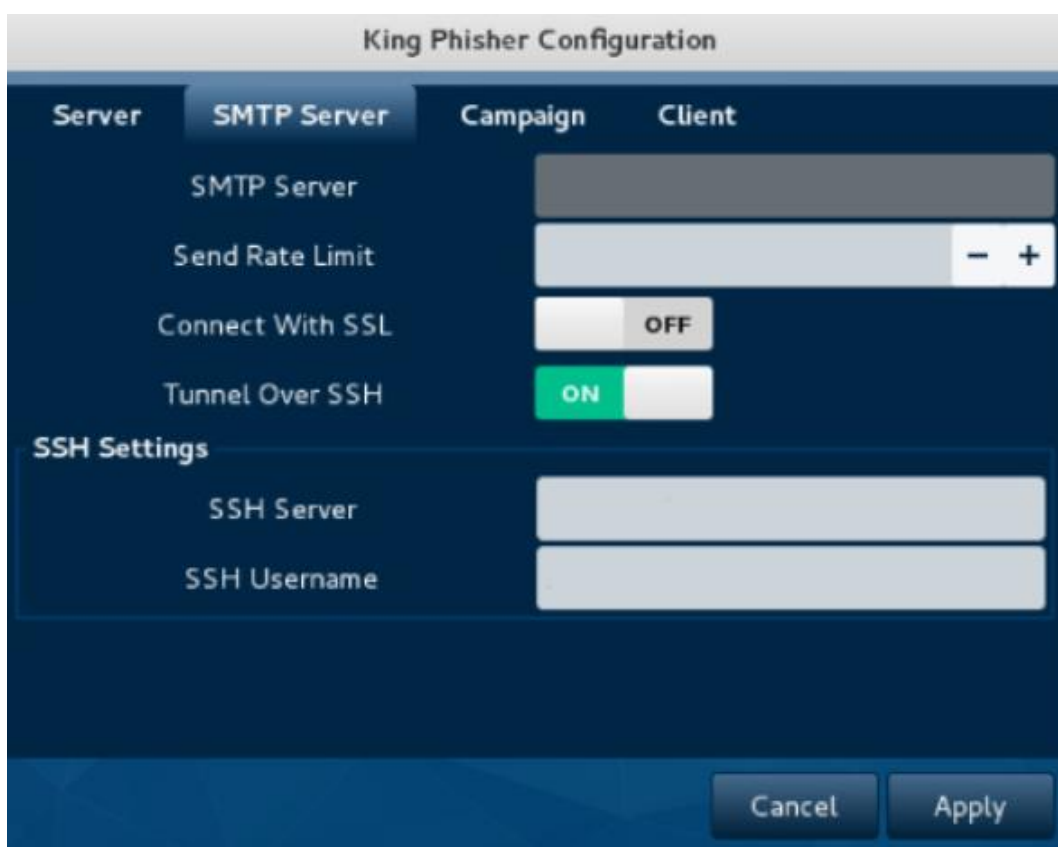


Рис 2.6 – Ведення облікові дані. King Phisher

Програмний продукт розроблений мовою Python і поширюється на умовах відкритої ліцензії, що надає спеціалістам можливість адаптувати та розширювати його можливості відповідно до конкретних завдань. У низці конфігурацій відсутність класичного централізованого веб-інтерфейсу ускладнює ідентифікацію інструмента під час імітації соціально-інженерних впливів, оскільки значна частина процесів виконується на серверному рівні або за допомогою скриптів, не привертаючи безпосередньої уваги користувачів.

Переваги:

- Прозорість і відкритість реалізації. Відкритий вихідний код дозволяє експертам аналізувати механізми роботи програми, вносити зміни та доповнювати функціонал залежно від потреб тестування або навчання.
- Підтримка різнорівневих сценаріїв. Інструмент придатний як для простих навчальних фішингових кампаній, так і для складних багатофазних симуляцій, що дає змогу всебічно оцінювати рівень захищеності інформаційних систем.
- Адаптивність налаштувань. Модульна структура та широкі можливості конфігурації забезпечують точне підлаштування кампаній під конкретні цілі, аудиторію та умови проведення тестування.

Недоліки:

- Потенціал неправомірного використання. За відсутності контролю інструмент може бути застосований у шкідливих цілях, що створює ризики проведення реальних кібератак.
- Правові та етичні обмеження застосування. Використання без відповідних дозволів може порушувати норми законодавства у сфері захисту інформації та персональних даних, тому допустиме лише в межах власних середовищ або за наявності офіційно оформленої згоди.
- Високий рівень вимог до користувача. Коректна експлуатація потребує достатнього досвіду й технічної підготовки у сфері кібербезпеки; нестача знань може призвести до помилкових налаштувань і некоректної інтерпретації результатів.

Застосування **King Phisher** передбачає наявність відповідного рівня технічної компетентності для досягнення достовірних і безпечних результатів. Неконтрольоване або незаконне використання несе як юридичні ризики, так і загрозу зловживань, тому відповідальний підхід до роботи з інструментом повинен поєднувати професійні навички з неухильним дотриманням етичних і правових норм.

Modlishka — це відкритий інструмент у вигляді HTTP-reverse-proxy, створений для дослідницьких цілей та етичного пентестування. Він проксірує трафік між користувачем і легітимним сервісом, що дозволяє в реальному часі фіксувати введені облікові дані й одноразові коди аутентифікації (MFA). Проєкт публічно доступний у репозиторіях і широко розглядається в технічній літературі та спільноті.

slowmistio/Modlishka- Phishing-NG

Modlishka. Reverse Proxy. 2FA authentication
Phishing NG.



Рис 2.7 – Modlishka

Технічно Modlishka працює як прозорий проміжний сервер: він приймає запити від жертви, пересилає їх до цільового сервісу та повертає відповіді, при цьому перехоплюючи й зберігаючи передані параметри сесій та токени. Інструмент підтримує налаштування для роботи з TLS, обробки мультидоменного трафіку і конфігурацій під конкретні платформи аутентифікації, що робить його придатним для відтворення реалістичних сценаріїв AiTM (Adversary-in-the-Middle).

У практичному використанні Modlishka застосовують для оцінки реальної стійкості механізмів входу (включно з MFA), тестування політик сесійного управління та перевірки, чи здатні захисні рішення виявляти проксі-атаки. Водночас інструмент має високий потенціал для зловживань, тому його

застосування обов'язково повинно відбуватися лише в рамках оформленого дозволу, із чітко визначеним обсягом робіт і заходами з мінімізації ризиків.

Переваги:

- Висока реалістичність сценаріїв. Modlishka дає змогу відтворювати складні атаки типу «людина-посередині» (AiTM) в умовах, наближених до реальних, що дозволяє оцінити ефективність механізмів захисту, зокрема MFA.
- Налаштовуваність і підтримка різних сервісів. Інструмент можна конфігурувати під різні цільові ресурси, він працює з TLS і здатний обробляти мультидоменний трафік, що робить його придатним для тестування широкого спектра сценаріїв.
- Освітня й дослідницька цінність. У контрольованому середовищі Modlishka демонструє практичні слабкі місця сучасних схем аутентифікації, сприяючи розробці додаткових захисних механізмів.

Недоліки:

- Сильний потенціал для зловживань. Оскільки інструмент може перехоплювати реальні токени та коди, його неправильне застосування може спричинити серйозні компрометації.
- Юридичні та етичні обмеження. Використання Modlishka без письмового дозволу власника системи може тягти за собою правову відповідальність; усі тестові активності мають бути формалізовані (scope, дозвіл, звітність).
- Складність виявлення і захисту. Reverse-proxy-атаки відбуваються в реальному часі, тому традиційні реактивні методи блокування доменів чи URL можуть виявитися недостатніми — для виявлення потрібні поведінкові та сесійні індикатори.

Для захисту від технік, подібних до Modlishka, рекомендують поєднувати технічні підходи (прив'язка сесій до пристрою/браузера, поведінковий аналіз сесій, додаткові перевірки при незвичних паттернах входу) з організаційними заходами (навчання користувачів, логування і процес реагування).

Gophish представляє собою open-source платформу для імітації фішингових атак, ефективну для проведення організованих і контрольованих навчальних чи пентестових кампаній.



Рис 2.8 – Gophish

Gophish належить до класу відкритих програмних рішень, що застосовуються для імітації фішингових інцидентів у безпечному та контрольованому середовищі. Широке поширення цього інструмента зумовлене поєднанням зручності в роботі, адаптивності параметрів і наявності засобів для детального аналізу результатів. Зрозумілий інтерфейс значно спрощує процес підготовки та запуску кампаній, завдяки чому платформа підходить як для практичного використання спеціалістами з інформаційної безпеки, так і для проведення навчальних заходів у межах організацій.

Однією з ключових особливостей Gophish є можливість тонкого налаштування вмісту фішингових матеріалів. Користувачі можуть змінювати шаблони електронних повідомлень, посилання, макети вебсторінок та інші складові відповідно до цільової аудиторії або обраного сценарію. Такий підхід дозволяє формувати правдоподібні симуляції, що відображають реальні загрози, з якими персонал може зіткнутися в повсякденній роботі.

Окрему увагу в Gophish приділено збору статистики та аналізу поведінки користувачів. Вбудовані механізми спостереження дають змогу фіксувати всі

етапи взаємодії з кампанією — від отримання листа до подальших дій, зокрема переходів за посиланнями або введення інформації. Отримані дані використовуються для оцінки рівня обізнаності працівників і виявлення напрямів, що потребують посилення захисних заходів.

Також платформа підтримує взаємодію з іншими рішеннями у сфері кібербезпеки. Її можна інтегрувати з системами моніторингу, аналізу подій чи управління ризиками, що дозволяє об'єднувати результати фішингових симуляцій із загальною картиною стану захищеності організації.

Додатковою перевагою є автоматизоване формування звітної документації з детальними показниками ефективності проведених кампаній. Такі звіти можуть слугувати основою для внутрішніх перевірок, коригування політик безпеки та розроблення рекомендацій щодо підвищення рівня кіберзахисту. У поєднанні з відкритою моделлю розробки та активною спільнотою користувачів це робить Gophish дієвим інструментом для аналізу та навчання у сфері соціальної інженерії.

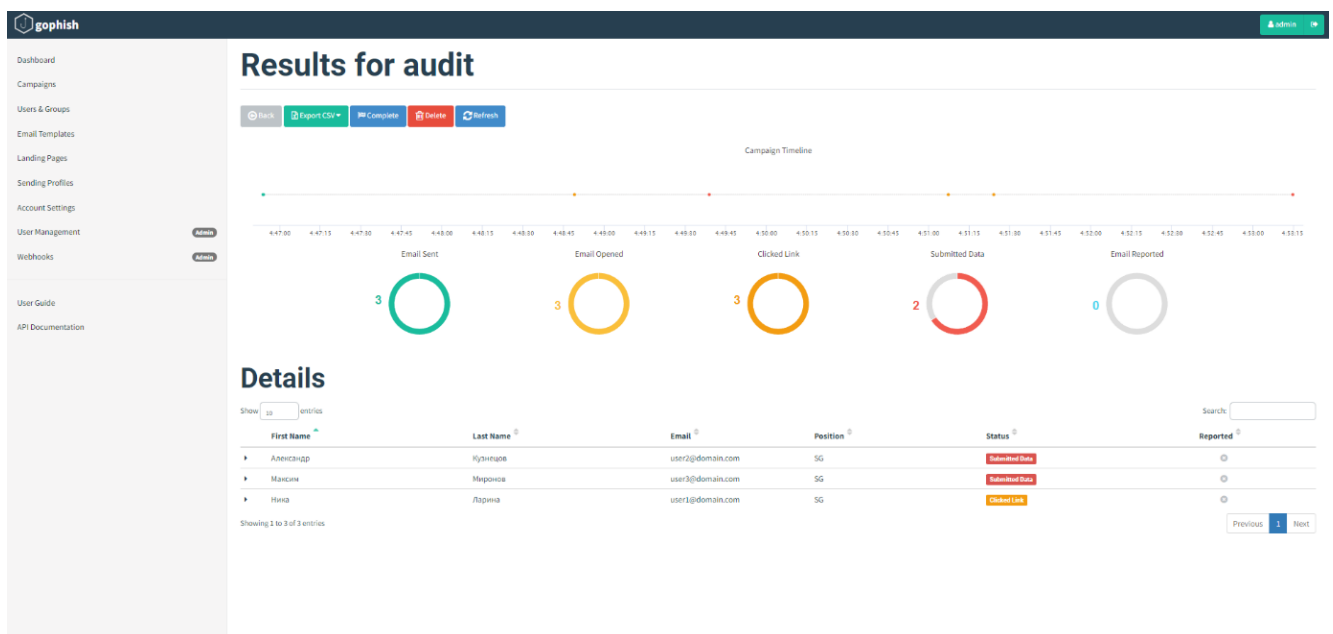


Рис 2.7 – Інтерфейс Gophish

Платформа Gophish орієнтована на спрощення процесу підготовки та проведення фішингових симуляцій завдяки наявності базових шаблонів повідомлень і допоміжних навчальних матеріалів. Це дозволяє значно зменшити витрати часу на створення кампаній і забезпечує стабільність результатів під час

повторного використання сценаріїв. Окремо варто відзначити підтримку автоматизованих механізмів, зокрема планування розсилок і налаштування послідовностей дій, що робить тестування більш системним і зручним для адміністрування.

Важливою складовою екосистеми Gophish є активний розвиток проєкту та участь спільноти користувачів. Регулярні оновлення, технічна підтримка й поява нових можливостей сприяють підвищенню стабільності роботи інструмента та його адаптації до сучасних вимог у сфері кібербезпеки. Такий підхід забезпечує швидке впровадження платформи в організаціях і подальшу підтримку під час масштабування або інтеграції з іншими рішеннями.

Переваги:

- **Оперативне впровадження.** Інструмент не потребує складної інсталяції, може бути розгорнутий на стандартній серверній інфраструктурі та має зрозумілу систему керування.
- **Широкі можливості кастомізації.** Користувачі можуть створювати власні шаблони електронних листів, імітовані сторінки входу, керувати логікою доставки та розподіляти отримувачів за групами.
- **Розвинена система аналізу.** Платформа збирає статистику щодо відкриття повідомлень, переходів за посиланнями та інших дій, що дозволяє оцінювати ефективність навчальних заходів.
- **Сумісність із зовнішніми сервісами.** Gophish може взаємодіяти зі сторонніми поштовими сервісами, системами збору логів і аналітичними платформами.
- **Відкрита модель розробки.** Доступ до вихідного коду полегшує аудит безпеки, модифікацію функціоналу та створення додаткових компонентів.
- **Придатність до масштабування.** Платформа однаково ефективна для локальних навчальних тестів і великих корпоративних кампаній із великою кількістю учасників.

Обмеження та ризики:

- Можливість неправомірного використання. Через відкритий доступ інструмент може бути застосований у протиправних цілях за відсутності належного контролю.
- Залежність від поштової інфраструктури. Результативність кампаній значною мірою визначається коректністю налаштування доменів і поштових політик; помилки конфігурації можуть призвести до блокування розсилок.
- Необхідність формального погодження. Законне використання вимагає попередньо визначених правил тестування, офіційних дозволів і процедур реагування.
- Менш розширений інтерфейс у порівнянні з комерційними продуктами. Деякі платні рішення пропонують ширший набір вбудованих функцій аналітики та управління навчальними програмами.
- Потреба в професійному аналізі результатів. Отримані показники необхідно правильно інтерпретувати з урахуванням технічних і людських факторів.

Підсумовуючи, Gophish є дієвим інструментом для проведення симуляцій фішингових атак і оцінювання рівня обізнаності персоналу, однак його ефективне застосування можливе лише за умови усвідомленого підходу, дотримання правових норм і належної оцінки потенційних ризиків.

Після порівняльного аналізу трьох розглянутих рішень встановлено, що Gophish та King Phisher добре підходять для планування, запуску та аналітики фішингових кампаній — обидва продукти надають інструменти для створення реалістичних симуляцій і вимірювання поведінкових метрик. При цьому кожен із них має свої характерні переваги й обмеження, які слід враховувати при виборі платформи залежно від цілей тестування.

На відміну від них, Social-Engineer Toolkit (SET) орієнтований насамперед на моделювання атак із елементами соціальної інженерії та на експлуатацію векторів проникнення; його функціонал більше спрямований на дослідження

вразливостей і побудову складних сценаріїв атак, ніж на масове управління навчальними фішинговими кампаніями.

Modlishka — потужний інструмент для відтворення складних проксі-атак, який має високу дослідницьку й навчальну цінність. Проте його застосування має бути суворо нормативно врегульованим: без належного дозволу, налаштувань та заходів безпеки використання цього інструмента може завдати реальної шкоди. У роботі з Modlishka пріоритетом має бути відповідальна методологія, орієнтована на мінімізацію ризиків і підвищення рівня захисту.

Виходячи з вимог цього дослідження — зокрема, необхідності простого розгортання, зручності налаштування кампаній, гнучкої персоналізації повідомлень і розвиненої аналітики — для практичної частини пентестування обрано Gophish. Цей вибір обґрунтований його зрозумілим інтерфейсом, можливістю швидкого створення сценаріїв і наявністю інструментів для систематичної оцінки ефективності симульованих атак, що робить його найбільш відповідним для задач з підвищення обізнаності персоналу та оцінки людського фактора в організації.

Висновок до другого розділу

Фішингові атаки становлять одну з найнебезпечніших кіберзагроз у сучасному цифровому просторі. Зловмисники активно застосовують прийоми соціальної інженерії, аби виманити конфіденційні дані та виконати шахрайські операції. Тому критично важливо впроваджувати надійні механізми захисту. До основних заходів належать навчання користувачів, використання антивірусів, ретельна перевірка посилань і вкладень, активація двофакторної автентифікації та регулярне оновлення програмного забезпечення. Найкращий результат забезпечує комплексне застосування цих методів, що істотно знижує ризик успішних фішингових атак.

Методи здійснення фішингу постійно вдосконалюються, а зловмисники активно впроваджують нові техніки психологічного впливу. Така динаміка вказує

на необхідність безперервного розвитку засобів кіберзахисту та підвищення обізнаності користувачів і працівників організацій. Розуміння сучасних тенденцій у сфері фішингу дає змогу ефективніше запобігати інцидентам. Підвищення кваліфікації персоналу, модернізація систем виявлення загроз і застосування новітніх технологій інформаційної безпеки є ключовими елементами у протидії цьому виду кіберзлочинності.

Аналіз характеристик трьох інструментів для проведення фішингових кампаній показав, що Gophish і King Phisher є одними з найефективніших рішень у цій сфері. Вони забезпечують зручні можливості для створення розсилок, керування кампаніями та оцінювання результатів. На відміну від них Social-Engineer Toolkit (SEToolkit) орієнтований переважно на методи соціальної інженерії та експлуатацію вразливостей, менше акцентуючи увагу саме на реалізації фішингових сценаріїв.

Для подальшого дослідження та оцінки ефективності фішингових атак у рамках пентестування було обрано інструмент Gophish, оскільки він відзначається більш широкими можливостями, розвиненим функціоналом та зручністю роботи.

РОЗДІЛ 3 АНАЛІЗ ФУНКЦІОНУВАННЯ ТА НАДІЙНОСТІ ПРОГРАМНИХ СИСТЕМ

3.1 Конфігурація сценарію атаки та здійснення тестового аналізу

Для якісного моделювання фішингових загроз у межах дозволеного тестування на проникнення необхідно ретельно продумати всі етапи та умови, що впливають на поведінку користувачів і роботу систем захисту. Водночас важливо підкреслити, що справжні фішингові атаки є протиправною діяльністю, яка може мати серйозні юридичні наслідки, тому подібні дії допускаються лише в рамках офіційного аудиту безпеки та за згодою організації.

Зазвичай перевірка стійкості до фішингових загроз відбувається у два послідовні етапи. На першому етапі проводиться контрольована симуляція атаки: тестові повідомлення надсилаються співробітникам без попередження, а спеціалісти фіксують, як користувачі реагують на потенційно шкідливий контент. Метою є оцінити природну поведінку працівників у ситуації, коли вони не очікують загрози.

Другий етап передбачає проведення аналогічного тесту, але вже за умов, коли персонал заздалегідь повідомлений про навчальне моделювання інциденту та свідомо намагається виявляти підозрілі ознаки. Такий підхід дозволяє оцінити не лише початковий рівень обізнаності, а й ефективність навчальних програм, внутрішніх політик безпеки та здатність користувачів активно протидіяти соціальній інженерії.

Перший етап дослідження

Атаки планується здійснити у двох середовищах: на локальному поштовому сервері hMailServer та на популярному хмарному сервісі Gmail. Усі сценарії будуть виконані виключно в межах легального пентестингу з метою оцінки стійкості систем до фішингових та інших соціально-інженерних загроз. Тестування дозволить визначити потенційні вразливості, проаналізувати поведінку серверів під час атак та сформулювати рекомендації щодо підвищення рівня безпеки.

У рамках дослідження для створення тестового поштового середовища був обраний hMailServer. Вибір саме цього рішення обумовлений низкою ключових переваг.

hMailServer є безкоштовним і повністю відкритим програмним забезпеченням, що робить його доступним для навчальних і дослідницьких цілей без додаткових фінансових витрат.

Сервер відзначається простотою встановлення та налаштування, що дозволяє швидко розгорнути локальний поштовий сервер із повним набором функцій — від створення доменів і користувачів до налаштування протоколів SMTP, POP3 та IMAP.

