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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту інформаційних ресурсів організації від фішингових атак на базі Syren Inbox Security»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

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

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

_____ Ксенія ГАЙДУР
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ГАЙДУР Ксенія
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APWG – Anti-Phishing Working Group

BEC – атака компрометації облікового запису електронної пошти

SaaS – бізнес-модель розгортання та реалізації програмного забезпечення, при якому постачальник розробляє додаток, ліцензує його, управляє ним, і надає споживачам доступ до ПЗ через Інтернет

ПЗ – програмне забезпечення

DLP – Email Data Loss Prevention

API – application programming interface

MX – mail exchanger

SVM - Support Vector Machines

ВСТУП

Актуальність дослідження. Актуальність дослідження зумовлена необхідністю розробки ефективних методів захисту від фішингових атак, які все частіше використовують методи соціальної інженерії та складні схеми обману. Захист інформаційних ресурсів організації від фішингових атак зумовлює керівників сфокусувати свою увагу на захист електронної пошти, яка є слабою ланкою в системі кіберзахисту.

На відміну від інших рішень, які перевіряють електронні листи лише один раз, Cyren Inbox Security постійно відстежує поштові скриньки співробітників на наявність прихованої соціальної інженерії та атак зловмисного програмного забезпечення.

Cyren Inbox Security проводить аналіз вмісту електронної пошти та контексту користувача після доставки, використовує машинне навчання, евристику, обробку природної мови та аналітику поведінки, щоб виявляти обхідні атаки та вчитися на них.

Дослідження в рамках цієї роботи спрямоване на розробку рекомендацій щодо налаштування та використання технології для забезпечення максимального рівня захисту від фішингових атак в організаціях різного масштабу.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології виявлення фішингових атакї на базі Cyren Inbox Security.

Об'єкт дослідження – захист інформаційних ресурсів організації.

Предмет дослідження – технологія захисту інформаційних ресурсів організації від фішингових атак на базі Cyren Inbox Security.

Мета роботи – розробити порядок застосування технології захисту інформаційних ресурсів організації від фішингових атак на базі Cyren Inbox Security. ї та рекомендації щодо реагування на інциденти та використання методів штучного інтелекту.

Наукові завдання:

дослідити сутність проблеми захисту інформаційних ресурсів організації від фішингових атак.

проаналізувати підходи захисту інформаційних ресурсів організації від фішингових атак;

проаналізувати існуючі рішення захисту інформаційних ресурсів організації від фішингових атак.;

проаналізувати методи та засоби захисту інформаційних ресурсів організації від фішингових атак на базі Cyren Inbox Security.

розкрити порядок реалізації технології забезпечення безпечної роботи гібридних працівників організації.

рекомендації щодо реагування на інциденти та використання методів штучного інтелекту

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту інформаційних ресурсів організації від фішингових атак на базі Cyren Inbox Security.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Цифрова трасформація кібербезпеки», яка відбулася 26 квітня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ та у фаховому журналі «Сучасний захист інформації».

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ

1.1. Дослідження проблеми захисту інформаційних ресурсів організації від фішингових атак

Фішинг вже багато років є однією з найпопулярніших хакерських (шахрайських) атак, яка є формою соціальної інженерії. Такий вид атаки передбачає собою обман та психологічну маніпуляцію з боку кіберзлочинців. Використання перевірених джерел, таких як лист на корпоративну електронну пошту, дзвінок від знайомої людини (родичі, друзі або ж навіть ваш керівник з роботи) та інше, суб'єкти загрози маскуються та спонукають користувачів (фактично своїх жертв) виконувати певні дії. Таким чином вони змушують людину надавати персональні дані, доступи до закритої інформації, як от банківський рахунок та дані кредитної картки, паролі та доступи до інших важливих та захищений джерел інформації, встановлення шкідлих файлів (які можуть бути націлені як на збір даних так і на шпигунство, виведення з ладу пристрої, а то і всієї захищеної мережі в цілому). З кожним роком тенденція використання фішингової атаки на електронну пошту постійно зростає як це проілюстровано на рис. 1.1, а й набуває змін і впроваджує нові способи впливу.

Для подальшого аналізу проблеми захисту від фішингових атак було використано дані, що зібрані робочою групою по боротьбі з фішингом (Anti-Phishing Working Group, APWG), яка є міжнародною коаліцією, некомерційною галузевою асоціацією та зосереджена на усуненні крадіжки особистих даних і шахрайства, які є результатом зростаючої проблеми фішингу [1].

Основні завдання які виконує APWG полягають у наступному:

- унікальні фішингові сайти, що є основним показником кількості повідомлень про фішинг у всьому світі.

- унікальні теми фішингових електронних листів, де враховуються листи-приманки, які містять різні теми електронних листів.

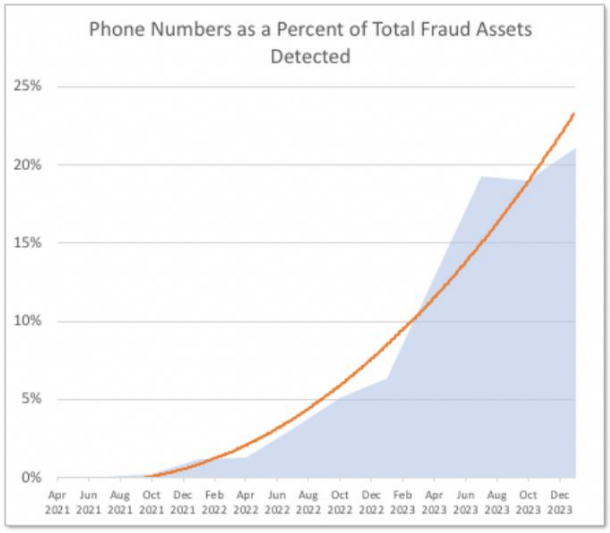


Рис 1.1. Тенденція збільшення фішингових атак [5]

- збір даних щодо кількості атакованих брендів шляхом вивчення звітів про фішинг і нормалізації написання назв брендів.

Згідно зі звітом за 1квартал 2023 [1], APWG зафіксувала:

- 1 624 144 фішингових атак, серед яких одним з найпопулярніших для кібератак направлень залишається фінансовий сектор, на який припало 23,5% від всіх атак, що менше на 4% порівняно з 2022 роком;
- фішинг націлений на криптовалюту падає до 2% через хвилювання які відбувались у криптоіндустрії через крах FTX у листопаді 2022 року;
- спостерігалося зростання обсягу фішингових або вішингових повідомлень голосової пошти на більше ніж 40%, якщо порівнювати з показниками за 2022 рік.

Аналіз найбільш популярних секторів для фішингових атак за 1 квартал 2023 року показав, що другим для популярності сектором для атаки стали послуги надання програмного забезпечення (SAAS), що становить 18,8% від загальної

кількості атак, атаки на компанії соціальних мереж зайняли третє місце у списку і складає 18,2% атак (рис.1.2).

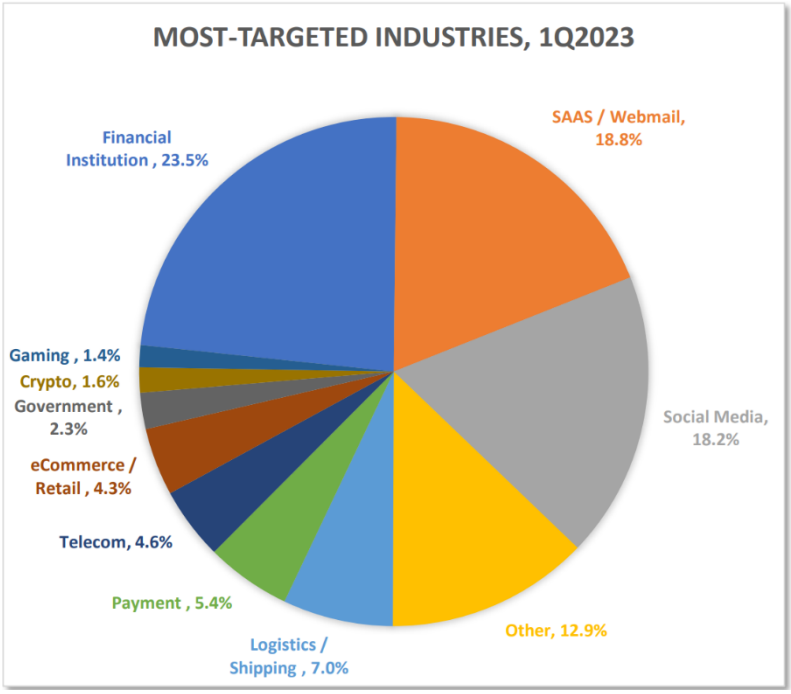


Рис.1.2. Найбільш популярні сектори для фішингових атак за 1 квартал 2023 року

Згідно зі звітом за 2 квартал 2023 [2] APWG зафіксувала:

- 1 286 208 фішингових атак, що стало третім показником за величиною кількості атак за квартал;
- фінансовий сектор залишається найбільш атакованим – 23,5% атак. Також зафіксовано що в загальному атаки були здійснені на банківські грошові перекази, де сума середнього банківського переказу становила 293 359 доларів США, а це на 57% більше в порівнянні з середніми сумами (не менш ніж 187 053 доларів) за перший квартал. А от обсяг атак впав до 29%, з чого можна зробити висновки, що зловмисники поступилися кількістю атак заради більшої наживи;
- найпопулярнішим шахрайством стали авансові комісії як метод виводу готівки – 44% від загальної кількості. Тобто задля виводу грошей злочинці просили, наприклад, подарункові карти популярних платформ (Amazon, Apple Store) замість звичайної оплати на банківський рахунок – 34% випадків;

- з’явився гібридний вид атаки – вішинг або ж так званий голосовий фішинг (5%). Атака працює наступним чином: жертва атаки отримує електронного листа де зазначено що було списано кошти за оплату товару чи якоїсь послуги і щоб скасувати оплату та отримати відшкодування необхідно зателефонувати за вказаним в листі номером. В таких листах задля довіри використовували такі бренди як PayPal Geek Squad, McAfee та інші;
- кількість унікальних тем для атак виконаних електронною поштою зменшилася майже в два рази, оскільки в середньому за перший квартал 2023 року показник становив понад 40 000 на місяць (рис.1.3)

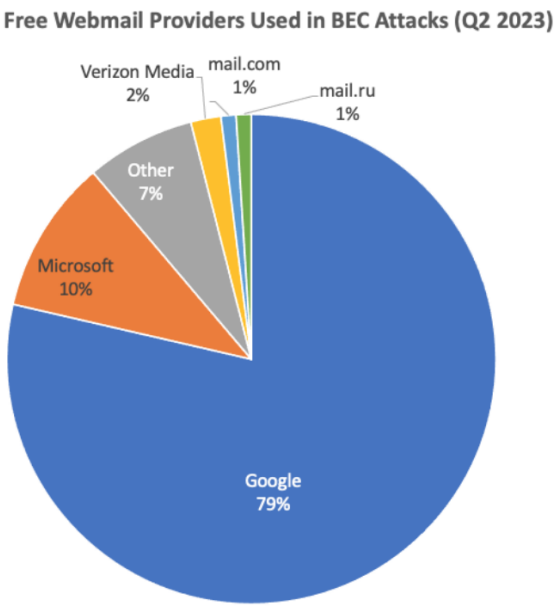


Рис. 1.3. Безкоштовні поштові сервіси які використовувалися в BEC-атаках [2]

Згідно з рис.1.4. фінансовий сектор на першому місці 2023 року - 23,5% від усіх атак, друге місце посідає кількість атак на компанії соціальних мереж – 22,3%, а третє атаки стали послуги надання програмного забезпечення (SAAS/Webmail), що становить 16,3%.

Згідно зі звітом за 3 квартал 2023 [3]:

- зафіксовано 999 956 фішингових атак, що на 37,5% менше в порівнянні з 1 кварталом 2023 року, фактично фішинг впав до рівня який спостерігався в кінці 2021 року;

- підкатегорія атак на голосову пошту фішинг/вішинг зросла до 40% вродовж 1-3 кварталів 2023 року;

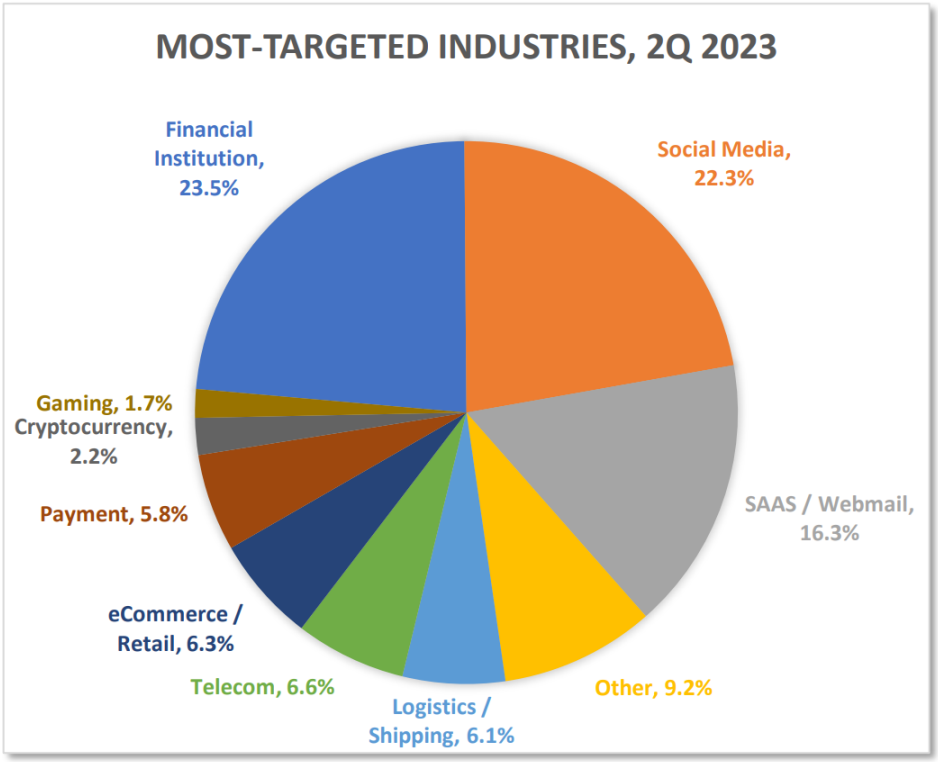


Рис. 1.4. Найбільш популярні сектори для фішингових атак за 2 квартал 2023 року

- атака на перекази банківських коштів в загальному припадала на середню суму в 164 645 доларів США, тобто середній показник впав на 44% порівняно з 2 кварталом 2023 року, що станов 293 359 доларів США;

- обсяг атак BEC на банківські перекази зріс на 55%;

- кількість унікальних тем для електронної пошти стабілізувалася на рівні близько 32 000 після середнього рівня понад 40 000 на місяць у першому кварталі 2023 року;

- виявлено 250 унікальних телефонних номерів, що використовувалися для гібридної вішингової атаки, які видавали себе за 15 різних брендів під час гібридних атак вішингу за 3 квартал;
- рекордно високий щодо атак квартал, який підтвердив, що не зважаючи на падіння показників у попередніх роках, фішинг знову піднявся рівня атак який спостерігався у 2021 році.

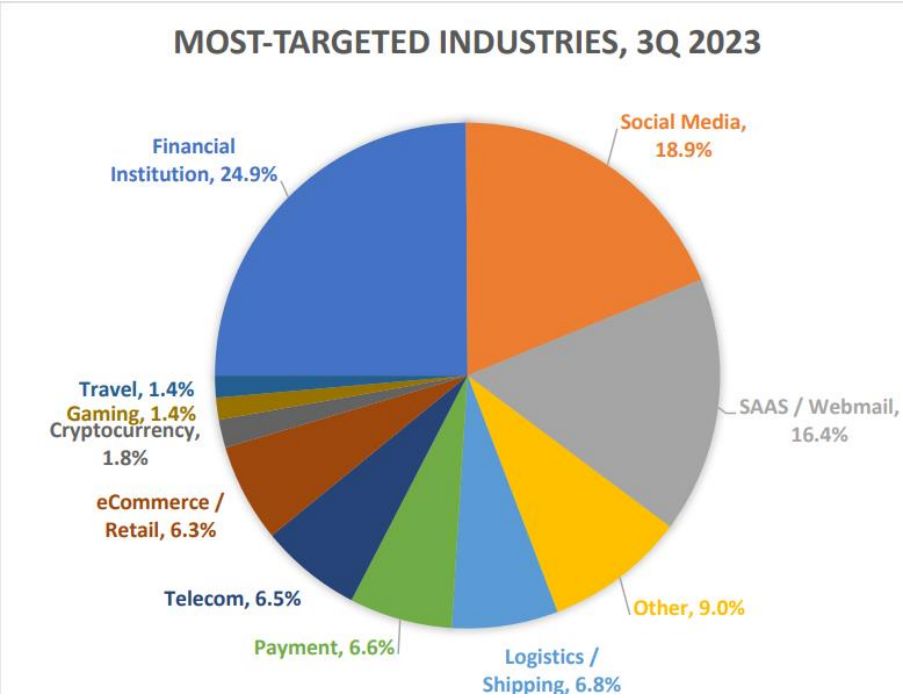


Рис. 1.5. Найбільш популярні сектори для фішингових атак за 3 квартал 2023 року

Фінансовий сектор залишається найбільш атакованим – 24,9% від усіх атак, друге місце посідають атаки на соціальні мережі – 18,9%, а третє місце зайняли SAAS/Webmail атаки -16,4%.

