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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби протидії атакам соціальної інженерії на електронну пошту інформаційній системі організації на базі Proofpoint»

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

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

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

_____Микита ТРЕТЯКОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ТРЕТЯКОВ Микита
(прізвище, ім'я)

Керівник д. т. н., професор ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ВСТУП

Актуальність теми. Кіберзлочинці давно змістили фокус своєї уваги з суто технічної інфраструктури на людей – найбільш слабку ланку будь-якої системи безпеки. Сьогоднішні атаки базуються не лише на використанні технічних недоліків програмного забезпечення (далі – ПЗ) та апаратних засобів, а й на експлуатації «людських вразливостей». Це означає, що зловмисники активно досліджують поведінкові патерни користувачів, їх емоційний стан та психологічні слабкості, щоб переконати їх надати доступ до конфіденційної інформації або виконати певні дії, що спричиняють фінансові збитки. Таким чином, навіть добре захищені системи можуть стати уразливими, якщо співробітники організацій не будуть відповідно підготовлені та обізнані.

Одним із найпоширеніших каналів для таких атак залишається електронна пошта (далі – ЕП). Хоча вона і є універсальним засобом комунікації, проте з самого початку ця платформа не була створена з дотриманням високих стандартів кібербезпеки. З цієї причини, саме через поштові сервіси проводяться, частіше за все, соціоінженерні кампанії, під час яких користувачам надсилаються повідомлення, що містять шкідливі посилання або вкладення. Такі повідомлення можуть бути надзвичайно переконливими, адже зловмисники ретельно вивчають мовні особливості, стиль спілкування та внутрішні процеси компаній, аби зробити свої листи максимально схожими на легітимні повідомлення.

Важливо зазначити, що високий рівень ефективності атак соціальної інженерії (далі – СІ) зумовлений їх динамічністю та постійним розвитком. Сучасні кіберзлодії активно впроваджують новітні технології, використовуючи штучний інтелект (Artificial Intelligence, далі – AI) для автоматизованого аналізу поведінки користувачів та генерації індивідуалізованих атак. Вони постійно вивчають нові техніки психологічного впливу, що дозволяє їм створювати надзвичайно правдоподібні сценарії для введення в оману як окремих осіб, так і цілих організацій.

Особливо актуальним ця проблема стає в умовах сучасних військових та гібридних конфліктів. Під час війни чи кризи атаки СІ можуть стати потужним інструментом дестабілізації, впливаючи як на державний, так і на корпоративний рівні. Наприклад, такі кампанії, спрямовані на державні установи чи військові організації, можуть стати причиною витоку критичних даних, розкриття місць дислокації військових частин або навіть створення умов для проведення масштабних кібератак. Крім того, дані операції, які проводяться через електронну пошту та соціальні мережі, можуть призводити до деморалізації населення, створюючи паніку та посилюючи загальну невпевненість у стабільності державних інституцій.

Враховуючи постійне зростання складності та чисельності кіберзагроз, традиційні методи захисту, орієнтовані виключно на технічні аспекти, виявляються недостатніми. Навіть найсучасніші антивірусні програми та системи захисту можуть не впоратися з атаками, що експлуатують людський фактор. Саме тому питання захисту ЕП набуває критичного значення для будь-якої організації. Сучасні платформи кібербезпеки, такі як Proofpoint, пропонують комплексні рішення, що включають не лише виявлення та блокування шкідливих повідомлень, але й аналіз підозрілої активності, навчання співробітників основам кібергігієни та швидке реагування на загрози.

Особливо важливо, щоб технології захисту постійно оновлювалися відповідно до нових викликів та методик атак, адже кіберзлочинці не стоять на місці, а постійно вдосконалюють свої підходи для досягнення максимальної ефективності. Таким чином, комплексна стратегія захисту, що поєднує технічні рішення з підвищенням обізнаності користувачів, є ключовою умовою для забезпечення безпеки в умовах постійних кіберзагроз.

Мета роботи. Метою роботи є аналіз загроз соціальної інженерії, що реалізуються через електронну пошту, з метою виявлення слабких місць інформаційних систем організації та розробки ефективних заходів протидії.

Об'єкт дослідження. Об'єктом даного дослідження виступає електронна пошта, як частина інформаційної системи організації.

Предмет дослідження. Методи та засоби запобігання та протидії атакам соціальної інженерії на електронну пошту, із застосуванням рішень платформи Proofpoint Core Email Protection.

Завдання кваліфікаційної роботи:

– Дослідити сутність проблеми атак СІ в системах ЕП.

– Проаналізувати існуючі рішення для протидії загрозам.

– Проаналізувати методи та засоби протидії загрозам на базі рішення Proofpoint.

– Розробити рекомендації щодо застосування рішення Proofpoint Core Email Protection в організації.

Методи дослідження. Аналіз наукових джерел і технічної документації, опрацювання стандартів та дослідження прикладів атак соціальної інженерії.

Практичне значення одержаних результатів. Розроблено рекомендації щодо впровадження Proofpoint Core Email Protection в інфраструктуру організації для захисту від соціоінженерних загроз.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Цифрова трансформація кібербезпеки», яка відбулася 24 квітня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СИСТЕМАХ ЕЛЕКТРОННОЇ ПОШТИ

1.1 Аналіз проблеми впливу атак соціальної інженерії на електронну пошту

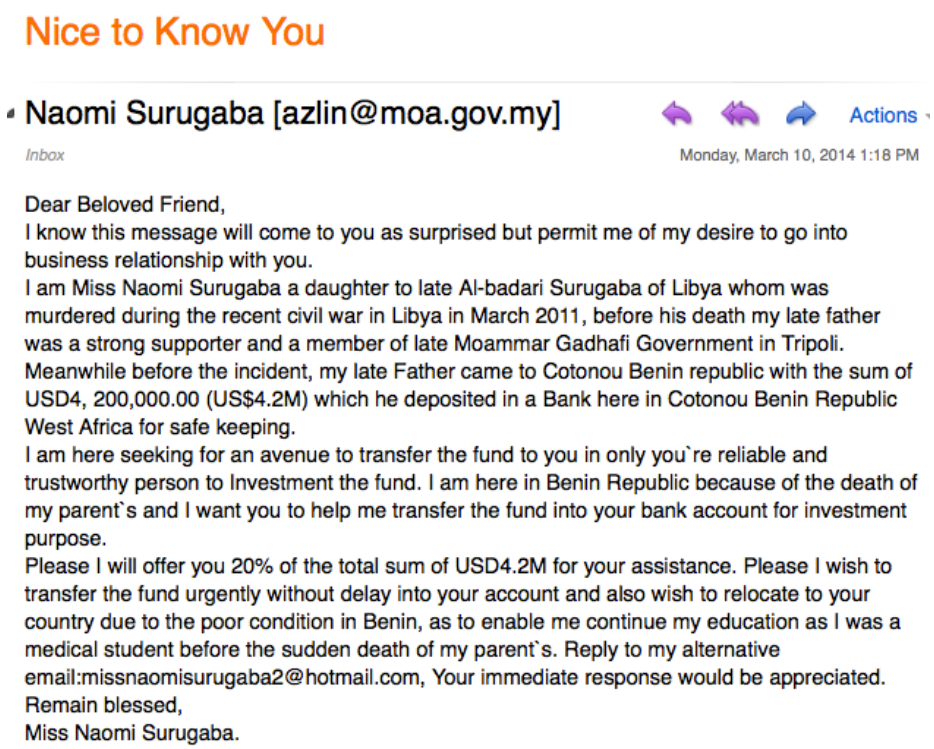
ЕП є універсальним інструментом комунікації, який відіграє критично важливу роль у сучасному бізнес-середовищі. За час свого існування ЕП трансформувалася з простого засобу передачі повідомлень у потужний інструмент бізнес-комунікацій. Щодня до поштових скриньок користувачів надходять мільярди електронних листів. Серед цього величезного потоку інформації лише невелика частина може бути класифікована як життєво необхідна, тоді як інша частина – або є надокучливою, або містить потенційно шкідливий контент.

Саме ця невизначеність у характері повідомлень створює сприятливе середовище для соціотехнічних атак, оскільки зловмисники можуть легко втягнути користувача в пастку, маскуючи свій шкідливий намір під виглядом легітимної комунікації [1].

Соціальні інженери розробляють свої повідомлення таким чином, щоб вони здавалися абсолютно природними, іноді навіть ідентичними внутрішнім комунікаціям організації. Основна мета зловмисників – обманом змусити одержувачів перейти за шкідливими посиланнями, завантажити скомпрометовані файли або добровільно надати конфіденційні дані.

Ця особливість атаки СІ критично небезпечна, оскільки полює на людську природу та емоції. Люди природньо схильні довіряти, допомагати або реагувати на авторитетні фігури, що робить їх вразливими до маніпуляцій.

Нижче можна розглянути приклад такого електронного повідомлення, що наробило багато шуму в інтернет-просторі (див. рис. 1.1.1-1.1.2):



Nice to Know You

Naomi Surugaba [azlin@moa.gov.my]

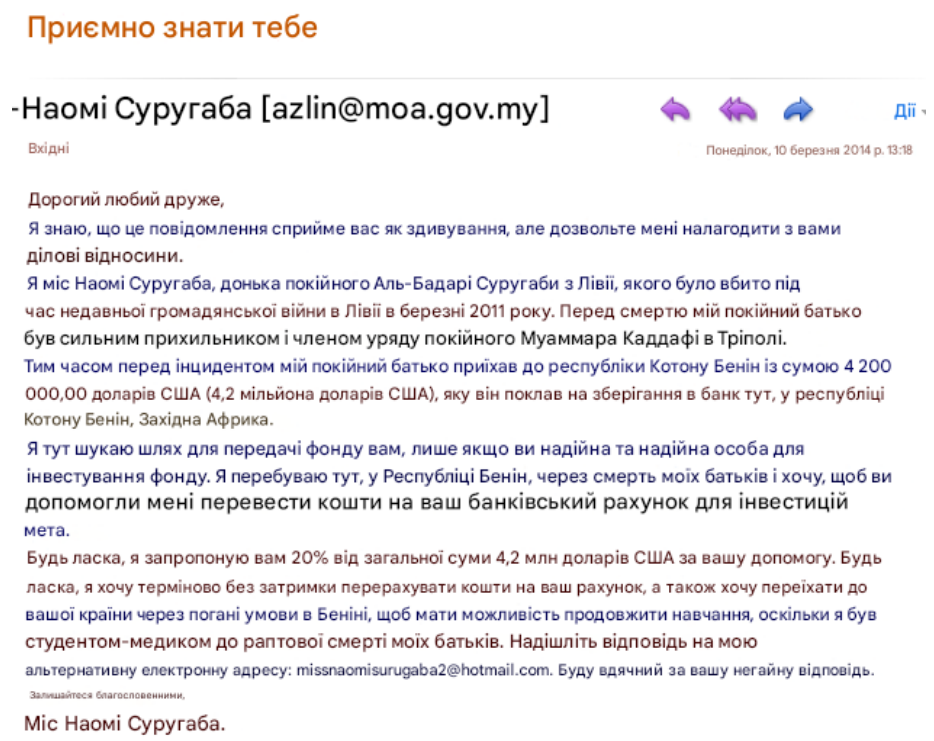
Actions

Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Рис. 1.1.1. Приклад фішингового електронного листа від «лівійського принца» (англ. версія) [8]