Забезпечує достатню гнучкість та масштабованість для проведення різних видів тестування, включаючи моделювання фішингових атак у безпечному середовищі. Він підтримує логування, фільтрацію листів, правила обробки та інтеграцію з іншими інструментами, що робить його зручним для аналізу поведінки поштової системи під час атак. Завдяки такому функціоналу hMailServer забезпечує умови, максимально наближені до роботи реальних корпоративних поштових серверів, що підвищує якість і достовірність результатів пентесту.

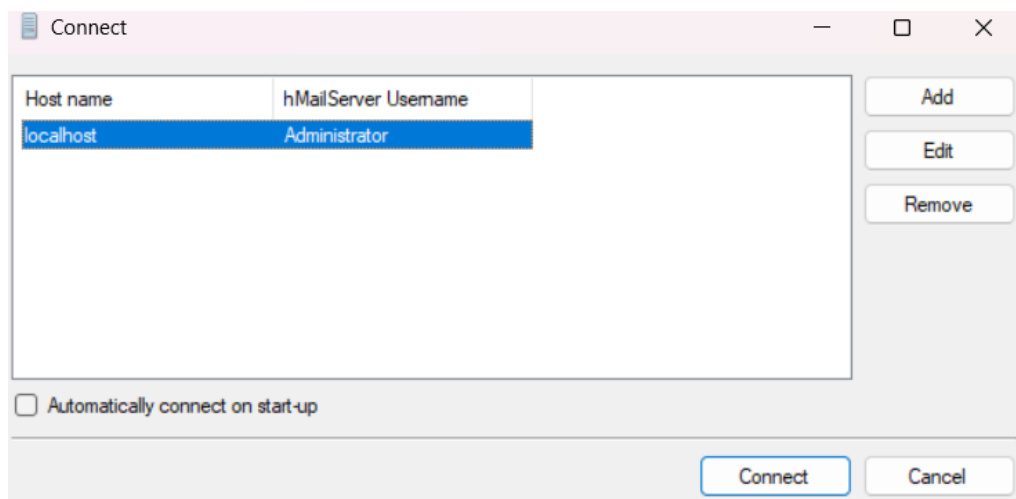


Рис 3.1 – Підключення до localhost

У локальному середовищі налаштовується власний поштовий домен через сервер hMailServer. На його основі створюються тестові поштові скриньки, які

виконуватимуть роль умовних «жертв» під час моделювання фішингової атаки (рис. 3.2). Такий підхід дає змогу безпечно відтворити реальні сценарії атак та проаналізувати ефективність захисних механізмів у контрольованих умовах.

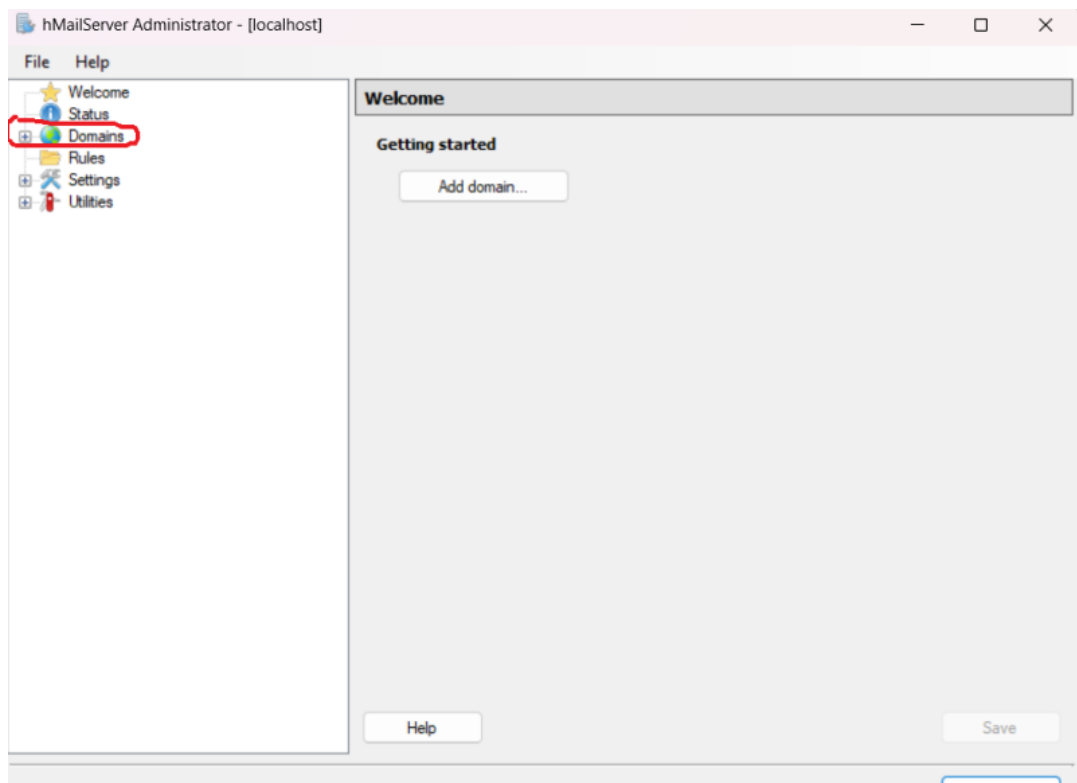


Рис 3.2 – Domains

Створюються поштові скриньки для тестових користувачів, а також окрема скринька, з якої здійснюватиметься фішингова розсилка до всіх адресатів (рис. 3.3). Це є важливим етапом, оскільки дає змогу максимально наблизити тестування до реальних умов: перевірити реакцію користувачів, оцінити ефективність системних механізмів захисту та виявити потенційні слабкі місця в обробці підозрілих повідомлень. Така симуляція допомагає сформувати повну картину ризиків і покращити рівень безпеки організації.

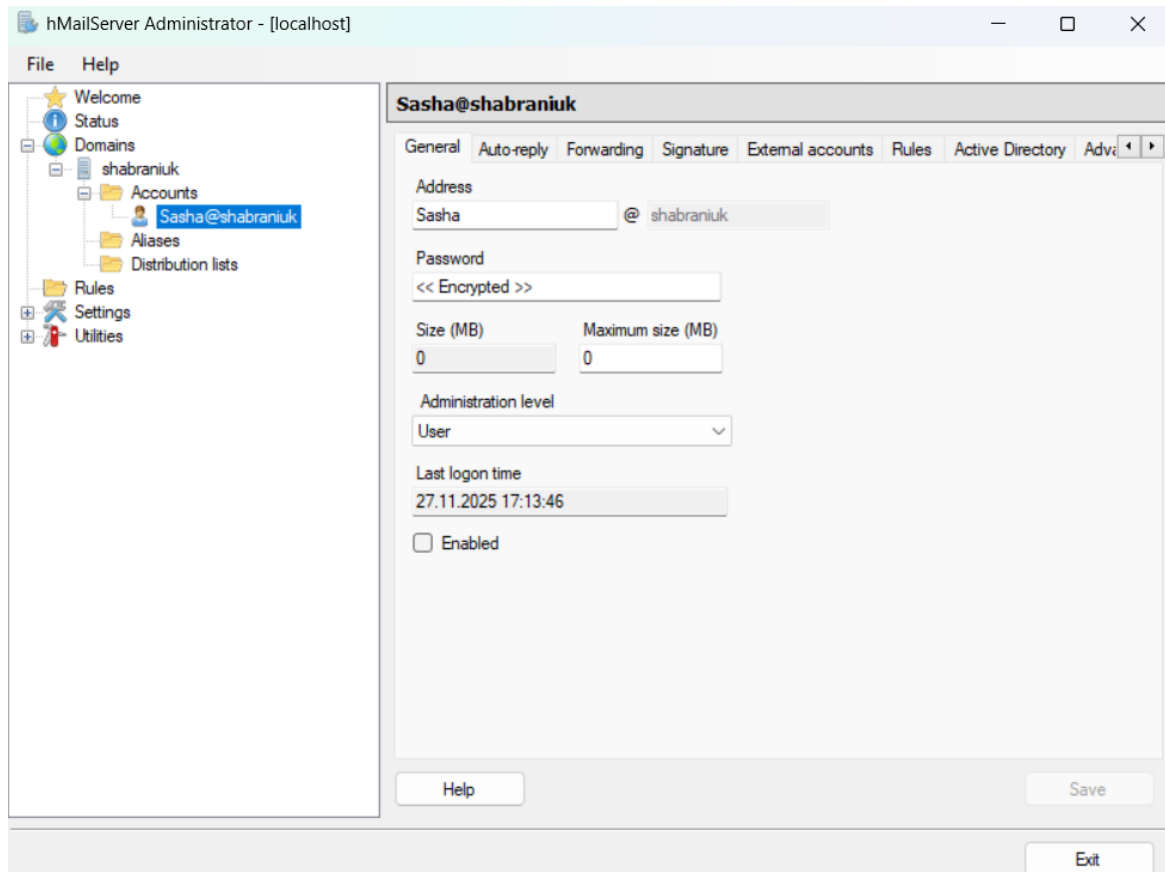


Рис 3.3 – Створена поштова скринька користувача

Для здійснення фішингової розсилки у локальному середовищі була створена окрема поштова скринька **support@shabraniuk**. Саме цей обліковий запис використовується як відправник тестових фішингових листів (рис. 3.4). Вибір технічної адреси формату “support” є важливим, оскільки вона виглядає як офіційний контакт служби підтримки, що підвищує рівень реалізму під час моделювання соціально-інженерних атак. Це дає можливість перевірити, наскільки користувачі довірятимуть такому листу, а також оцінити ефективність наявних механізмів захисту та фільтрації у реальних умовах. Використання окремої скриньки також забезпечує контрольованість і безпеку тестування, дозволяючи ізолювати усі тестові розсилки від основних робочих облікових записів.

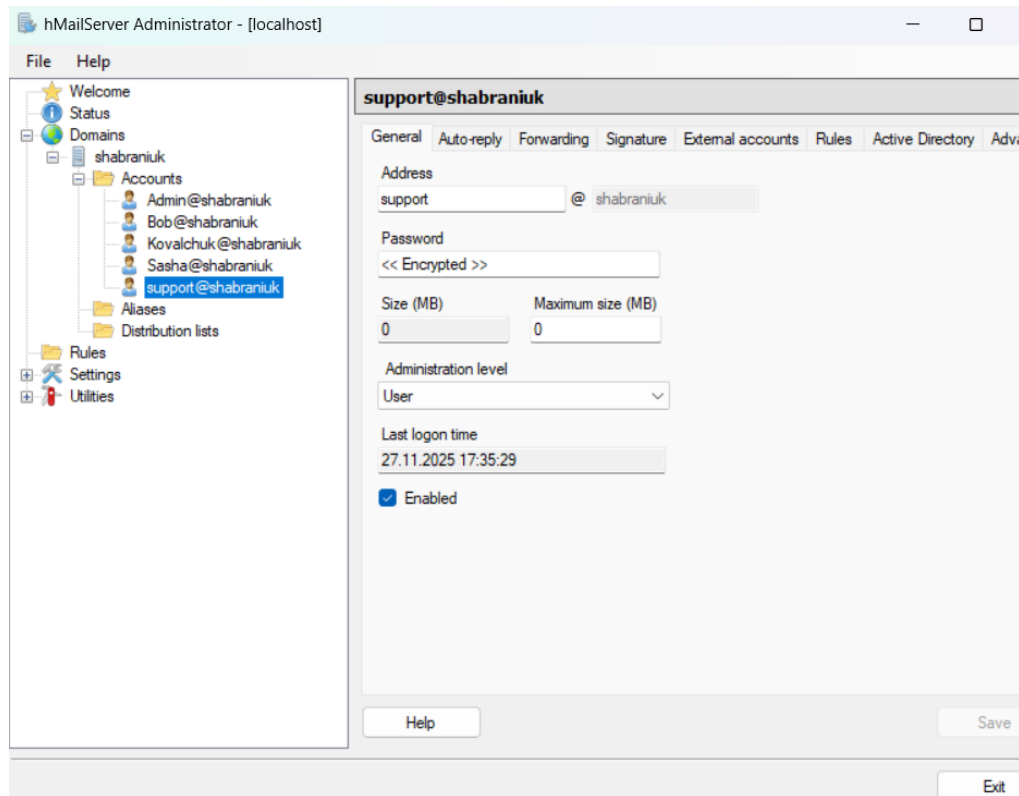


Рис 3.4 – support@shabraniuk

Після створення тестових поштових скриньок у локальному середовищі наступним етапом є налаштування взаємодії між Gophish та поштовим сервером hMailServer. Це дозволяє організувати повноцінну фішингову розсилку у межах пентестингу, використовуючи локальну інфраструктуру, що повністю виключає ризики для реальних користувачів та зовнішніх систем.

Для інтеграції Gophish із hMailServer використовується протокол SMTP. Локальний сервер hMailServer виступає як SMTP-реле, через яке Gophish надсилатиме фішингові повідомлення на створені раніше тестові адреси. У hMailServer попередньо перевіряється доступність SMTP-служби та правильність налаштувань IP-діапазонів, що дозволяють приймати з'єднання з локального хоста. Також конфігуруються параметри автентифікації, оскільки надсилання листів відбувається від імені окремої технічної скриньки — support@shabraniuk.

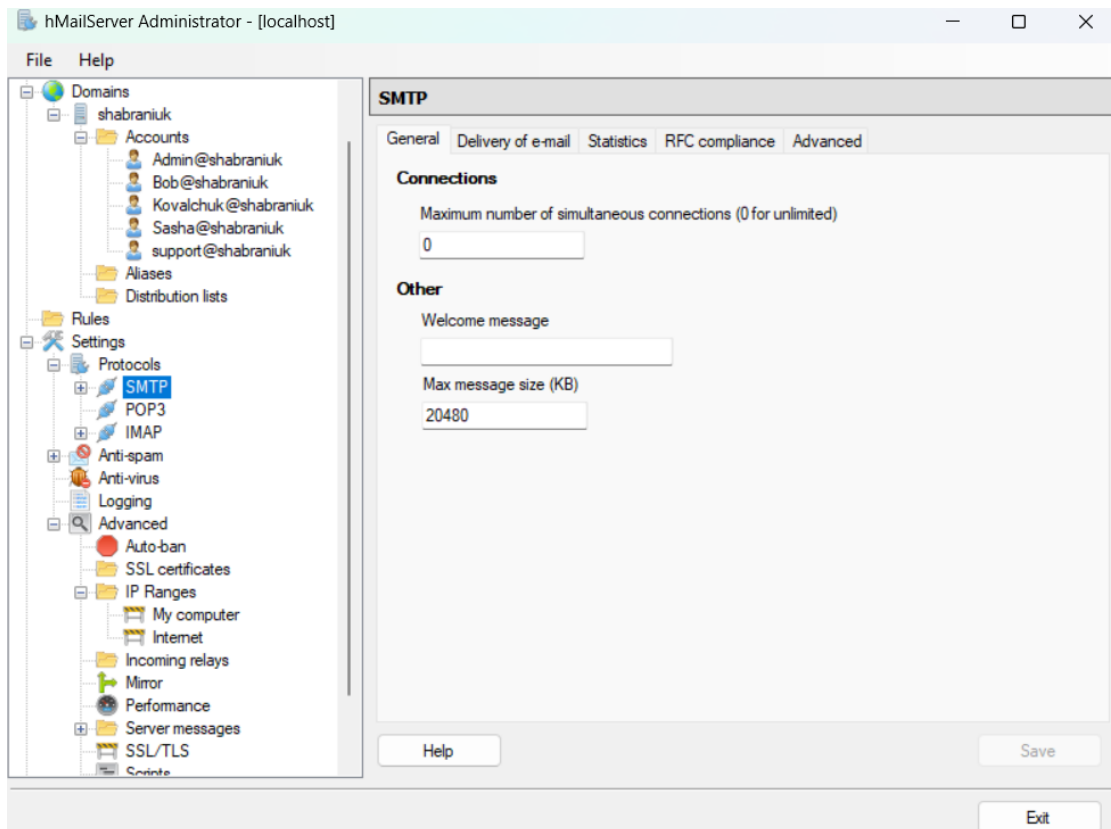


Рис 3.5 – Перевірка підключення протокола SMTP

Gophish працює на локальній машині (127.0.0.1) і розглядається hMailServer як локальний клієнт. Однак під час надсилення листів він може формувати як локальні запити (local-to-local), так і запити з локальної адреси до зовнішньої (local-to-external). Тому для забезпечення коректної роботи необхідно увімкнути автентифікацію SMTP.

У розділі Require SMTP authentication активуються такі параметри:

- Local to local e-mail addresses
- Local to external e-mail addresses

Це дає змогу Gophish авторизуватися за допомогою створеної поштової скриньки (наприклад, support@shabraniuk) та коректно надсилати всі типи повідомлень у межах тестового середовища.

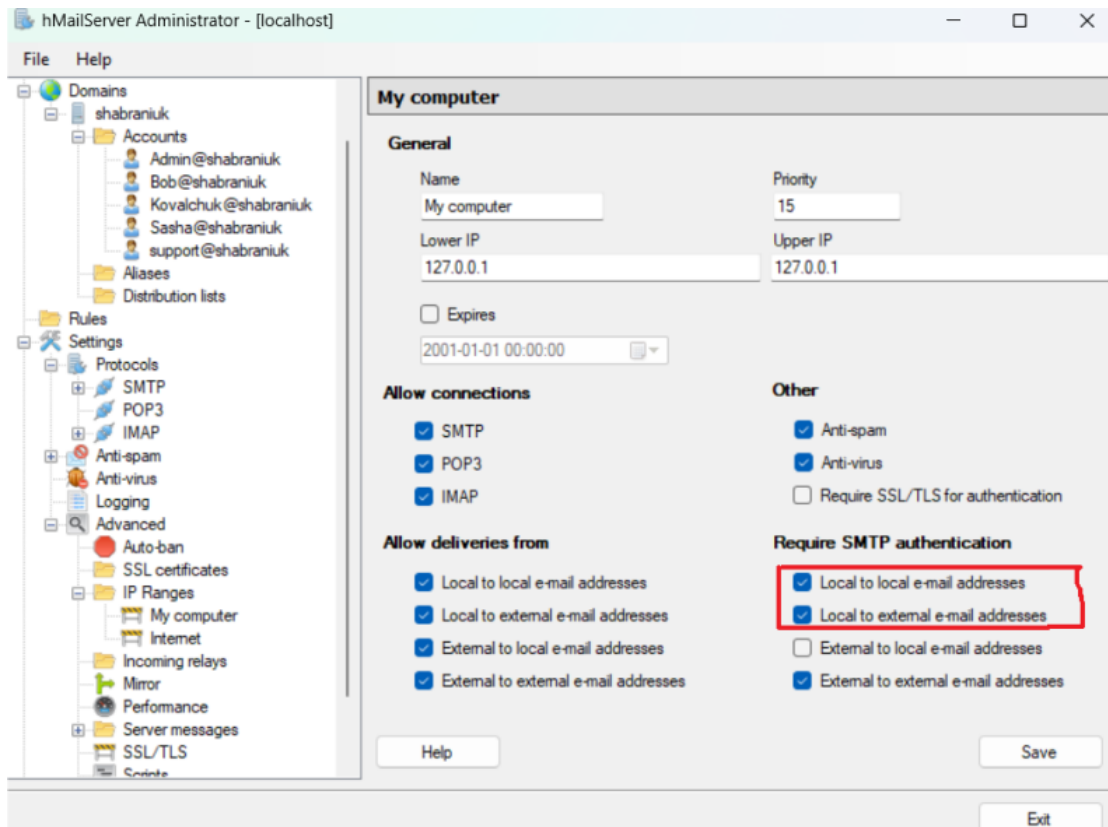


Рис 3.6 – активація Local to local e-mail addresses, Local to external e-mail addresses

Після успішного створення та прив'язки поштових скриньок до локального сервера наступним етапом є отримання IP-адреси машини, на якій розгорнуто hMailServer. Це необхідно для подальшої роботи через поштовий клієнт, наприклад Thunderbird, який буде використовуватись для перевірки функціональності локальної поштової інфраструктури.

Для входу до створених поштових скриньок у поштовому клієнті потрібно ввести облікові дані — логін та пароль користувача. Крім цього, під час налаштування обов'язково зазначаються параметри сервера: IP-адреса поштового сервера, а також номери портів для протоколів IMAP (приймання пошти) та SMTP (відправлення пошти).

Встановлення та налаштування поштового клієнта дозволяє перевірити, чи коректно працюють створені облікові записи, чи надходять та відправляються листи всередині локального середовища, а також підтвердити повну працездатність розгорнутого поштового сервера.