Також цього кварталу спосткрігалося що 79% BEC атак використовували безкоштовний домен веб-пошти, що менше на 8% порівняно з попереднім кварталом. Решта 21% BEC атак використовували зловмисно зареєстровані домени та скомпрометовані облікові записи електронної пошти, де Google став найпопулярнішим провайдером веб-пошти серед кіберзлочинців адреси Gmail становили 84% облікових записів веб-пошти шахраїв.

Отримання грошей через подарункові картки також залишається популярною атакою, де найчастіше вимагали картки Amazon і Apple Store.

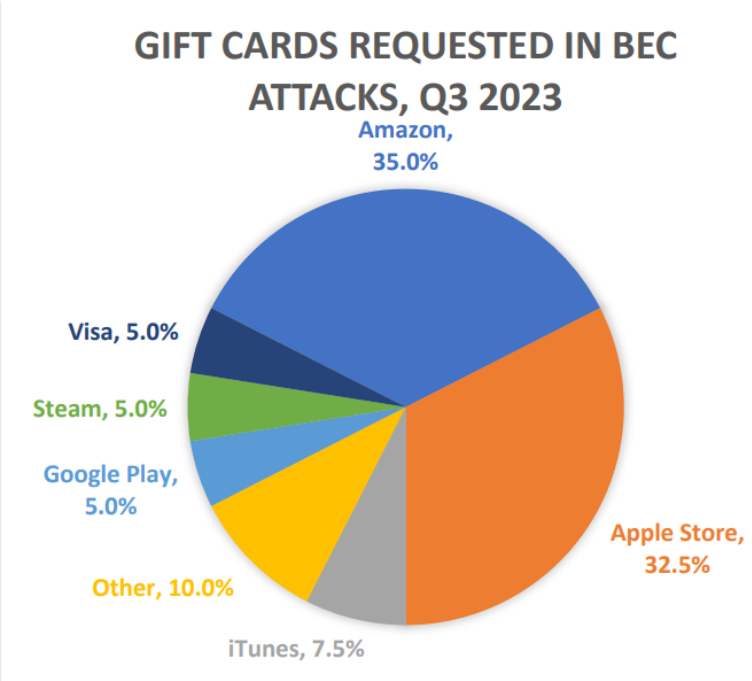


Рис. 1.6. Запити на подарункові карти у BEC атаках

Згідно зі звітом за 4 квартал 2023 [4]:

- Зафіксовано 1 077 501 фішинг-атак, у підсумку це близько п’яти мільйонів (4 987 809) фішинг-атак за весь 2023 рік, через що він вважається найгіршим роком для фішингу в історії перейшовши планку яка була зафіксована у 2022 році з кількістю атак у 4,7 мільйона
- Атаки за 4 квартал 2023 року стали найнижчим зафіксованм показником, оскільтки їх кількість частково скоротилася через закриття програми безкоштовного доменного імені Freenom. Цей безкоштовній сервіс видавав домени рівня .TK, .ML, .GA, .CF і .GQ і використовувся злочинцями на протязі багатьох років. Фактично через цей сервіс виконувалися 14% атак у всьому світі і 60% фішингових доменів про які повідомлялося ще у 2022. Проте у січні 2023 Freenom припинили безкоштовну реєстрацію доменів, а пізніше взагалі оголосили про повний вихід з бізнесу доменними іменами.

- Кількість унікальних тем у електронних листах трохи впала, проте загальна кількість таких повідомлень залишається на одному рівні в порівнянні з попередніми кварталами.
- Різкий зріст кількості атак на платформи соціальних мереж, що склало 42,8% від всіх фішингових атак.
- Фішинг за допомогою телефонних дзвінків (голосовий фішинг або «вішинг») зростає з кожним кварталом.
- Кількість нападів на банківські перекази теж зростає, але середня сума на яку скорюється атака знизилася до 56 195 доларів США, і це не зважаючи на те, що кількість банківських перевірок зросла на 24%.
- Шахрайство з подпрунковими картками було найпопулярнішим й становило 37,6%. Далі за популярністю йдуть випадки шахрайства з авансовою комісією – 30,6%, перенарахування заробітної плати – 9,2%.
- Найпопулярніші початальники безкоштовної веб-пошти через які кіберзлочинці скоюють атаки: Google – 52%, Microsoft – 21%, Apple – 20%

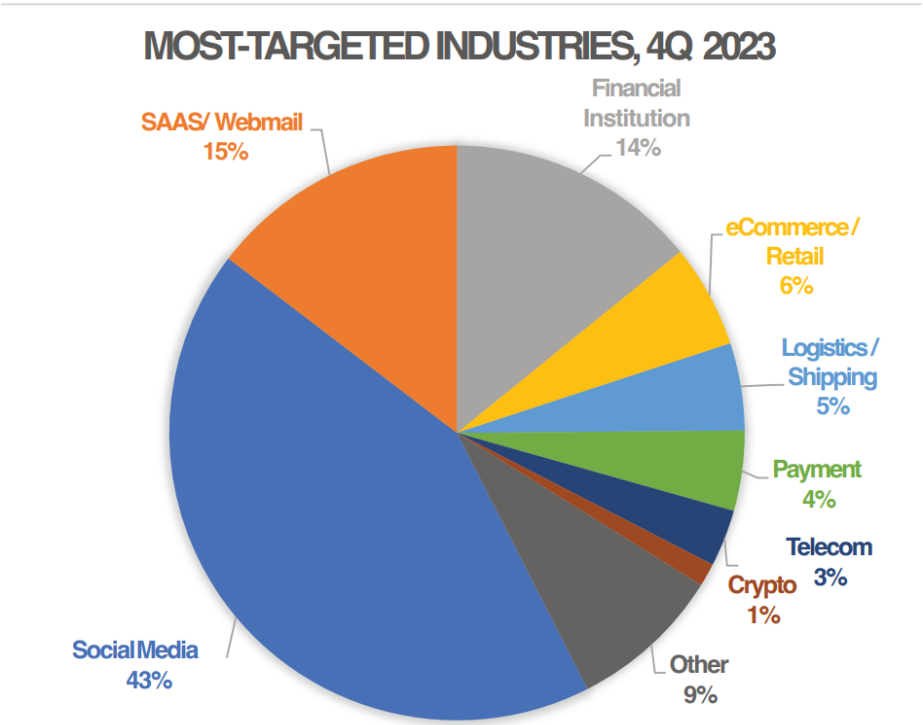


Рис. 1.7 Найбільш популярні сектори для фішингових атак за 4 квартал 2023 року

Перше місце згідно з рис. посіли фішингові атаки наплатформи соціальних медіа – 42,8% від всіх атак, що є різким стрибком в показниках в порівнянні з 18,9% атак за 3 квартал 2023 року. Друге місце отримав сектор SAAS/Webmail атаки – 15%, а фінансовий сектор, який стабільно тримався на першому місці, в цей раз посідає третє отримавши 14% від усіх атак порівняно з показником у 24,9% за попередній квартал.

Отже для організацій важливим питання є захист від фішингових атак, що дозволить зазистити інформаційні ресурси організації.

Згідно зі звітом APWG за 1-й квартал 2024 року [5]:

Зафіксовано лише 963 994 фішингових атак, що в свою чергу стало найнижчим показником із 4-го кварталу 2021 року

Кількість отриманих звітів зменшилася, проте кількість унікальних кампаній створених за допомогою електронної пошти зросла на 64% порівняно з 4-им кварталом 2023 року, що свідчить про те, що кіберзлочинці урізноманітнювали рядки тем своїх електронних листів, щоб обійти розроблену фільтрацію електронної пошти

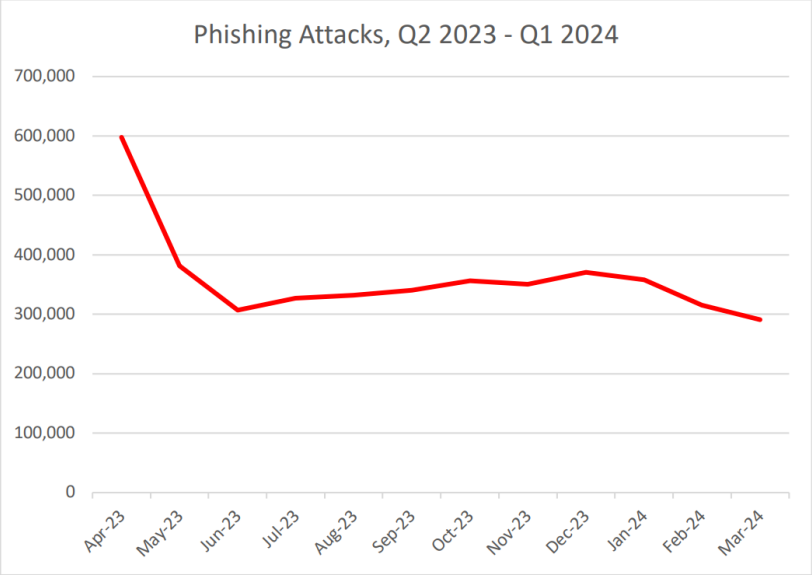


Рис. 1.8 Фішингові атаки, кв.2 2023 – кв.1 2024 [5]

- Телефонний фішин поширюється безконтрольно. Номери телефонівикористані для фішингу становили понад 20% пов’язаних із шахрайством активів
- Фішинг за допомогою телефонних дзвінків — так званий голосовий фішинг або «вішинг» постійно збільшується з кожним кварталом
- Середня сума банківського переказу, яка була атакована кіберзлочинцями становила 84 059 доларів США, тобто показник зріс майже на 50% в порівнянні з показником за попередній квартал

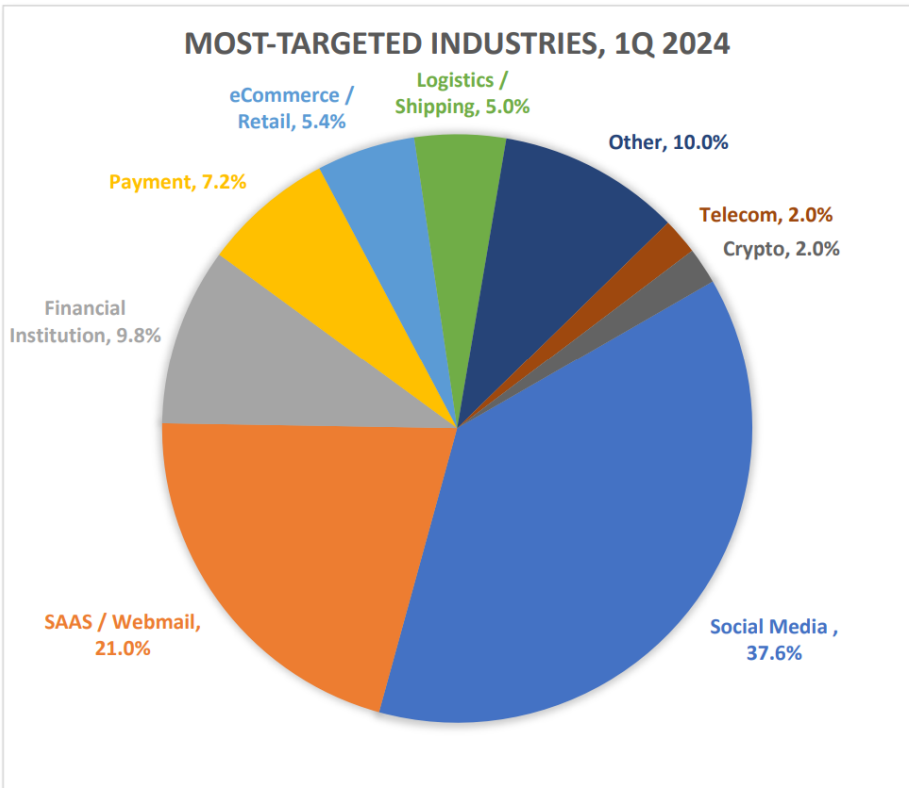


Рис. 1.8. Найбільш популярні сектори для фішингових атак за 1 квартал 2024 року

Платформи соціальних медіа залишаються найбільш атакованим сектором – 37,4%. Друге місце сектор SAAS/Webmail – 21%, а третє знову отримав банківський сектор – 9,8%

1.2. Аналіз підходів до захисту інформаційних ресурсів організацій від фішингових атак

Для того щоб підібрати правильний підхід до захисту від фішингових атак важливо розуміти як вони працюють, оскільки такий вид атаки може бути гіпернацілений або ж навпаки може бути спроба вплинути на як можна більшу кількість цілей, тобта стати масованою [7]. Проте найголовніше, що такі атаки завжди будуть маскуватися під законні компанії чи їх представників, звичайно що для такої дії кіберзлочинці ретельно вивчають всю доступну інформацію про свою ціль.

В будь якому разі злочинці в загальному завжди намагаються отримати, згідно з наданими даними в розділі 1.1, доступ до фінансових даних, облікових записів та персональних даних (особисту ідентифікаційну інформацію як фінансові рахунки, медичні записи, намери та паролі від кредитних карток та будь який соціальних мереж, секретні відомості, конфіденційна інформація) для подальшого їх використанні у своїх цілях. Іноді достатньо всього однієї точки витоку даних, яка трохи згодом може стати великою проблемою для організацій будь якого розміру, типу та рівня [6]. Саме тому фішинг являється великою проблемою, адже найчастіше подібні атаки є дешевими, ефективними та потребують мінімальних зусиль з боку шахраїв.

З розвитком технологій шахраї також отримають більші кількість інструментів та способів впливу і в залежності від того що саме хоче досягти зловмисник обирається певний тип фішингової атаки [7]:

- Фішинг електронної пошти: цим терміном називають будь-яке шкідливе повідомлення електронної пошти, яке має на меті змусити користувачів розкрити будь-яку особисту чи конфіденційну інформацію. Як правило намагаються викрасти облікові дані, особисту інформацію (PII) чи корпоративну комерційну таємницю.
- Фішинг рибалки: електронні листи надсилаються конкретним людям в організації, які є власниками облікових записів із високим рівнем привілеїв для

отримання доступу до конфіденційних даних, змусити надіслати зловмиснику гроші (викуп) або ж завантажити певне зловмисне програмне забезпечення.

- Маніпуляції з посиланнями: в повідомлення вкладаються посилання на шкідливий сайт, який спрямовує одержувачів на контрольований шахраями сервер, де необхідно пройти автентифікацію на підробленій сторінці входу, яка передає облікові дані зловмиснику.
- Китобійний промисел (шахрайство з генеральним директором): повідомлення надсилаються високопоставленим співробітникам компанії, під виглядом запита від генерального директора або іншого керівника, який необхідно виконати.
- Зловмисне програмне забезпечення: користувачів обманом змушують натиснути на посилання чи відкрити вкладений файл, через який потім завантажується шкідливе програмне забезпечення на пристрої. Програми-вимагачі чи клавіатурні шпигуни – класичні вкладення зловмисного програмного забезпечення, які можуть викрасти дані.
- Smishing: через SMS-повідомлення жертву змушують скористатися наданими посиланнями після чого отримати доступ до смартфонів за допомогою шкідливих сайтів. Таке повідомлення може обіцяти знижки, винагороди чи безкоштовні призи.
- Vishing: завдяки програмам для зміни голосу залишають повідомлення жертвам, що вони повинні зателефонувати за шахрайським номером.
- Wi-Fi «злий близнюк»: фальсифікують безкоштовний Wi-Fi та змушують користувачів підключитися до зловмисної точки доступу для здійснення експлойтів «людина посередині» (man-in-the-middle).
- Фармінг: це двофазова атака, використовується для викрадення даних облікового запису. На першому етапі встановлюється зловмисне програмне забезпечення яке перенаправляє жертву до підробленого веб-сайту, де обманом змушують розкрити облікові дані. Отруєння DNS шкідливим програмним забезпеченням також використовується для перенаправлення користувачів на підроблені домени.

- Фішинг рибалки: через соціальні мережі, зловмисники відповідають на публікації жертви, видаючи себе за офіційну організацію та обманом змушують розкривати облікові дані та конфіденційну інформацію.
- Водяна діра: кіберзлочинець знаходить скомпроментований сайт та використовує його вразливість для того щоб обманом змусити цільових користувачів завантажити зловмисне програмне забезпечення через яке зможе викрадати дані.

В наведеному прикладі розглянуто тільки деякі типи фішингових атак, насправді їх є безліч і як вже стверджувалося раніше, постійно відбувається впровадження нових способів атакувати цільового користувача, а іноді й створюються різні гібриди з вже існуючих типів. Проте всі ці атаки об’єднує те, що в них присутня соціальна інженерія, тобто користувач є однією з перешкод на шляху зловмисника, які необхідно подолати.

Отже одним з перших кроків, які обов’язково необхідно впроваджувати в організаціях – це навчання співробітників як відрізнити справжні повідомлення від обману і як необхідно діяти в ситуаціях якщо було отримано підозріле повідомлення.