Приємно знати тебе

-Наомі Суругаба [azlin@moa.gov.my]

Дії

Вхідні

Понеділок, 10 березня 2014 р. 13:18

Дорогий любий друже,
Я знаю, що це повідомлення сприйме вас як здивування, але дозвольте мені налагодити з вами ділові відносини.
Я міс Наомі Суругаба, донька покійного Аль-Бадарі Суругаби з Лівії, якого було вбито під час недавньої громадянської війни в Лівії в березні 2011 року. Перед смертю мій покійний батько був сильним прихильником і членом уряду покійного Муаммара Каддафі в Тріполі.
Тим часом перед інцидентом мій покійний батько приїхав до республіки Котону Бенін із сумою 4 200 000,00 доларів США (4,2 мільйона доларів США), яку він поклав на зберігання в банк тут, у республіці Котону Бенін, Західна Африка.
Я тут шукаю шлях для передачі фонду вам, лише якщо ви надійна та надійна особа для інвестування фонду. Я перебуваю тут, у Республіці Бенін, через смерть моїх батьків і хочу, щоб ви допомогли мені перевести кошти на ваш банківський рахунок для інвестицій мета.
Будь ласка, я запропоную вам 20% від загальної суми 4,2 млн доларів США за вашу допомогу. Будь ласка, я хочу терміново без затримки перерахувати кошти на ваш рахунок, а також хочу переїхати до вашої країни через погані умови в Беніні, щоб мати можливість продовжити навчання, оскільки я був студентом-медиком до раптової смерті моїх батьків. Надішліть відповідь на мою альтернативну електронну адресу: missnaomisurugaba2@hotmail.com. Буду вдячний за вашу негайну відповідь.
Залишайтеся благословенними,
Міс Наомі Суругаба.

Рис. 1.1.2. Приклад фішингового електронного листа від «лівійського принца» (укр. версія) [8]

У контексті електронних листів атаки CI створюють враження, що вони походять з надійних джерел – від колеги, начальника чи відомої установи. Це хибне відчуття безпеки призводить до помилок у судженнях, що робить ЕП ефективним засобом для такого виду атак [2].

Згідно зі звітом Q4 про ландшафт кіберзагроз у 2024 році (Q4 2024 Cyber Threat Landscape) [3], ключовою тенденцією був постійний розвиток фішингових методів і підходів, про що свідчить продовження соціотехнічних технік як домінуючих методів атак. У 2024 році фішинг продовжував залишатися домінуючим методом початкового доступу. Порівняно з 2023 роком, зросла кількість випадків використання CI (див. рис. 1.2):

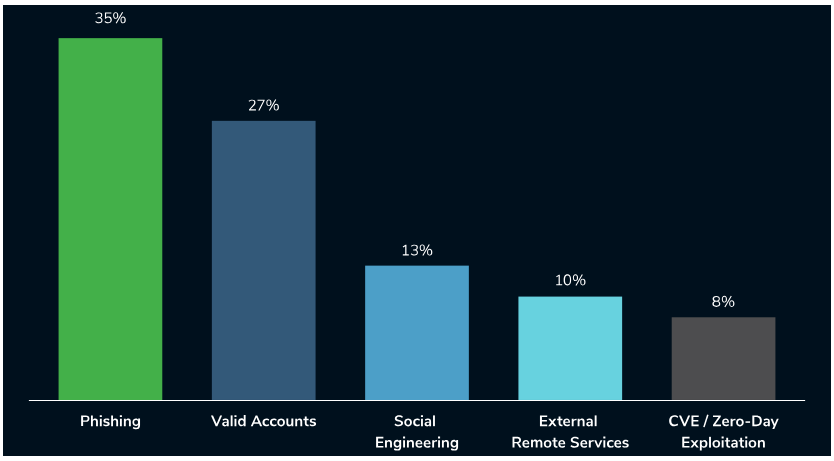


Рис. 1.2. Найпопулярніші методи первинного доступу у 2024 році [3]

Необхідно зазначити, що кількість випадків компрометації ЕП стрімко зросла, що зробило її найпоширенішим типом загроз у 2024 році (див. рис. 1.3):

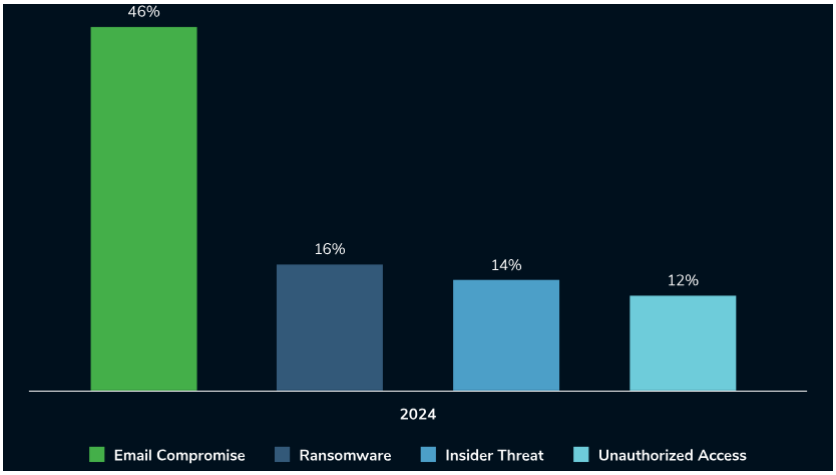


Рис. 1.3. Найпопулярніші типи інцидентів у 2024 році [3]

Більшість випадків компрометації ЕП в цій категорії були пов’язані з фінансовим шахрайством, таким як фальшиві рахунки-фактури, видача себе за постачальника або виведення коштів із зарплатного фонду.

1.2 Класифікація атак соціальної інженерії на електронну пошту

Як було зазначено вище, одне з найбільших слабких місць у стратегії кібербезпеки будь-якої організації – це людські помилки. Атаки СІ використовують цю вразливість, змушуючи людей, які нічого не підозрюють, порушувати безпеку та розкривати конфіденційну інформацію.

Тому єдиний спосіб не стати жертвою СІ через ЕП – це вивчити методи, психологічні тригери та технологічні інструменти, які використовують зловмисники. Шахраї використовують багато різних типів атак СІ, але деякі загальні ознаки можуть допомогти їх виявити та уникнути [4].

Серед основних видів таких атак можна виділити:

– *Фішингова атака електронною поштою – Phishing email attack.* Даний метод один із найпопулярніших видів атак. У цій афері кіберзлочинець надсилає фіктивний електронний лист, який нібито надійшов від надійного джерела (наприклад, банку або онлайн-сервісу). Шахраї використовують такі електронні листи, щоб виманити особисту інформацію (наприклад, паролі та імена користувачів у зв’язці, номери кредитних карток) [5].

Процес типової фішингової атаки можна побачити нижче (див. рис. 1.4):

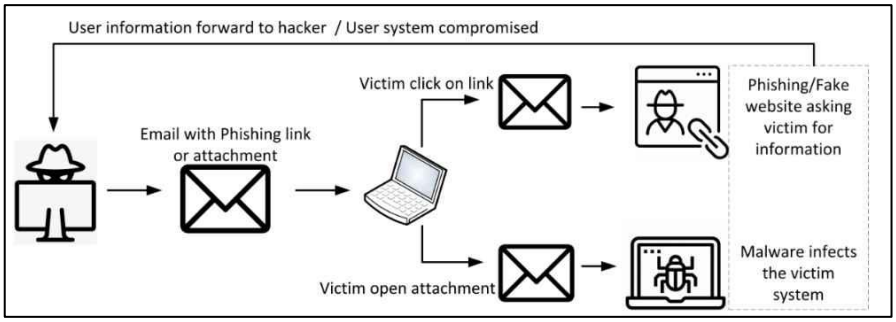


Рис. 1.4. Процес типової фішингової атаки електронною поштою [13]

– *Цільова фішингова атака – Spear Phishing attack.* Такі атаки схожі на звичайну фішингову атаку, проте націлені вони на конкретну людину чи організацію [6].

Зловмисники зазвичай заздалегідь вивчають свої цілі через соціальні мережі або додаткову загальнодоступну інформацію, щоб створити максимально персоналізований фішинговий лист, який з великою ймовірністю дійсно обдурить жертву. Соціальні інженери вкладають багато зусиль у створення переконливих та вигідних сценаріїв, які спонукають потенційну жертву відповісти на листа або виконати вказівки, надані в електронному повідомленні [7].

У свою чергу *цільовий фішинг* розділяється на такі основні тактики атак, як:

– *Шахрайство з керівниками – CEO fraud.* При такій тактиці зловмисник видає себе за високопоставленого керівника, щоб обманом змусити жертву здійснити бажану дію.

Під час даної атаки, співробітники та підлеглі можуть не ставити під сумнів серйозність запитів, особливо якщо вони надходять від керівника, який має владні повноваження.