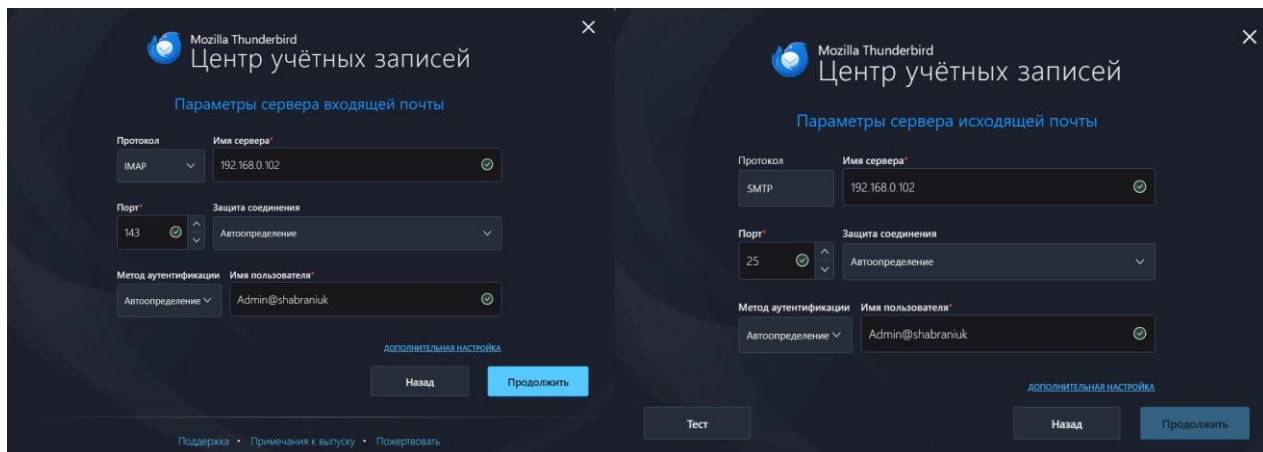


Рис 3.6 – Підключення поштової скриньки до Thunderbird

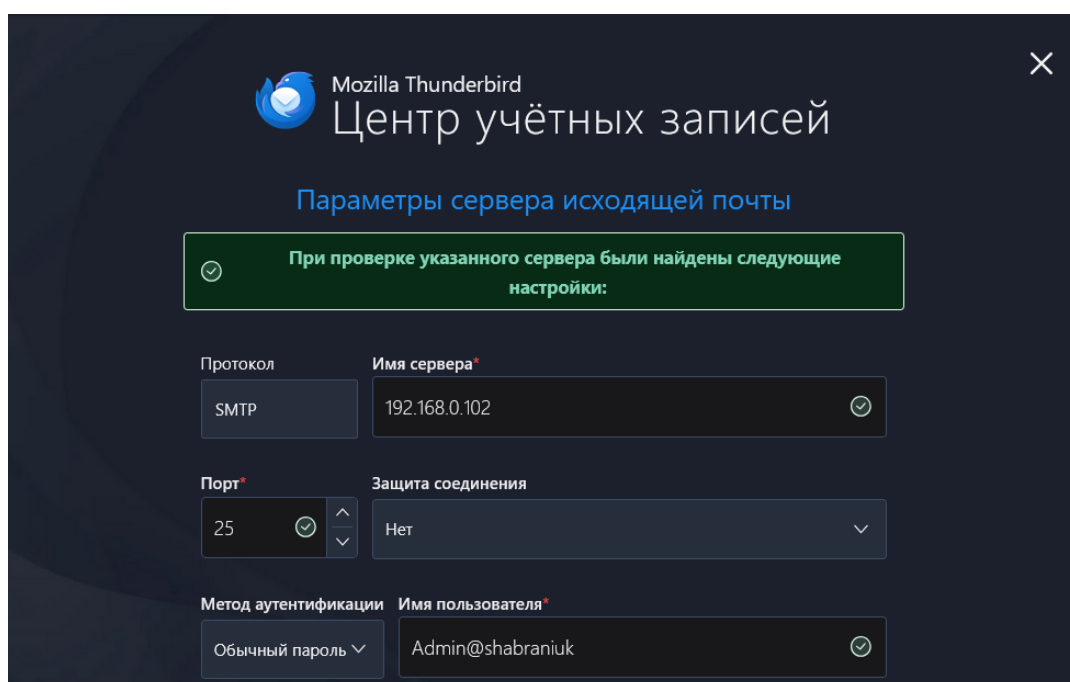


Рис 3.7 – Підключення до серверу

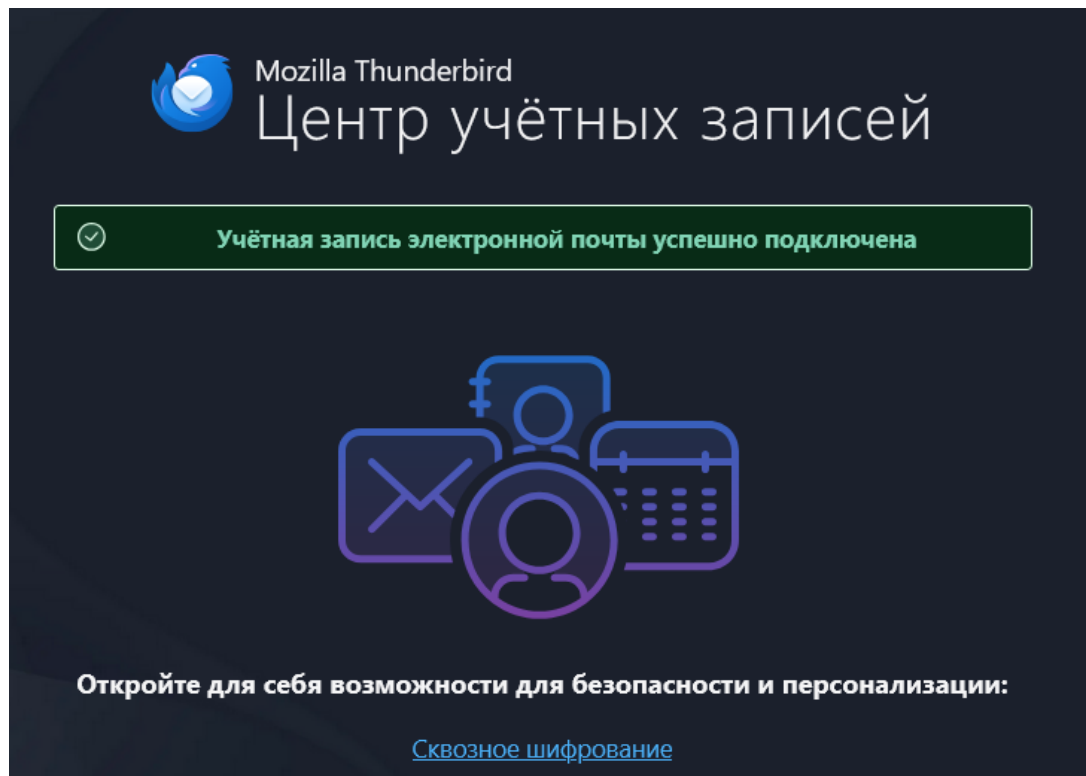


Рис 3.8 – успішно підключена пошта до Thunderbird

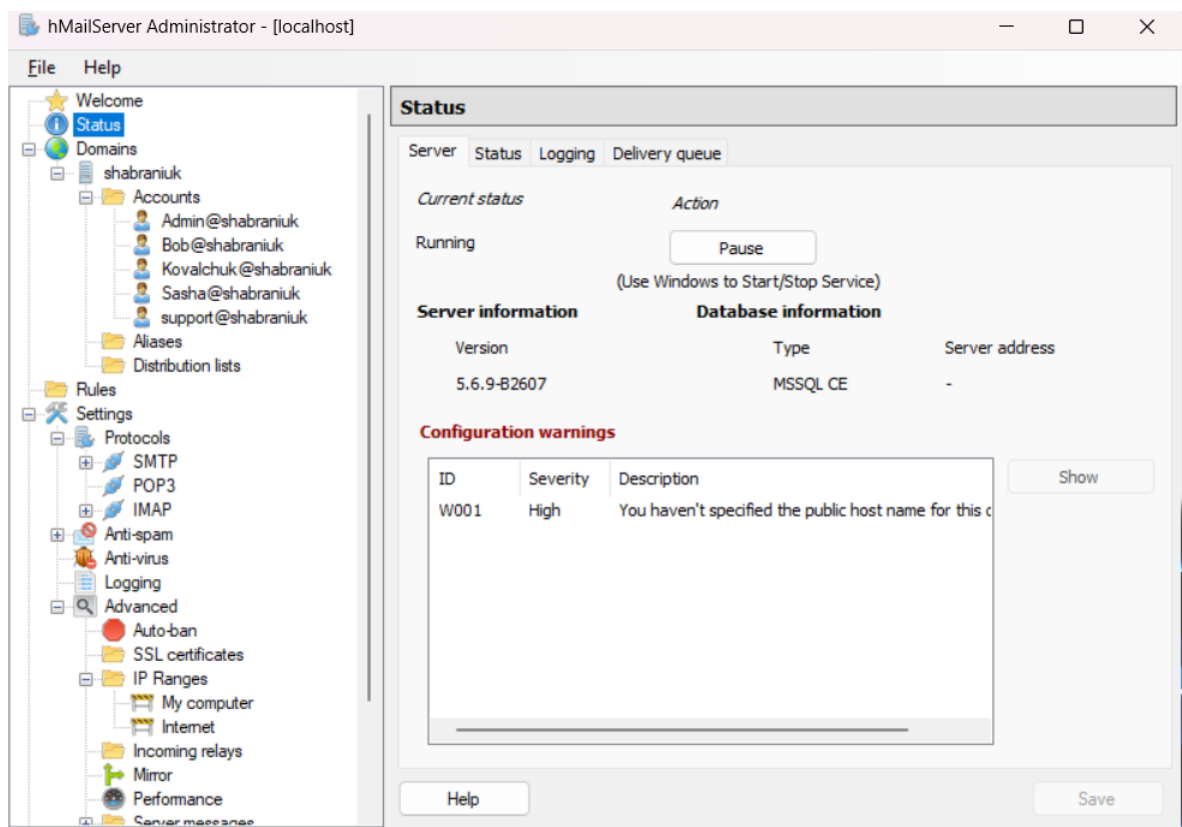


Рис 3.9 – Status локального сервера

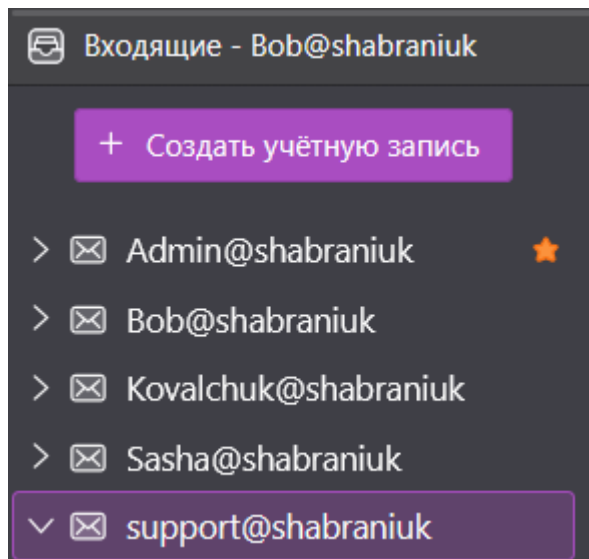


Рис 3.10 – Добавлення поштових скриньок

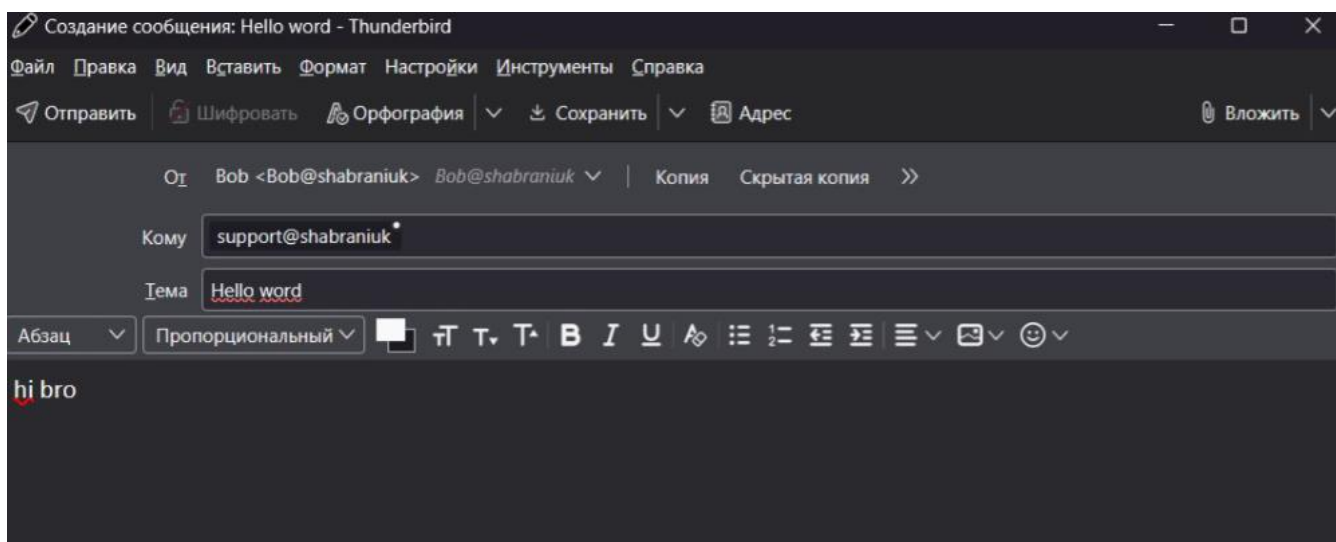


Рис 3.11 – Відправлення повідомлення з однієї пошти на іншу

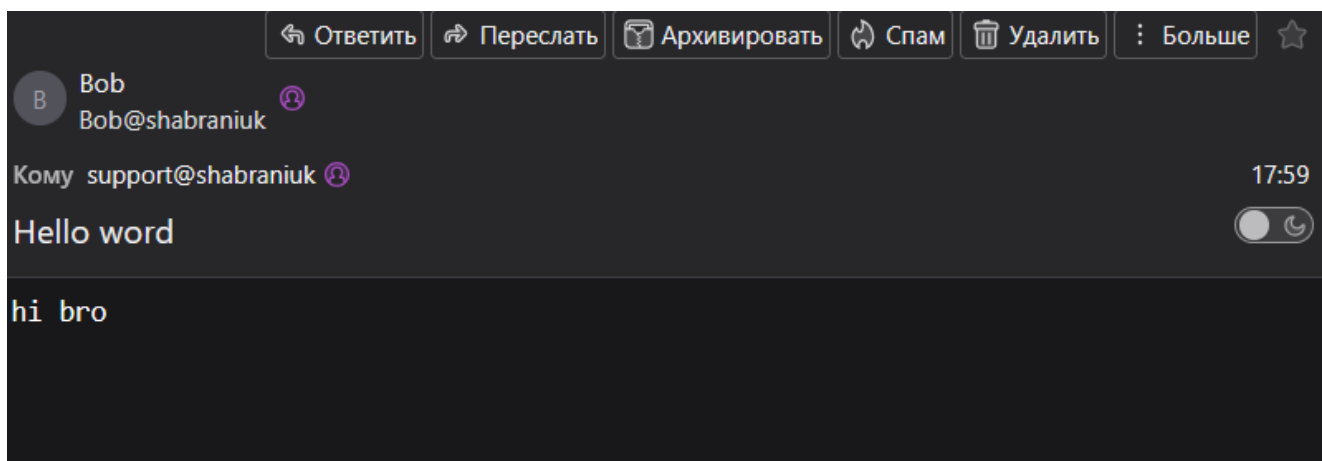


Рис 3.12 – Отримання відправленого повідомлення

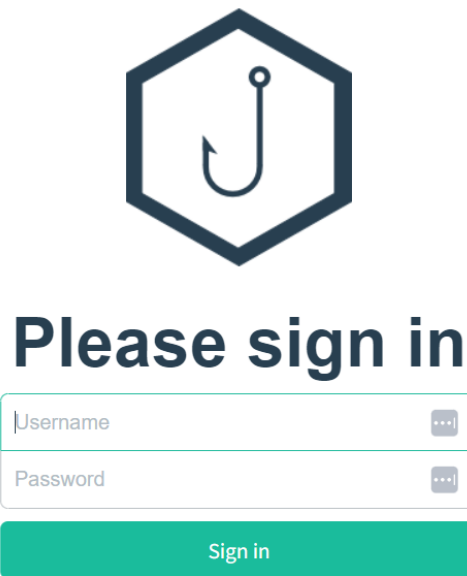


Рис 3.13 – Логін та пароль (Gophish)

Після входу в систему завантажується основний інтерфейс Gophish.

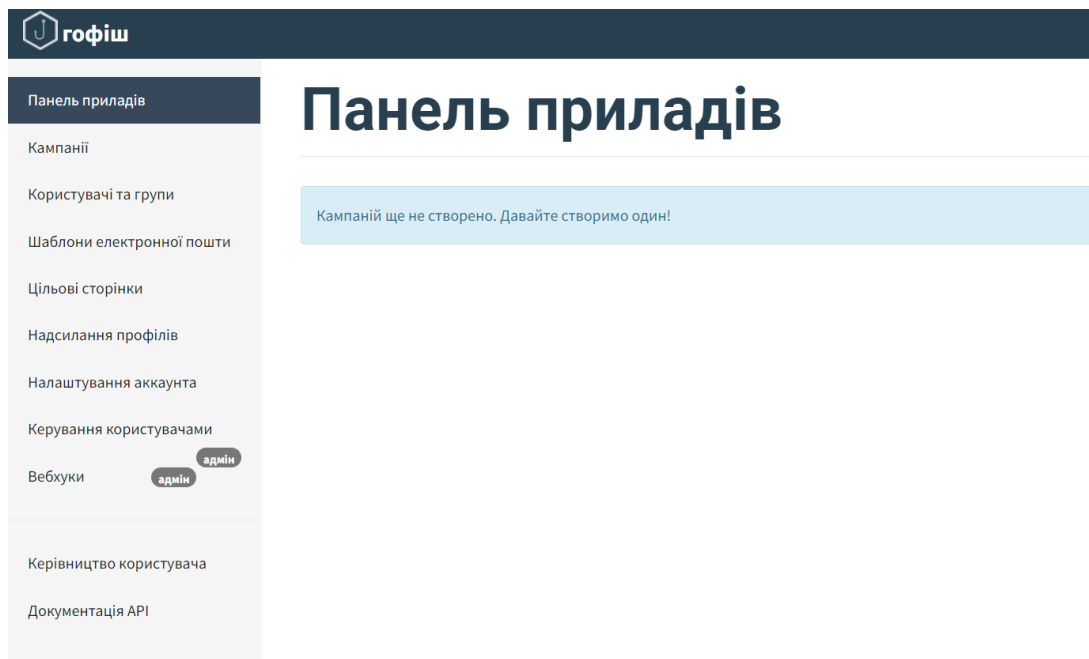


Рис 3.14 – Інтерфейс Gophish

У Gophish можна сформувати окрему фішингову кампанію, налаштувавши її з нуля. На початковому етапі необхідно визначити список цільових отримувачів — додати окремих користувачів або сформувати групи, які братимуть участь у тестуванні (Рис. 3.13). Після цього потрібно створити або імпортувати фальшиву веб-сторінку, що слугуватиме місцем, куди жертва буде перенаправлена для

введення своїх даних. Саме цей сайт виконуватиме роль пастки для фіксації введеної інформації під час симуляції атаки (Рис. 3.15).

New Group

Name:

phished

+ Bulk Import Users

Download CSV Template

First Name

Last Name

Email

Position

+ Add

Show

10

 entries

Search:

First Name	Last Name	Email	Position	
Admin	shabraniuk	admin@shabra...	WordPress	
Bob	shabraniuk	bob@shabraniuk	WordPress	
Kovalchuk	shabraniuk	kovalchuk@sha...	WordPress	
Sasha	shabraniuk	sasha@shabran...	WordPress	

Showing 1 to 4 of 4 entries

Previous

1

Next

Close

Save changes

Рис 3.15 – Додані користувачі

На наступному етапі формується фішингова розсилка — створюється електронний лист із вмонтованими переходами на підготовлений фальшивий вебресурс (Рис. 3.14). Саме ці повідомлення будуть автоматично відправлятися на поштові скриньки користувачів, визначених як цільова аудиторія тестування.

New Template ×

Name:

WordPress Re-Login

✉ Import Email

Envelope Sender: ?

WordPress.org<support@shabraniuk>

Subject:

[WordPress.org Forums] Pleas re-login to the system to keep your account safe

Text

HTML

```
Hi {{.FirstName}}  
We would like to inform you that due a recent incident, we logged out all user  
from WordPress.org.  
Preas "{{.URL}}" again with your email&nbsp;{{.Email}} to keep your account  
Regards, WordPress administration
```

☒ Add Tracking Image

+ Add Files

Рис 3.4 – Створенний лист

Після підготовки фішингового листа наступним кроком є конфігурація підставної вебсторінки. Цей елемент є ключовим для всієї симуляції, оскільки саме на підроблений сайт будуть перенаправлятися користувачі та, не підозрюючи небезпеки, вводитимуть свої дані.

Нова цільова сторінка

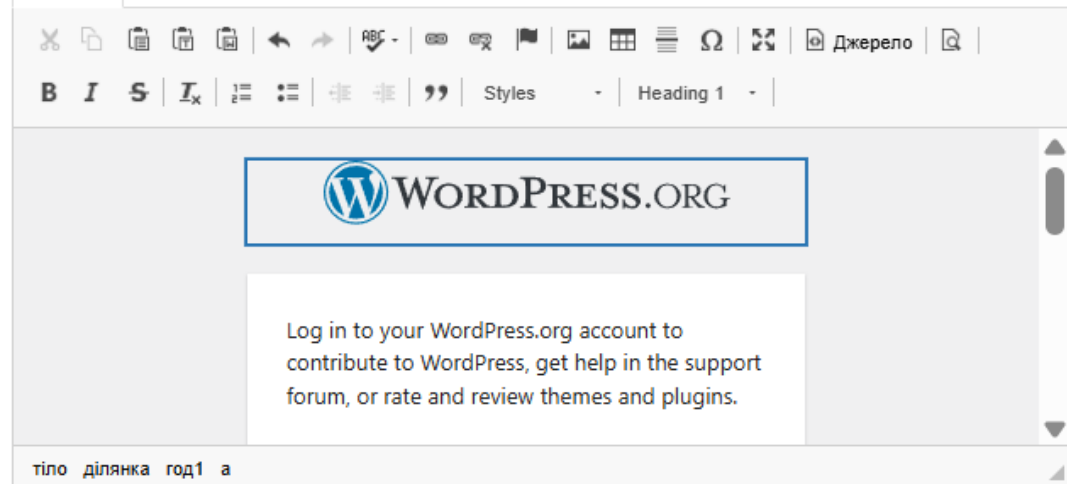


Ім'я:

Login WordPress.org

Імпорт сайту

HTML



☒ Захоплення надісланих даних?