Дослідження проведене IBM/Ponemon Cost of a Data Breac у 2023 році [8] надає результати проведеного аналізу чи дійсно впливає позитивно на організації та компанії добре навчені працівники з питань фішингу. І результат дійсно вражає, адже було виявлено що найбільшим фактором витрат стали погано навчені робітники. Тож швидкість виявлення зловмисних повідомлень, які все ж дійшли до користувача мажуть заощадити мільйони компаніям та організаціям.

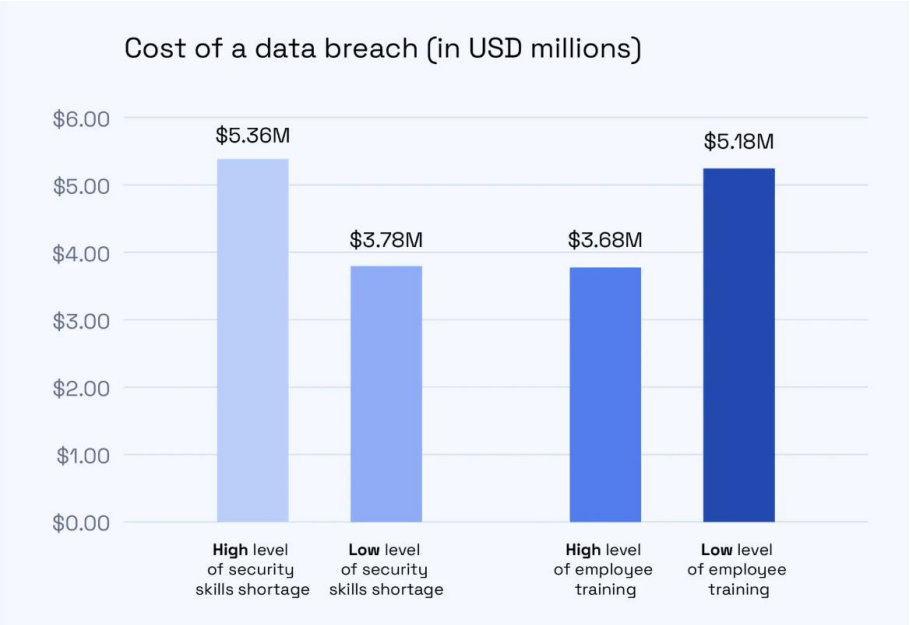


Рис. 1.9. Збитки від витоку даних (у мільйонах доларів США)

Ефективність навчання працівників може залежати від різних факторів і показники можуть змінюватися в залежності від різних ділових та культурних особливостей тої чи іншої країни, галузі та специфіки їхньої діяльності. Тобто організації та компанії мають підлаштовувати існуючі методики під потреби свого бізнесу.

Continent	Success rate %	Miss rate %	Failure rate %
Europe	63.70%	32.92%	3.15%
Oceania	58.02%	38.20%	3.77%
North America	57.61%	38.65%	3.74%
South America	51.93%	44.83%	3.24%
Africa	49.61%	44.84%	5.55%
Asia	47.90%	47.16%	4.94%

Рис. 1.10. Ефективність навчання безпеки відповідно до континентів проведення. Дані результати були отримані в результаті одного року навчання користувачів Hoxhunt.

Отже звітування про загрози зросло у 9 разів, а 2/3 працівників змогли повідомити про реальну загрозу, у зв’язку з даними показниками зменшився середній час очікування, тобто зросла швидкість реагування на загрозу, що в результаті може значно пом’якшити ризик впливу. А найшвидші 5% репортерів можуть прискорити реакцію операційного центру безпеки, що надає можливість не тільки швидкого реагування, а іноді й усунення загрози ще до її активації. З часом завдяки таким навчанням продуктивність буде тільки рости і покращуватися.

Поради для малого бізнесу як діяти в разі фішингу [9]:

Перш ніж натискати на будь-які посилання необхідно що це дійсно посилання, веб-сайт, номер телефону чи особа якій можна довіряти. Якщо все таки виникають сумніви, то можна поспілкуватися з колегою поділившись думками щодо отриманого повідомлення. Також можна зателефонувати тому постачальнику, клієнту або ж колезі від котрого було отримано електронний лист з використанням тих даних (наприклад, номер телефону який ви отримали безпосередньо від них чи від колег у який впевнені) які є достовірними.

В разі якщо атака вже відбулася необхідно максимально зменшити її шкоду, для цього негайно потрібно змінити всі паролі безпеки до яких міг отримати доступ шахрай, від’єднати від мережі комп’ютер чи інший пристрій який зазнав нападу, оскільки він може бути заражений шкідливим програмним забезпеченням, яке може поширюватися локальною мережею. Потрібно дотримуватися процедур які встановлені компанією (це ще раз підтверджує необхідність навчання працівників як діяти в разі фішингової атаки). Також якщо стався витік даних чи стає зрозуміло що дані зазнали ушкоджень потрібно проінформувати про це постраждалі сторони для того щоб ті мали змогу вжити заходів для захисту конфіденційної інформації.

Проте окрім опрацювання людського фактору через який фішингова атака може досягти успіху, важливо впроваджувати технічні рішення для забезпечення захисту[6]. Багаторівневий підхід тут підходить якнайкраще, адже поєднання технічного процесуального та людського підходів гарантують дійсно ефективний захист для конфіденційних даних організацій будь-якого типу та маштабу.

Існує 4 основних кроки на яких варто будувати захист систем та мережі:

Перший крок, необхідно максимально ускладнити доступ до користувачів. В цьому допоможуть різноманітні програми антивіруси та -шпигуни, антифішингові програми та системи. Регулярне оновлення складних паролей, використання багатофакторної автентифікації для забезпечення доступу до даних тільки конкретним персонам. А також обмеження доступу до локальної мережі шляхом впровадження VPN або брандмауера

Другий крок, навчання користувачів (працівників) як визначити та діяти в разі фішингової атаки, оскільки вони є найслабшою ланкою в системі безпеки. Надати просту систему звітування про будь-які підозрілі повідомлення та інформувати про нові види атак.

Третій крок, проведення регулярного моніторингу та аудиту задля захисту від впливу непомічених фішингових повідомлень та їх вчасного виявлення. Обов’язково мати резервні копії всіх необхідних та критичних даних та політику їх відновлення.

Четвертий крок, швидко реагувати на інциденти. Задля цього потрібно створити план реагування для мінімізації наслідків, сформувати групу швидкого реагування. В разі ушкоджень даних від атаки користувачі мають бути попереджені та проінформовані як необхідно діяти та яких заходів безпеки вжити. Подібні інциденти мають аналізуватися та проводитися навчання на їх основі для зменшення ризику подібної ситуації.

Для захисту інформаційних ресурсів організації, виявлено, що електронна пошта працівників є слабкою ланкою, коли мова йде про фішингові атаки і як наслідок призводять до витоку конфіденційної інформації або насанкціонованого доступу до інформаційних ресурсів.

Отже, основним підходом для захисту інформаційних ресурсів організації є впровадження технології захисту електронної пошти організації, яка є найбільш вразливою для фішингових атак. Навчання працівників організації виявляти фішингові атаки не завжди мають успіх. Тому для захисту інформаційних ресурсів від фішингових атак проведемо аналіз існуючих рішень для захисту від фішингових атак.

1.3. Аналіз існуючих рішень захисту від фішингових атак

Згідно з проведеним дослідженням проблеми захисту інформаційних ресурсів організації, фішингові атаки дуже часто несуть масований характер, з чого можна зробити висновок, що людського ресурсу не вистачить для обробки та виявлення загроз при такій великій кількості атак, а отже необхідно використовувати програми які надають відповідні рішення.

Proofpoint Email Protection [10] захищає та контролює вхідну та вихідну електронну пошту. Дане рішення використовує машинне навчання і багаторівневі методи виявлення та вчасного блокування шкідливих повідомлень. Надає точний контроль над широким спектром загроз як повідомлення від самозванців, фішинг, спам, масова розсилка та шкідливі вкладення у електронні листи, а також виконує динамічну класифікацію сучасних загроз. До того ж дане рішення є гнучким, підтримує локальні, хмарні, гібридні інсталяції та прекрасно маштабується, оскільки за допомогою спеціальних політик безпеки та правилами для маршрутизації пошти є можливість зробити максимально персоналізоване налаштування під потреби компанії.

Основні переваги Proofpoint Email Protectio:

- Блокування фішингових атак, шахрайства BEC, шкідливого програмного забезпечення та інших вкладень у повідомлення як віруси, тощо
- Використовується динамічний аналіз репутації для оцінки локальних та глобальних IP-адрес для визначення відхилити чи прийняти з’єднання електронною поштою
- Має потужну функцію інтелектуального пошуку для перевірки даних журналу, метаданих з атрибутами, звідки і куди надходять електронні листи
- Функція попередження користувачів з описом ризику пов’язаного з конкретним повідомлення, таким чином зменшується ризик потенційного компроментування, оскільки користувачі будуть обережніше з потенційно небезпечними повідомленнями
- Підвищена продуктивність за рахунок швидкого відстеження та гігієни

електронної пошти

- Завдяки спеціальним налаштуванням програма є гнучким рішенням та може бути використана як для малого бізнесу так і для великих компаній, оскільки політики та правила програми можуть бути повністю налаштовані під маштаби організацій
- Завдяки автоматизації роботи безпеки та реагування на загрози забезпечується висока операційна ефективність
- Надаються базові можливості захисту, проте можливе розширення захисту шляхом інтеграції додаткової автентифікації, шифрування електронної пошти, захисту від цільових атак на співробітників компанії шляхом впровадження інших рішень як Proofpoint Targeted Attack Protection, Email Fraud Defense, Email Encryption або Email Data Loss Prevention (DLP).
- Затримка електронної пошти менше хвилини
- 99% перенаправленого чи заблокованого спаму

Barracuda Email Protection [11] об’єднує у собі штучний інтелект та високий рівень інтеграції з Microsoft Office 365 для забезпечення комплексного хмарного рішення, що захищатиме від потенційно руйнівних атак.

Barracuda має унікальну архітектуру на базі API (application programming interface), завдяки якій відбувається вивчення штучним інтелектом історії електронної пошти та унікальних шаблонів спілкування користувачів для створення ідентичності кожного з них, виявлення можливих аномалій в метаданих та вмісті повідомлення, знаходити та блокувати фішингові атаки в реальному часі. Такий підхід заснований на історичних моделях дає більший результат, аніж підхід заснований на політиках для виявлення атак соціальної інженерії, адже зафіксовано унікальні дані кожного з користувачів.

Програма допомагає вберегти обліковий запис від захоплення шляхом зупинки фішингових атак націлених на збір облікових даних через які кіберзлочинець може заходити обліковий запис та глибше вивчити свою ціль і вчинити внутрішню атаку скориставшись отриманим доступом. За для забезпечення захисту від подібних атак відстежується будь яка аномальна

поведінка електронної пошти і вразі виявлення можливої загрози надсилається сповіщення до відповідних IT-спеціалістів. А також, окрім виявлення загроз, Barracuda Email Protection допомагає просканувати та виявити слабкі місця електронної поштової скриньки для швидкого їх усунення.

Основні переваги Barracuda Email Protection:

- Зупинка, захист, виявлення та блокування фішингових атак в реальному часі
- Використання штучного інтелекту для виявлення загроз, а також виконує навчання комунікаційних моделей користувачів на його базі
- Має комплексний захист від персоналізованих атак.
- Виявлення аномалій у метаданих та вмісті електронних листів.
- Сповіщення про загрозу для спеціалістів та користувачів про фішингову атаку, атаку захоплення облікового запису чи інші підозрілі дії та аномалії в реальному часі.
- Надається звітність щодо атак які були виявлені з часом, статистика атак типу BEC та інших фішингових атак й аналітика середовища загроз.
- Архітектура на основі API, яка забезпечує швидке та просте налаштування, нульовий вплив на продуктивну роботу мережі або ж досвід користувача, а також пряме підключення до Microsoft Office 365 завдяки глибокій інтеграції.

Cyren Inbox Security (CIS) [12] захищає від фішингових повідомлень, в тому числі й безпеку електронної пошти Microsoft Office 365, таким чином програма забезпечує необхідний критичний рівень безпеки безпосередньо у папці користувача “Вхідні повідомлення”. Безперервна робота Cyren забезпечується провідною у світі хмарі GlobalView™, таким чином відбувається постійне відстеження повідомлень, які з різних причин змогли оминути інші засоби захисту. CIS значно скорочує час, витрати та зусилля команди IT-спеціалістів завдяки автоматичному виявленню та усуненню цільових фішингових атак.

Програма Cyren Inbox для постійного виявлення загроз електронною поштою використовує власну інтеграцію API з Office 365. Таким чином

відбувається безперервне сканування кожного повідомлення яке надійшло або вже знаходиться у поштовій скринці й відшукуються будь-які ознаки фішингової атаки на базі механізмів штучного інтелекту та машинного навчання. Для виявлення загроз використовується найновіша інформація від Cyren GlobalView™, завдяки чому Cyren Inbox Security використовує досвід високошвидкісного виявлення у великому масштабі від GlobalView™ для виявлення затримки детонації атак та відстеження нових загроз, що змогли обійти інші рівні безпеки й змогли опинитися у корпоративних поштових скриньках

CIS надає можливості для виправлення та керування інцидентами, що забезпечує швидке й повне видалення загроз з усіх вхідних електронних повідомлень. Виявляє та усуває, як кластери повідомлень, так і окремі зловмисні повідомлення, що мають однакову зловмисну «ДНК». Таке автоматизоване міжкорпоративне відновлення використовується для всіх уражених поштових скриньок в організації, а також може бути застосоване додатково до кількох орендарів. До того ж Cyren Inbox має зручну консоль, в якій легко налаштувати політики виправлення як для окремих осіб, так і для груп. Завдяки простим робочим процесам керування інцидентами усуваються накладні витрати на розслідування для команди безпеки чим забезпечується швидке реагування та виправлення наслідків фішингової атаки.

Cyren Inbox Security покращує ефективність навчання користувачів як правильно реагувати на фішингові повідомлення й робить їх важливою та активною лінією захисту в боротьбі з подібними атаками. Програма містить потужні інтуїтивно зрозумілі інструменти, які дозволяють користувачу просканувати будь яке підозріле повідомлення в Outlook й повідомити команду IT-спеціалістів про можливе зловмисне повідомлення, завдяки чому команда безпеки не перенавантажена сповіщеннями й може швидше реагувати на реальні загрози.

Основні переваги Cyren Inbox Security:

- Швидко розгортається, оскільки є повністю хмарним рішенням й не потребує додаткового обладнання та має повну інтеграцію з Microsoft Office 365
- Проводить безперервне виявлення загроз, має автоматичне сканування

під час реєстрації користувачів, постійне повторне сканування всіх повідомлень та аналіз поштової скриньки завдяки чому захищає від самозванця всіх співробітників компанії

- Виконує автоматичне відновлення повідомлень при помилкових спрацюваннях та політику виправлень як для кожного користувача окремо, так і для групи
- Повністю інтегрується в Outlook й надає розширені права користувачам для миттєвого сканування за вимогою та негайного повідомлення до служби реагування на інциденти, результати аналізу повідомлень також надаються користувачам
- Служба реагування Cyren доступна для користувачів 24 години, 7 днів на тиждень та весь рік; виконує експертизу на замовлення, надає швидку відповідь на повідомлення та допомагає зменшити кількість сповіщень

Загалом Cyren Inbox Security має низку переваг порівняно з програмами Proofpoint Email Protection і Barracuda Email Protection. На відміну від Proofpoint, що зосереджений саме на багаторівневому виявленні загроз та гнучких налаштуваннях для великих і малих організацій, Cyren Inbox пропонує безперервний захист безпосередньо у папці "Вхідні повідомлення", а це забезпечує додатковий рівень безпеки навіть якщо загрози оминули інші бар'єри. До того ж, Cyren автоматично постійно перевіряє всі повідомлення та усуває загрози з усіх поштових скриньок одночасно, тоді як Proofpoint більше орієнтований на політики захисту та динамічний аналіз.

В порівнянні з Barracuda, яка теж використовує штучний інтелект для виявлення загроз й фокусується на аномаліях у метаданих, Cyren має свою повністю автоматизовану систему реагування з можливістю постійного сканування вже наявних повідомлень у поштовій скриньці. І хоча Barracuda глибоко інтегрований в Microsoft Office 365, проте все ж менш ефективна в швидкому автоматичному виправленні наслідків атаки на рівні користувача.

Тож Cyren Inbox Security перевершує конкурентів у швидкості та ефективності реагування на загрози. З огляду на всі ці переваги, вибір на користь

Cyren Inbox Security є очевидним, і саме ця програма буде використовуватися для подальшого дослідження.

Висновки до розділу 1

1 Проведено дослідження проблеми щодо захисту інформаційних ресурсів організації від фішингових атак, яке показало що фішингові атаки є однією з найбільш розповсюджених атак.