Нижче наведено приклад такого електронного повідомлення (див. рис. 1.5.1-1.5.2):

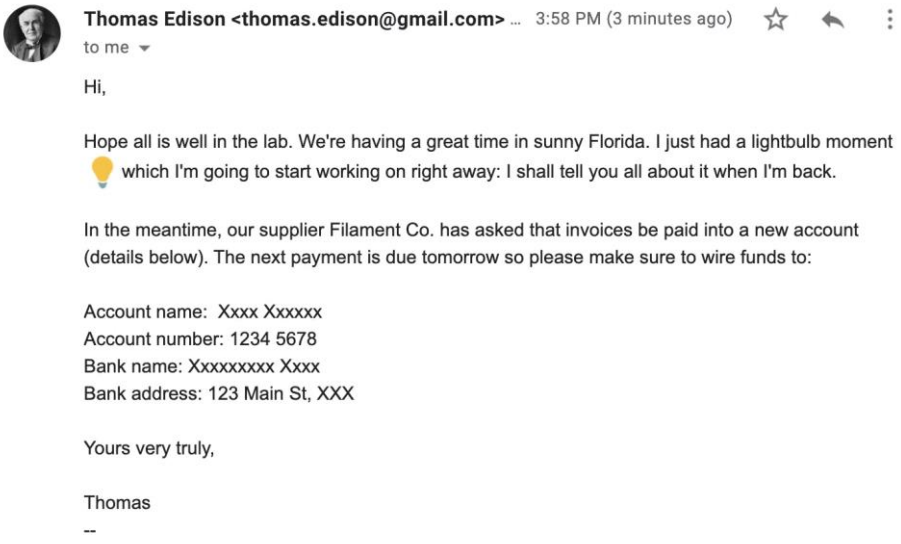
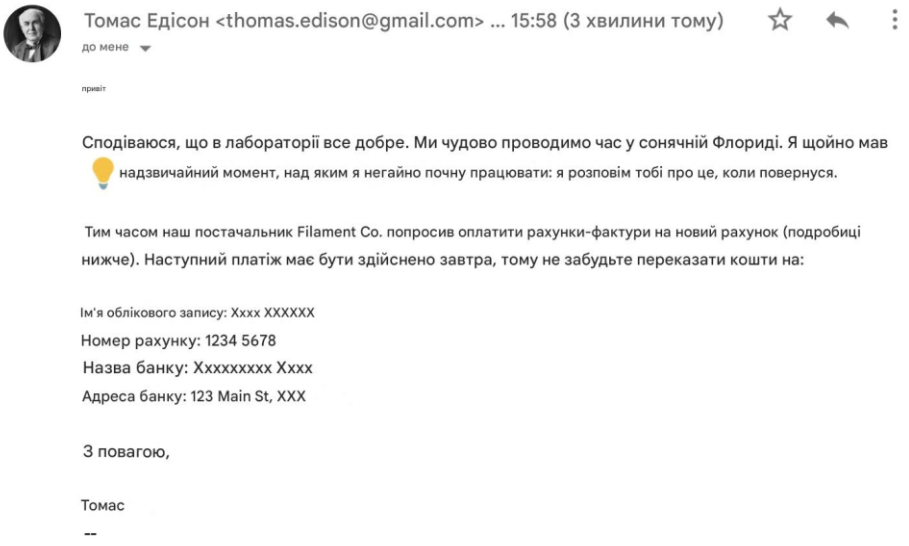


Рисунок 1.5.1. Приклад електронного листа, надісланого за допомогою тактики «CEO fraud» (англ. варіант) [10]


Томас Едісон <thomas.edison@gmail.com> ... 15:58 (3 хвилини тому)

до мене

привіт

Сподіваюся, що в лабораторії все добре. Ми чудово проводимо час у сонячній Флориді. Я щойно мав надзвичайний момент, над яким я негайно почну працювати: я розповім тобі про це, коли повернуся.

Тим часом наш постачальник Filament Co. попросив оплатити рахунки-фактури на новий рахунок (подробиці нижче). Наступний платіж має бути здійснено завтра, тому не забудьте переказати кошти на:

Ім'я облікового запису: Xxxx XXXXXX
Номер рахунку: 1234 5678
Назва банку: Xxxxxxxxx Xxxx
Адреса банку: 123 Main St, XXX

З повагою,

Томас
--

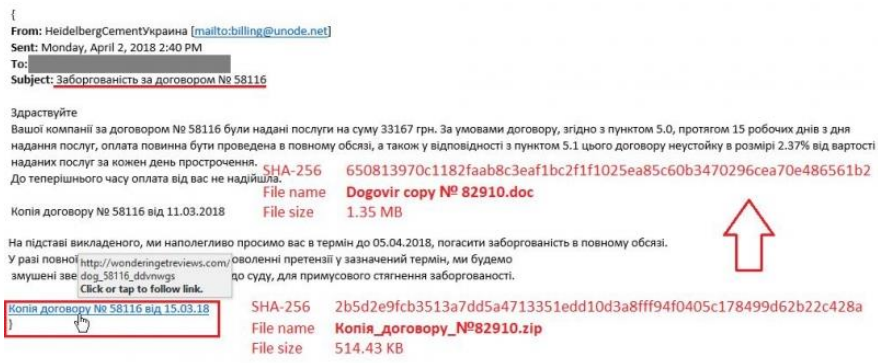
Рис. 1.5.2. Приклад електронного листа, надісланого за допомогою тактики «CEO fraud» (укр. варіант) [10]

– *Китобійний фішинг – Whale Phishing, Whaling.* Даний різновид фішингу націлений на керівників високого рівня або осіб, які мають доступ до конфіденційної інформації. Зловмисники націлені на «велику рибу» – «китів» організації.

Китобійні атаки часто включають в себе високий ступінь складності та хитромудрі методи СІ, щоб побудувати довіру та авторитет зловмисника.

Соціальний інженер може провести ретельне дослідження посадових обов'язків, історії роботи та особистого життя жертви, щоб створити максимально персоналізований і переконливий електронний лист.

Нижче наведено приклад такого електронного повідомлення (див. рис. 1.6):


From: HeidelbergCementУкраина [mailto:billing@unode.net]
Sent: Monday, April 2, 2018 2:40 PM
To:
Subject: Заборгованість за договором № 58116

Здраствуйте
Вашої компанії за договором № 58116 були надані послуги на суму 33167 грн. За умовами договору, згідно з пунктом 5.0, протягом 15 робочих днів з дня надання послуг, оплата повинна бути проведена в повному обсязі, а також у відповідності з пунктом 5.1 цього договору неустойку в розмірі 2.37% від вартості наданих послуг за кожен день прострочення.
До теперішнього часу оплата від вас не надійшла.

SHA-256 650813970c1182faab8c3eaf1bc2f1f1025ea85c60b3470296cea70e486561b2
File name Dogovir copy № 82910.doc
File size 1.35 MB

Копія договору № 58116 від 11.03.2018

На підставі викладеного, ми наполегливо просимо вас в термін до 05.04.2018, погасити заборгованість в повному обсязі.
У разі повної http://wonderingetreviews.com/ оволенні претензії у зазначений термін, ми будемо
змушені зве до суду, для примусового стягнення заборгованості.
dog_58116_ddvnwgs
Click or tap to follow link.

Копія договору № 58116 від 15.03.18

SHA-256 2b5d2e9fcb3513a7dd5a4713351edd10d3a8fff94f0405c178499d62b22c428a
File name Копія_договору_№82910.zip
File size 514.43 KB

Рис. 1.6. Приклад електронного листа, надісланого за допомогою тактики «Whaling» [16]

– *Фішингова атака з клонуванням – Clone Phishing.* Зловмисники створюють копію легітимного електронного листа, модифікують його, додаючи шкідливе вкладення або посилання, і повторно надсилають його одержувачу або іншим особам зі свого списку контактів.

При фішинг-атаці з клонуванням зловмисник зазвичай починає з отримання легітимного електронного листа, надісланого жертві в минулому (наприклад, маркетингового або рекламного листа від перевіреного бренду). Потім зловмисник створює ідентичну копію листа, часто використовуючи той самий брендинг і макет, але з кількома ключовими відмінностями. Наприклад, зловмисник може змінити адресу ЕП відправника, посилання в листі або вкладені файли, намагаючись надати листу більш термінового або легітимного вигляду.

Нижче наведено приклад такого електронного повідомлення (див. рис. 1.7):

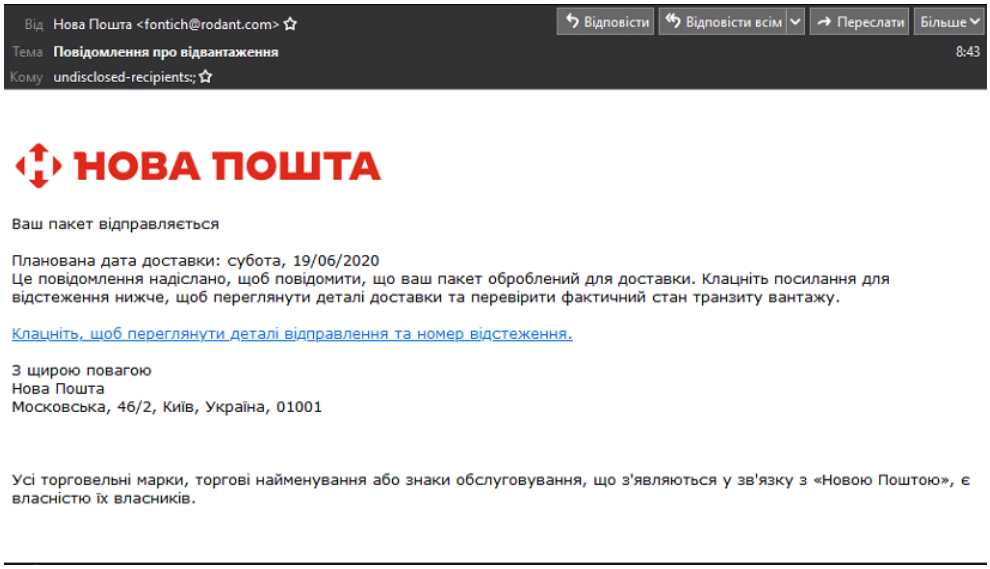


Рис. 1.7. Приклад електронного листа, надісланого за допомогою тактики «Clone Phishing» [14]

– *Доставка шкідливого програмного забезпечення, далі – ШПЗ, – Malware Delivery.* ШПЗ може бути доставлене з метою отримання несанкціонованого доступу (далі – НСД) до конфіденційної інформації або заподіяння шкоди комп’ютерним системам. ШПЗ може мати кілька форм, включаючи програми-вимагачі та шпигунські ПЗ.