☒ Захоплення паролів

⚠ Попередження: Облікові дані наразі **не зашифровані**. Це означає, що захоплені паролі зберігаються в базі даних у відкритому вигляді. Будьте обережні!

Перенаправити на:?

http://example.com

Скасувати

Зберегти сторінку

Рис 3.5 – Створений вебсайт

Edit Landing Page



Name:

Login WordPress.org

Import Site

HTML



```
_stq.push([ "clickTrackerInit", "124570481", "0" ]);  
/* ]]> */  
</script>  
  
<div id="wporg-locale-switcher-container"> </div>  
  
</body></html>
```

Рис 3.6 – HTML підробленого вебсайта

Фішингову сторінку можна створити вручну за допомогою HTML або ж імпортувати справжній веб-ресурс і внести до його структури мінімальні зміни. Після цього переходять до одного з ключових етапів — налаштування SMTP-сервера, через який здійснюватиметься розсилання електронних повідомлень. Оскільки Gophish не має власного механізму відправки листів, для тестування застосовують сторонні поштові сервіси. У межах проведеного експерименту використовувався SMTP-сервер

Новий профіль надсилання

✕

Ім'я:

phishprofile

Тип інтерфейсу:

SMTP

SMTP-адреса від:

support@shabraniuk

Ведучий:

smtp.192.168.0.102:25

Ім'я користувача:

support

Пароль:

.....

☒ Ігнорувати помилки сертифіката

Заголовки електронного листа:

X-Custom-Header

{{.URL}}-gophish

+Додати власний заголовок

Показати 10 записи

Пошук:

Заголовок

Значення

У таблиці немає даних

Показано від 0 до 0 з 0 записів

Попередній

Далі

Рис 3.7 – Налаштування поштового сервера

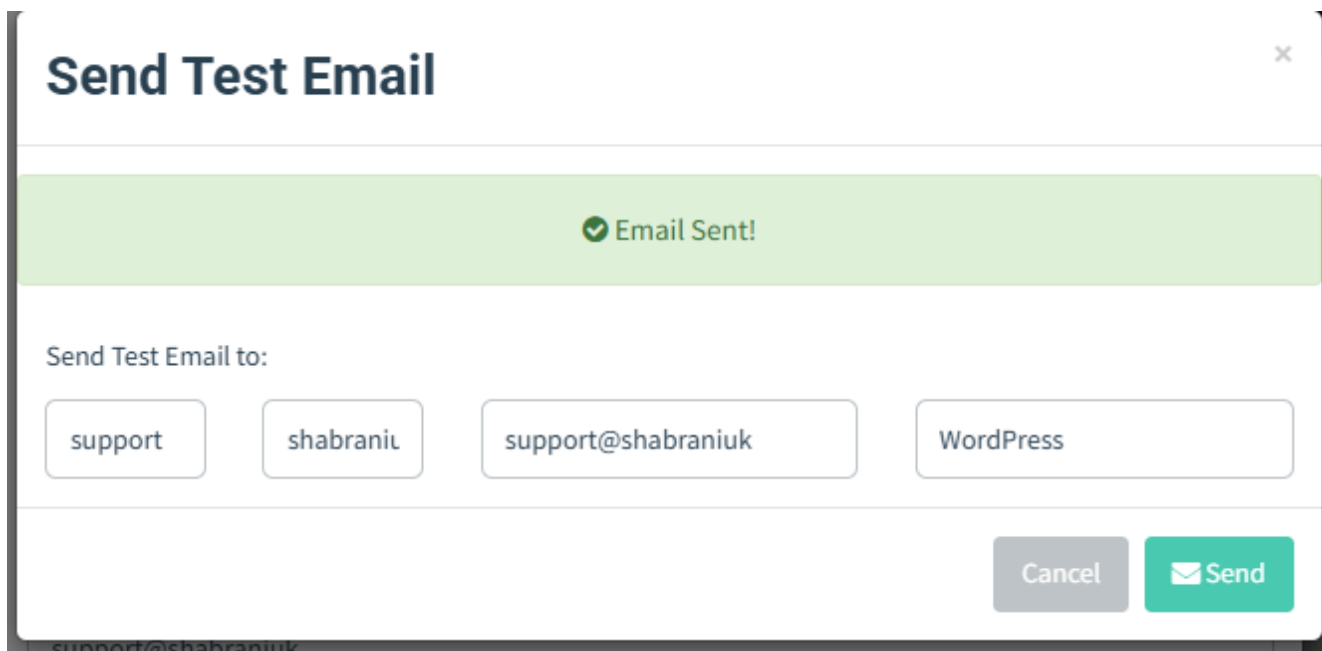


Рис 3.10 – Відправлення тестового листа.

Факт того, що тестове повідомлення було успішно відправлено та відображається у списку надісланих листів, свідчить про коректну роботу налаштувань. Це підтверджує, що SMTP-сервер функціонує правильно і може використовуватися для подальшої розсилки фішингових повідомлень.

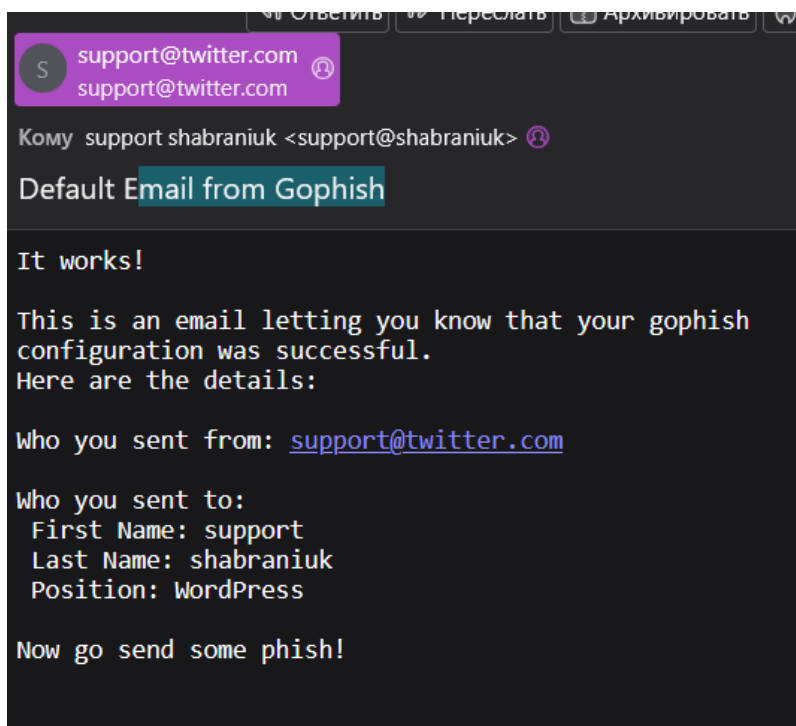


Рис 3.11 – Отримання тестового листа на локальну поштову скриньку

Далі переходять до формування самої фішингової кампанії. На етапі її налаштування обирають підготовлені заздалегідь елементи: шаблон електронного листа, сторінку для збору введених даних, профіль відправника та список адресатів. Також необхідно вказати URL, за яким розміщуватиметься підроблена веб-сторінка. Якщо Gophish працює у віртуальному середовищі, у цьому полі зазначають IP-адресу відповідної машини. У цьому дослідженні використовується спеціально призначена фішингова IP-адреса.

The screenshot shows the 'Нова кампанія' (New Campaign) form in Gophish. The form includes the following fields and options:

- Ім'я:** A text input field containing 'one'.
- Шаблон електронного листа:** A dropdown menu with 'Повторний вхід у WordPress' (WordPress login again) selected.
- Цільова сторінка:** A dropdown menu with 'Вхід WordPress.org' (WordPress.org login) selected.
- URL-адреса:** A text input field with a help icon, containing 'http://127.0.0.1:80'.
- Дата запуску:** A date and time picker showing 'November 30th 2025, 6:42 pm'.
- Надсилати електронні листи (необов'язково):** A checkbox that is currently unchecked.
- Профіль надсилання:** A dropdown menu with 'фіш-профіль' (phishing profile) selected.
- Buttons:** A button with an envelope icon and the text 'Надіслати тестовий електронний лист' (Send test email) is visible next to the profile dropdown.
- Групи:** A text input field with a dropdown arrow, containing 'x фішинг' (x phishing).
- Footer:** Two buttons at the bottom right: 'Закрити' (Close) in grey and 'Запуск кампанії' (Launch campaign) in green.

Рис 3.12 – Створення кампанії

Після формування кампанії фішингові листи почали надходити на вибрані поштові адреси.

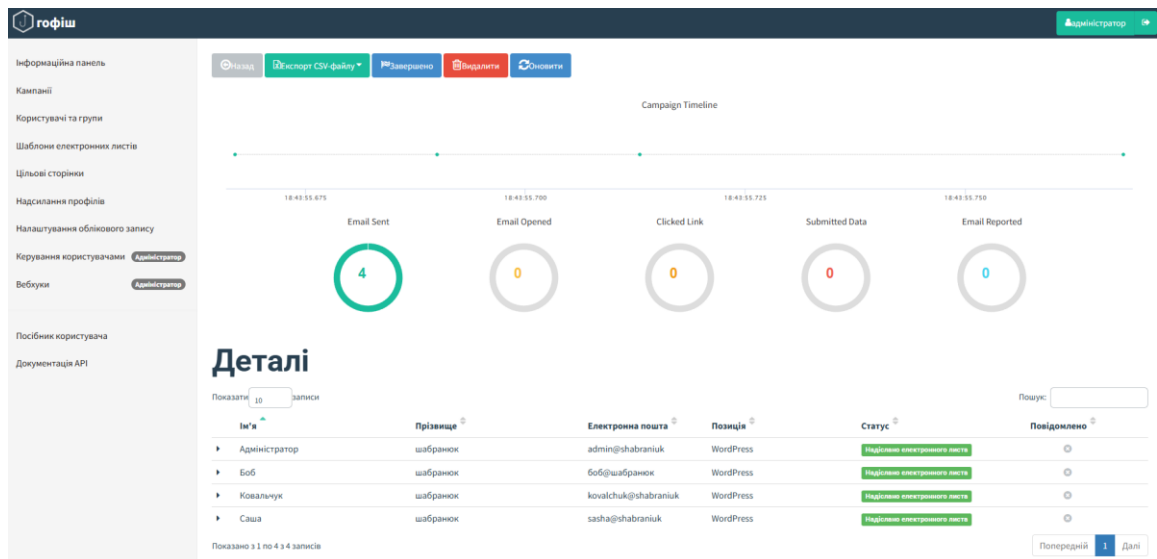
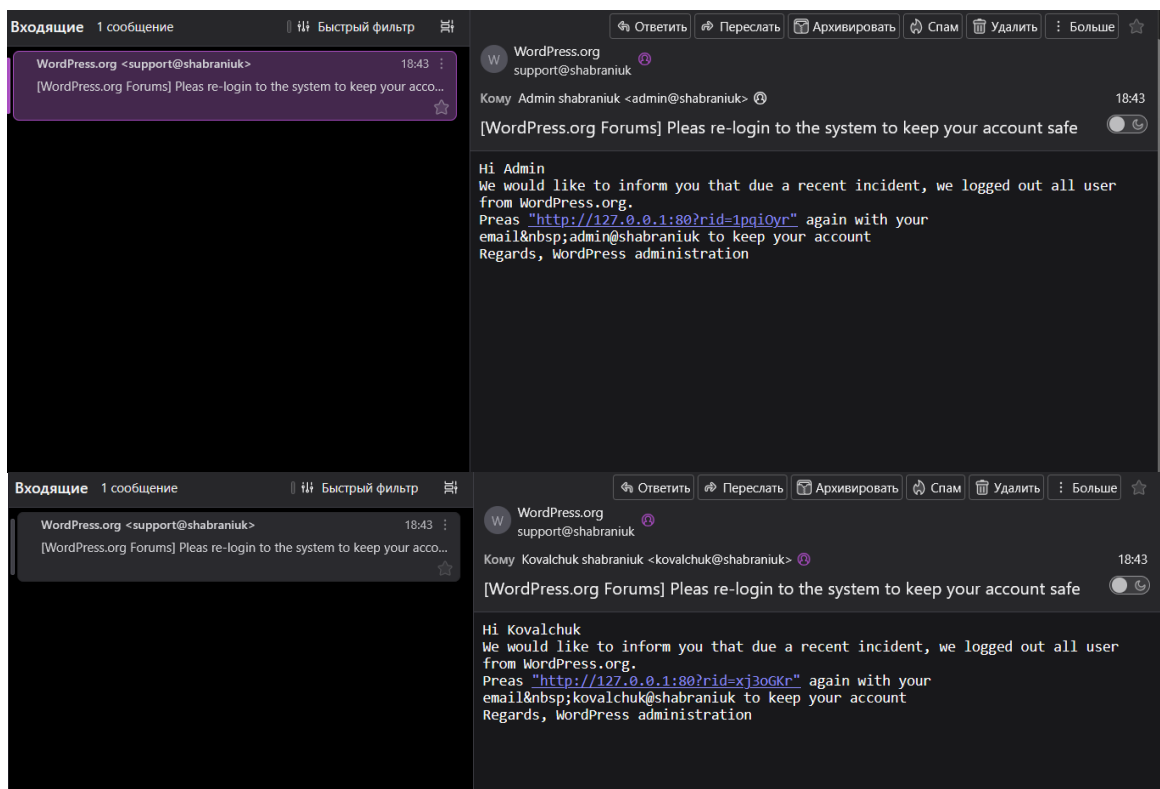


Рис 3.13 – Моніторинг компанії

Розсилку було успішно доставлено на всі чотири зазначені електронні адреси. Один із отримувачів уже відкрив повідомлення, ознайомився з ним і перейшов на тестову фішингову сторінку, де залишив свої дані (Рис.3.14).



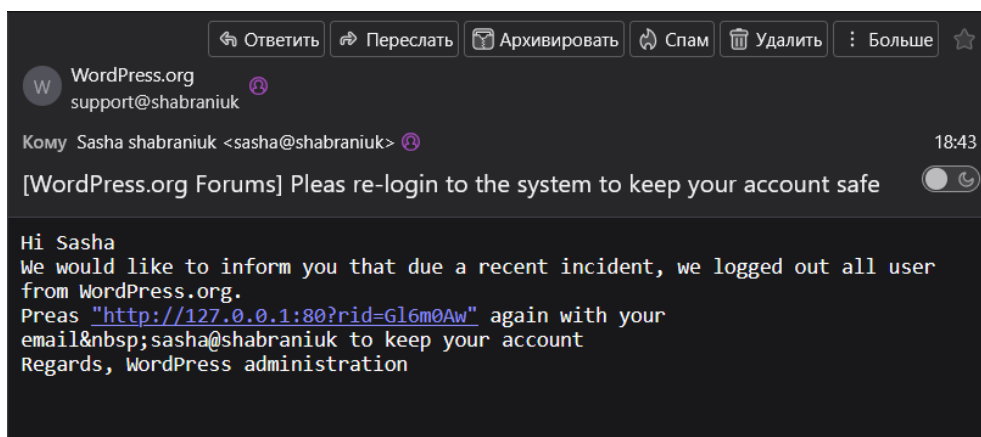


Рис 3.14 – 3.15 – Отримані листи на скриньках.

Після переходу за отриманим посиланням користувач потрапляє на імітовану вебсторінку, зовнішній вигляд якої максимально наближений до справжнього сайту, тому на перший погляд вона не викликає жодних підозр (Рис.3.16)

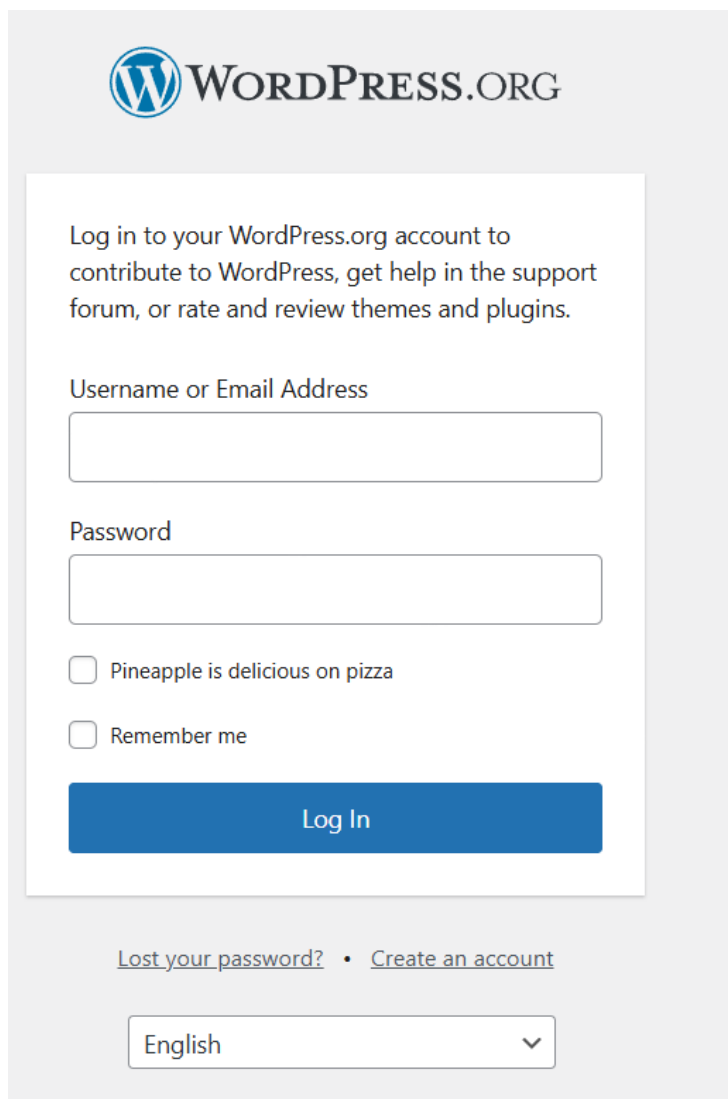


Рис 3.16 – Підроблений сайт.

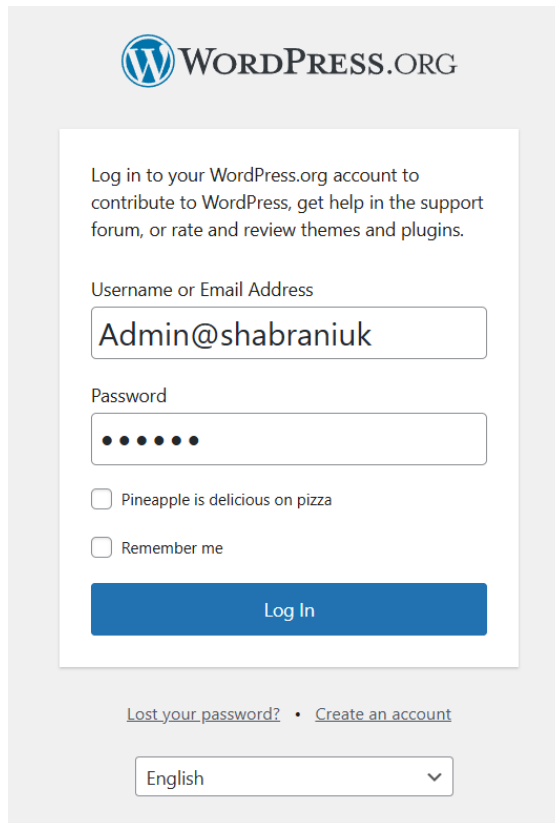


Рис 3.17 – Ведення даних

Після того як користувач вводить свої дані у форму, система одразу перенаправляє його на офіційний сайт WordPress.org, тому ззовні все виглядає абсолютно звично. Однак у подібних ситуаціях важливо пам'ятати, що ненадійні сторінки чи підроблені сервіси можуть перехоплювати введену інформацію. Для адміністратора платформи, як-от Gophish, у звітах може відображатися отримання введених даних, що використовується в навчальних тренуваннях із кібербезпеки. Такий приклад нагадує, наскільки важливо перевіряти справжність сайтів, посилань та форм перед тим, як вводити особисті або конфіденційні відомості.