2. Визначено, що електронна пошта працівників організаціє є найбільш вразливою до фішингових атак, компрометація якої може призвести до несанкціонованого доступу до інформаційних ресурсів організації

3. Проведено аналіз рішень захисту інформаційних ресурсів від фішингу, які здатні виявляти фішингові атаки, які несуть масований характер, і тому людського ресурсу не вистачить для обробки та виявлення загроз великій кількості атак, а отже необхідно використовувати технології які надають відповідні рішення.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЙ ВІД ФІШИНГОВИХ АТАК CYREN INBOX SECURITY

2.1. Призначення, можливості та функції продукту Cyren Inbox Security

Хмарна компанія Cyren Inc була заснована у 1991 році й спеціалізувалася на технологіях пов'язаних з інтернет-безпекою. Cyren надає широкий спектр послуг, куди входить безпека DNS, веб-безпека, боротьба зі спамом, фільтрація URL-адрес, захист від програм-вимагачів, виявлення фішингу та шкідливого програмного забезпечення й запобігання атакам ботнетів. Не зважаючи на успішне впровадження технологічних рішень компанія Cyren Inc. у травні 2023 році уклала угоду про викуп окремих активів компанією Data443 Risk Mitigation, Inc., а в 2023 році оголосила про своє закриття, тож починаючи з 2023 року продукти Cyren представляє Data443 й продовжує їх підтримувати та розвивати [13].

Cyren Inbox Security by Data443 (CIS) засновано на роботі хмарних обчислень та технологіях безпеки для виявлення всіх фішингових атак, які оминають безпекові перепони і надає найсучасніші можливості для виявлення загроз з боку кіберзлочинців, сюди входить постійна перевірка в реальному часі всіх заголовків повідомлень електронної пошти, корисного навантаження, URL-адрес і вкладень. До того ж програма використовує машинне навчання для опанування виявлення нових типів та способів впливу зі сторони фішингових атак, виявлення шаблонів IP репутації, кластеризація, обробка мови та захист від самозванців, які бажають проникнути в захищену систему [14].

Саме завдяки машинному навчанню та власному API CIS захищає користувача від нових загроз, які постійно з'являються та покращуються, адже проводиться безперервний моніторинг поведінки як поштової скриньки так і взаємодії користувачів з повідомленнями, відстежуються будь-які аномалії та кореляція даних, а головне що все відбувається у реальному часі і не потребує

додаткової інсталяції обладнання завдяки існуванню у хмарному середовищі, де відбуваються всі необхідні обчислення для коректної роботи програми.

Cyren Inbox Security — це рішення, що ідеально підходить для виявлення та реагування на вхідні повідомлення (IDR), надає автоматизоване виправлення та керування інцидентами для швидкого реагування на загрози, а також автоматизоване міжкорпоративне усунення спалахів фішингу, цей функціонал дозволяє встановлювати критичний рівень захисту для електронної пошти не ззовні, а саме у вхідній пошті, посилюючи таким чином загальну безпеку корпоративної поштової мережі.

Cyren Inbox Protection Manager [15] допомагає уникнути фішингових атак, які використовують наступні методи: відкладена активація URL-адрес, URL-адреси, приховані у вкладення, справжні та дійсні сертифікати SSL, складне шифрування, обфускація HTML, тощо. Виявляє шахрайство BEC, фішинг, CEO, цілеспрямовані атаки соціальної інженерії, нові фішингові zero-day кампанії та запобігає захопленню облікових записів, викрадення будь-яких облікових даних й постійно моніторить внутрішню електронну пошту.

Це рішення є ненав’язливим, оскільки воно може бути як самостійним, так і доповнити вже існуючий безпечний шлюз електронної пошти й при цьому не має необхідності змінювати MX-запис (mail exchanger) чи впроваджувати будь-які зміни в поточній інфраструктурі. Все що потрібно зробити для початку роботи з програмою Cyren це надати доступ до потоку електронної пошти, налаштувати політику фільтрації та виправлення, включаючи гнучке застосування різних політик основуючись на правилі різних користувачів та груп.

Функціонал продукту Cyren Inbox Protection Manager це 100% хмарна служба SaaS, що забезпечує швидке розгортання, просте керування та є досить недорогим вішенням для користування. Має легку інтеграцію з SIEM і SOAR та повну з Microsoft Office 365 та виконує автоматичне «ретро» сканування під час реєстрації користувача чим гарантує відсутність постійних загроз у поштовій скриньці. Допомагає скоротити час SOC для відповіді й усунення загроз електронної пошти,

зберегти ресурси завдяки автоматизації процесів, а також долучає до забезпечення безпеки безпосередніх користувачів поштових скриньок.

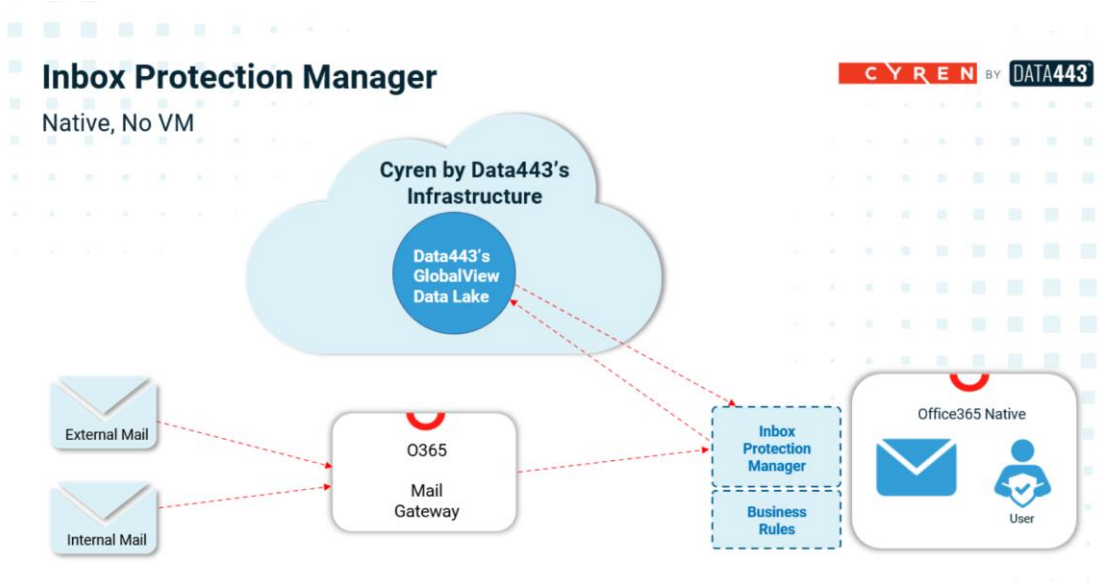


Рис. 2.1. Архітектура надбудови IPM

Основний функціонал Cyren by Data443:

- Захист вхідного фішингу за допомогою аналізу URL-адрес у реальному часі, моделюванню доступа, виявлення BEC та інших атак соціальної інженерії, двоюрідних доменів та стандартизованого методу перетворення символів punycode.

- Неперервне виявлення загроз за допомогою постійного сканування та аналізу поведінки поштової скриньки, використання методу розумної кластерізації повідомлень та наявність автоматичного відновлення повідомлення в разі помилкового спрацювання програми.

- Автоматизована відповідь та рекомендації завдяки наявності політик виправлення як для кожного користувача окремо, та і для певної групи користувачів, управління інцидентами та справами. Попереджувальні й інформаційні банери про можливу загрозу в електронних листах та можливість переміщувати виявлені загрози в окрему папку. Наявне міжорганізаційне відновлення та детальна криміналістика, яку можна експортувати в разі потреби

- Виявлення користувача з крауд-сорсу за допомогою кнопки для користувачів про сканування та звіту про можливу загрозу, вивчення дій користувача в рамках його поштової скриньки та відслідковування аномалій поведінки включаються в систему автоматично, а також цикл зворотного зв’язку самовідновлення, якщо відбулося хибне спрацьовування програми

2.2. Принцип роботи Cyren Inbox Security

Cyren Inbox Security by Data443 представляє собою керовану цілодобову службу, завдяки постійній роботі програми, яка займається виявленням й відслідковуванням будь-яких змін, інцидентів, атак чи аномальної поведінки, експерти з реагування на загрози можуть бути зосереджені саме на розслідуванні, аналізі та вирішенні інцидентів із наявними загрозами, про які повідомляє безпосередньо програма та користувачі поштової скриньки Microsoft Office 365, а також на розслідуванні всіх підозрілих інцидентів із низьким рівнем довіри, що були виявлені системою CIS.

Робота аналітиків у програмі відбувається через Cyren Inbox Security UI (рис.2.2). Коли експерт отримує доступ до головного екрану Cyren UI, одразу відображається вся інформація відносно інцидентів, які сталися за певний період часу (наприклад, за останню добу, тиждень, місяць), дані параметри повність налаштовуються під потреби (рис.2.3). Після налаштування одразу надається загальна інформація про те, скільки було виявлено інцидентів, атак за вказаний проміжок часу, загальна кількість надісланих листів до поштових скриньок й про виявлені загрози такі, як атаки типу BEC, фішинг, шкідливе ПЗ, а також спам/скам(рис.2.4).

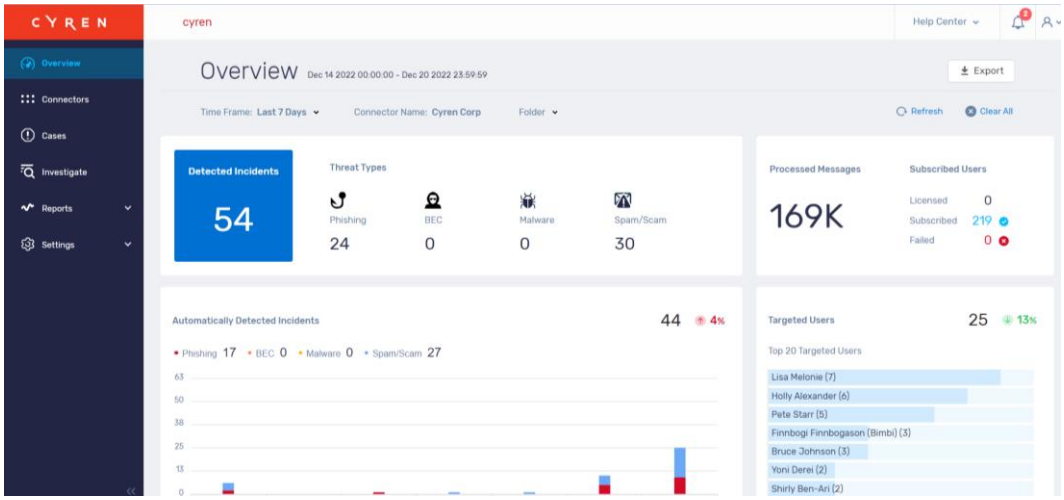


Рис.2.2. Головний екран Cyren Inbox Security

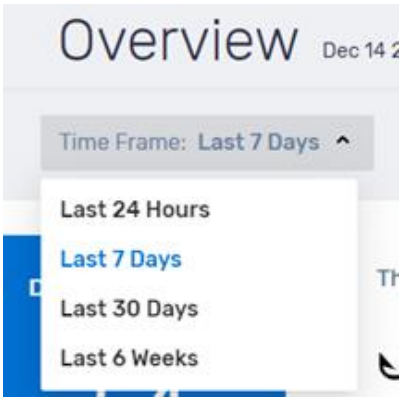


Рис.2.3. Час, для показу інцидентів за певний період

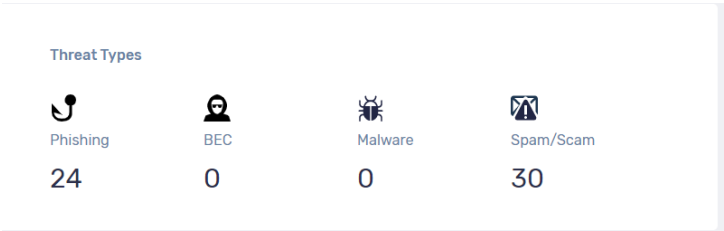


Рис.2.4. Виявлені загрози

У вкладці «Cases» можна знайти всі інциденти, що було виявлено самою системою або ж ті, які були надіслані користувачами, на основі їх підозри на фішинг або ж BEC в електронному лист (рис.2.5). Також тут надана детальна інформація про кожен з кейсів: який саме тип загрози й ким її було виявлено (системою, адміністратором чи користувачем), дата та ідентифікатор даного інциденту, чи є цей кейс закритим чи все ще потребує додаткового розслідування з

боку експертів. Коли аналітику необхідно знайти конкретний інцидент серед інших, він завжди може це зробити за відповідним ідентифікатором, статусом (закритий/відкритий) або ж за поштовою адресою користувача, який отримав даний лист.

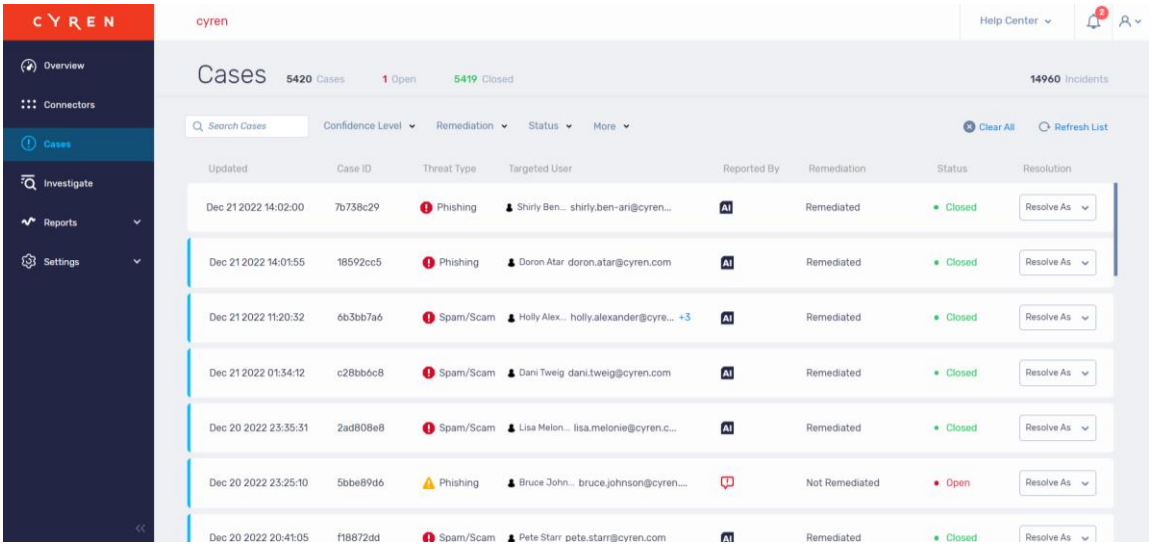


Рис.2.5. Вкладка «Cases»

У вкладці «Connectors» аналітик може налаштовувати політики та правила, за якими при отриманні шкідливого електронного листа будуть спрацьовувати налаштовані умови (рис.2.6). Наприклад, при отриманні повідомлення, в якому буде виявлено фішинг або ж зловмисний додаток, лист просто не дійде до отримувача, оскільки система виявить його та одразу видалить для того, щоб користувач піддався даній атаці. Окрім видалення отриманого повідомлення присутні такі варіанти як: переміщення листа до визначеної папки (наприклад, до видалених повідомлень), блокування шкідливих посилань та додатків, додання попереджального банеру до листа.

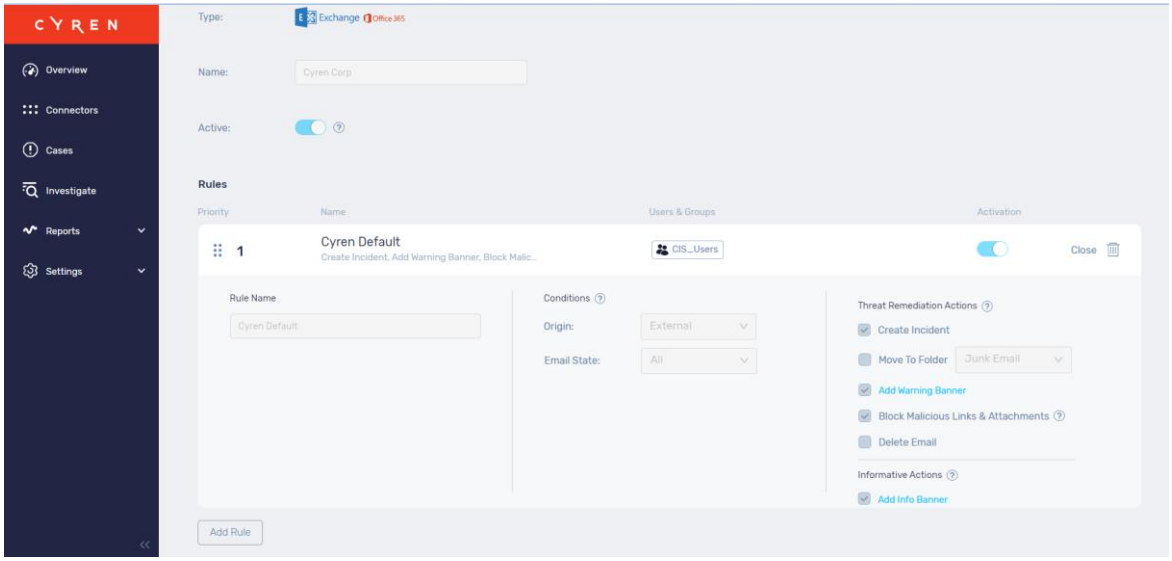


Рис.2.6. Вкладка «Connectors»

У вкладці «Settings» можна здійснювати налаштування акаунтів, визначити головних адміністраторів й налаштувати попереджувальні банери для користувачів, що будуть вказувати на можливу загрозу стосовно отриманого повідомлення.