Нижче наведено приклад такого електронного повідомлення (див. рис. 1.8):

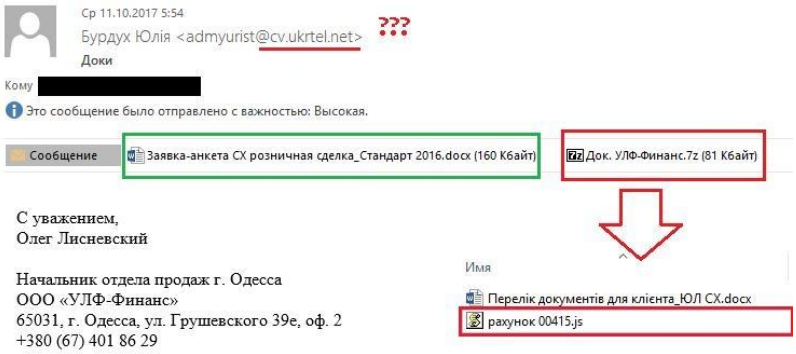


Рис. 1.8. Приклад електронного листа, надісланого за допомогою тактики «Malware Delivery» [16]

– *Компрометація ділової ЕП – Business email compromise, далі – BEC.* Дану тактику цілеспрямованого фішингу використовують для отримання доступу до системи ЕП організації та здійснення шахрайських дій. Зазвичай це компрометація облікового запису ЕП одного з працівників. А в подальшому використання даного облікового запису для того, щоб видавати себе за дійсного працівника для надсилання електронних листів з проханням переказати кошти та/або конфіденційну інформацію [9].

Нижче наведено приклад такого електронного повідомлення (див. рис. 1.9.1-1.9.2):

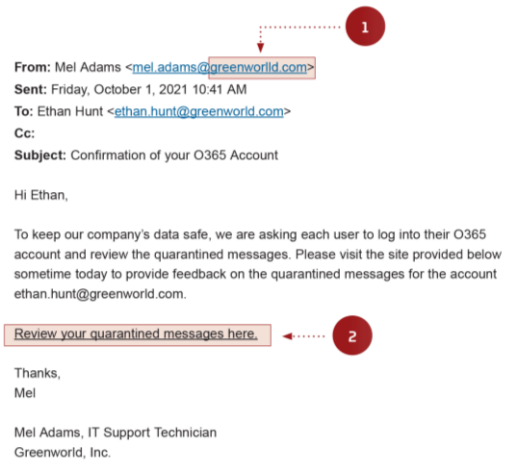


Рис. 1.9.1. Приклад електронного листа, надісланого за допомогою тактики «BEC» (англ. варіант) [11]

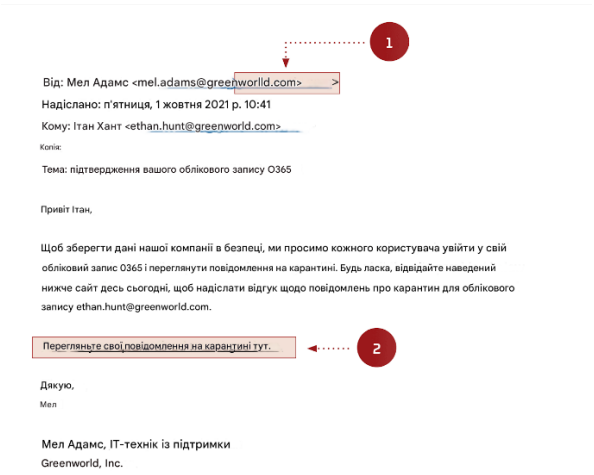


Рис. 1.9.2. Приклад електронного листа, надісланого за допомогою тактики «BEC» (укр. варіант) [11]

Тому важливо виявляти пильність і ретельно перевіряти всі вхідні електронні листи, особливо ті, в яких запитують конфіденційну інформацію або просто вони здаються підозрілими [7]. Людський фактор може призвести до пропусків або помилок через втому, поспіх чи звичку, що відкладає перевірку підозрілих листів. Таким чином, автоматизація процесу перевірки та обробки електронних повідомлень набуває особливої актуальності.

1.3 Аналіз існуючих методів протидії атакам соціальної інженерії в корпоративному середовищі

Розвиток AI призвів як до використання його в інструментах захисту від кіберзагроз, так і до значного ускладнення кібератак. Найслабшою ланкою в кіберзахисті більшості компаній так і залишаються її працівники, тож злочинці використовують генеративний AI для створення діпфейків, фішингових листів та повідомлень у месенджерах та ЕП. Проте рішення для кіберзахисту теж не стоять на місці, адже новітні продукти вендорів застосовують AI для виявлення та

блокування таких загроз.

Отже, деякі з можливостей захисту та запобігання атакам CI, на які варто звернути увагу, включають [17]:

Рішення на основі захисту ЕП

Сканування ЕП – Email Scanning. Виявляючи та блокуючи шкідливі електронні листи ще до того, як вони потраплять до поштової скриньки працівника, сканування ЕП зменшує ймовірність того, що працівник ненавмисно піддасться соціоінженерній атаці та наразить організацію на небезпеку.

Рішення для сканування ЕП можуть працювати двома способами. Одна з головних відмінностей полягає в тому, як вони вбудовуються в систему корпоративної ЕП. Два найпоширеніші підходи включають:

– *На основі Secure Email Gateway (далі – SEG).* Деякі рішення для сканування ЕП змінюють запис DNS MX організації, щоб вказати на її хмарне рішення для сканування ЕП. Усі листи спочатку надсилатимуться до сканера, що дозволить йому перевіряти листи та фільтрувати шкідливий вміст, перш ніж перенаправляти їх на поштовий сервер компанії або агента передачі пошти для доставки.

– *На основі Application Programming Interface (далі – API).* Рішення для сканування ЕП на основі API використовують API, що надаються поширеними рішеннями для веб-пошти (наприклад, Microsoft 365). Трафік ЕП проходить звичайну маршрутизацію, але перевіряється перед тим, як потрапити до поштових скриньок користувачів. Крім того, інтеграція на основі API забезпечує додаткову функціональність (наприклад, можливість відкликати листи з вхідних, якщо вони виявилися шкідливими після доставки, а також перевіряти вихідні листи на наявність конфіденційного контенту).

Коли листи проходять через поштовий сканер, він може використовувати різні методи для виявлення шкідливого вмісту. Серед них – сканування на наявність сигнатур відомих варіантів ШПЗ та використання AI і машинного навчання (Machine Learning, далі – ML) для виявлення нових загроз або вмісту ЕП, що вказує на потенційну атаку CI [18].

Пісочниця для вкладень – Attachment Sandboxing. Ізольована перевірка вкладень бере кожне окреме повідомлення з вкладенням і перевіряє файл самостійно, витягуючи його з повідомлення. Потім він поміщає вкладення у віртуальне захищене середовище або «пісочницю» і відкриває його, щоб виявити будь-яку шкідливу активність або спроби завантажити додаткові компоненти, які також можуть виконувати шкідливі дії [19].

Знешкодження та реконструкція контенту – Content Disarm and Reconstruction, далі – CDR. Злочинці часто використовують документи Microsoft Office та інші документи для доставлення ШПЗ через макроси та інші вбудовані функції. Рішення CDR можуть деконструювати документ, видаляти шкідливі функції та відновлювати очищену версію, яку можна безпечно надіслати одержувачу [17]. Цей процес у режимі реального часу видаляє експлойти, уникаючи негативного впливу на продуктивність бізнесу [22].

Рішення на основі захисту кінцевих пристроїв та мереж

Захист кінцевих точок та розширений захист кінцевих точок – Endpoint Detection and Response / Extended Detection and Response, далі – EDR/XDR. Дані рішення допомагають організаціям виявляти, розслідувати та реагувати на інциденти безпеки. Однак вони відрізняються за сферою застосування та можливостями [20].

EDR підтримує функцію реагування на інциденти шляхом збору, аналізу та візуалізації інформації, підтвердженої на кінцевих пристроях (персональних комп’ютерах, серверах тощо) у вигляді телеметрії. Зокрема, вона збирає таку поведінку, як створення та видалення файлів, запуск додатків, надсилання та отримання файлів, незалежно від того, чи є вона законною чи зловмисною, і порівнює її з методами кібератак, підтвердженими в минулому постачальниками систем безпеки, щоб визначити пріоритети підозрілої поведінки, представити події, на які слід звернути увагу, і візуально відобразити процес вторгнення загрози в легкій для розуміння манері.

Використовуючи EDR для відстеження ланцюжка процесів, який візуалізує серію процесів вторгнення в кінцеву точку, можна підтвердити, що атака почалася

з ЕП.

Однак, оскільки EDR візуалізує лише кінцевий пристрій, на якому встановлено датчик, він не надає детальної інформації про електронний лист, такої як відправник/одержувач, тема листа, посилання, що містяться в листі, тощо. Тому співробітники служби безпеки повинні досліджувати підозрілі електронні листи, порівнюючи результати досліджень EDR з журналами відправлення та отримання поштового сервера, що в кінцевому підсумку вимагає зусиль персоналу для пошуку першопричини.

Ось де XDR стає в нагоді. Як випливає з назви, XDR розширює можливості EDR для виявлення та реагування. XDR збирає телеметрію, тобто дані про активність файлів і процесів, незалежно від того, чи є вони законними або шкідливими, з різних рівнів безпеки, включаючи ЕП, сервери, хмарні робочі навантаження і мережі на додаток до кінцевих точок, а потім співвідносить і візуалізує дані, щоб автоматично визначити, чи відбулася кібератака і які дії необхідно вжити.

XDR співвідносить і візуалізує інформацію кінцевих точок і інформацію ЕП, тому співробітникам служби безпеки не потрібно виконувати нудне і трудомістке завдання з розслідування та аналізу підозрілих електронних листів на основі інформації EDR і журналів відправлення та отримання ЕП для виявлення першопричини. Крім того, на основі елементів, виявлених під час розслідувань XDR, можна розробити контрзаходи, що робить розслідування та реагування більш ефективними [21].

Аналіз поведінки користувачів та організацій – User and Entity Behavior Analytics, далі – UEBA. Дане рішення дозволяє передбачити, чи був користувач вже скомпрометований, спостерігаючи за тенденціями входу в систему, звичками використання електронної пошти та середовищами браузерів, якими користується одержувач. UEBA відстежує типову поведінку користувачів, щоб, коли трапиться щось незвичне, виділити це.