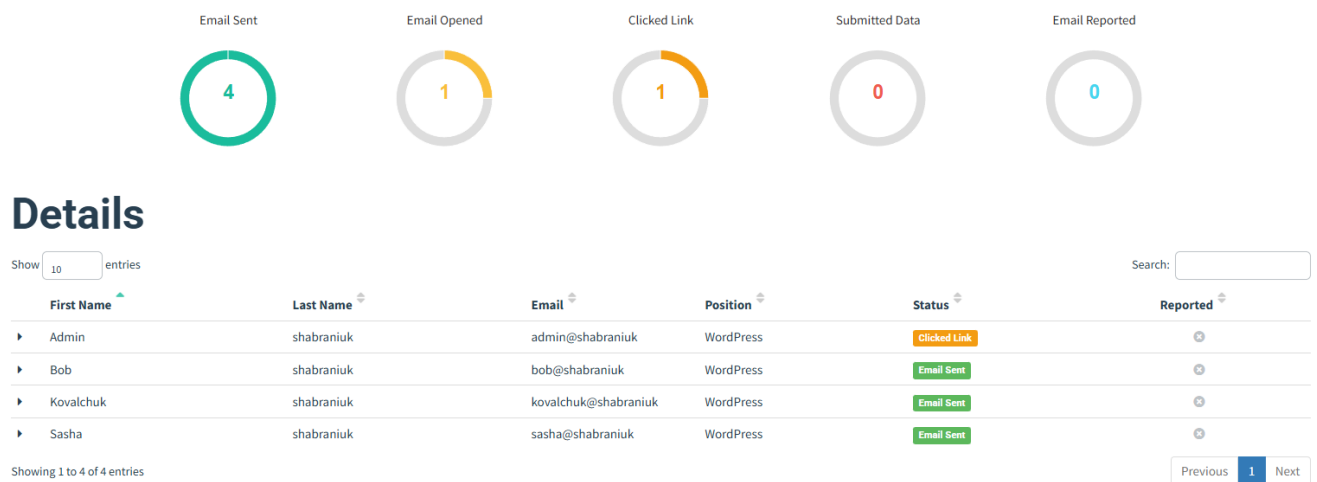


Рис 3.18 – Admin@shabraniuk переглянув повідомлення

Після того як адміністратор ввів свої логін і пароль, система перенаправила його на офіційний сайт WordPress, тож зовні все виглядало звичайно. Водночас у Gophish з'явилася інформація про введені дані, що свідчить про фіксацію цього тестового сценарію в межах навчального тренування з кібербезпеки.

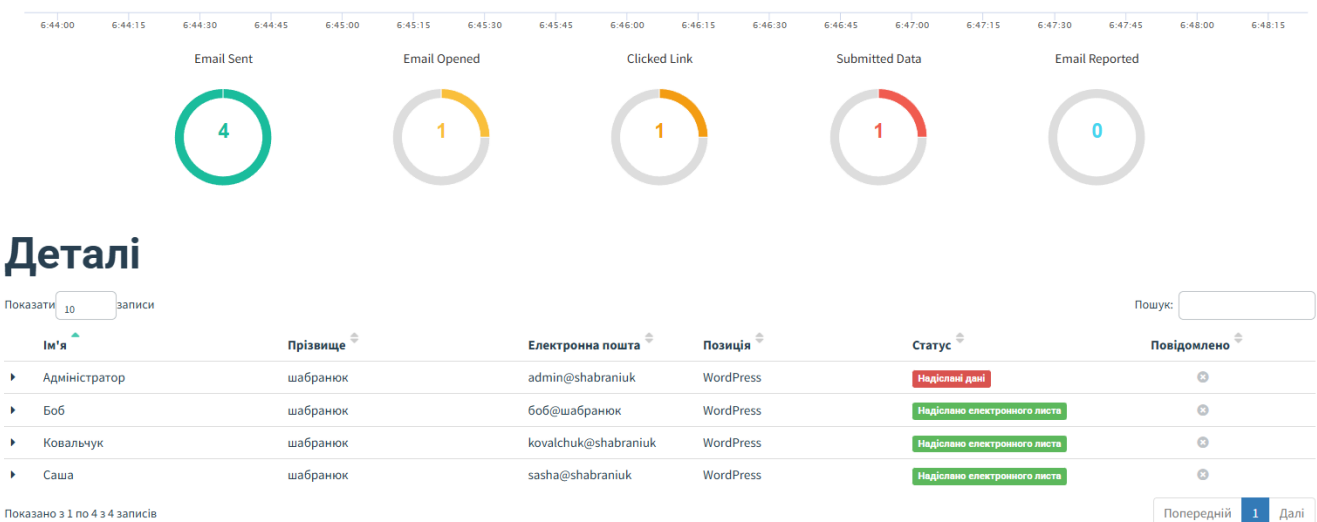


Рис 3.19 – Відправлені дані користувача

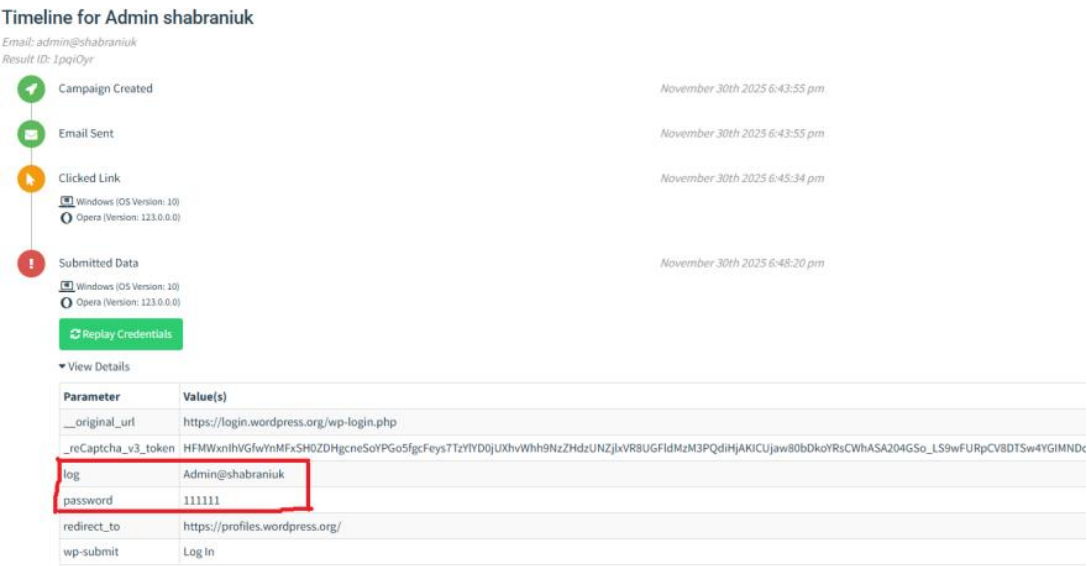


Рис 3.20 – Логін та пароль користувача

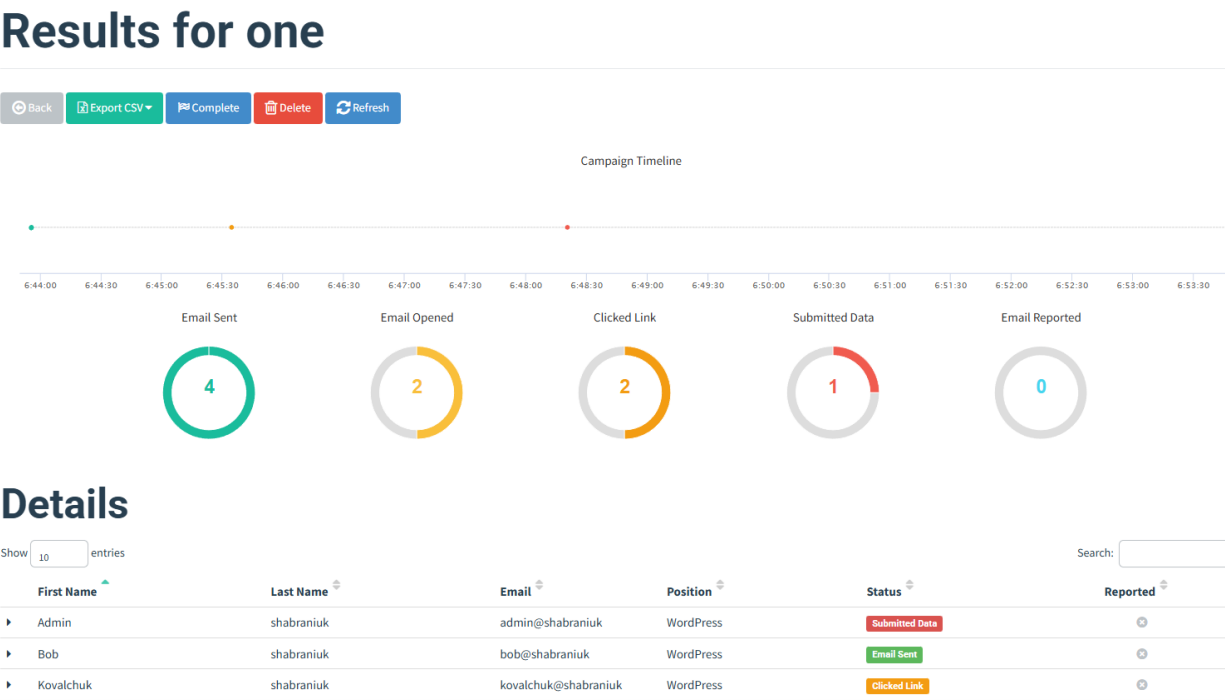


Рис 3.21 – Інший користувач тільки переглянув повідомлення

Timeline for Sasha shabraniuk

Email: sasha@shabraniuk

Result ID: G6m0Aw

The timeline shows the following events:

- Campaign Created** (November 30th 2025 6:43:55 pm)
- Email Sent** (November 30th 2025 6:43:55 pm)
- Clicked Link** (November 30th 2025 6:56:03 pm)
 - Windows (OS Version: 10)
 - Opera (Version: 123.0.0.0)
- Submitted Data** (November 30th 2025 6:56:20 pm)
 - Windows (OS Version: 10)
 - Opera (Version: 123.0.0.0)

[Replay Credentials](#)

▼ View Details

Parameter	Value(s)
__original_url	https://login.wordpress.org/wp-login.php
log	Шабранюк
password	Sanjasanja
pineapple	yes-it-is
redirect_to	https://profiles.wordpress.org/
rememberme	forever
wp-submit	Log In

Рис 3.22 – Дані іншого користувача

Після завершення навчального фішингового сценарію важливо перейти до питання безпеки та розглянути способи протидії подібним загрозам. Тому варто відкрити локальний поштовий сервер і переглянути доступні механізми захисту. Одним із корисних інструментів є функція **Auto-ban**, яка автоматично блокує підозрілу активність, наприклад занадто часті спроби входу або нетипові підключення. Аналіз і правильне налаштування цього модуля допомагають підвищити загальний рівень безпеки поштової системи та запобігати небажаним діям у майбутньому.

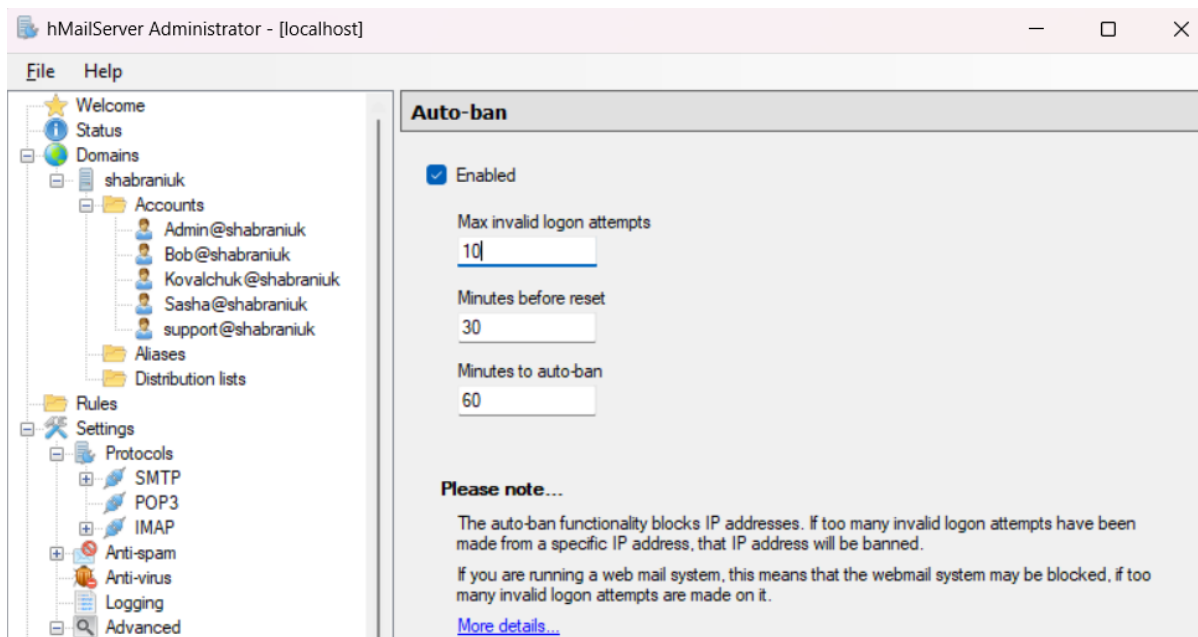


Рис 3.23 – Функція Auto-ban

Ще одним важливим елементом захисту є своєчасне блокування або відключення поштових акаунтів, які надсилають небажані чи фішингові посилання. На локальному сервері адміністратор може оперативно відстежувати підозрілу активність — наприклад, масову розсилку повідомлень із сумнівним вмістом. Якщо такий акаунт виявлено, його можна тимчасово призупинити або повністю вимкнути, щоб припинити подальше поширення небезпечних листів. Подібні дії дозволяють мінімізувати ризики, захистити інших користувачів у мережі та запобігти можливим інцидентам у майбутньому.

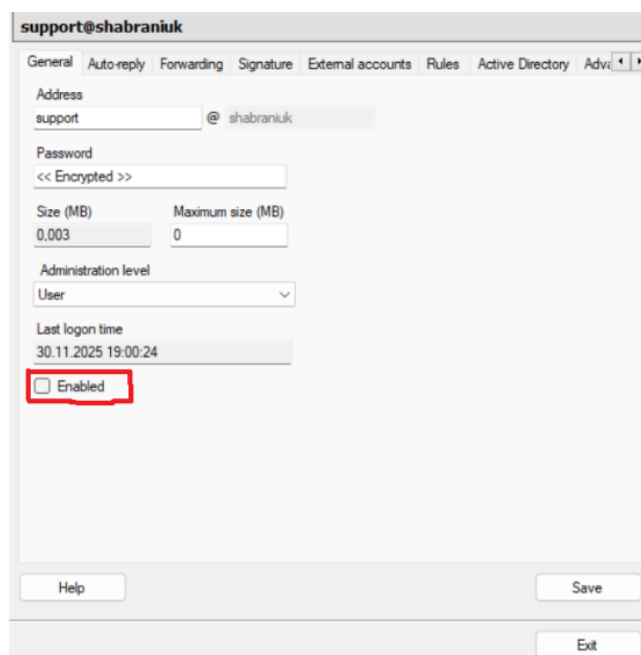


Рис 3.24 – Відключення support@shabraniuk від локального сервера

Після виконаних заходів захисту можна помітити, що Gophish більше не здатний розпочати навчальну симуляцію. Це відбувається тому, що локальний поштовий сервер заблокував IP-адресу, з якої надходили підозрілі запити. У списку автоматичних блокувань видно IP **192.168.0.102**, який потрапив під *auto-ban* через надмірну або нетипову активність.

Подібне блокування є очікуваним результатом роботи захисних механізмів: сервер розцінює часті або нестандартні запити як потенційну загрозу та автоматично блокує їх, запобігаючи подальшій розсилці небажаних повідомлень. Це демонструє, що налаштовані засоби безпеки ефективно працюють і можуть стримувати небезпечні дії на ранніх етапах.

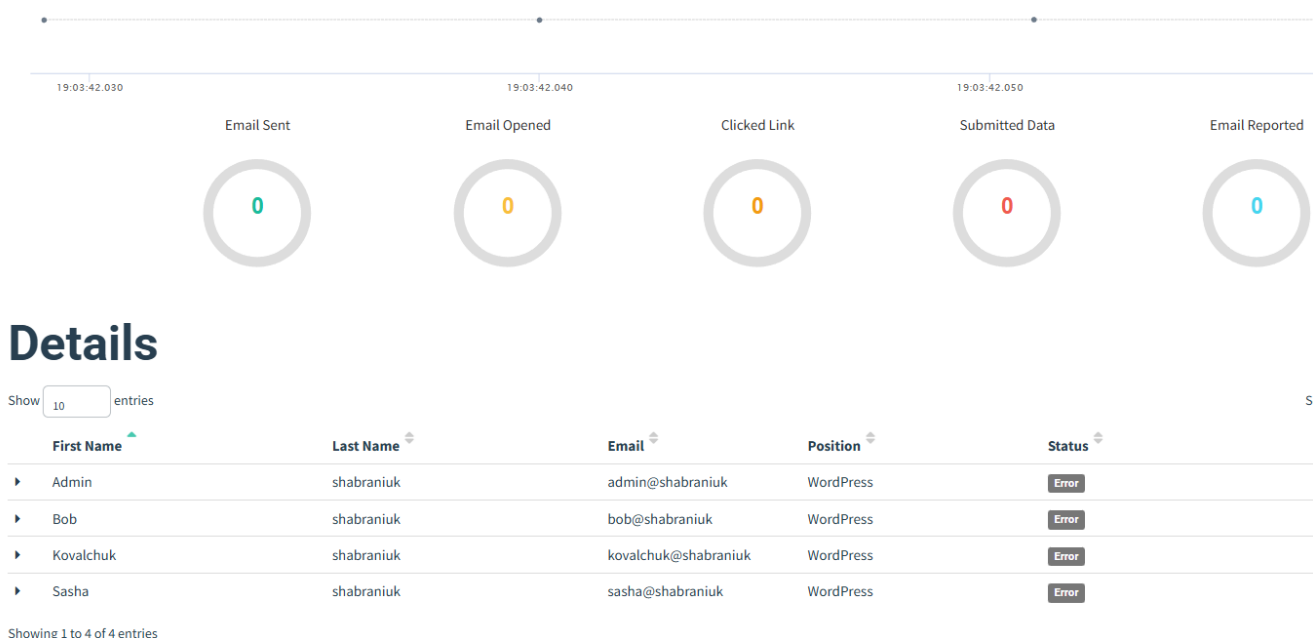


Рис 3.25 – Помилка Gophish

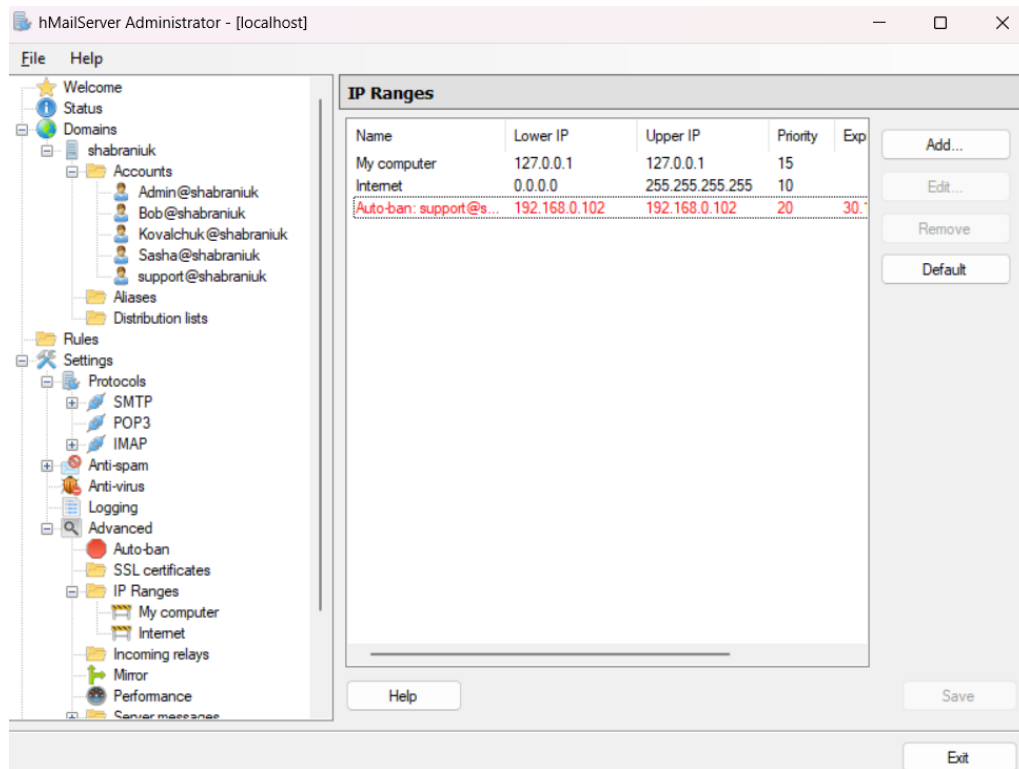


Рис 3.26 – Auto-ban 192.168.102

Також одним із способів підвищення безпеки є вимкнення певних можливостей у конфігурації локального поштового сервера. Наприклад, адміністратор може відключити протокол SMTP, а також заборонити надсилання листів у напрямках local-to-local та local-to-external.

Чому це робиться?

- **Блокування SMTP.** Вимкнення SMTP тимчасово зупиняє будь-які спроби надсилання пошти через сервер. Це особливо корисно, коли виявлено підозрілу активність — таким чином запобігають подальшому розповсюдженню небажаних чи потенційно небезпечних повідомлень.
- **Вимкнення local-to-local.** Якщо поштові акаунти всередині локальної мережі не можуть надсилати листи одне одному, це зменшує ризик розповсюдження фішингових чи шкідливих листів всередині організації. Так адміністратор обмежує можливість "внутрішнього" поширення загрози.
- **Вимкнення local-to-external.** Заборона надсилання пошти з локальних адрес на зовнішні сервіси запобігає виходу підозрілих повідомлень за межі мережі. Це дозволяє утримувати ситуацію під контролем і не допустити надсилання потенційно небезпечних листів стороннім користувачам.