Cyren Inbox Security надає декілька типів попереджувальних банерів, за допомогою яких звертається увага користувача на можливу загрозу й забезпечується більш обережне ставлення до отриманого листа і скоріше за все аналітик буде повідомлений про дану загрозу. Такі банери можуть налаштовуватись окремо під кожну організацію й її потреби, можна замінити текст та умови, при яких він буде з’являтись перед користувачем. Нижче на рисунку 2.7 наведено приклад банеру, який попереджає про виявлення можливого посилання з фішингом та рекомендує не переходити на за посиланням на іншу сторінку.

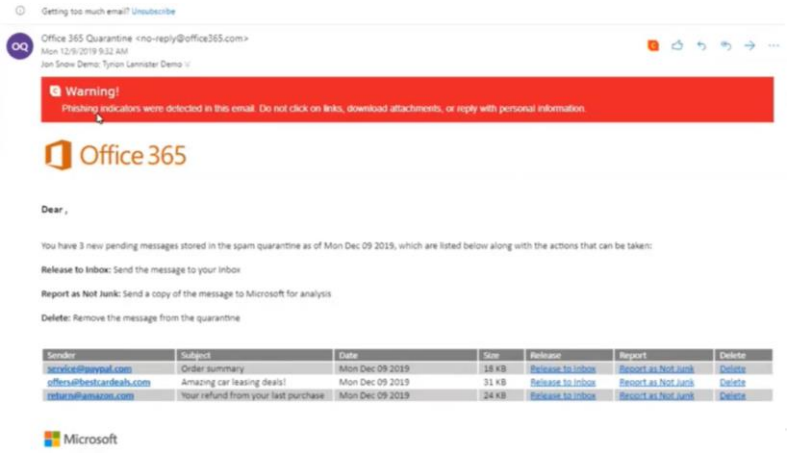


Рис.2.7. Попередження про фішинг

Окрім банера про загрозу можна додатково налаштувати інформаційний банер, що буде попереджати про підозру щодо листа, який був надісланий від зовнішнього невідомого системі користувача, якщо отримувач листа дослідивши повідомлення погоджується з підозрою системи щодо можливої загрози й сумнівного вмісту повідомлення, то користувач може передати даний лист аналітику, який в свою чергу проведе розслідування даного інциденту (рис.2.8).

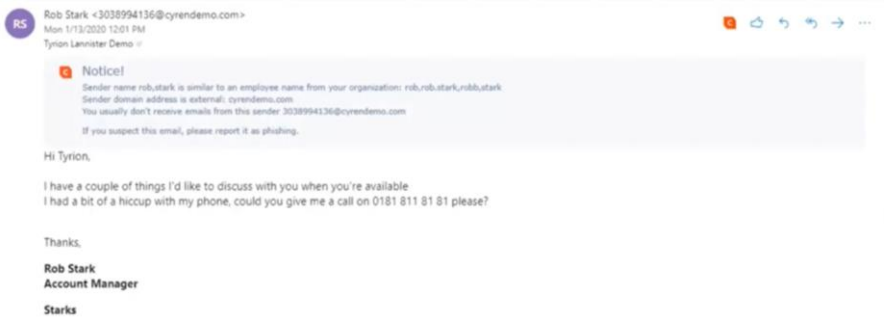


Рис.2.8. Приклад інформаційного банера

Окрім банерів, які надсилаються системою, бувають випадки коли користувач самостійно визначає що даний лист містить підозріле повідомлення, в такому випадку він може скористатися плагіном, який сканує лист на можливі заховані загрози та в разі необхідності є можливість повідомити аналітиків про виявлену загрозу. У випадку, якщо сканер показує що повідомлення є «чистим»,

але одержувач листа впевнений в загрозі, яку несе даний електронний лист, він також може відправити його на перевірку до експертів з поміткою phishing/spam/malware. Аналітик обов'язково перевірить такий відгук й після проведення розлідування закриє даний кейс з відповідним лейблом (рис.2.9).

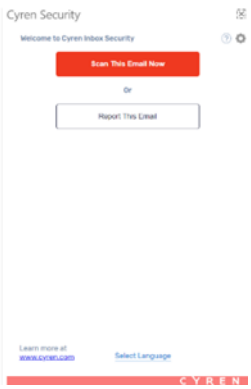


Рис.2.9. Плагін для сканування листів

Отже після перевірки аналітиком отриманого повідомлення й закриття кейсу, користувач обов'язково отримує повідомлення про те чи була в результаті виявлена загроза в електронному листі чи все таки він був дійсно «чистим».

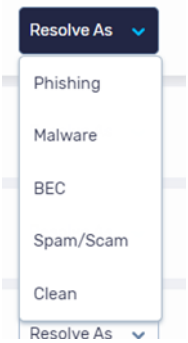


Рис.2.10. Рішення, як саме закрити кейс

Отже, застосування технології Cyren inbox security, дозволить автоматизувати процес виявлення фішингових атак на інформаційні ресурси організацій.

Висновки до 2 розділу

1. Визначено архітектуру Cyren inbox security, яка аналізує URL-адреси у реальному часі, проводить постійне сканування та аналіз поведінки поштової скриньки, надає відповідь та рекомендації завдяки наявності політик виправлення для кожного користувача.

2. Розглянуто основний функціонал Cyren inbox security, який дозволяє виявляти фішингові атаки на електронну пошту організації.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЙ ВІД ФІШИНГОВИХ АТАК CYREN INBOX SECURITY

3.1. Рекомендації застосування технології Cyren Inbox Security для розслідування інцидентів

З кожним роком все більше компаній піддаються атакам, які реалізуються через використання електронної пошти рядового співробітника компанії. Як результат може бути здійснено викрадення даних облікового запису задля отримання доступу до конфіденційних даних та ресурсів компанії, а також порушення робочого процесу через ураження системи та виток даних.

Саме тому, при створенні політик безпеки, значна увага з боку керівництва компанії та адміністраторів безпеки надається захисту корпоративних електронних пошт працівників. З огляду на статистики, які були представлені раніше, помітно, що кількість фішингових атак набуває неймовірної кількості й збільшується з кожним роком за чисельністю та методами впливу. Причому більшість таких атак націлена на звичайного працівника, який через незнання та слабку захищеність може проконтактувати зі шкідливим повідомленням та його вкладеннями, а отже таким чином співробітник дає можливість кіберзлочинцю отримати доступ до критичної інформації компанії.

Технологія Cyren Inbox Security надає можливість налаштувати необхідні політики безпеки спираючись на специфіку галузі в якій працює компанія, а робота експерта з розслідування інцидентів полягає в перевірці вмісту електронного листа, репутації відправника й всіх вкладень та посилань які надходять разом з повідомленням виявленим програмою або ж безпосередньо користувачем поштової скриньки, в даному випадку працівником компанії.

Програмне забезпечення безпеки може виявити більшу частину загроз, проте з різних причин деякі з них можуть бути розпізнані як «безпечні» й пропущені до користувача. Зазвичай такі ситуації відбуваються через те, що кожного дня з’являються все новіші методи, типи й способи доставки фішингових атак у вигляді

зловмисних вкладень (програми шпигуни, віруси, тощо) до користувача. Таким чином використання послуг Cyren Inbox Security може покращити рівень захисту компанії, оскільки кожен виявлений інцидент буде розглянутий експертами з безпеки, що в свою чергу гарантує вживання тих чи інших мір з забезпечення інформаційної безпеки.

Надалі буде покроково розглянуто принцип роботи експерта з безпеки на базі роботи технології Cyren Inbox Security.

Як вже було вказано раніше технологія Cyren має плагін, який легко інсталюється в поштову скриньку й надає можливість користувачу надавати репорт та перевіряти кожне з електронних листів які йому надходять, шляхом сканування повідомлення. Перевірка листа відбувається дуже швидко і вже впродовж трьох секунд працівник отримає результат цього сканування, «Phishing not found» (рис. 3.1) в разі якщо отримана інформація не містить шкідливого вмісту та «Phishing found» (рис. 3.2) в разі якщо результат є протилежним, тобто була знайдена загроза у вмісті повідомлення й тоді система надає застереження, що не варто натискати на посилання чи відповідати на нього.

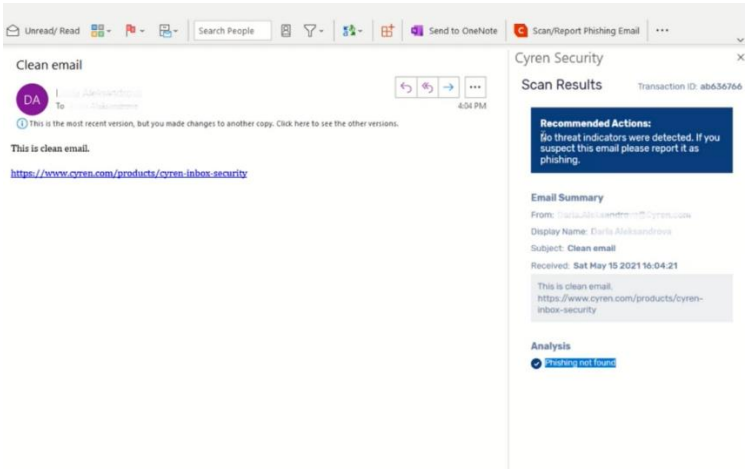


Рис.3.1. Результат сканування «Phishing not found»

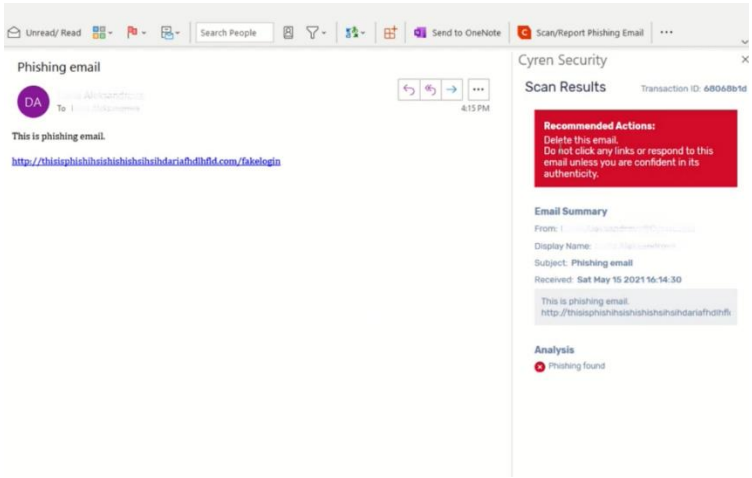


Рис.3.2. Результат сканування «Phishing found»

Після отримання результату, навіть в разі «чистого» листа (якщо користувач впевнений, що є загроза), можна повідомити експерта з безпеки про отриманий лист та надіслати відгук з вказаною причиною – індикатором загрози (додаток, посилання чи текст електронного листа). Для виконання цієї дії необхідно скористатися кнопкою «Report as phishing», обрати індикатори які висвітлюють можливу загрозу та за побажанням написати детальну інформацію щодо цього електронного листа (рис. 3.3).

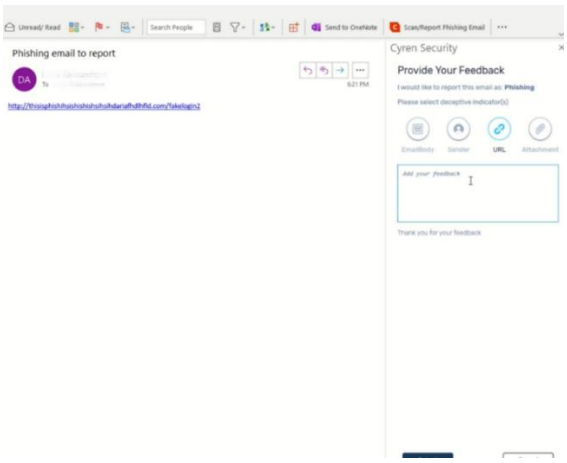


Рис.3.3. Створення відгуку «Report as phishing» на отриманий лист

Після відправлення репорту його отримує експерт з безпеки в CIS UI й з цього моменту починається розслідування інциденту. При проведенні перевірки в першу чергу перевіряються всі посилання, автоматично завантажувального зловмисного

додатку та наявність фішингу, далі перевіряється відправник та його активність. Аналітик на основі отриманих результатів робить висновки (рис. 3.4) та закриває кейс з відповідним ідентифікатором (фішинг, BEC, скам/спам, шкідливе ПЗ, чистий – «Clean»).

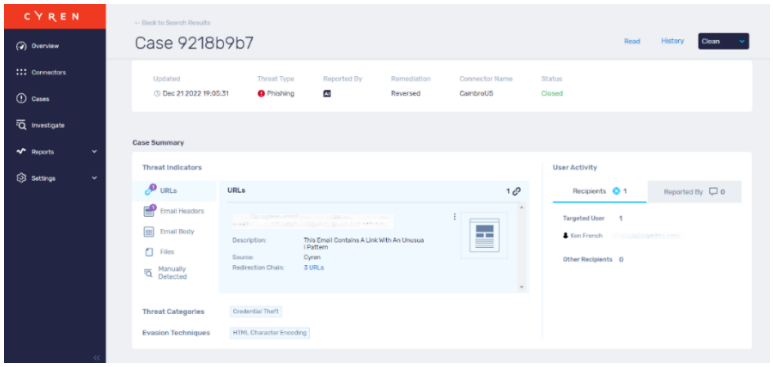


Рис.3.4. Приклад кейсу закритого з ідентифікатором «Clean»

Найчастіше фішинг можна зустріти у вигляді вкладення, яке кіберзлочинець маскує під вигляд чеку для оплати з назвою «Invoice for …», що має максимально офіційний вигляд з номером замовлення, іменем отримувача чи PDF-файлом з певною інформацією всередині. Далі буде розглянуто приклад кейсу від співробітника компанії, який надіслав на перевірку електронний лист з підозрою на BEC атаку (рис. 3.5).

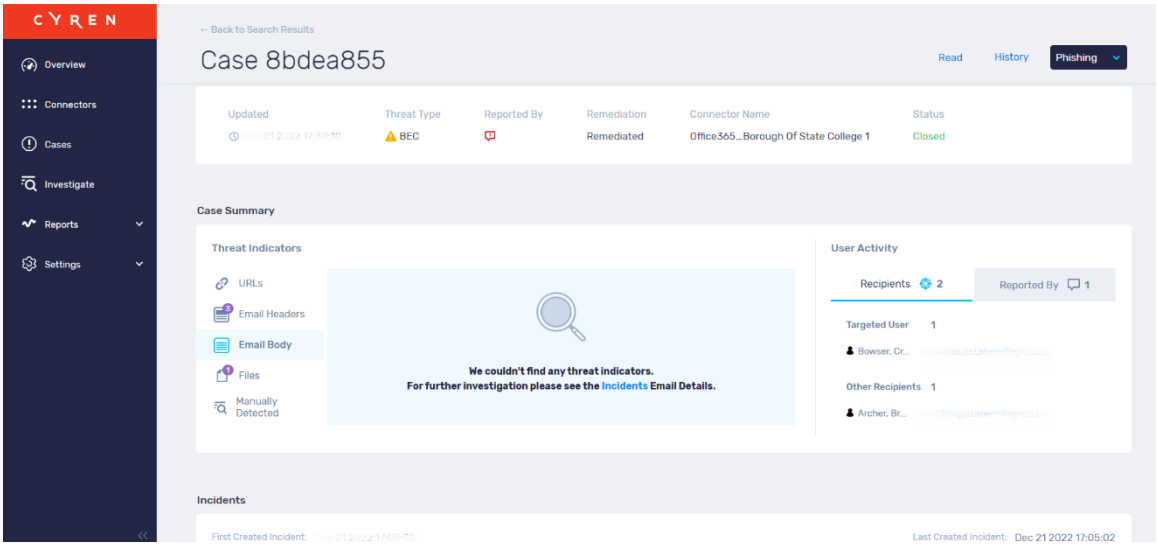


Рис.3.5. Відгук користувача

В даному випадку репорт було надіслано не програмою, а внутрішнім користувачем компанії, повідомлення не містить додаткового опису, проте присутній ідентифікатор, що вказує на підозру щодо BEC атаки, надісланий ззовні компанії, проте адреса відправника дуже схожа на працівника компанії (рис. 3.6).

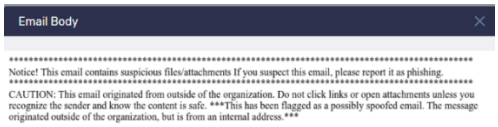


Рис.3.6. Надісланий лист працівнику компанії

Зважаючи на ідентифікатор, в першу чергу відбувається перевірка (рис. 3.7) вкладення на вміст фішингової сторінки чи шкідливого ПЗ. В результаті в даному повідомленні система автоматично виявила загрозу та ідентифікувала її як категорію Phishing, при відкритті вкладеного повідомлення автоматично завантажується сторінка браузера та відображається шкідлива підроблена сторінка для входу в обліковий запис Microsoft (рис. 3.8).