Це особливо важливо, якщо організацією використовується застарілий поштовий шлюз. Ці шлюзи розташовуються перед вхідними повідомленнями, але

за своєю архітектурою вони відключають захист від Google або Microsoft [22].

Отже, сучасні методи протидії атакам CI в корпоративному середовищі охоплюють широкий спектр технічних рішень і організаційних заходів, які мають на меті виявлення, запобігання та нейтралізацію потенційних загроз. Атаки CI, такі як фішинг, цільовий фішинг (а також його види), або BEC, все частіше використовуються зловмисниками для маніпулювання співробітниками компаній задля отримання конфіденційної інформації або доступу до внутрішніх систем.

Сучасна система протидії CI ґрунтується на комплексному підході, який враховує як технологічні, так і поведінкові аспекти захисту.

Багаторівневий, інтегрований підхід дозволяє не лише реагувати на відомі загрози, але й виявляти нові, раніше не зафіксовані атаки завдяки використанню AI, ML та великих масивів аналітичних даних. Така система створює надійну основу для подальшого аналізу та впровадження спеціалізованого рішення Core Email Protection (від вендора в розрізі кібербезпеки Proofpoint) – комплексного інструменту захисту корпоративної ЕП, який буде детально розглянуто у наступному розділі.

2 МЕТОДИ ТА ЗАСОБИ ПРОТИДІЇ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Архітектура та основні компоненти рішення Proofpoint Core Email Protection

Proofpoint Core Email Protection – рішення на основі AI/ML, яке захищає ЕП, блокуючи сучасні загрози до, після та безпосередньо під час доставки. Воно забезпечує ефективну видимість поверхні атак на людей, показуючи, кого і як атакують [23].

Core Email Protection побудоване на гнучкій хмарній платформі та використовує низку власних технологій, зокрема аналіз бігдата, ML, глибоку перевірку контенту, безпечне зберігання, вдосконалене шифрування, інтелектуальну маршрутизацію повідомлень, динамічний аналіз ШПЗ та віртуальні пісочниці, щоб протистояти сучасному ландшафту загроз, який швидко змінюється.

Дане рішення існує в інфраструктурному підході Software-as-a-Service (далі – SaaS) та може бути розгорнуте за допомогою унікальної хмарної архітектури, яка використовує як центри обробки даних, так і додаткові брандмауери клієнтів (детальний огляд архітектури наведено на рис. 2.1).

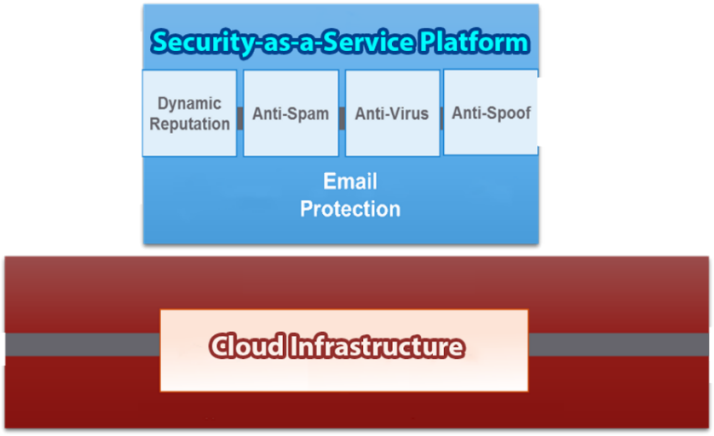


Рис. 2.1. SaaS-архітектура комплексного підходу до безпеки ЕП Core Email Protection [33]

Комплексне платформенне рішення забезпечує захист від загроз та безпечну комунікацію. Даний продукт побудований на SaaS-архітектурі, захищаючи дані не лише під час їх надходження на підприємство, а також під час виходу з нього через локальну та хмарну ЕП [33].

Основний компонент Core Email Protection – Nexus

Core Email Protection використовує Proofpoint Nexus Language Model (далі – LM), графіки взаємозв'язків, ML та Computer Vision (далі – CV), щоб зупинити найсучасніші загрози ЕП. Він спирається на унікальні дані про загрози, отримані з понад 3 трильйонів електронних листів, які скануються щороку. Платформа автоматично зупиняє такі загрози, як BEC, фішинг з використанням QR-кодів та цільовий фішинг.

Proofpoint Nexus – це комплексна платформа для аналізу загроз на основі AI/ML та аналізу загроз у реальному часі. Nexus зменшує ризики, які люди створюють для своїх організацій, особливо перед обличчям зростаючої кількості фішингових атак, проникнення ШПЗ та захоплення хмарних облікових записів. Nexus безперервно аналізує мільярди електронних листів, веб-повідомлень і хмарних взаємодій, щоб виявити і нейтралізувати ці загрози до того, як вони скомпрометують дані і системи [26].

Proofpoint Core Email Protection використовує кожну з описаних нижче моделей Nexus [28]:

– *Nexus Threat Intelligence (далі – TI).* Nexus TI інтегрує величезні обсяги даних про загрози для покращення можливостей виявлення в продуктах Proofpoint. Вона забезпечує оновлення інформації про нові загрози, тактику зловмисників і вразливості системи в режимі реального часу. Завдяки зосередженості на розширеній розвідці загроз, Nexus TI гарантує, що рішення Proofpoint випереджають кіберзагрози, що розвиваються, пропонуючи проактивне виявлення та захист. Ця система є ключем до підтримки стійкої позиції безпеки проти сучасних кібер-супротивників.

– *Nexus LM.* Дана модель використовує можливості передових мовних моделей AI для боротьби з BEC. Він ретельно досліджує вміст ЕП, щоб виявити

загальні елементи, притаманні спробам BEC, такі як транзакційна мова та терміновість. Розпізнаючи тонкі лінгвістичні патерни та поведінкові ознаки, Nexus LM ідентифікує підозрілі електронні листи ще до того, як вони можуть завдати шкоди. Це передове рішення додає критично важливий рівень захисту, пропонуючи чудовий захист від витончених атак через ЕП.

– *Nexus Relationship Graph (далі – RG).* Nexus RG використовує AI для моніторингу та оцінки поведінки користувачів, посилюючи захист кібербезпеки. Використовуючи поведінкову аналітику, ML та виявлення аномалій, Nexus RG виявляє відхилення від нормальних дій користувачів, які можуть свідчити про потенційну загрозу.

– *Nexus ML.* Наявна модель використовує передове машинне навчання для посилення наших можливостей виявлення загроз. Використовуючи такі методи, як контрольоване навчання, неконтрольоване навчання та ансамблеві методи, Nexus ML забезпечує масштабовані та надійні рішення для захисту. Ця основна технологія AI гарантує, що Proofpoint може виявляти і нейтралізувати широкий спектр нових загроз, забезпечуючи комплексний захист у різних сферах кібербезпеки.

– *Nexus CV.* Це модуль на основі AI, призначений для виявлення та нейтралізації загроз на основі зору. Завдяки передовій технології – CV – виявляє загрози, приховані у візуальних елементах, таких як фішингові сайти, QR-коди, шкідливі вкладення та підроблені електронні листи. Зосереджуючись на візуальних векторах загроз, цей модуль підвищує рівень безпеки, надаючи потужну відповідь на атаки з використанням вбудованих зображень та іншого графічного контенту.

2.2 Функціональні можливості системи та порівняльний аналіз з іншими системами

Працівники відділу Security Operations Center (далі – SOC) можуть працювати швидше завдяки інтегрованим робочим процесам на основі пошуку та сповіщень під час роботи з наявним технічним продуктом. Вони також можуть скористатися перевагами автоматичного виправлення повідомлень та навчання користувачів у режимі реального часу [26].

Технологічні рішення у сфері кібербезпеки від вендора Proofpoint можуть похвалитися унікальною комбінацією даних про загрози. Nexus навчається на трильйонах глобальних точок даних – хостах, зібраних більше ніж за 20 років від тисяч клієнтів. Proofpoint поєднує методи AI/ML з аналізом загроз та інтеграцією пісочниць, що робить механізми виявлення більш точними. Оскільки набори даних є всеосяжними, інструменти не тільки «бачать» більше загроз, але й генерують менше хибних спрацьовувань [34].

Також інтуїтивно зрозумілий інтерфейс спрощує управління інцидентами, дозволяючи аналітикам, швидко розслідувати та реагувати на загрози безпеки. Завдяки чітким поясненням та автоматизованим робочим процесам команди витрачають менше часу на ручну роботу і можуть більш ефективно сортувати та усувати інциденти.

Ця ефективність у поєднанні з можливостями продуктів SIEM/SOAR призводить до значного підвищення ефективності. Завдяки оптимізації процесу сортування для автоматичного видалення шкідливих повідомлень клієнти часто спостерігають скорочення часу на усунення загроз електронною поштою більше ніж на 90% [23].

Також необхідно пам’ятати, що у кожного постачальника послуг знайдуться конкуренти на відповідному ринку послуг. Тому й у даному випадку з вендором Proofpoint наявні конкуренти, що можливо можуть обіграти даний продукт, незважаючи на його багатий та потужний функціонал.

Наявні конкурентні продукти на ринку кібербезпеки

Proton Mail. Даний приклад – сервіс ЕП з нульовим доступом, побудований на основі криптографії з відкритим вихідним кодом [30].

Ключові особливості:

– наскрізне шифрування з нульовим доступом;

– самознищення листів, термін дії яких закінчується;

– додаток Proton Bridge для інтеграції з десктопними клієнтами;

– асистент для написання та формалізації листів Proton Scribe AI.

Варіативність інтеграції в інформаційну систему (далі – ІС):

– поєднання з Proton Calendar, Proton Drive, Proton VPN та менеджером паролів;

– розширення для браузерів Chrome та Firefox.

Trend Vision One. Це уніфікована платформа Trend Micro XDR для аналітики і кібербезпеки з додатковим модулем Email & Collaboration Security Core, що забезпечує розширений захист від загроз ЕП [31].

Ключові особливості:

– профілактика, виявлення та автоматизоване реагування на основі AI;

– централізоване виявлення загроз на кінцевих точках, в ЕП, хмарі та мережах;

– налаштовувані дашборди та плейбуки;

– експертне керування послугами та підтримка SOC 24/7.