Таке обмеження функціональності тимчасово ізолює поштовий сервер, щоб зупинити розсилку та мінімізувати наслідки, доки адміністратор аналізує логіку подій і налаштовує додаткові засоби захисту.

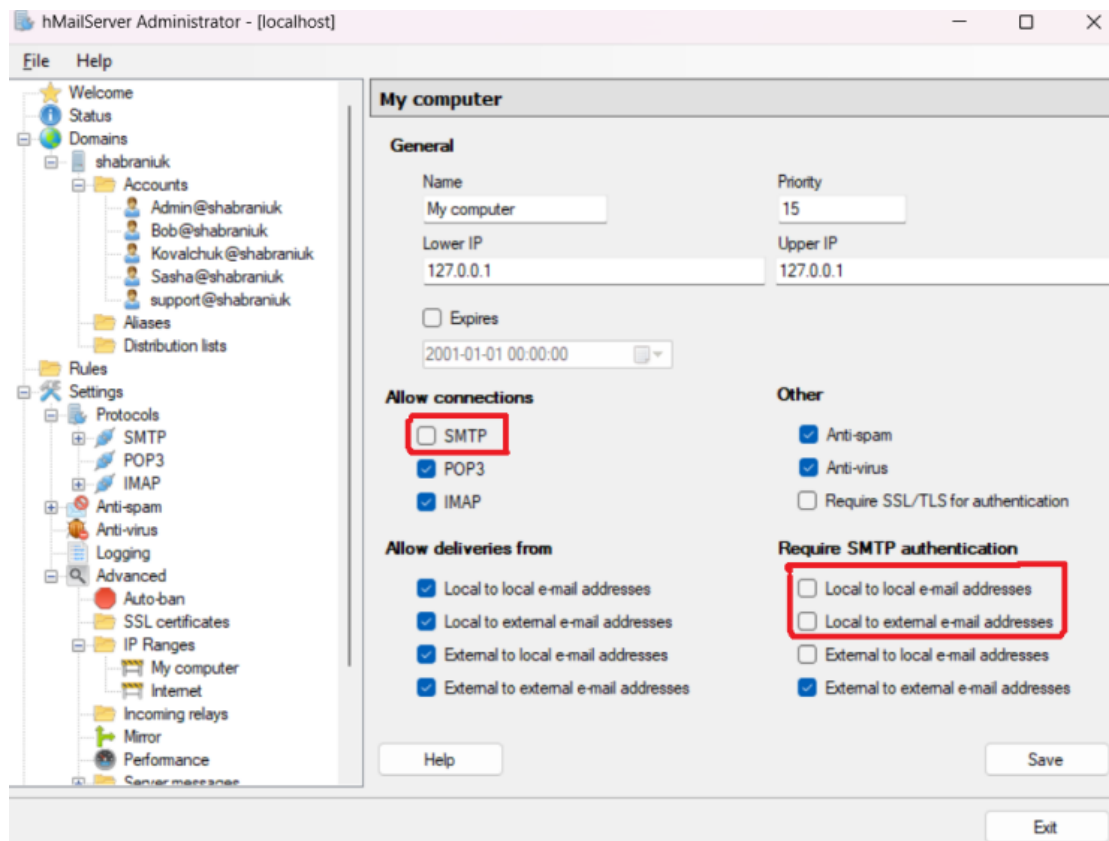


Рис 3.27 – Відключення

У процесі тестування захисних механізмів локального поштового сервера можна спостерігати, що платформа Gophish припиняє роботу та виводить повідомлення: «Перевищено максимальну кількість спроб підключення – EOF». Дане повідомлення є показником того, що сервер розірвав з'єднання у відповідь на некоректні або надмірні спроби підключення з боку клієнта.

Скорочення EOF (End Of File) вказує на те, що під час встановлення з'єднання сервер передчасно завершив обмін даними та закриття сесії. Це характерна поведінка для поштових серверів, коли спрацьовують механізми безпеки, спрямовані на захист від підозрілої активності.

Деталі

Показати 10 записи

Ім'я	Прізвище	Електронна пошта	Позиція	Статус
Адміністратор	шабраниук	admin@shabraniuk	WordPress	Помилка

Хронологія для адміністратора shabraniuk

Електронна пошта: admin@shabraniuk
ID результату: SqKhfz

- Кампанія створена 30 листопада 2025 р., 19:10:22
- Помилка надсилання електронного листа 30 листопада 2025 р., 19:10:22
 - Переглянути деталі
 - Помилка: Перевищено максимальну кількість спроб підключення – EOF

Боб	шабраниук	боб@шабраниук	WordPress	Помилка
Ковальчук	шабраниук	kovalchuk@shabraniuk	WordPress	Помилка
Саша	шабраниук	sasha@shabraniuk	WordPress	Помилка

Рис 3.28 – Перевищено максимальну кількість спроб підключення – EOF

Також одним із ключових засобів захисту електронної пошти є використання протоколів SSL/TLS, які забезпечують шифрування трафіку між клієнтом та поштовим сервером. Увімкнення обов'язкової автентифікації через SSL/TLS значно підвищує рівень безпеки системи, оскільки передавання логінів, паролів та інших даних відбувається у зашифрованому вигляді.

У випадку, коли на сервері активовано вимогу встановлювати з'єднання лише через SSL або TLS, будь-яка система чи клієнт, який не підтримує або неправильно налаштований для роботи з захищеним з'єднанням, не може успішно пройти автентифікацію. У таких умовах сервер відхиляє запити, що надходять з некоректними параметрами шифрування, і достроково припиняє сесію.

Хронологія для адміністратора shabraniuk

Електронна пошта: admin@shabraniuk
ID результату: 4x6t5Ed

- Кампанія створена 30 листопада 2025 р., 19:20:46
- Помилка надсилання електронного листа 30 листопада 2025 р., 19:20:46
 - Переглянути деталі
 - Помилка: Перевищено максимальну кількість спроб підключення – 530. Для автентифікації потрібне SSL/TLS-з'єднання.

Боб	шабраниук	боб@шабраниук	WordPress	Помилка
Ковальчук	шабраниук	kovalchuk@shabraniuk	WordPress	Помилка
Саша	шабраниук	sasha@shabraniuk	WordPress	Помилка

Рис 3.29 – Помилка через SSL/TLS

Також для запобігання фішинговим розсилкам у hMailServer було створено спеціальне правило блокування фішингової розсилки. Воно дає змогу автоматично визначати листи, що відповідають ознакам фішингової атаки (зокрема, розсилки, сформовані Gophish), та одразу зупиняти їх відправлення. Таке правило дозволяє контролювати поштовий трафік, мінімізувати ризики компрометації користувачів і імітує механізми корпоративного захисту, що застосовуються для протидії фішинговим загрозам.

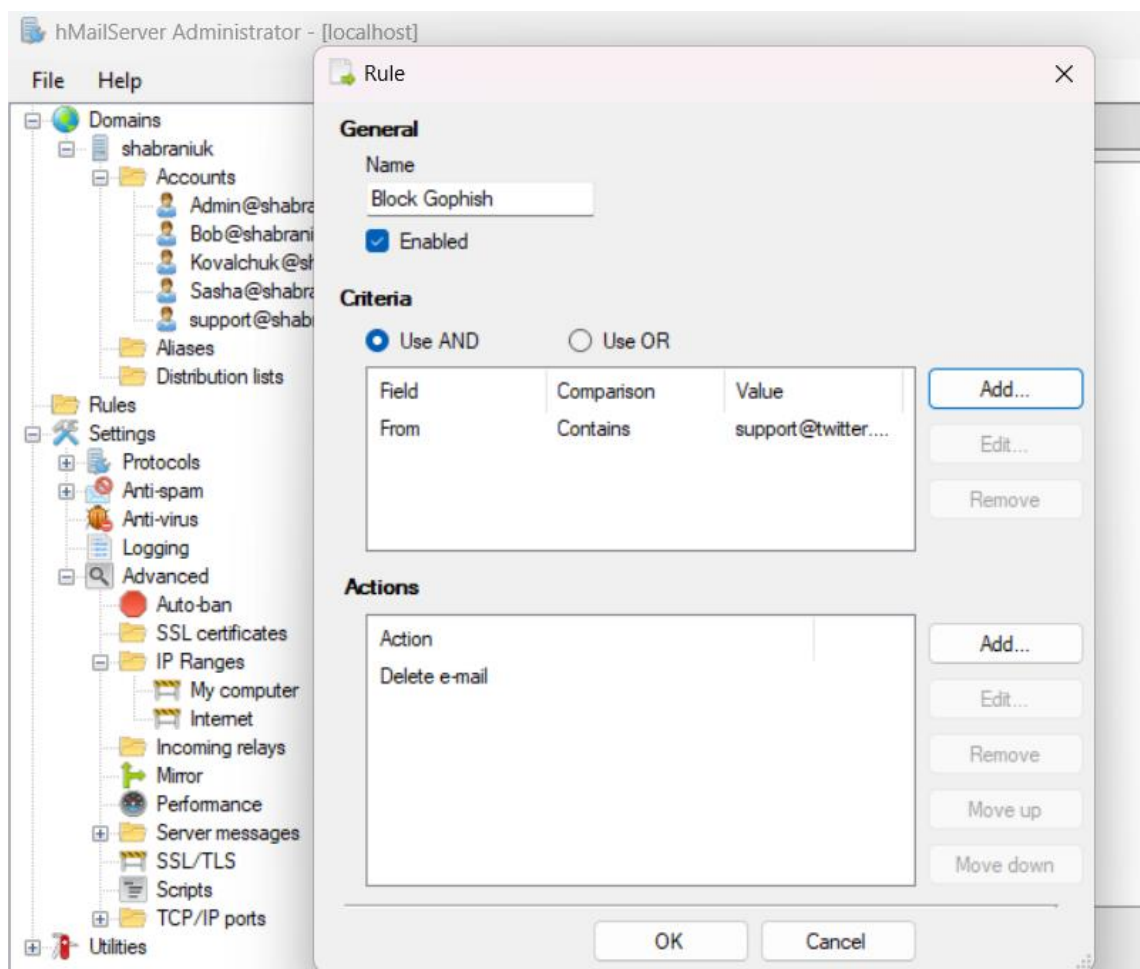


Рис 3.31 – Правило Block Gophish

Другий етап дослідження

Після проведення дослідження методів атаки та захисту від фішингових розсилок на локальному поштовому сервері потрібно доцільно розглянути, як подібні загрози обробляє один із найпоширеніших та технологічно розвинених поштових сервісів — **Gmail**. Завдяки багаторівневій системі безпеки Gmail є

показовим прикладом того, як сучасні хмарні рішення реалізують виявлення, фільтрацію та блокування потенційно шкідливих повідомлень.

Фішингові розсилки виконуватимуться безпосередньо через Gophish. Налаштування проводиться так само, як і під час роботи з локальним сервером, але замість внутрішніх адрес у сценарій будуть додані облікові записи зовнішніх поштових сервісів — виключно в дозволених та навчальних умовах.

Edit Group ×

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

[+ Add](#)

Show entries Search:

First Name	Last Name	Email	Position	
root	bob	rootbob19@gm...	WordPress	
Sasha	Kotoshuk	sashakotoshuk1...	WordPress	
Ser	Koval	serkoval1909@...	WordPress	
Олександр	Шабранюк	shabraniuk@g...	WordPress	

Showing 1 to 4 of 4 entries

[Previous](#) [1](#) [Next](#)

[Close](#) [Save changes](#)

Рис 3.32 – Додавлені google пошти

Наступним кроком є налаштування SMTP-сервера, через який виконуватиметься надсилання тестових електронних повідомлень. Оскільки Gophish не має власного вбудованого механізму відправлення листів, для навчальних демонстрацій можна використовувати сторонній поштовий сервіс, що підтримує SMTP-доступ. У межах дослідження як приклад застосовується зовнішній SMTP-сервер із адресою smtp.gmail.com та портом 587.

Під час попереднього налаштування на локальному сервері для надсилання листів використовувався стандартний порт 25. У разі переходу до зовнішнього SMTP-сервера параметри змінюються відповідно до вимог постачальника. Для

демонстрації роботи Gophish застосовується сервер Gmail із адресою smtp.gmail.com, який працює через порт 587. Це дозволяє наочно показати різницю між локальними й зовнішніми налаштуваннями SMTP у навчальному середовищі.

Edit Sending Profile

Name:

Interface Type:

SMTP

SMTP From: ?

Host:

Username:

Password:

☒ Ignore Certificate Errors ?

Email Headers:

Show entries Search:

Header	Value
No data available in table	

Рис 3.33 – Налаштування поштового сервера

Для підключення необхідно вводити не пароль від електронної скриньки, а спеціальний пароль застосунку, який створюється в налаштуваннях у розділі “Безпека” (Security).

Щоб його згенерувати, потрібно зайти в керування обліковим записом електронної пошти та відкрити параметри безпеки, тому що під час спроби

надіслати тестовий електронний лист через Gophish було зафіксовано помилку автентифікації:

534 5.7.9 Потрібен пароль програми. Перевищено максимальну кількість спроб підключення.”

Ця помилка виникає в тому випадку, коли для доступу до зовнішнього сервера Gmail використовується звичайний пароль облікового запису. Оскільки служба Google блокує такі підключення з міркувань безпеки, сервер SMTP вимагає застосування спеціального пароля додатка, який створюється у налаштуваннях Google-акаунту при увімкненій двофакторній автентифікації.

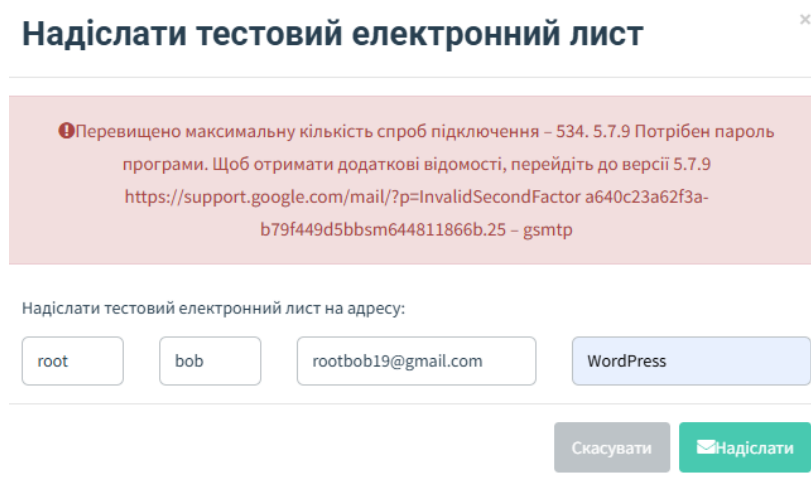


Рис 3.34 – Помилка gmail

Таким чином, проблема пов'язана не з конфігурацією Gophish чи локального сервера, а з політикою безпеки Gmail, яка забороняє використання не коректних програм без окремого пароля доступу. Для успішної автентифікації необхідно створити App Password у налаштуваннях Google та ввести його як SMTP-пароль.

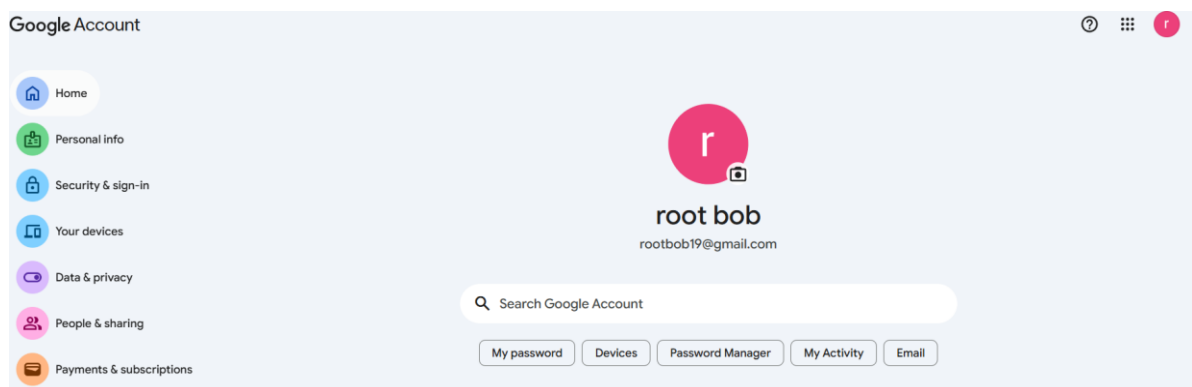


Рис 3.35 – Управління google

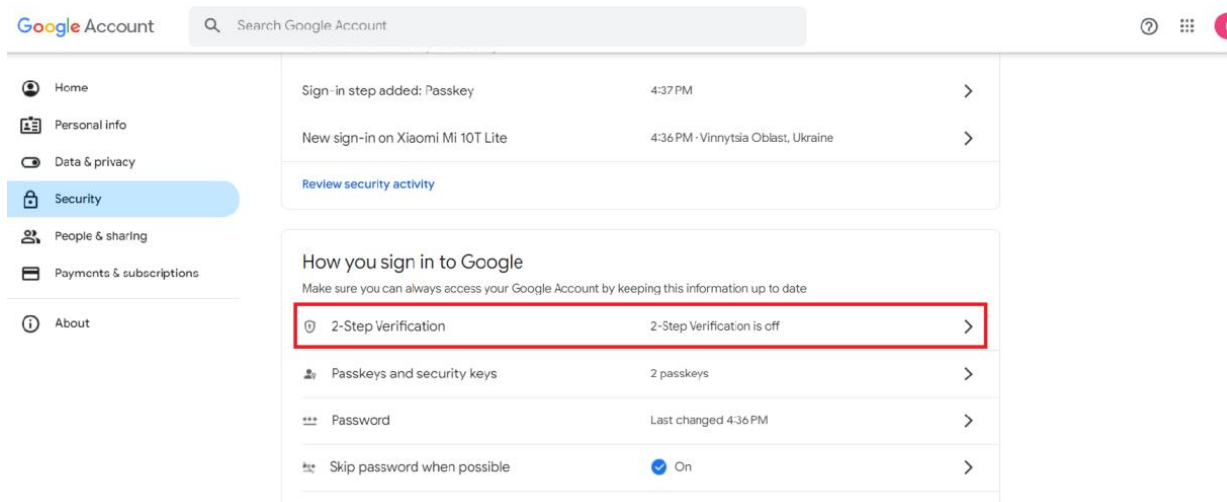


Рис 3.36 –2FA пошти

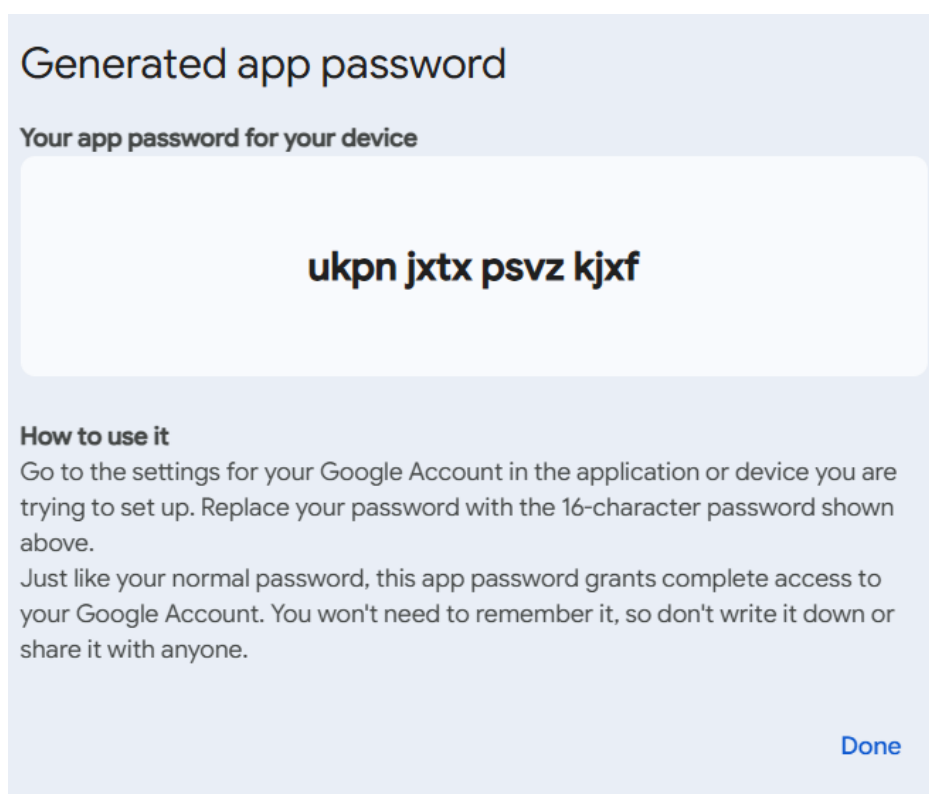


Рис 3.37 – Пароль для застосунку

Після створення пароля для застосунку в розділі **Безпека**, користувач може підвищити рівень захисту, увімкнувши **двофакторну автентифікацію**. Вона забезпечує додаткову перевірку особи та допомагає захистити доступ навіть тоді, коли основний пароль може бути відомий стороннім. Після активації 2FA можна сформувати окремий пароль для застосунків і надалі безпечно керувати електронною поштою та іншими можливостями Gophish з посиленням захистом.