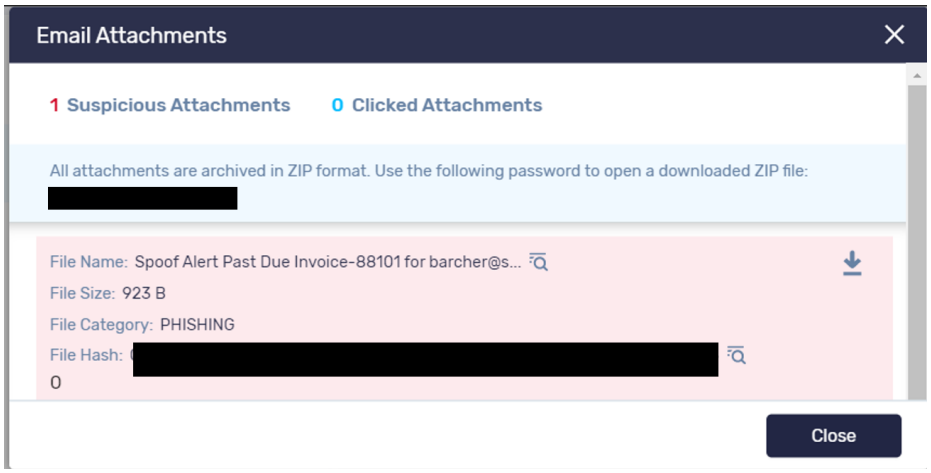


Рис.3.7. Перевірка вкладення на шкідливий вміст

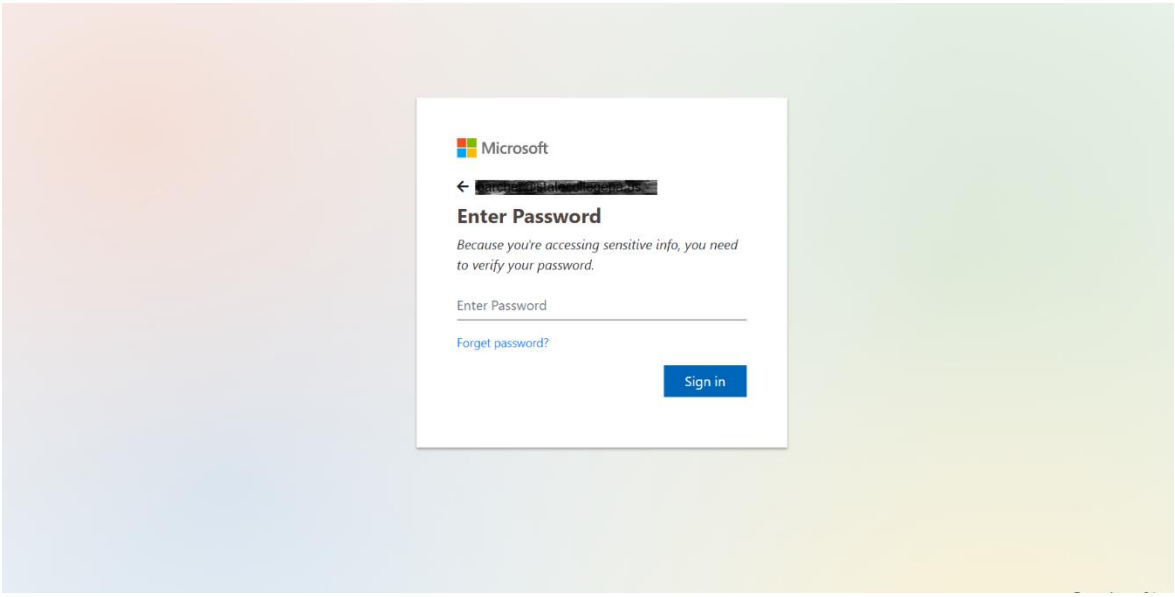


Рис.3.8. Сторінка браузера з підробленим входом в обліковий запис

В цьому випадку атака націлена на отримання паролю та доступу до надісланої інформації. На сторінці що відкрилася за посиланням користувачу пропонують ввести пароль від облікового запису, але кожного разу пароль буде відмічений як не вірний скільки б разів не була введена комбінація, оскільки головна мета кіберзлочинця отримати доступ до облікового запису (рис. 3.9).

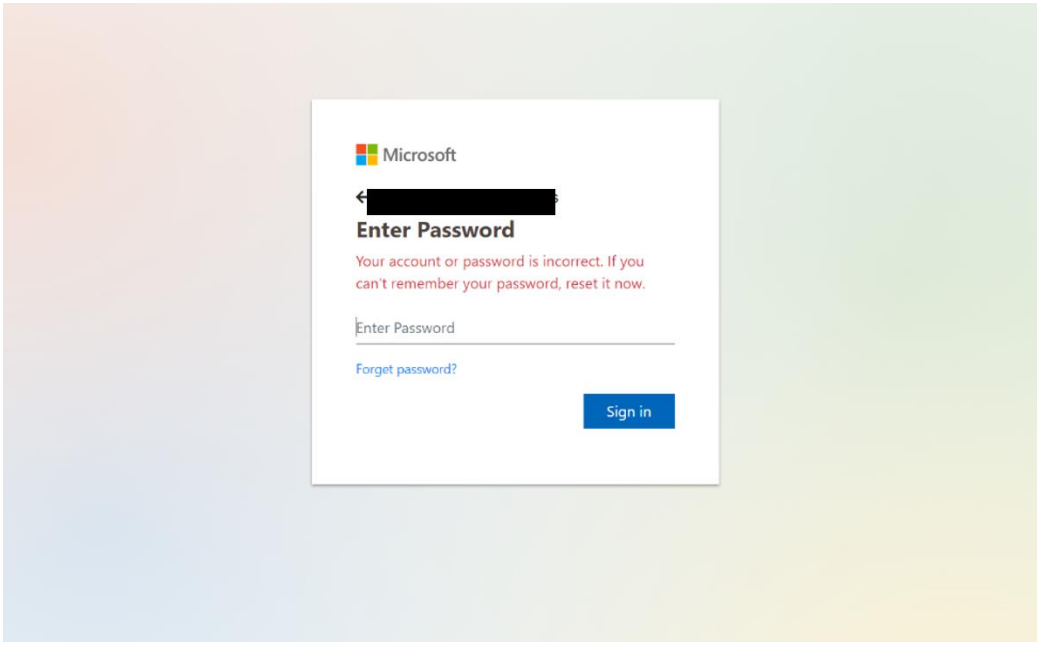


Рис.3.9. Спроба ввести пароль

За для запобігання проведення повторної атаки й заборонити системі пропускати листи від того самого відправника з використанням тих самих даних експерту з безпеки потрібно заблокувати відправника з ідентифікатором Phishing, в разі якщо даний електронний лист було відправлено з внутрішньої електронної адреси співробітника (підробленої шахраями пошти), то необхідно заблокувати хеш вкладення, й надалі система буде ідентифікувати цю адресу як шкідливу.

Після проведення всіх необхідних процедур, експерт з безпеки закриває кейс з відповідним рішенням, в даному випадку вказано ідентифікатор «Phishing». Як тільки кейс позначається завершеним на нього починають діяти правила і політики відповідно до встановлених висновків щодо шкідливих повідомлень – блокування вкладення й перенесення листа до папки «Видалені» (рис.3.10).

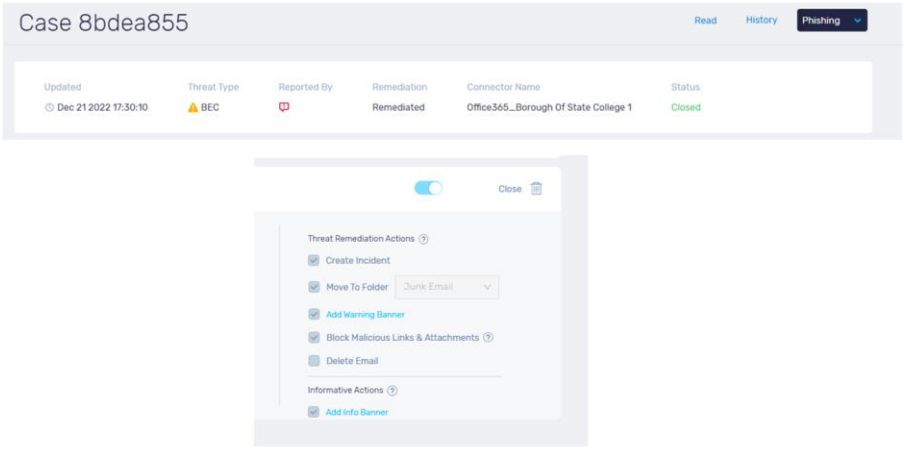


Рис.3.10. Закриття кейсу та встановлення правила

В інших випадках можна зустріти інциденти, які базуються на тому, що співробітнику компанії надсилають електронний лист з посиланням на сховище в якому розміщено файл для огляду (рис. 3.11). Подібні електронні посилання найчастіше розміщені на доменах my.sharepoint.com, така сторінка браузера має дуже схожий вигляд до інтернет версії OneNote. Для перегляду інформації файлу користувач має скористатися кнопкою «View Documents Online Here», після натискання його буде перенаправлено на сторінку браузера що буде мати вигляд офіційної сторінки входу до облікового запису Microsoft (рис. 3.12). Проте якщо

звернути увагу на посилання (рис. 3.13), то можна помітити відмідності від дійсно офіційного сайту й зрозуміти що даний вхід в систему є шахрайським.

Рис. 3.13. Посилання на шахрайську сторінку

При спробі ввести будь-які дані – електронна пошта та комбінація пароля для входу в обліковий запис (будь ці дані дійсні чи не дійсні), в кожному з цих випадків буде сфабриковано момент автентифікації та авторизації до облікового запису (рис. 3.14), в той самий час будь-яка інформація введена на даній шахрайській сторінці й надіслана буде отримана кіберзлочинцем й надалі він буде вчиняти спроби скористатися отриманими даними для фішингових атак.

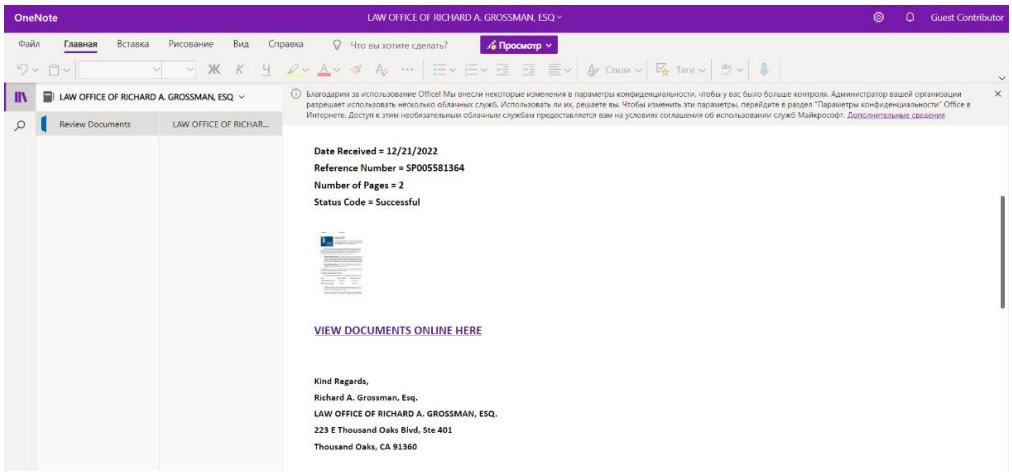


Рис.3.11. Сховище зі шкідливим файлом

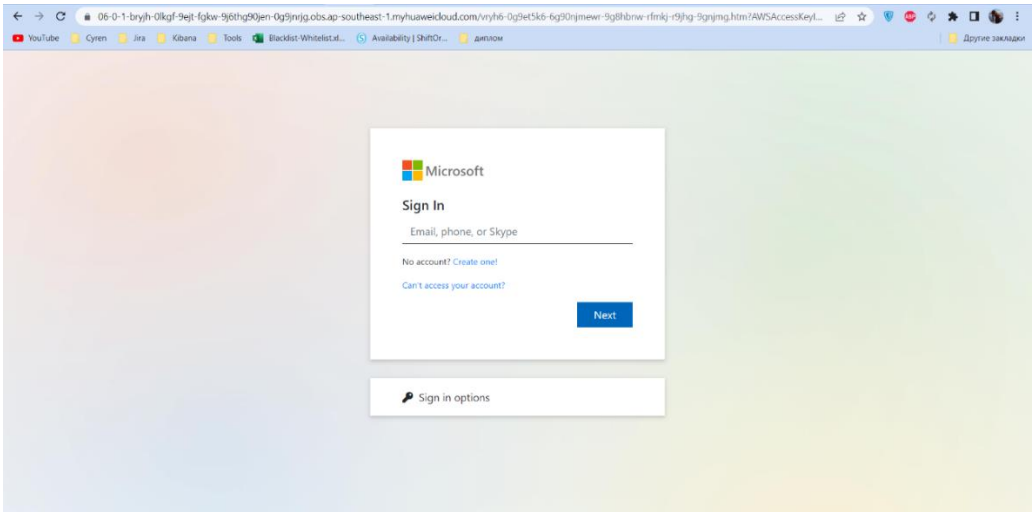


Рис.3.12 – Шахрайська сторінка входу в обліковий запис

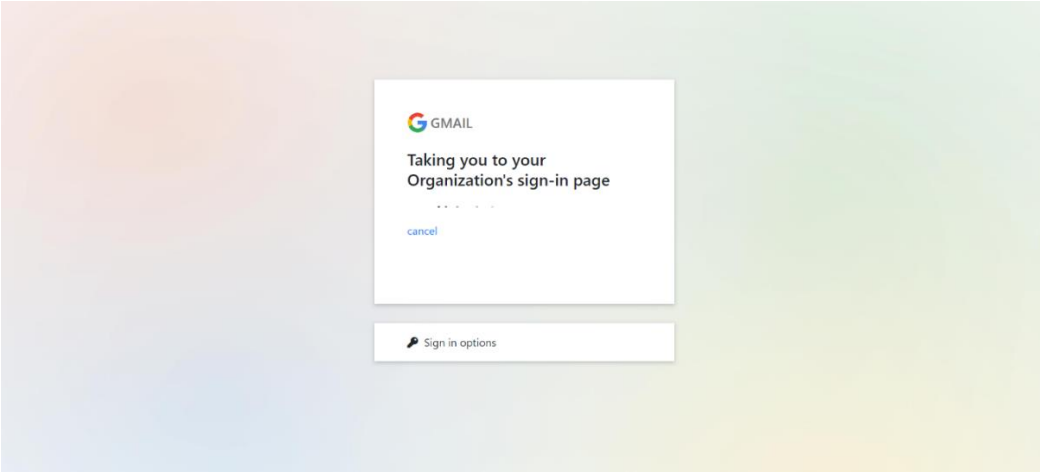


Рис.3.14. Результат введення недійсних даних для входу в обліковий запис

Отже при опрацюванні даного інциденту експерт з безпеки після отримання повідомлення від працівника, які містить файл та репутацію відправника. Результатом розслідування є підтвердження підозри, що даний електронний лист містить посилання з фішингом на сторінці з кнопкою, яка перенаправляє користувача на підроблений сайт для крадіжки конфіденційних даних (в даному випадку дані для входу в обліковий запис). Надалі такий електронний лист буде заблоковано з поміткою Phishing, а кейс закрито з ідентифікатором Phishing й програма автоматично застосує заздалегідь налаштовані компанією правила й політики як діяти (блокування всіх посилань, перенесення листа до папки

«Видалені», додавання попереджувального банера для користувачів) в разі повторного отримання подібного листа.

Тобто завданням експерта з безпеки є ретельна перевірка кожного отриманого повідомлення про інцидент, який був виявлений системою чи безпосередньо користувачем (співробітником). Схема порядку дій експерта приведена в таблиці нижче (рис. 3.15). Якщо співробітники компанії недостатньо обізнані з питань безпеки, а програма з різних причин розпізнала повідомлення як «чисте», то шахраї дуже легко отримають доступ до конфіденційних даних компанії. Так само через недостатню обізнаність користувачі можуть давати репорти на чисті повідомлення, що може гальмувати роботу експертів з безпеки, проте в будь якому разі кожний отриманий на перевірку лист буде проходити повноцінний процес розслідування інцидентів й кожен кейс буде закрито з відповідним ідентифікатором (BEC, шкідливе ПЗ, фішинг, скам/спам, clean)

Рис.3.15. Технологія процесу розслідування інцидентів експертом з безпеки

3.2. Рекомендації виявлення фішингових атак в електронній пошті з використанням методів штучного інтелекту

Для вирішення проблеми виявлення фішингових атак в електронній пошті організації, можна застосувати концепцію, в основу яких покладено методи штучного інтелекту. Ідея концепції полягає у застосуванні методів машинного навчання, які дозволяють проводити аналіз великих обсягів даних. А фішингові атаки можуть виявлятися саме через аналіз великих обсягів даних. Однією перевагою методів машинного навчання є те, що такі методи будуть виявляти неправомірні тенденції, відомі тактики та практики проведення атак такого типу.

В основі побудови концептуальної моделі виявлення фішингових атак, закладено основні типи поширених фішингових атак, з якими частіше за все можуть стикатися організації [8], які показано в таблиці 1.

Розуміння природи і фізичного змісту ознак фішингових атак дозволить на першому кроці отримати вхідні дані моделі $X(x_1, x_2, x_3 \ldots x_n,)$. Другим кроком буде визначення методики обробки вхідних даних. Третій крок полягає в застосуванні алгоритмів машинного навчання, які базуються на різних математичних концепціях та методах обробки даних. Наприклад, використання алгоритмів класифікації та регресії базуються на регресійних або класифікаційних моделях. Четвертий крок передбачає отримання результату моделі виявлення фішингових атак за обраними ознаками цільової функції Y (0, 1). Останній крок повинен включати в себе перевірку адекватності побудованої моделі виявлення фішингових атак в інформаційній системі організації (рис 3.16).