Варіативність інтеграції в ІС:

– вбудована інтеграція з продуктами Trend Micro для захисту кінцевих точок, хмарних і мережевих рішень;

– інтеграція з рішеннями Security Information & Event Management та/або Security Orchestration, Automation & Response (далі – SIEM/SOAR) (наприклад, Splunk, IBM QRadar);

– захист хмарних додатків та інструментів для спільної роботи.

ePrism Email Security. EdgeWave ePrism Email Security Suite забезпечує хмарну фільтрацію спаму та вірусів з автоматичним обходом відмови та

безперервністю для малих і середніх підприємств та розподілених організацій [32].

Ключові особливості:

– антиспам та антивірус для вхідної та вихідної пошти;

– аварійне копіювання та безперервність пошти під час збоїв;

– політики Data Loss Prevention та перевірка вмісту;

– веб-адміністрування та звітність.

Варіативність інтеграції в ІС:

– SMTP ретрансляція з існуючими поштовими серверами;

– інтеграція API-інструментів (REST-архітектури) для SIEM і платформ архівування.

Перейдемо до порівняння ключових відмінностей продуктів, за якими можна зробити остаточний результат про обране нами рішення.

Порівняння основних відмінностей вищезгаданих продуктів представлено у таблиці 2.1:

Табл. 2.1.

Таблиця порівнянь основних відмінностей конкурентних продуктів захисту ЕП на ринку кібербезпеки [29]

Критерій оцінки	**Proofpoint Core Email Protection**	**Proton Mail**	**Trend Vision One**	**ePrism Email Security**
Підтримувані платформи	Хмара.	Windows, Mac, Linux, хмара, iPhone, iPad, Android.	Хмара.	Хмара.
Цільова аудиторія	Компанії, які шукають рішення для покращення своїх послуг та збільшення продажів.	Всім, кому потрібна безпечна адреса електронної пошти з вбудованим наскрізним шифруванням.	Компанії, які шукають спеціалізовану платформу для захисту від загроз.	Будь-яка компанія чи організація, яка шукає рішення для покращення безпеки своєї електронної пошти.

Продовження Табл. 2.1.

Критерій оцінки	Proofpoint Core Email Protection	Proton Mail	Trend Vision One	ePrism Email Security
Направлення роботи	Антифішинг, шифрування ЕП, безпека ЕП, SEG.	Поштові клієнти, шифрування ЕП, хостинг ЕП, керування ЕП, шифрування.	Розширений захист від загроз, безпека з AI, управління поверхнею атаки.	Розширений захист від загроз, Безпека ЕП, SEG.
Безкоштовна версія	–	+	–	+
Безкоштовна пробна версія	+	+	+	+
Ціноутворення	Бізнес план: $3.03 за користувача на місяць Професійний план: $5.86 за користувача на місяць.	Mail Plus план: $4.99 на місяць Безліміт план: $12.99 на місяць.	Оплата за фактом залежить від функцій.	Від $5 на рік за користувача; також доступні знижки за великі обсяги.
Служба підтримки клієнтів	24/7 жива підтримка, онлайн підтримка.	Онлайн підтримка, база знань.	24/7 жива підтримка, онлайн підтримка.	Онлайн підтримка, документація.
Загальний рейтинг	91% клієнтів готові рекомендувати.	89% клієнтів готові рекомендувати.	88% клієнтів готові рекомендувати.	78% клієнтів готові рекомендувати.

Отже, чотири провідні рішення в сфері захисту ЕП – Proofpoint Email Protection, Proton Mail, Trend Vision One і ePrism – пропонують різні підходи: від шифрування до виявлення загроз на основі AI/ML. У той час як Proton Mail відмінно захищає конфіденційність за допомогою наскрізного шифрування, а Trend Vision One надає уніфіковану аналітику XDR, Proofpoint вирізняється поєднанням засобів захисту до і після доставки.

Proofpoint Core Email Protection – це перше в галузі рішення, яке пропонує як захист від загроз CI до доставки, так і поведінкове виправлення на основі AI після

доставки, що гарантує, що навіть висококваліфіковані атаки можуть бути заблоковані. Жоден інший постачальник у цьому порівнянні не забезпечує наскрізний захист життєвого циклу загрози з таким же рівнем ефективності.

Працюючи на базі LM Nexus, Proofpoint аналізує поведінку користувачів, репутацію відправника та інформацію про загрози з мільярдів електронних листів, щоб виявити аномалії, які вказують на фішинг. Цей динамічний підхід адаптується до еволюції тактик атак швидше, ніж статичні системи на основі правил, що використовуються іншими провайдерами.

Також завдяки глибокій інтеграції на рівні API Proofpoint без проблем вбудовується в існуючі стеки безпеки.

В цілому, хоча всі чотири рішення пропонують цінні можливості, унікальне поєднання багатоступеневого захисту від CI, аналітики та корпоративної інтеграції робить Proofpoint Core Email Protection оптимальним вибором для компаній, які прагнуть захистити своє поштове середовище від все більш витончених атак CI.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ТА ПРАКТИЧНОГО ЗАСТОСУВАННЯ PROOFPOINT CORE EMAIL PROTECTION

3.1 Архітектура інтеграції Proofpoint в інформаційну систему організації

Платформа Core Email Protection надає два можливих варіанта архітектурного впровадження: розгортання SEG пристрою та API-інструментів (див. рис. 3.1) [24].

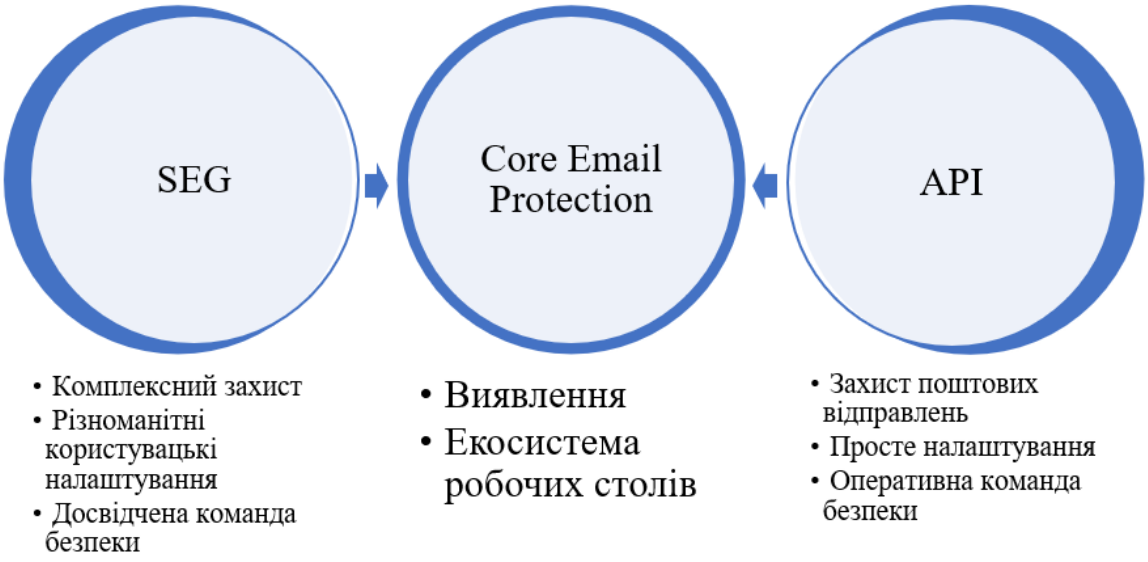


Рис. 3.1. Рішення Core Email Protection можливо розгорнути на основі SEG пристрою та API-конфігурацій [24]

Отже, розглянемо два даних архітектурних підходи:

1. Архітектурний підхід на основі SEG. SEG – метод захисту від ШПЗ, атак CI та спаму. Дане архітектурне рішення є традиційним підходом до захисту ЕП.

Архітектура для налаштування пристроїв SEG подібна до брандмауера (див. рис. 3.2.1-3.2.2). ЕП спрямовується безпосередньо на шлюз SEG, де пошта перевіряється на наявність ШПЗ та фішингових листів.

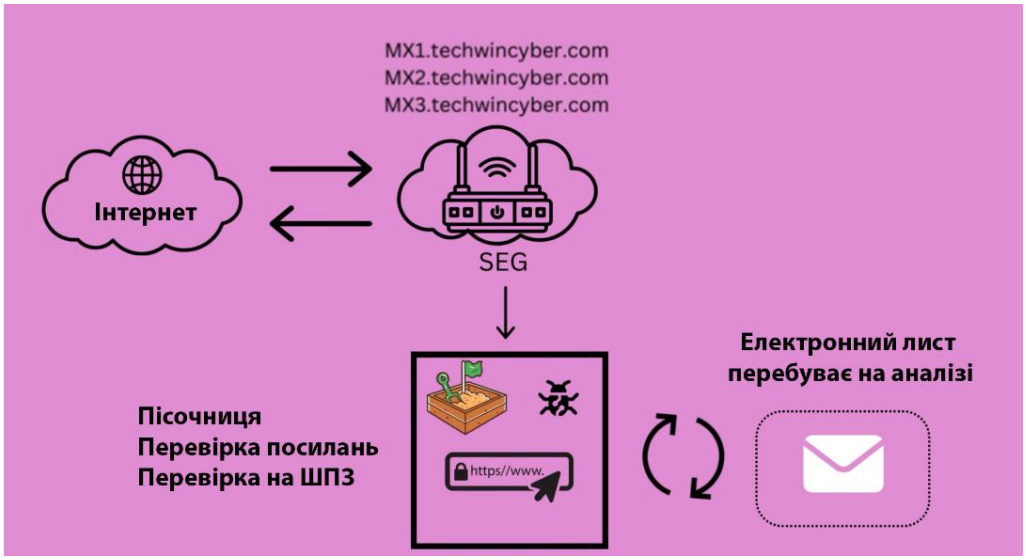


Рис. 3.2.1. Впровадження рішення безпеки ЕП на основі SEG, під час роботи якого лист проходить обробку [25]