Надіслати тестовий електронний лист

×

✔ Листа відправлено!

Надіслати тестовий електронний лист на адресу:

root

bob

rootbob19@gmail.com

WordPress

Скасувати

Надіслати

Рис 3.37 – Тестове повідомлення на gmail.com.

Успішність налаштування підтверджується тим, що тестове повідомлення було коректно відправлене та відображене у папці «Надіслані». Це свідчить про те, що SMTP-сервер працює належним чином, з'єднання встановлено коректно, і система готова до подальшого надсилання електронних листів.

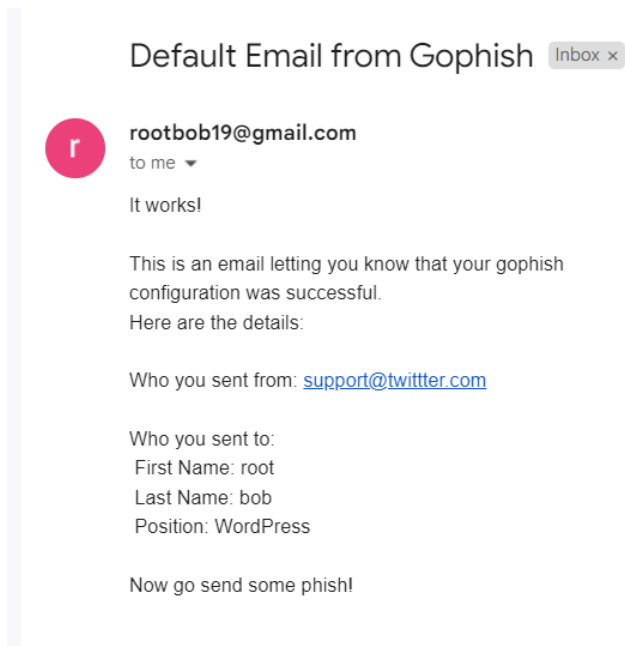


Рис 3.38 – Отримання повідомлення

Нова кампанія



Ім'я:

one

Шаблон електронної пошти:

Повторний вхід у WordPress

Цільова сторінка:

Увійдіть на WordPress.org

URL: ?

http://127.0.0.1:80

Дата запуску

December 6th 2025, 3:39 pm

Надсилати електронні листи (необов'язково) ?

Надсилання профілю:

phishprofile

Надіслати тестовий електронний лист

групи:

фішинг

Закрити

Запуск кампанії

Рис 3.39 – Створення компанія для gmail.com

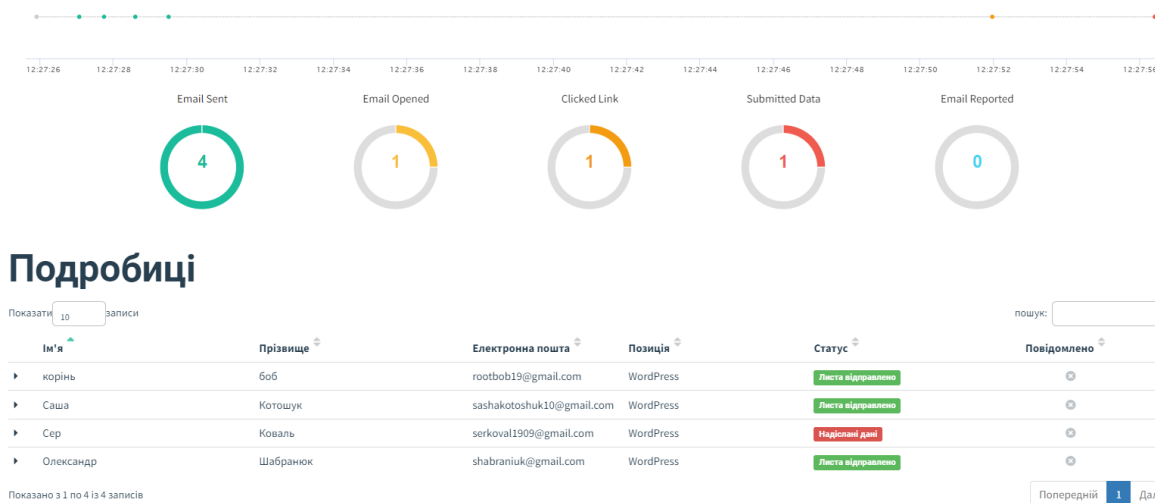


Рис 3.40 – Розсилка розпочата

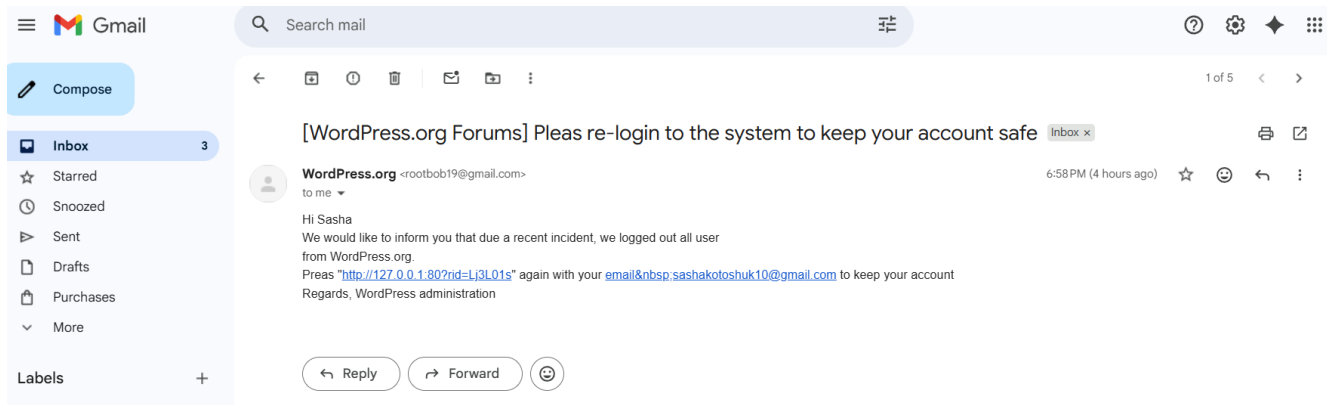


Рис 3.41 – Отримане повідомлення на Gmail

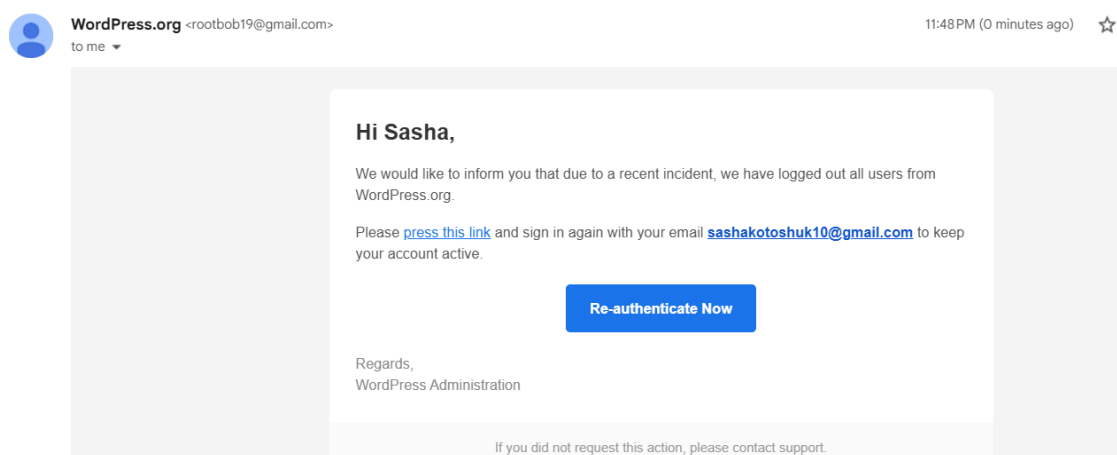


Рис 3.42 – Отримане повідомлення на Gmail через HTML

!

Надіслані дані

7 грудня 2025 р., 23:35:19

Windows (версія ОС: 10)

Опера (версія: 124.0.0.0)

Облікові дані для повторного відтворення

▼Переглянути деталі

Параметр	Значення(я)
__оригінальна_URL-адреса	https://login.wordpress.org/wp-login.php
_reCaptcha_v3_token	HFemhwaRFRNAIwe1hFVEJUVQMwMi4Pd24uNQIWNi0uBjIwKj40Gnx4ERxqfDJQPDEaLT1mHhsDU11KeDcgdgN1VTQdayE0IAsjJz0_KtQFSGkvUi4oZlZ9HGUBCloUBigvK2YbfzNjQXJIVGB-SF5-S2tMawFQBUgzeGpxdnonLw8UCWoBHHRBbn5RWHorQAUXMi4tEjIAljwhGA9
колода	support@gmail.com
пароль	Саша1909
перенаправити_на	https://profiles.wordpress.org/
wp-submit	Увійти

Рис 3.43 – Отримані дані від користувача

Після того як у ході експерименту оригінальний шаблон листа був замінений на спрощений HTML-текст, система фільтрації Gmail класифікувала

повідомлення як підозріле. Це пояснюється тим, що такі листи часто мають ознаки, характерні для автоматично згенерованих або фішингових повідомлень.

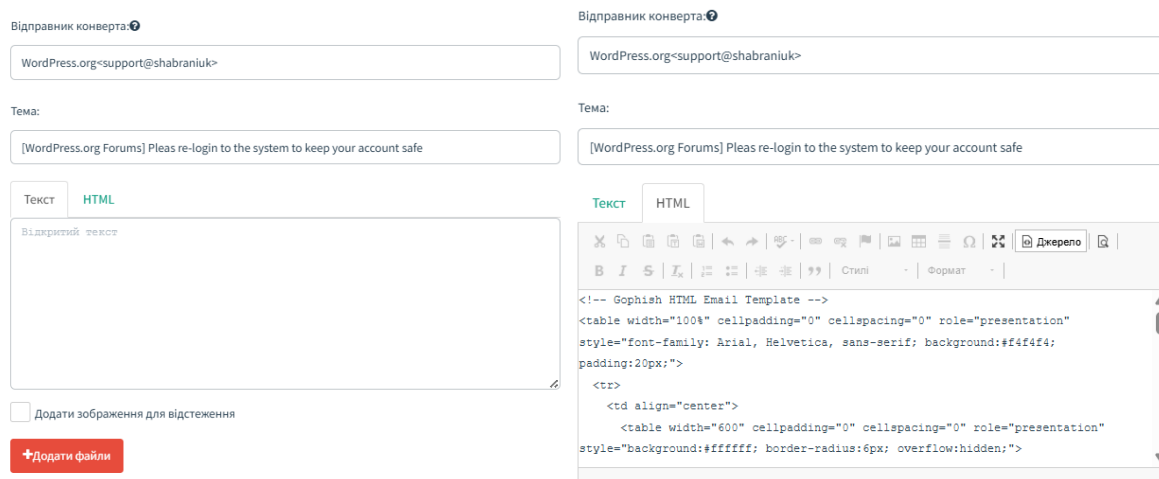


Рис 3.43 – Заміна листа

Спрощення листа до елементарного HTML-тексту призвело до того, що повідомлення втратило ознаки легітимного листа та набуло ознак фішингової активності. Як наслідок, система безпеки Gmail класифікувала його як підозріле та автоматично перемістила до папки «Спам» (Рис 3.45).

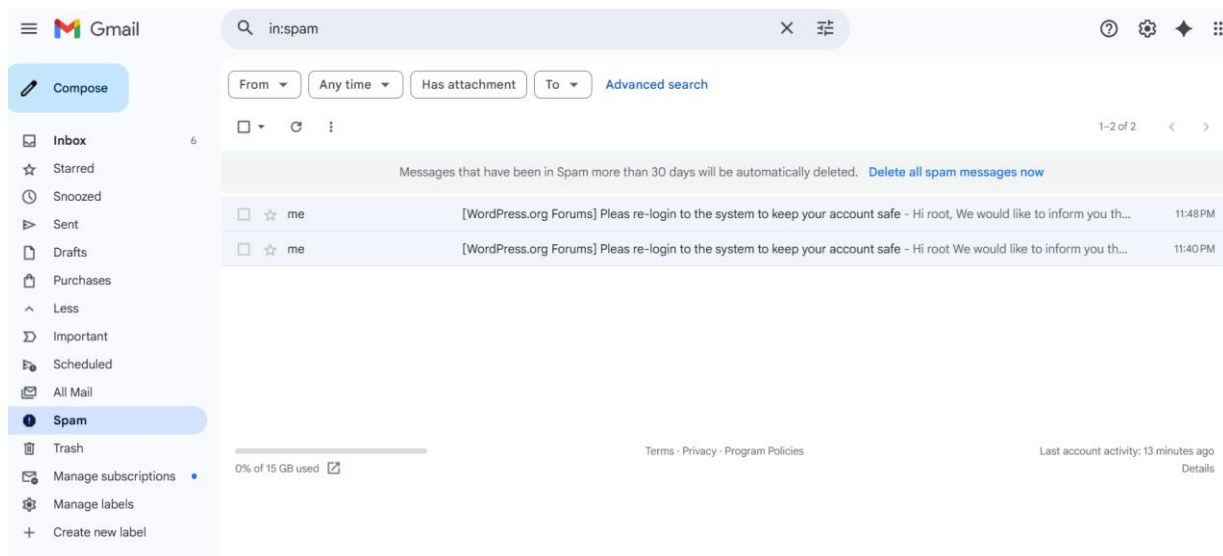


Рис 3.45 – Gmail spam

Також здійснювалося ще одне відправлення з сервера, який не належить домену, зазначеному у полі «Від кого», що призвело до невідповідності механізмів автентифікації електронної пошти, таких як SPF, DKIM та DMARC. Через це поштовий сервіс не зміг підтвердити, що лист справді походить від організації, ім'я якої використано в адресі відправника. Додатково наявність

посилання на нестандартну або локальну вебадресу та текст, який містить заклик повторно авторизуватися, підвищили рівень підозри. Сукупність цих факторів спричинила автоматичне спрацьовування захисних механізмів Gmail і відображення банера з попередженням про можливу фішингову атаку.

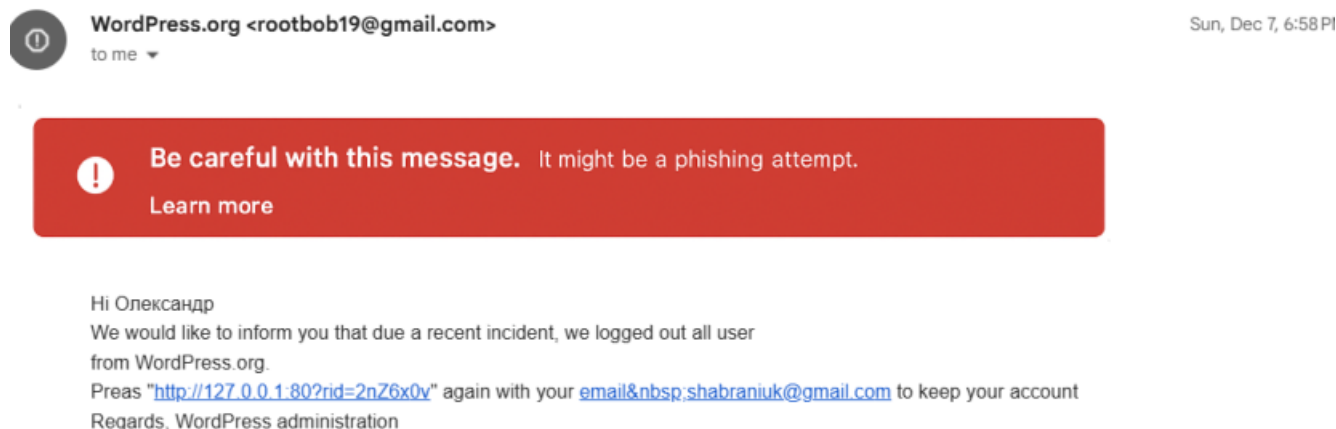


Рис 3.46 – Червоний банер від Gmail

На зображенні (рис 3.46) показано інтерфейс електронної пошти Gmail, у якому відкрито лист, що був автоматично позначений системою як потенційно небезпечний. У верхній частині повідомлення відображається великий червоний банер із попередженням **Be careful with this message. It might be a phishing attempt**, який вказує на те, що Gmail виявив ознаки можливого фішингу. Безпосередньо під попередженням розміщений текст листа, оформлений від імені **WordPress.org**, де отримувача просять повторно авторизуватися за посиланням. Наявність такого банера демонструє, що служба безпеки Gmail автоматично аналізує структуру та вміст листа й попереджає користувача у випадку, коли повідомлення може становити ризик.

Поява сірого попереджувального банера в інтерфейсі Gmail свідчить про те, що поштовий сервіс виявив потенційні ознаки небезпеки в отриманому повідомленні, однак не класифікував його як однозначно фішингове (рис 3.47).

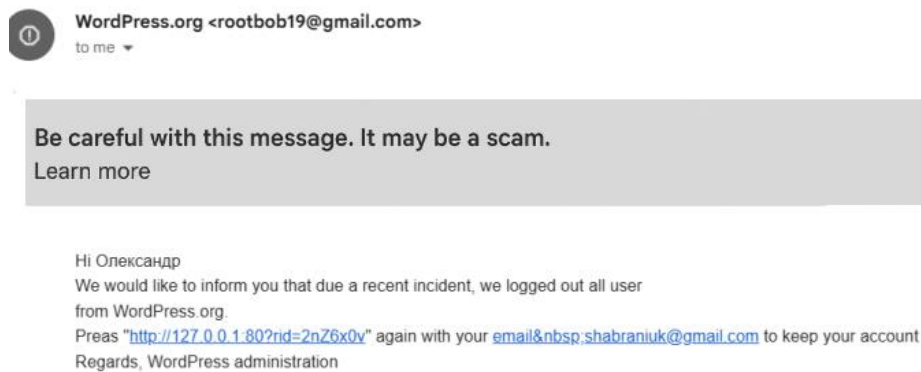


Рис 3.47 – Сірий банер від Gmail

Такий банер з'являється у випадках, коли лист формально проходить базові перевірки доставки, але має нетипові характеристики, зокрема використання маловідомого або неперевіреного сервера відправлення, імітацію відомого сервісу або наявність підозрілого посилання. Gmail у цьому випадку застосовує превентивний механізм захисту, попереджаючи користувача про можливі ризики та рекомендує проявляти обережність під час взаємодії з листом. Це демонструє гнучкий підхід системи безпеки, коли повідомлення не блокується повністю, але його рівень довіри знижується.

Також було навмисно використано тестову конфігурацію поштового надсилання, у якій домен відправника не мав коректно налаштованих механізмів автентифікації (SPF, DKIM та DMARC). Також адреса відправника не відповідала реальному домену SMTP-сервера, з якого здійснювалося надсилання повідомлення (Рис 3.48).

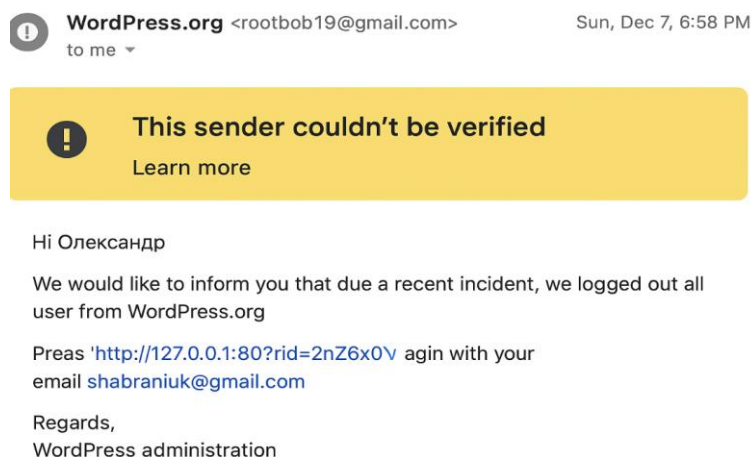


Рис 3.48 – Попередження Gmail про неперевіреного відправника (Unverified sender)

У результаті Gmail не зміг підтвердити справжність відправника та автоматично застосував захисний механізм, відобразивши попередження **This sender couldn't be verified**. Це свідчить про те, що поштовий сервіс аналізує технічні заголовки листа та виявляє невідповідності між доменом, сервером надсилання та політиками автентифікації.

Також поштова служба Gmail надає користувачам можливість вручну повідомляти про фішингові повідомлення за допомогою функції Report phishing (Рис 3.49).