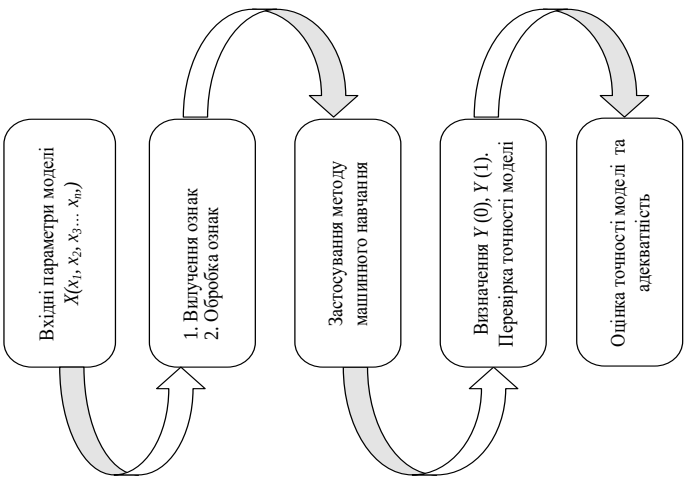


Рис. 3.16. Концептуальна модель виявлення фішингових атак

Призначення даної концепції полягає у виявлені з високою точністю та низьким рівнем помилкових спрацьовувань, щоб захистити користувачів інформаційної системи організації від кіберзагроз, які несуть в собі фішингові атаки.

Ознаки фішингових атак

Виявлення ознак фішингових атак, яке передбачає дослідження на базі машинного навчання та передбачає визначення вхідних даних (ознак) та аналіз різних ознак вебзастосунків та їх вмісту для виявлення шаблонів, типових для спроб проведення фішингових атак. На рис. 3.17 показано основні частини URL-адрес, які будуть використовуватись як вхідні дані для вилучення ознак.

Опишемо основні ознаки, які моделі машинного навчання можуть використовувати для виявлення фішингу з використанням аналізу URL-адрес:

– Невідповідність URL-адрес: вимагають перевірку, розбіжностей між відображеною URL-адресою та фактичною цільовою URL-адресою.

– URL Shorteners: виявлення використання служб скорочення URL, які можуть приховати справжнє призначення.

– Маніпуляції субдоменами: пошук зміни в субдоменах, щоб імітувати законні веб-сайти.

– Перевірка IP-адреси: порівняння домену URL-адреси з її IP-адресою, щоб виявити підозрілі відхилення.

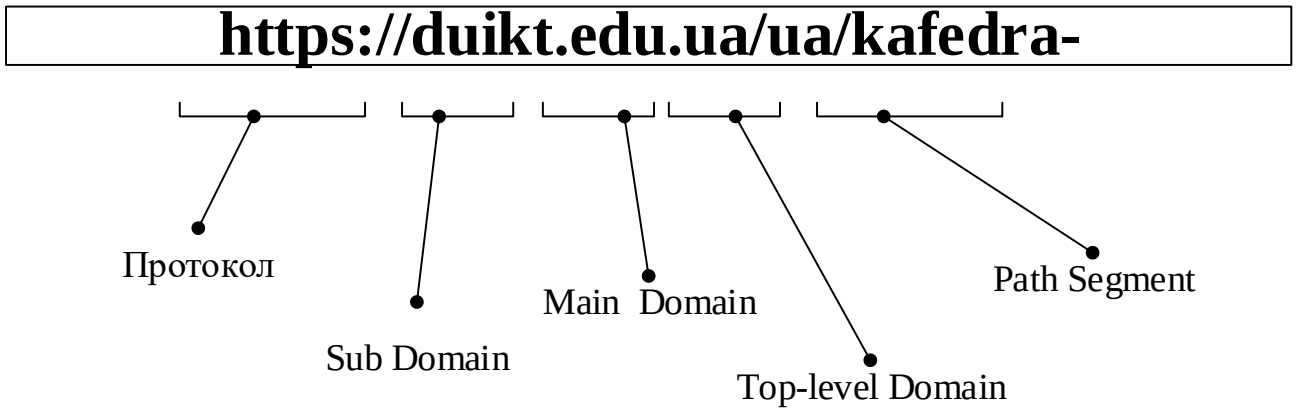


Рис.3.17. Складові URL-адреси

Отже, прийняття рішення про фішингову атаку для відповідних ознак можна визначити наступним чином:

1) *Скорочення послуги (x_1)*

Сервіси скорочення URL-адрес скорочують довгу URL адресу до значно коротшої довжини і перенаправляють на початкове посилання цільового веб-сайту.

Наприклад: URL-адресу "https://www.techopedia.com/phishing-statistics" скорочено до " surl.li/xxx/". Скорочене посилання surl.li або bit.ly перенаправляє на оригінальну URL-адресу https://www.techopedia.com/phishing-statistics". Ці скорочені посилання законно використовуються для аналітики. Навіть якщо кожна скорочена URL-адреса не є фішинговою, більшість з них потенційно можуть бути фішинговими [6].

$$f(URL) = \begin{cases} ficshing, \text{якщо } URL \text{ короткий} \\ Legatimate, \quad \text{інакше} \end{cases} \tag{1}$$

Зловмисники використовують ці сервіси для маскування несправжніх URL-адрес.

2) *Наявність IP-адреси (x_2)*

Використання IP-адреси замість URL-домену є тривожною ознакою зловмисних намірів. Приклад:

"http://125.98.3.123/fake.html"

$$f(domain) = \begin{cases} ficshing, \text{ якщо доменна частина має } IP \\ Legatimateб \quad \text{Інакше} \end{cases} \tag{2}$$

3) *PageRank (x_3)*

PageRank (PR) - це імовірнісний алгоритм, який використовує Google у своїй пошуковій системі для оцінки якості веб-сайтів і ранжування веб-сторінок відповідно до результатів пошуку. PageRank працює, перевіряючи кількість і характер асоціацій зі сторінкою, щоб приблизно оцінити, наскільки важливим є сайт.

У контексті алгоритму PageRank виявлення фішингу включає ідентифікацію шаблонів або характеристик на веб-сторінках, які вказують на те, що вони ймовірно шахрайські або зловмисні. Основні ознаки, за якими можна виявити фішинг в рамках алгоритму PageRank:

Шаблони зв'язків. Неприродні посилання – це фішингові веб-сайти можуть мати неприродні шаблони посилань, наприклад раптовий наплив посилань із низькоякісних або підозрілих веб-сайтів. Ферми посилань включають в себе сторінки, які беруть участь у фермах посилань або інших схемах маніпулювання посиланнями, імовірно, мають нижчу якість і можуть вказувати на спроби фішингу.

Якість вмісту. Низькоякісний вміст полягає у тому що фішингові сторінки часто містять неякісний вміст, зокрема орфографічні помилки, граматичні помилки або безглуздий текст. Дублювання вмісту зосереджено на тому, що сторінки з дубльованим або плагіатним вмістом можуть свідчити про фішинг або спам.

Характеристики URL-адреси. Оманливі URL-адреси - це фішингові веб-сайти, які часто використовують оманливі URL-адреси, які імітують законні сайти. Виявлення URL-адрес із неправильно написаними доменними іменами чи додатковими субдоменами може допомогти виявити спроби фішингу.

Переспрямування URL-адреси. Фішингові сторінки можуть використовувати методи переспрямування URL-адрес, щоб приховати справжню URL-адресу призначення, спрямовуючи користувачів на шкідливі сайти.

Репутація сторінки. Фішингові веб-сайти часто використовують нещодавно зареєстровані домени, щоб уникнути виявлення. Виявлення нещодавно зареєстрованих доменів може допомогти визначити можливі спроби фішингу.

Репутація домену. Сторінки, розміщені в доменах з історією зловмисної діяльності або низькою репутацією, швидше за все, є фішинговими сайтами.

Структура сторінки та функціональність. Фішингові сторінки часто містять фальшиві форми входу або запитують конфіденційну інформацію від користувачів. Виявлення сторінок із підозрілими формами чи полями введення може допомогти виявити спроби фішингу.

Отже, основною гіпотезою для визначення ознаки буде те, що більш значущі сайти, швидше за все, отримають більше посилань з інших сайтів. Це відіграє важливу роль у виявленні фішингових сайтів, оцінюючи сайт від 0 до 1. Веб-сайт є важливим або вважається з найкращою якістю, якщо:

$$f(URL) = \begin{cases} ficshing, \text{якщо PageRank} < 0{,}5 \\ Legatimate, \text{ інакше} \end{cases} \quad (3)$$

4) DoubleSlashRedirecting *(x_4)*

Коли в URL-адресі з'являється послідовність «//», вона зазвичай позначає початок компонента шляху URL-адреси. У більшості випадків це за своєю суттю не означає фішинг. Однак під час спроб фішингу зловмисники можуть неправильно використовувати послідовність "//" або маніпулювати нею, щоб створити оманливі URL-адреси, які на перший погляд здаються законними. Ось як зловмисники можуть цим скористатися:

Підробка легітимних веб-сайтів полягає в тому, що зловмисники можуть створювати фішингові URL-адреси, які починаються з «//», за якою йде законне доменне ім'я. Наприклад, вони можуть створити URL-адресу на зразок "//example.com", щоб вона виглядала так, ніби вона є частиною домену "example.com". Ця техніка має на меті змусити користувачів ввести в оману, що вони відвідують законний веб-сайт, тоді як насправді вони переспрямовуються на фішинговий сайт.

Обфускація та переспрямування полягає в тому, що зловмисники можуть використовувати "//" у поєднанні з методами переспрямування URL-адреси, щоб приховати справжнє призначення URL-адреси. Використовуючи засоби скорочення URL-адрес або інші методи перенаправлення, зловмисники можуть приховувати шкідливі URL-адреси за, здавалося б, нешкідливими, що ускладнює користувачам виявлення спроб фішингу.

Наявність символу "//" всередині URL-адреси означає, що користувач буде перенаправлений на іншу сторінку або веб-сайт. Наприклад, URL має вигляд:

"http:/www.legitimate.com//http://www.phishing.com." Ми перевіряємо позицію символу "//" в URL-адресі. Допустимо, щоб символ "//" знаходився на 8-й позиції URL-адреси

$$f(URL) = \begin{cases} ficshing, \text{якщо позиція DoubleSlash } > 8 \\ Legatimate, \text{ інакше} \end{cases} \quad (4)$$

5) HTTPs TOKEN *(x_5)*

Використання «HTTPS TOKEN» як терміна в контексті фішингу може бути дещо неоднозначним, оскільки воно не має прямого відношення до поширеної техніки фішингу. Однак можна інтерпретувати деякі поширені тактики фішингу.

Підроблений HTTPS полягає в тому, що деякі спроби фішингу можуть використовувати HTTPS, щоб створити видимість легітимності. Зловмисники можуть отримати SSL-сертифікати для своїх фішингових веб-сайтів, завдяки чому вони виглядають безпечними за допомогою протоколу HTTPS. Це може змусити користувачів подумати, що сайт безпечний, хоча насправді він шкідливий. У цьому випадку частина «HTTPS» може бути використана, щоб ввести користувачів в оману, щоб переконати, що сайт безпечний і надійний. Приклад:

http://https-www-pay-it-apps-mpp-home.solar.com/

Неправильне використання термінології дозволяє фішерам створити відчуття достовірності під час своїх спроб фішингу. Використання таких термінів, як «HTTPS» або «токен», може бути спробою зробити фішингове повідомлення більш законним або переконливим для одержувача, особливо якщо одержувач не знайомий із технічними деталями веб-безпеки.

$$f(URL) = \begin{cases} ficshing, \text{якщо «HTTPS» використовується в домені} \\ Legatimate, \text{ інакше} \end{cases} \quad (5)$$

Кожна ознака з вилучених даних складе перелік вхідних даних, для яких буде застосовано алгоритм машинного навчання. Дані для дослідження були взяті з [9]. Набір даних містить 48 ознак , отриманих із 5000 фішингових веб-сторінок і 5000 законних веб-сторінок. Перші п’ять рядків датасету зображено на рис. 3.18 [9].

	id	NumDots	SubdomainLevel	PathLevel	UrlLength	NumDash	NumDashInHostname	AtSymbol	TildeSymbol	NumUnderscor
0	1	3	1	5	72	0	0	0	0	
1	2	3	1	3	144	0	0	0	0	
2	3	3	1	2	58	0	0	0	0	
3	4	3	1	6	79	1	0	0	0	
4	5	3	0	4	46	0	0	0	0	

Рис.3.18. Набір даних фішингових сторінок

Для виявлення статистичної залежності між ознаками у наборі даних застосовано кореляцію Спірмена. Отримана матриця кореляції за тепловою шкалою (рис. 3.19), дозволяє виявити та оцінити статистичну залежність між ознаками в нашому наборі даних.

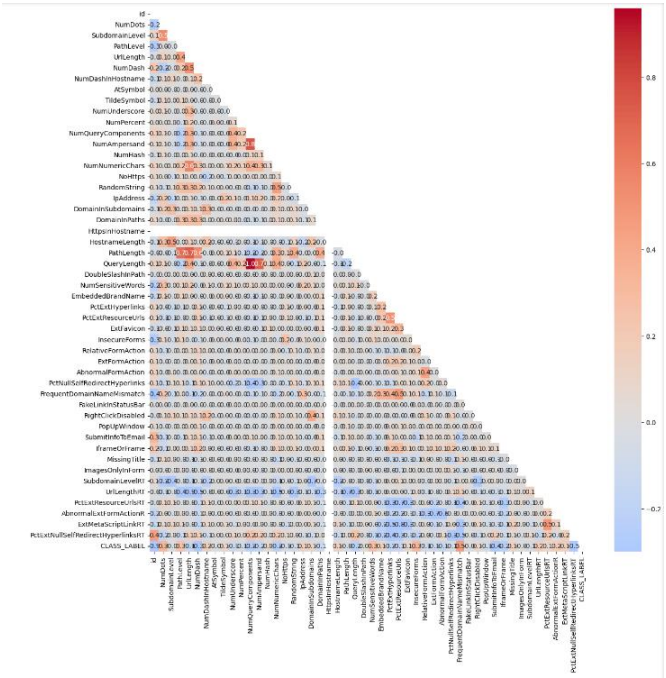


Рис.3.19. Матриця кореляції Спірмена

Особливість кореляції Спірмена полягає в тому, що вона вимірює ступінь монотонної залежності між двома змінними, не обов'язково лінійну. Така матриця

зручна для аналізу та виявлення нестандартних зв'язків, які можуть бути присутніми в даних. Аналіз отриманої матриці показує, що між отриманими даними є відносно мала кількість висококорельованих даних, які б можна було б зменшити.

Розуміння, яка кількість фішингових даних є в отриманому в [9] зображено на рис.3.20. Дані фішингового датасету мають відповідні *Label i* поділені 50 на 50 з легітимними даними.

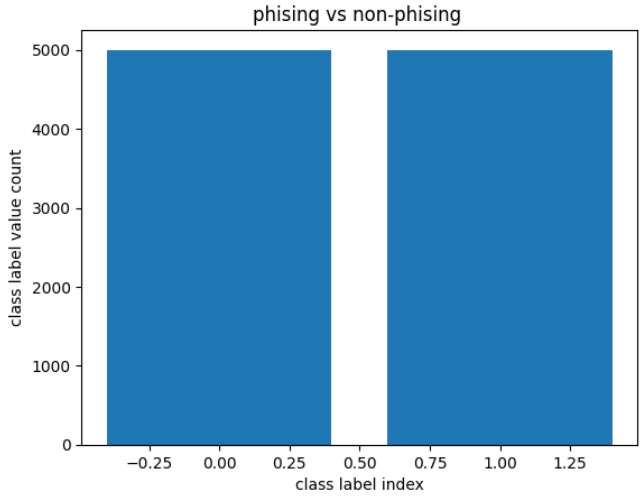


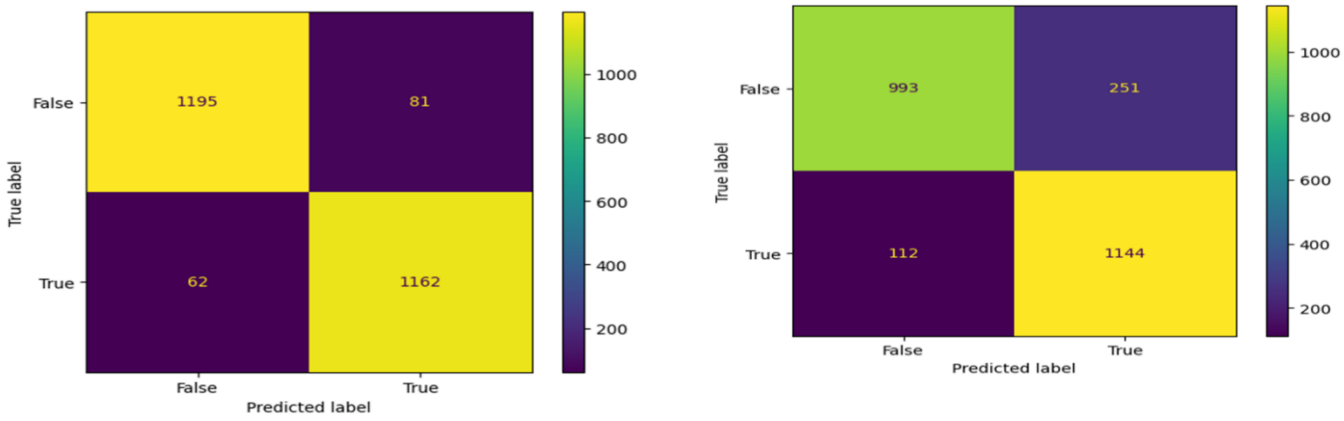
Рис. 3.20. Розподіл фішингових та легітимних даних

Прикладом алгоритму машинного навчання, як інструменту виявлення аномалій в даній роботі пропонується метод опорних векторів (SVM - Support Vector Machines). Даний алгоритм машинного навчання використовується для класифікації та регресії. SVM є інструментом який має свої переваги. Векторні представлення вхідних даних у представлені у високорозмірному просторі функцій, що дозволяє SVM ефективно розділяти дані, що мають складні зв'язки. Це особливо є важливим при аналізі великих обсягів вхідних даних, що часто відбувається в області кібербезпеки.