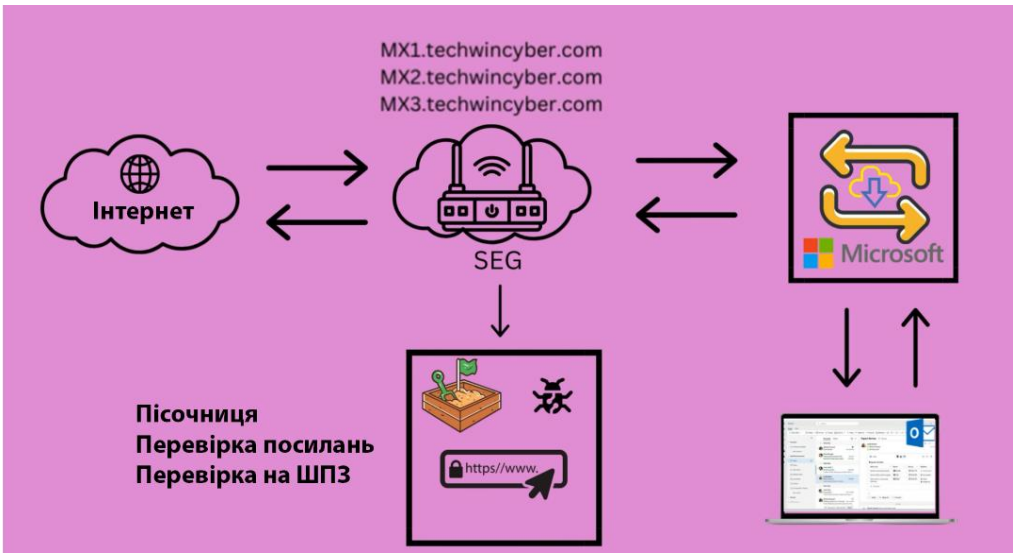


Рис. 3.2.2. Впровадження рішення безпеки ЕП на основі SEG, під час роботи якого лист пройшов оброку [25]

При такому підході необхідні налаштування, під час яких відбувається заміна MX-записів на шлюз SEG. Тепер коли користувач в мережі Інтернет буде надсилати пошту на електронну адресу організації, буде виконуватися пошук DNS, при якому буде повертатися налаштований MX-запис. У висновку, всі листи надсилаються автоматично на захищений шлюз, перш ніж бути перенаправленими на поштовий хост компанії (наприклад, поштововики Microsoft або Google).

2. Архітектурний підхід на основі API. Даний варіант архітектури зосереджений безпосередньо навколо організаційного поштового хосту, а хост – це місце, куди надсилаються всі електронні листи (див. рис. 3.3).

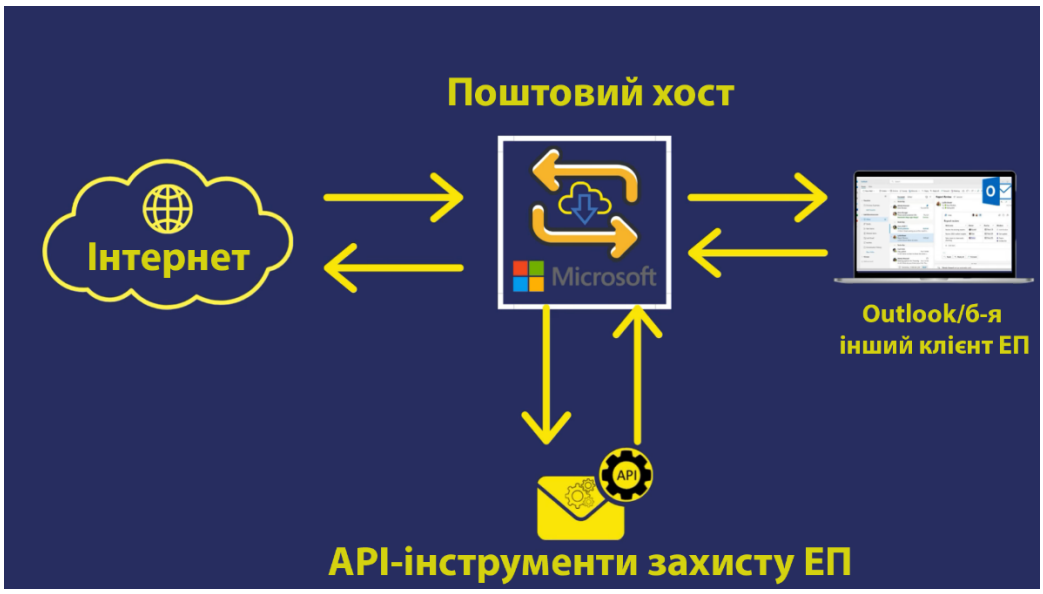


Рис. 3.3. Впровадження рішення безпеки ЕП на основі API

Це може бути поштовий сервер Microsoft або Google. Налаштувавши API всередині пошти, додатки ЕП використовують API-платформи як інтеграцію для перегляду, використання електронних листів та взаємодію з поштою.

API інструменти приносять користь організації вже під час налаштування завдяки їх інтеграції з хостом ЕП.

Процес встановлення досить швидкий і простий. Розгортання даного архітектурного варіанту не потребує налаштування MX записів. Також конфігурація цих інструментів вимагає лише надання базових прав, таких як доступ до читання та запису до поштових скриньок користувачів. Після надання цих прав API-інструменти можуть почати обробляти ЕП майже одразу.

Процес інсталяції дозволяє організаціям тестувати різні інструменти, щоб побачити, який з них найкраще відповідає їхнім потребам [25].

Вибір правильного підходу

Коли необхідно обрати підхід до захисту ЕП, рішення стосується не лише безпеки, а й того, як працює організація. Кожен підхід має свої переваги. Але якщо

керівництво організації зробить неправильний вибір, це може призвести до неефективної роботи, збільшення витрат і прогалин у безпеці [27].

Нижче, на табл. 3.1, можна детально розглянути відмінності двох архітектурних підходів під час інтеграції Core Email Protection в інформаційну систему компанії:

Табл. 3.1.

Таблиця порівнянь двох підходів інтеграції рішення захисту ЕП від Proofpoint [27]

Критерій вибору	**Архітектура на основі API**	**Архітектура на основі SEG**
Час для розгортання	Підхід API забезпечує швидкий та ефективний захист без значних змін в інфраструктурі.	Хоча компромісом є довший час розгортання, підвищена видимість і контроль над загрозами ЕП можуть значно знизити ризики.
Microsoft-орієнтація	Команди обміну повідомленнями (відповідальні за записи MX і маршрутизацію пошти) можуть віддати перевагу рішенням на основі API, оскільки вони не вимагають перенаправлення ЕП через зовнішній SEG. А команди безпеки (зосереджені на виявленні та реагуванні на загрози) отримують вигоду від додаткових рівнів захисту, що надаються інструментами на основі API, які покращують існуючу систему безпеки Microsoft.	SEG найкраще підходить для організацій, які хочуть отримати рішення, що додає кілька рівнів захисту для додаткової відмовостійкості.
Інфраструктура ЕП	Компанії з централізованою IT-командою часто вважають, що безпека на основі API відповідає їхнім потребам.	Компанії з декількома поштовими середовищами, складними політиками маршрутизації або потребами у дотриманні нормативних вимог часто

Продовження Табл. 2.1

Критерій вибору	Архітектура на основі API	Архітектура на основі SEG
Інфраструктура ЕП		потребують точності та контролю, які забезпечує SEG.

Обираючи між SEG та засобами захисту ЕП на основі API, не варто запитувати, який із них кращий. Краще запитати самого себе, який варіант найкраще відповідає пріоритетам організації, інтеграції з Microsoft та потребам інфраструктури [27].

Примітка. Але в подальшому наявна кваліфікаційна робота буде побудована відносно архітектури на основі API-інструментів.

3.2 Технічна реалізація та конфігурація системи

Налаштування продукту Core Email Protection передбачає інтеграцію системи з існуючим поштовим середовищем організації (як правило, шляхом спрямування всього вхідного та вихідного трафіку через шлюз Proofpoint). Процес конфігурації також включає налаштування політик, які визначають, як сканувати та обробляти ЕП. Ці політики охоплюють фільтрацію спаму, виявлення ШПЗ, запобігання фішингу та запобігання втраті даних. Налаштовуючи ці правила, адміністратори можуть пристосувати систему до конкретних вимог безпеки та стандартів відповідності.

Головне вікно платформи (див. рис. 3.4), через яке здійснюються всі активні дії та переходи на функціональні модулі:

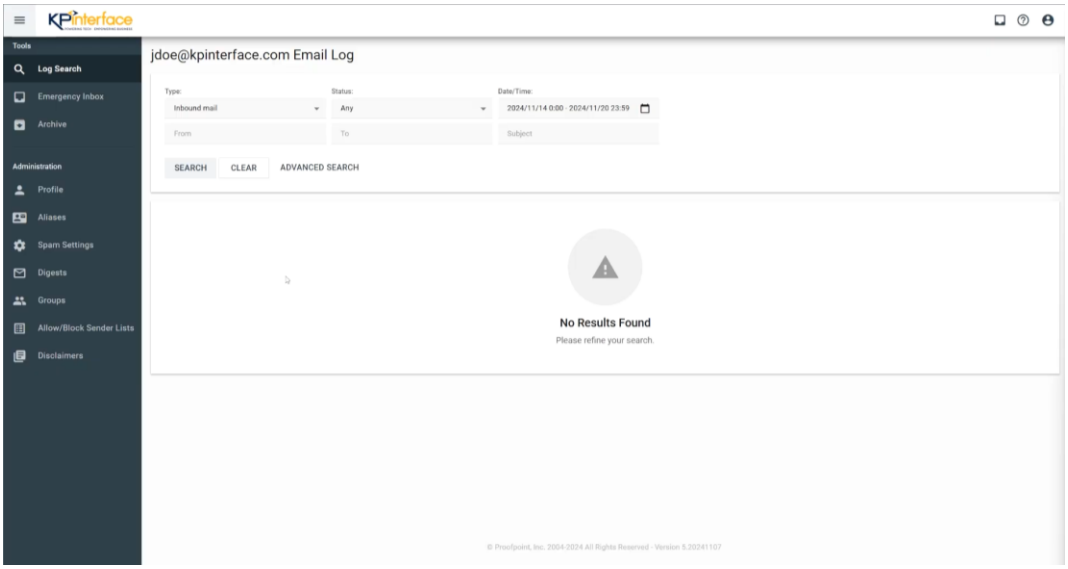


Рис. 3.4. Головна сторінка рішення Core Email Protection [36]

Буде також доступ до додаткових функцій, таких як перегляд поштових вкладень на карантині, конфігурація та керування списками відправників, що дозволяють блокувати адреси ЕП.