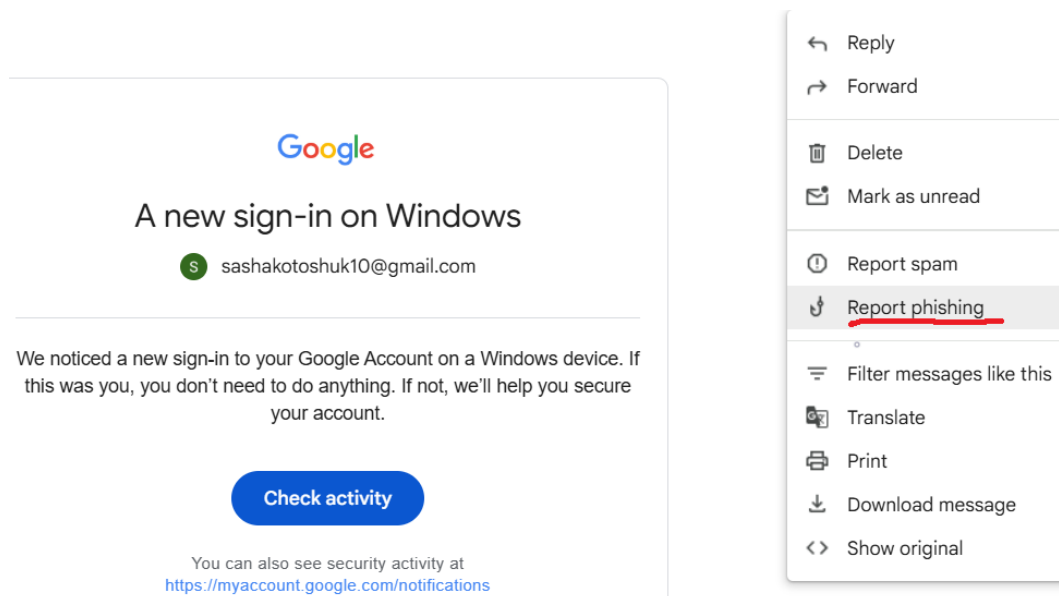


Рис 3.49 – Report phishing

Ця функція застосовується незалежно від платформи, з якої було надіслано лист, зокрема й у випадках використання інструментів тестування безпеки, таких як Gophish. Після позначення листа як фішингового повідомлення Gmail автоматично переміщує його до папки Spam та використовує отриману інформацію для подальшого навчання своїх алгоритмів виявлення загроз. Таким чином, навіть навчальні або тестові фішингові розсилки, створені за допомогою Gophish, можуть бути виявлені та заблоковані механізмами колективного захисту Gmail.

Також під отриманим листом можна перейти в розділ *Original Message*. У цьому вікні відображаються технічні заголовки та службова інформація про лист: дані про відправника, IP-адресу сервера, результати перевірок SPF, DKIM і

DMARC, час доставки та інші параметри, за якими Gmail оцінює автентичність повідомлення. Це дозволяє детальніше проаналізувати, чому лист був позначений як підозрілий, небезпечний або взагалі нормальним.

Original Message

Message ID	<1765144129062438600.23476.6435001416595329296@DESKTOP-GI02DQM>
Created at:	Sun, Dec 7, 2025 at 11:48 PM (Delivered after 1 second)
From:	"WordPress.org" <rootbob19@gmail.com> Using gophish
To:	Олександр Шабранюк <shabraniuk@gmail.com>
Subject:	[WordPress.org Forums] Pleas re-login to the system to keep your account safe
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more

[Download Original](#) [Copy to clipboard](#)

Рис 3.47 – Звіт Gmail Original Message

На представленому зображенні продемонстровано детальну технічну інформацію про електронний лист, отриману через меню **Show original** у Gmail. У цьому звіті система відображає ключові параметри автентифікації повідомлення, що дозволяють визначити його справжність або фіксувати потенційні ознаки фішингу.

У верхній частині відображається **Message ID**, що є унікальним ідентифікатором листа, створеним під час його надсилання. Нижче наведено точний час відправлення та доставлення повідомлення. Поле **From** містить адресу відправника, яка у даному випадку створена через Gophish, а поле **To** показує адресу одержувача. Особливу увагу привертають записи SPF, DKIM та DMARC — три основні технології автентифікації електронної пошти.

На даному скріншоті всі вони мають статус **PASS**, що означає, що сервер Gmail успішно підтвердив:

- **SPF (Sender Policy Framework):** IP-адреса відправника дозволена доменом gmail.com;
- **DKIM (DomainKeys Identified Mail):** цифровий підпис повідомлення визнано дійсним;
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** перевірка пройшла відповідно до політики домену.

Ці результати свідчать про те, що з технічної точки зору лист відповідає стандартам автентифікації, що значно ускладнює виявлення фішингових спроб на цьому етапі. Саме це дозволяє продемонструвати⁶, у яких випадках Gmail не здатен автоматично заблокувати шкідливий лист, якщо зловмисник використовує справжні сервери автентифікації та коректні записи.

У межах роботи було проведено контрольоване тестування фішингових атак на локальний поштовий сервер hMailServer та хмарний сервіс Gmail. Під час дослідження виконано налаштування базових механізмів захисту локального сервера та проаналізовано реакцію Gmail на підозрілі повідомлення. Результати показали, що Gmail використовує багаторівневу систему захисту від фішингу, тоді як локальні поштові сервери потребують додаткових налаштувань для підвищення рівня безпеки.

3.2 Оцінювання ефективності захисту поштових систем

Оцінювання ефективності механізмів захисту електронної пошти є важливою складовою дослідження інформаційної безпеки, оскільки поштові сервіси залишаються одним із основних векторів атак для фішингу, соціальної інженерії та доставки шкідливого контенту. У межах роботи було проведено тестову розсилку фішингових листів через платформу Gophish на локальний SMTP-сервер hMailServer та на публічний сервіс Gmail з метою оцінки їх реакції на потенційно небезпечні повідомлення.

У процесі дослідження встановлено, що Gmail використовує багаторівневу модель захисту, яка включає перевірку автентичності відправника (SPF, DKIM, DMARC), аналіз технічних заголовків, фільтрацію HTML-контенту, оцінку поведінкових аномалій та механізми машинного навчання. Якщо політики автентифікації не відповідають вимогам або структура листа виглядає підозрілою, Gmail автоматично переміщує повідомлення до теки «Spam», блокує завантаження зовнішніх ресурсів та додає попереджувальні банери («Be careful with this message», «This message might be a phishing attempt»). Додатково система

може позначати відправника як «Unverified sender», якщо домен або IP-адреса не проходять перевірку автентичності.

Для детального аналізу Gmail надає інструмент Show Original, у якому відображаються технічні заголовки листа, зокрема результати SPF, DKIM і DMARC перевірок, реальна IP-адреса сервера, шлях передавання листа та інші метадані. Це дозволяє точно визначити, чому лист був класифікований як небажаний, і які механізми спрацювали під час фільтрації.

У межах дослідження, окрім аналізу захисних механізмів Gmail, було проведено детальне тестування локального поштового сервера hMailServer. Це рішення дозволяє створювати окремі домени, поштові скриньки та гнучко керувати правилами обробки кореспонденції, що робить його зручним інструментом для моделювання поштової інфраструктури. Паралельно з тестами у хмарному середовищі були виконані атаки на локальний SMTP-сервер, розгорнутий через hMailServer. Такий підхід дав змогу оцінити поведінку фішингових листів у контрольованому середовищі, де адміністратор самостійно визначає політики автентифікації та фільтрації.

Під час роботи було підтверджено, що hMailServer коректно приймає й обробляє тестові повідомлення, надіслані через платформу Gophish, після чого передає їх до поштового клієнта Thunderbird. Окремої уваги заслуговує можливість створення власних правил фільтрації: у рамках експерименту було налаштовано правило, яке автоматично блокувало або переміщувало у визначену директорію всі листи, що надходили з сервера Gophish. Для фільтрації використовувалися перевірки заголовків, ключових слів та IP-джерел.

Отримані результати підтверджують, що навіть локальний SMTP-сервер може забезпечити дієвий рівень захисту від фішингових повідомлень, якщо правильно налаштувати механізми фільтрації. Проведені атаки показали, що система працює стабільно, а реалізовані правила ефективно реагують на підозрілу активність, демонструючи можливість створення надійного захисту без використання складних хмарних технологій.

Для тестування на стороні користувача застосовувався поштовий клієнт Thunderbird, який підтримує ручний перегляд технічних заголовків, аналіз HTML-вмісту, попередження про підозрілі вкладення та можливість локально фільтрувати листи за вказаними правилами. Thunderbird показує повідомлення про потенційно небезпечний контент, блокує автоматичне завантаження зображень і дозволяє користувачу швидко ідентифікувати можливі ознаки фішингу.

Таблиця 3.1 відображає порівняльний аналіз механізмів захисту електронної пошти хмарного сервісу Gmail та локального поштового сервера hMailServer. У таблиці розглянуто тип платформи, способи виявлення фішингових повідомлень, реакцію на підозрілі листи, можливості аналізу заголовків, гнучкість налаштувань і методи блокування фішингових розсилок, зокрема створених за допомогою платформи Gophish.

Таблиця 3.1

Порівняння можливостей захисту від фішингових розсилок у Gmail та hMailServer

Критерії	Gmail	hmailServer
Тип платформи	Хмарний поштовий сервіс Google	Локальний SMTP/IMAP/POP3 сервер
Виявлення фішингу	Машинне навчання, поведінковий аналіз, контент-фільтрація	Базова фільтрація, можлива розширена через <i>Rules</i>
Реакція на підозрілі листи	Переміщення в Spam, банери «Be careful», блокування зображень	Переміщення у папки за правилами, блокування за умовами
Аналіз заголовків листа	Show original з докладною інформацією	Відображення у протоколах сервера або у клієнті (Thunderbird)
Гнучкість налаштувань	Обмежена (Google керує безпекою)	Максимальна, адміністратор контролює все
Створення правил/фільтрів	Фільтри Gmail, автоматичні системні політики	Розширені <i>Rules</i> (ключові слова, IP, заголовки, напрямок)
Блокування Gophish	Автоматичне переміщення в Spam через невідповідність SPF/DKIM/DMARC	Створено спеціальне правило блокування листів із Gophish

На основі проведеного аналізу можна зробити висновок, що сучасні поштові системи — як публічні, так і локальні — здатні ефективно виявляти та блокувати більшість фішингових листів. Gmail забезпечує максимальний рівень захисту завдяки комплексному використанню SPF/DKIM/DMARC, поведінкового аналізу та машинного навчання. Локальний hMailServer також може бути налаштований для протидії небажаним розсилкам через систему правил і фільтрів. Поштова програма Thunderbird, у свою чергу, дає змогу кінцевому користувачу безпечно взаємодіяти з поштою та самостійно оцінювати ризики. Сукупність цих рішень демонструє ефективність багаторівневої моделі захисту електронної пошти та її важливість у запобіганні успішним фішинговим атакам.

Висновок до третього розділу

У ході виконання роботи було проведено контрольоване дослідження фішингових атак у локальному та хмарному поштових середовищах, зокрема на базі сервера hMailServer та сервісу Gmail. Під час експерименту здійснювалося налаштування основних механізмів захисту локального поштового сервера, а також аналізувалася реакція Gmail на надсилання підозрілих електронних повідомлень. Отримані результати засвідчили, що Gmail реалізує багаторівневу систему протидії фішингу, яка включає перевірки SPF, DKIM і DMARC, аналіз вмісту листів, поведінкові алгоритми та елементи машинного навчання.

Водночас встановлено, що локальні поштові сервери, зокрема hMailServer, можуть забезпечувати ефективний захист лише за умови коректного налаштування правил фільтрації, обмежень та механізмів контролю поштового трафіку. Додаткову роль у підвищенні безпеки відіграє поштовий клієнт Thunderbird, який надає користувачеві інструменти для аналізу листів і прийняття обґрунтованих рішень щодо потенційно небезпечних повідомлень. Сукупність отриманих результатів підтверджує ефективність багаторівневої моделі захисту електронної пошти та її ключову роль у зниженні ризику успішної реалізації фішингових атак.

ВИСНОВКИ

В результаті проведеного дослідження отримані наступні висновки:

1. Фішингові атаки та методи соціальної інженерії є одними з найбільш небезпечних кіберзагроз у сучасному цифровому середовищі. Вони становлять серйозну небезпеку як для окремих користувачів, так і для організацій та підприємств, оскільки спрямовані на отримання конфіденційної інформації, фінансові махінації та несанкціонований доступ до інформаційних ресурсів.
2. Аналіз теоретичних аспектів фішингу та соціально-інженерного шахрайства дозволив систематизувати основні види атак, зокрема spear phishing, vishing, smishing, whaling та pharming, а також визначити їх характерні ознаки та принципи реалізації. Встановлено, що різноманітність і постійна еволюція цих методів значно ускладнює їх своєчасне виявлення.
3. Результати дослідження засвідчили необхідність застосування комплексного підходу до протидії фішинговим загрозам, який має включати технічні засоби захисту, організаційні заходи, підвищення рівня обізнаності користувачів, а також розвиток нормативно-правової бази та міжнародної співпраці у сфері кібербезпеки.
4. У практичній частині роботи проведено аналіз інструментів для реалізації фішингових кампаній у межах пентестування. Встановлено, що інструменти Gophish та King Phisher є найбільш ефективними для моделювання фішингових атак, тоді як Social-Engineer Toolkit орієнтований переважно на методи соціальної інженерії та експлуатацію вразливостей. Для подальшого дослідження обрано інструмент Gophish як найбільш функціональне та зручне рішення.
5. У межах експериментального дослідження виконано контрольоване тестування фішингових атак на локальному поштовому сервері hMailServer та у хмарному поштовому сервісі Gmail. Отримані результати показали, що Gmail використовує багаторівневу систему захисту, яка включає перевірки

SPF, DKIM і DMARC, аналіз вмісту повідомлень, поведінкові алгоритми та елементи машинного навчання.

6. Встановлено, що локальний поштовий сервер hMailServer може забезпечувати базовий рівень захисту від фішингових атак лише за умови коректного налаштування правил фільтрації, контролю поштового трафіку та обмежень доступу. Без належного адміністрування локальні поштові сервери є більш уразливими порівняно з хмарними поштовими сервісами.
7. Додаткову роль у забезпеченні безпеки електронної пошти відіграє поштовий клієнт Thunderbird, який надає користувачеві можливість аналізувати електронні листи, переглядати технічні заголовки та самостійно оцінювати потенційні ризики, що підтверджує важливість людського фактора у системі кіберзахисту.
8. Загалом результати роботи підтверджують ефективність багаторівневої моделі захисту електронної пошти, яка поєднує технічні засоби, правильне налаштування поштових серверів, використання надійних поштових сервісів і підвищення обізнаності користувачів, що суттєво знижує ризик успішної реалізації фішингових атак.

Підсумовуючи оцінювання ефективності захисту поштових систем, можна зазначити, що найбільш результативним є багаторівневий підхід до протидії фішинговим атакам. Хмарні сервіси, зокрема Gmail, забезпечують високий рівень захисту завдяки використанню протоколів SPF, DKIM і DMARC, а також інтелектуальних механізмів аналізу вмісту листів. Локальні поштові сервери, такі як hMailServer, можуть бути ефективними лише за умови правильного налаштування фільтрів і правил безпеки. Отримані результати підтверджують важливість комплексного поєднання технічних засобів і обізнаності користувачів для зниження ризику фішингових атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ENISA — ENISA Threat Landscape 2024 [Електронний ресурс] – Режим доступу: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
2. Verizon (2024). Data Breach Investigations Report (DBIR) [Електронний ресурс] – Режим доступу: <https://www.verizon.com/business/resources/reports/dbir/>
3. Statista (2024). Digital population worldwide as of 2024. [Електронний ресурс] – Режим доступу: <https://www.statista.com/statistics/617136/digital-population-worldwide/>
4. INTERPOL (2024). Global Crime Trend Report 2024 . [Електронний ресурс] – Режим доступу: <https://www.interpol.int/en/Crimes/Cybercrime>
5. World Economic Forum (2024). Global Risks Report 2024. [Електронний ресурс] – Режим доступу: <https://www.weforum.org/publications/global-risks-report-2024/>
6. Фішинг – визначення, види та приклади фішингу.[Електронний ресурс] – Режим доступу:<https://termin.in.ua/fishynh/>
7. Методики розслідування фішингових атак з використанням інструментів OSINT. [Електронний ресурс] – Режим доступу: <https://openarchive.nure.ua/server/api/core/bitstreams/63036cab-5814-4191-ab31-5cf94f4da284/content>
8. Cybersecurity: social engineering. [Електронний ресурс] – Режим доступу: <https://www.consilium.europa.eu/en/policies/cybersecurity-social-engineering/>
9. Social Engineering vs Phishing: Understanding the Differences. [Електронний ресурс] – Режим доступу: <https://www.keystrike.com/blog/social-engineering-vs-phishing-understanding-the-differences>
- 10.What Is Social Engineering and Are You at Risk? . [Електронний ресурс] – Режим доступу: <https://www.avg.com/en/signal/what-is-social-engineering>
- 11.Social engineering attacks: The most common techniques, examples, and countermeasures. [Електронний ресурс] – Режим доступу: https://nordvpn.com/uk/blog/social-engineering/?srsId=AfmBOooI_8qzCXrmTYgvEqjP8vOf8vffia3dfV_ERmWmMqub1RjnaKHD

- 12.Avoiding Social Engineering and Phishing Attacks .[Электронный ресурс] – Режим доступа:<https://www.lsu.edu/its/units/it-security/avoid-phishing.php>
- 13.From: Canadian Centre for Cyber Security, Social engineering – ITSAP.00.166[Электронный ресурс] – Режим доступа:<https://www.cyber.gc.ca/en/guidance/social-engineering-itsap00166>
- 14.What is vishing?[Электронный ресурс] – Режим доступа:<https://www.cisco.com/site/us/en/learn/topics/security/what-is-vishing.html>
- 15.What Is Vishing? Definition, Methods, and Prevention Best Practices for 2022.[Электронный ресурс] – Режим доступа:<https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-vishing/>
- 16.What is Vishing? And Why are Vishing Scammers.[Электронный ресурс] – Режим доступа: <https://intersys.co.uk/2023/10/09/what-is-vishing-and-why-are-vishing-scammers-the-hollywood-actors-of-the-cyber-crime-world/>
- 17.What is pharming and how to prevent an attack.[Электронный ресурс] – Режим доступа:<https://www.lrqa.com/en/insights/articles/what-is-pharming-and-how-to-prevent-an-attack/>
- 18.Pharming Attack. [Электронный ресурс] – Режим доступа: <https://www.sciencedirect.com/topics/computer-science/pharming-attack>
- 19.What is a whaling attack (whale phishing)? .[Электронный ресурс] – Режим доступа: <https://www.malwarebytes.com/whaling-attack>
- 20.What is a Whaling Attack in Security? .[Электронный ресурс] – Режим доступа: <https://cmitsolutions.com/blog/what-is-a-whaling-attack-in-cyber-security/>
- 21.What Is a Whaling Attack? Identify & Prevent Whale Phishing? .[Электронный ресурс] – Режим доступа: <https://phoenixnap.com/blog/whaling-attack>
- 22.Clone PhishingWhat Happens When Scammers Impersonate Someone You Trust?.[Электронный ресурс] – Режим доступа:<https://chargebacks911.com/clone-phishing/>

23. What Is Smishing and How Organizations Can Protect Themselves [Електронний ресурс] – Режим доступу: <https://arcticwolf.com/resources/blog/smishing-what-it-is-how-to-protect-yourself/>
24. Smishing Attack in Cyber Security. [Електронний ресурс] – Режим доступу: <https://www.wallarm.com/what/smishing-attack-what-is-it>
25. What is Smishing (SMS Phishing)? Examples & Tactics . [Електронний ресурс] – Режим доступу: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-smishing/>
26. Clone Phishing: Understanding the Risks. [Електронний ресурс] – Режим доступу: <https://bolster.ai/glossary/clone-phishing>
27. Spear Phishing, PHISHING ATTACKS ARE ON THE RISE . [Електронний ресурс] – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/spear-phishing>
28. Боровик, А.В. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посіб. / А.В. Боровик, І.М. Копотун. – Луцьк : ВолиньПоліграф, 2019. – 304 с [Електронний ресурс] – Режим доступу: https://fpk.in.ua/images/biblioteka/3bac_pravo/borovyk--.pdf
29. Кібербезпека: вразливі моменти. Юридична газета [Електронний ресурс] – Режим доступу: <https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html>
30. Закон України. Про основні засади забезпечення кібербезпеки України. (Відомості Верховної Ради (ВВР), 2017, № 45, пр. 403) {Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, пр. 241} [Електронний ресурс] – Режим доступу: https://fpk.in.ua/images/biblioteka/3bac_pravo/borovyk--.pdf
31. Загальний регламент про захист даних (GDPR). [Електронний ресурс] – Режим доступу: <https://gdpr-text.com/uk/>
32. Кодекс України про адміністративні правопорушення. [Електронний ресурс] – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/80732-10>

- 33.Кримінальний кодекс України.[Електронний ресурс] – Режим доступу:<https://zakon.rada.gov.ua/laws/show/2341-14>.
- 34.ЗАКОН УКРАЇНИ №2297–VI. Про захист персональних даних[Електронний ресурс] – Режим доступу:<https://www.president.gov.ua/documents/2297vi-11567>
- 35.Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2022. Вип. № 1(11).АНАЛІЗ ФІШИНГ-АТАК. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАПОБІГАННЯ ТА ЗАХИСТУ. Кравченко В.С., Руденко О.В., Доманов І.О., Казначей С.М. Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки [Електронний ресурс] – Режим доступу:<file:///C:/Users/hh824/Downloads/152-Текст%20статті-297-1-10-20220506.pdf>
- 36.IT Admin's Guide to Protecting Against Phishing Attacks. [Електронний ресурс] – Режим доступу: <https://www.bitlyft.com/resources/admin-guide-protecting-phishing-attacks>
- 37.Аналіз розвитку, типові цілі та механізми здійснення фішингових атак.[Електронний ресурс] – Режим доступу:<https://periodicals.karazin.ua/cscs/article/view/23089/21099>
- 38.Phishing attacks: defending your organisation .[Електронний ресурс] – Режим доступу: <https://www.ncsc.gov.uk/guidance/phishing>