Фішингові сайти можуть мати складні залежності між характеристиками, що потребують моделі, здатної розділити класи в не лінійних формах. SVM може використовувати ядро для перетворення даних в високорозмірний простір, де вони можуть бути краще розділені.

SVM є ефективним інструментом для виявлення аномалій, таких як фішинг, завдяки своїм властивостям, які дозволяють працювати з високорозмірними даними, нелінійними залежностями та невеликими вибірками.

У даному дослідженні метод опорних векторів (SVM) використано для аналізу даних щодо виявлення фішингу і розглядається у розрізі застосування різних типів ядр. Лінійне ядро та радіально-базисна функція (RBF) використано в SVM. Основною відмінністю між застосуванням лінійного та RBF ядра полягає в їхніх властивостях розділення даних. Лінійне ядро використовує лінійні границі рішення, тоді як RBF може розділяти дані, використовуючи не лінійні границі рішення, що робить його корисним для нелінійних вибірок даних. Застосування використання даних моделей для даних з фішингом полягає у визначені алгоритму, який дозволить отримати вищі результаті точності моделі для класифікації вхідних даних. Дослідження виконувалось в середовищі Jupyter Notebook з використання бібліотек машинного навчання на мові Python.



а) б)

Рис.3.21. а) Матриця плутанин SVM – linear; б) Матриця плутанин SVM – RBF

Аналіз результатів отриманих даних для обчислення точності виявлення фішингових атак проводився з використання матриці плутанин. Матриця плутанини - це інструмент, який зручно використовувати для оцінки

продуктивності моделі класифікації. Візуалізація процесу прогнозування дозволяє порівнювати фактичні значення класів з передбаченими моделлю. Результати матриці плутанини показано для SVM – linear та SVM – RBF відповідно на рис.3.21. Отриманні данні необхідні для обчислення метрик точності та чутливості моделі.

Обчислення метрик класифікації дозволило отримати значення загальної точності (Accuracy), точності (Precision), яка вказує на відсоток правильно виявлених позитивних прогнозів серед всіх позитивних прогнозів та чутливості (Recall), яка вказує на відсоток правильно виявлених позитивних класів [10]. Розрахунки проводились за формулами (6), (7), (8) та показано в таблиці 3.1.

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (6)$$

$$Precision = TP / (TP + FP) \quad (7)$$

$$Recall = TP / (TP + FN) \quad (8)$$

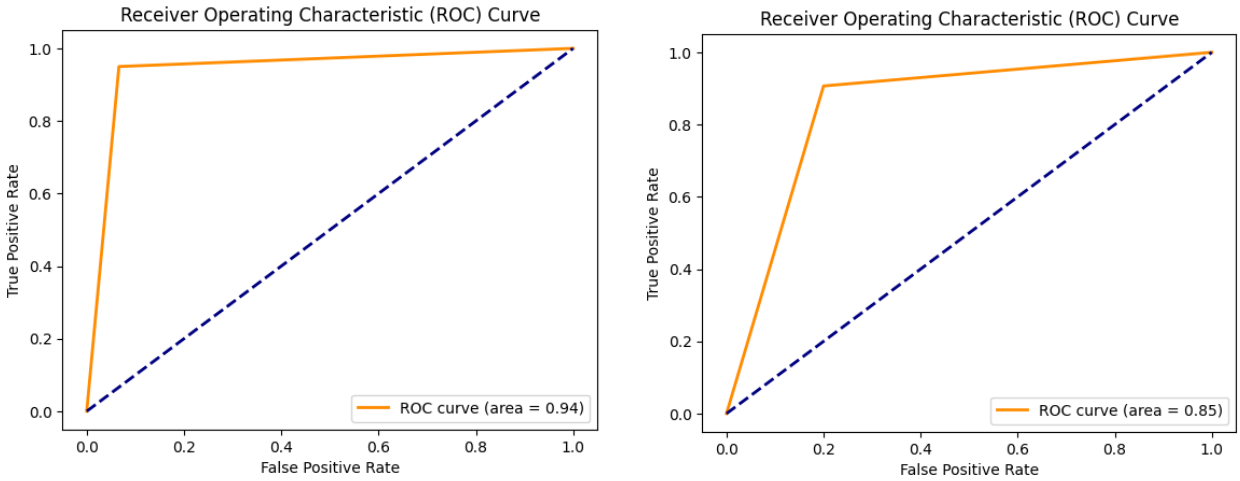
Таблиця 3.1

Результати обчислення метрик класифікації

	SVM- linear	SVM-RBF
Accuracy	0.942	0.8548
Precision	0.9374034003091191	0.8200716845878137
Recall	0.9498825371965545	0.910828025477707

Аналіз обчислених метрик класифікації показав, що кращі результати надає SVM- linear, в порівнянні з SVM – RBF. Це пов’язано з тим, що дані лінійно роздільні або кількість їх ознак невелика в порівнянні з обсягом даних. Отже, лінійне ядро підходить для задач, де взаємозв'язки між ознаками та вихідною змінною лінійні.

Використання додаткових метрик, таких як крива ROC надають змогу визначити адекватність класифікатора та порівняти його з іншими отриманими моделями, як це показано на рис.3.22.



а) б)

Рис.3.22. а) метрика ROC для SVM- linear; б) метрика ROC для SVM- RBF

Чим більше площа під кривою ROC, тим краще модель робить прогнози щодо визначення класів. Отже, отримані в попередньому кроці результати підтверджуються результатами отриманих ROC кривих, з яких видно що площа SVM - linear більша і відображає частку правильно виявлених позитивних прикладів відносно загальної кількості позитивних прикладів.

Запропонована концептуальна модель виявлення фішингових атак дозволяє за запропонованими етапами виявляти фішингові атаки з використанням методів машинного навчання.

Cyren inbox security є гарною платформою для впровадження запропонованої концепці виявлення фішингових атак.

3.3 Розробка рекомендацій щодо захисту інформаційних ресурсів від фішингових атак

Згідно з даними звітів від Anti-Phishing Working Group фішингові атаки на корпоративну електронну пошту потроху зростали починаючи з 15%, які можна було спостерігати з початком 2023 року і дійшли до відмітки у 21% від усіх атак, який спостерігався на початку 2024 року. Це доводить необхідність захисту корпоративної електронної пошти, оскільки кількість атак на сектор

SAAS/Webmail постійно зростає, а втрата критичних даних може значно вплинути на репутацію, критичні дані якими володіє компанія та її фінансовий стан.

Для якісного захисту корпоративної пошти компанії можуть скористатися послугами та технологіями, які надає програма Cyren Inbox Security by Data443. Дане рішення має багато переваг, серед яких можна виділити легку імплементацію у вже існуючу систему, завдяки тому, що дане рішення є повністю хмарним або ж використовувати його як окрему систему захисту. Програма повністю контролює й відслідковує діяльність в середині кожної скриньки та аналізує вміст листа будь-то текстові повідомлення URL-адреси чи інші шкідливі вкладення, завдяки використанню штучного інтелекту, який допомагає відстежувати загрози у поштовій скринці.

Cyren Inbox Security, швидко й легко, підключається до поштових скриньок працівників компанії та дозволяє фільтрувати всі вхідні повідомлення та їх вміст в залежності від налаштованих правил і політик компанії. До того ж великою перевагою є залучення безпосереднього користувача поштової електронної скриньки, що допомагає виявити аномалії в отриманому листі чи заховану загрозу, яку з різних причин не змогла виявити програма. Це налаштування програми дозволяє опрацьовувати інциденти та навчати систему захисту реагувати на нові типи та види загроз за допомогою машинного навчання.

Завдяки Cyren Inbox можна автоматизувати велику кількість процесів, що дає можливість експертам з безпеки приділити більше уваги інцидентам та швидше виявляти й усувати загрози.

Дослідження щодо користі навчання співробітників від IBM/Ponemon Cost of a Data Breac у 2023 році (пункт 1.2) довело що підняття обізнаності працівників щодо інформаційних загроз може значно покращити захист з середини компанії, адже одним з найпопулярніших прийомів шахраїв є викрадення облікових записів працівників чи керівників, після чого можна спостерігати виток конфіденційних даних та/чи коштів компанії. В будь якому разі будуть понесені репутаційні та фінансові збитки, що можуть сягати мільйони доларів.

А отже дуже важливо захищати електронну корпоративну пошту компанії, як від зовнішніх, так і від внутрішніх чинників, що можуть вплинути на інформаційну безпеку організації.

Висновки до розділу 3

1. Розроблено рекомендації щодо застосування технології виявлення фішингових атак на базі Cyren inbox security для розслідування інцидентів, що дозволить покращити рівень захисту інформаційних ресурсів організації, оскільки кожен виявлений інцидент буде розглянутий експертами з безпеки, що в свою чергу гарантує вживання тих чи інших мір з забезпечення інформаційної безпеки.

2. Розроблено рекомендації щодо використання методів штучного інтелекту для виявлення фішингових атак на основі розробленої концепції, яка використовує аналіз URL-адрес.

3. Розроблено рекомендації щодо захисту корпоративної електронної пошти від фішингових атак.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи отримано наступні наукові результати:

1 Проведено дослідження проблеми щодо захисту інформаційних ресурсів організації від фішингових атак, яке показало що фішингові атаки є однією з найбільш розповсюджених атак.

2. Визначено, що електронна пошта працівників організаціє є найбільш вразливою до фішингових атак, компрометація якої може призвести до несанкціонованого доступу до інформаційних ресурсів організації

3. Проведено аналіз рішень захисту інформаційних ресурсів від фішингу, які здатні виявляти фішингові атаки, які несуть масований характер, і тому людського ресурсу не вистачить для обробки та виявлення загроз великій кількості атак, а отже необхідно використовувати технології які надають відповідні рішення.

4. Визначено архітектуру Cyren inbox security, яка аналізує URL-адреси у реальному часі, проводить постійне сканування та аналіз поведінки поштової скриньки, надає відповідь та рекомендації завдяки наявності політик виправлення для кожного користувача.

5. Розглянуто основний функціонал Cyren inbox security, який дозволяє виявляти фішингові атаки на електронну пошту організації.

6. Розроблено рекомендації щодо застосування технології виявлення фішингових атак на базі Cyren inbox security для розслідування інцидентів, що дозволить покращити рівень захисту інформаційних ресурсів організації, оскільки кожен виявлений інцидент буде розглянутий експертами з безпеки, що в свою чергу гарантує вживання тих чи інших мір з забезпечення інформаційної безпеки.

7. Розроблено рекомендації щодо використання методів штучного інтелекту для виявлення фішингових атак на основі розробленої концепції, яка використовує аналіз URL-адрес та підвищує точність виявлення фішингових атак на електронну пошту організації

ПЕРЕЛІК ПОСИЛАНЬ

1. Phishing activity Trend report 1st quarter 2023 [Електронний ресурс] – Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q1_2023.pdf?_gl=1*kzu8a*_ga*MTMwNzM1ODc4LjE3MjczNzIyMDA.*_ga_55RF0RHXSR*MTcyNzUyNTE4Ni40LjEuMTcyNzUyNTE4OS4wLjAuMA

2. Phishing activity Trend report 2nd quarter 2023 [Електронний ресурс] – Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf?_gl=1*kzu8a*_ga*MTMwNzM1ODc4LjE3MjczNzIyMDA.*_ga_55RF0RHXSR*MTcyNzUyNTE4Ni40LjEuMTcyNzUyNTE4OS4wLjAuMA

3. Phishing activity Trend report 3rd quarter 2023 [Електронний ресурс] – Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q3_2023.pdf?_gl=1*kzu8a*_ga*MTMwNzM1ODc4LjE3MjczNzIyMDA.*_ga_55RF0RHXSR*MTcyNzUyNTE4Ni40LjEuMTcyNzUyNTE4OS4wLjAuMA

4. Phishing activity Trend report 4th quarter 2023 [Електронний ресурс] – Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf?_gl=1*kzu8a*_ga*MTMwNzM1ODc4LjE3MjczNzIyMDA.*_ga_55RF0RHXSR*MTcyNzUyNTE4Ni40LjEuMTcyNzUyNTE4OS4wLjAuMA

5. Phishing activity Trend report 1st quarter 2024 [Електронний ресурс] – Режим доступу: 5. https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf?_gl=1*kzu8a*_ga*MTMwNzM1ODc4LjE3MjczNzIyMDA.*_ga_55RF0RHXSR*MTcyNzUyNTE4Ni40LjEuMTcyNzUyNTE4OS4wLjAuMA

6. Phishing attacks: defending your organization [Електронний ресурс] – Режим доступу: https://www.ncsc.gov.uk/guidance/phishing

7. What Is Phishing? [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/us/threat-reference/phishing

8. Phishing & Cyber Security Trends Report (Updated for 2024) [Електронний ресурс] – Режим доступу: https://hoxhunt.com/guide/cyber-security-trends-report#strongexecutive-summarystrong

9. Cybersecurity for small business phishing [Електронний ресурс] – Режим доступу: https://www.ftc.gov/system/files/attachments/phishing/cybersecurity_sb_phishing.pdf

10. Proofpoint Email Protection. Detect and Block Both Malicious and Malware-less Email Threats [Електронний ресурс] – Режим доступу: 10. https://www.proofpoint.com/sites/default/files/data-sheets/pfpt-us-ds-email-protection-v24.pdf

11. Barracuda Email Protection [Електронний ресурс] – Режим доступу: 11. https://assets.barracuda.com/assets/docs/dms/DS_Phishing-and-impersonation-protection_US.pdf

12. Cyren Inbox Security [Електронний ресурс] – Режим доступу: 12. https://data443.com/wp-content/uploads/2023/11/Cyren-Inbox-Security-data-sheet_2023.pdf

13. Data443 Risk Mitigation, Inc. All Things Data Security [Електронний ресурс] – Режим доступу: https://data443.com/why-data443/

14. Cyren Inbox Security [Електронний ресурс] – Режим доступу: https://digpath.co.uk/cyren/#:~:text=CIS%20protects%20against%20new%2C%20previously,if%20an%20email%20is%20malicious

15. Cyren Inbox Protection Manager [Електронний ресурс] – Режим доступу: https://data443.com/wp-content/uploads/2024/09/Cyren-Inbox-Protection-Manager-Datasheet.pdf

16. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

17. Cost of a data breach 2023 | IBM. IBM in Deutschland, Österreich und der Schweiz. https://www.ibm.com/reports/data-breach

18. Phishing. NIST. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

19. Alanezi, M. (2021). Phishing Detection Methods: A Review. Technium: Romanian Journal of Applied Sciences and Technology, 3(9), 19–35. https://doi.org/10.47577/technium.v3i9.4973

20. Buchyk, S., Shutenko, D., & Toliupa, S. Phishing Attacks Detection. Information Technology and Implementation. (IT&I-2022), November 30 - December 02, 2022, Kyiv, Ukraine. pp.193-201. https://ceur-ws.org/Vol-3384

21. Indrasiri, P. L., Halgamuge, M. N., & Mohammad, A. (2021). Robust Ensemble Machine Learning Model for Filtering Phishing URLs: Expandable Random Gradient Stacked Voting Classifier (ERG-SVC). IEEE Access, 9, 150142–150161. https://doi.org/10.1109/access.2021.3124628

22. Rushton, J. (2024, 1 березня). 50+ Phishing Statistics You Need to Know – Where, Who & What is Targeted. Cyber Threats. https://www.techopedia.com/phishing-statistics

23. Chiew, K. L., Tan, C. L., Wong, K., Yong, K. S. C., & Tiong, W. K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. Information Sciences, 484, 153–166. https://doi.org/10.1016/j.ins.2019.01.064

24. Phishing Dataset for Machine Learning. Kaggle: Your Machine Learning and Data Science Community. https://www.kaggle.com/datasets/shashwatwork/phishing-dataset-for-machine-learning

25. Haidur, G. I. (2021). Detection of traffic anomalies in the information systems of organizations using Machine Learning methods on the base of algorithms for forecasting category fields. Telecommunication and Information Technologies, 73(4). https://doi.org/10.31673/2412-4338.2021.044153

КОПІЇ ДЕМОНСТРАЦІЙНИХ АРКУШІВ