Почнемо з того, з чим більшість користувачів Core Email Protection взаємодіють щодня – *Daily Digest Emails – Щоденний Дайджест Листів* (див. рис. 3.5.1–3.5.2).

Детальний огляд щоденного дайджесту листів

Більшість користувачів в основному взаємодіють з платформою Proofpoint через модуль, який надає зручний підсумок карантинних повідомлень.

Функції дайджесту:

– *preview* (безпечний перегляд вмісту поштового вкладення на карантині);

– *release* (доставити лист на карантин до вашої поштової скриньки);

– *release & approve* (доставити лист до організаційної поштової скриньки та додати відправника до білого списку, щоб майбутні імейли від нього не потрапляли до карантину; необхідно зауважити, що білі списки на рівні користувача можуть бути замінені фільтрами або правилами на рівні організації);

– *block* (назавжди заборонити відправнику або домену доставляти ЕП до організаційної скриньки).

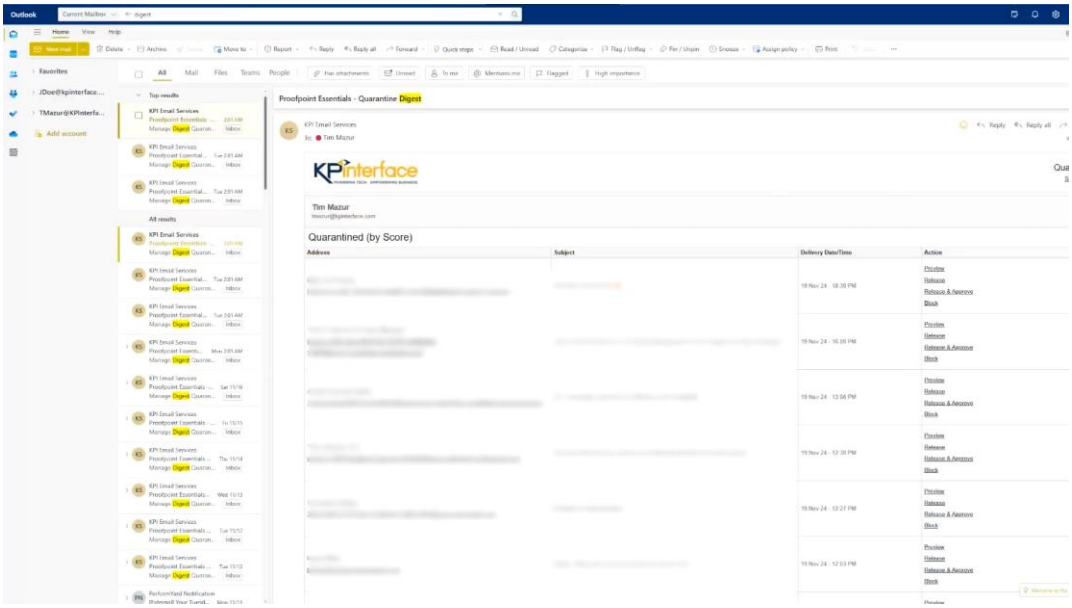


Рис. 3.5.1. Огляд щоденного дайджесту листів [36]

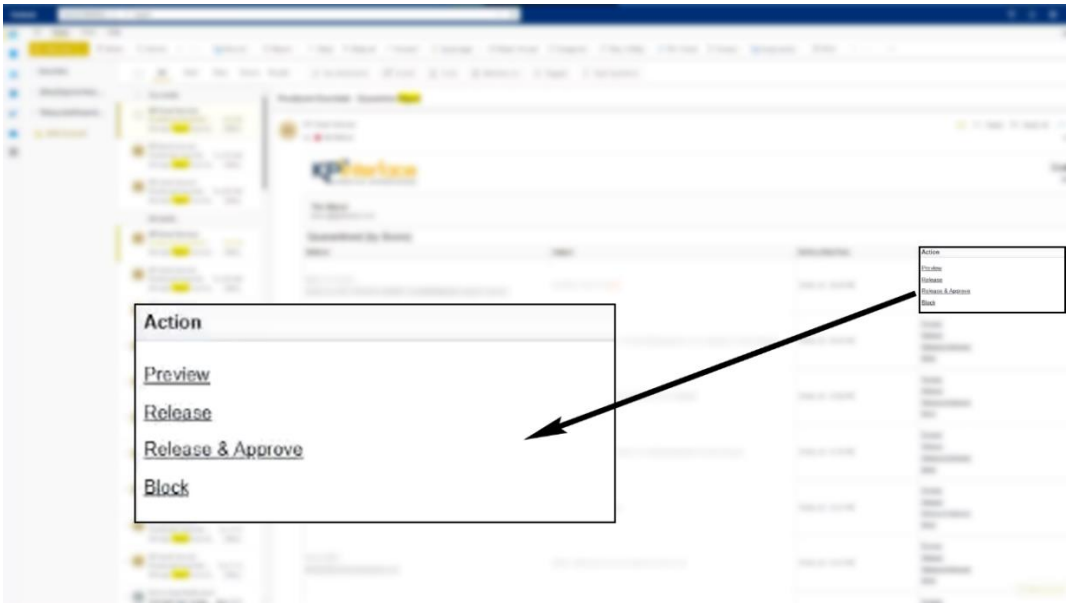


Рис. 3.5.2. Огляд супутніх функцій [36]

Дайджест листів дозволяє легко керувати вкладеннями на карантині безпосередньо зі своєї поштової системи, без входу на портал Proofpoint.

Навігація порталом Proofpoint

Після входу на портал перша сторінка, на яку можна потрапити – це сторінка журналювання ЕП (див. рис. 3.6):

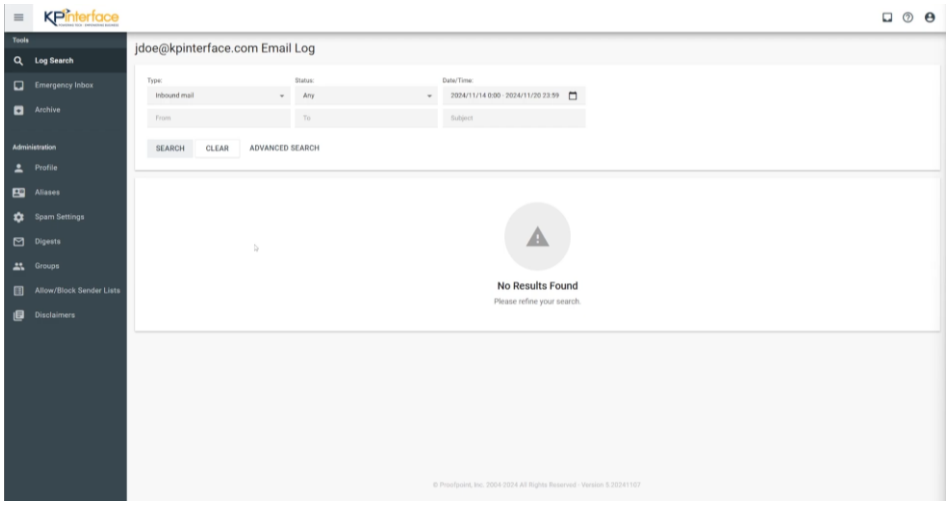


Рис. 3.6. Сторінка журналювання ЕП [36]

В даному функціональному модулі можна побачити кілька фільтрів для перегляду листів, такі як:

– *type* (випадаючий список; щоб переглянути електронний лист, який було отримано – «inbound mail», або який було відправлено – «outbound mail») (див. рис. 3.7):

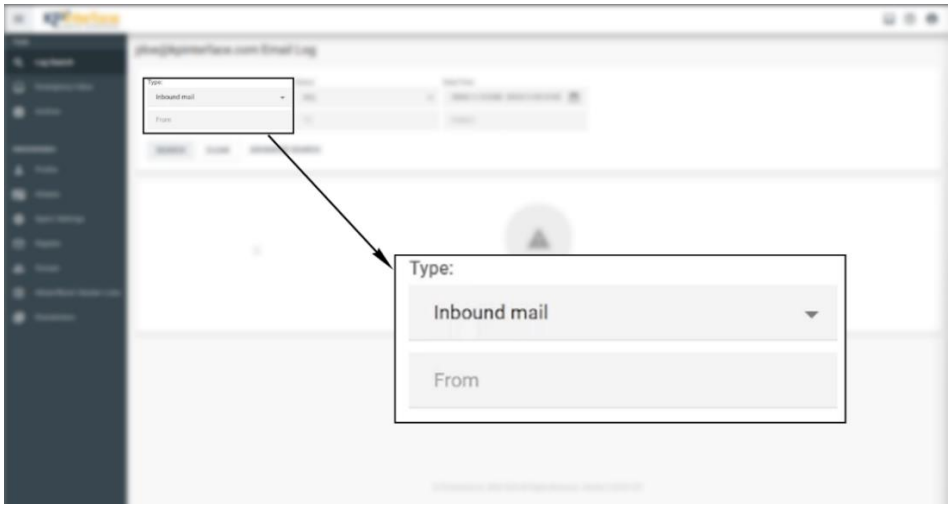


Рис. 3.7. Фільтр «type» для сортування електронних листів [36]

– *status* (тут можна вибрати, які типи листів є потреба бачити) (див. рис. 3.8):
  - *any* (даний фільтр витягує всі листи, включно з тими, що доставлені у поштову скриньку організації);
  - *quarantined* (всі листи, які наразі не доставлені);
  - *reported (misclassified)* (листи, про які було повідомлено в пункті

перевірки як про спам після того, як вони були доставлені як чисті);

- *blocked* (листи, які були заблоковані через вірус або ШПЗ; заблоковані повідомлення не можуть бути розблоковані);
- *cleared* (всі доставлені листи);
- *cleared (but cued for delivery)* (відкладені листи, які очікують на доставку);
- *cleared (but bounced by destination)* (листи, які було доставлено, але відхилено адресатом);
- *cleared (released from quarantine)* (повідомлення, які спочатку було поміщено в карантин, але звільнено для доставки);
- *in attachment defense sandbox* (це листи із вкладеннями, які Proofpoint перемістив у пісочницю, де він перевіряє вкладення на наявність будь-якого типу корисного навантаження або ШПЗ).

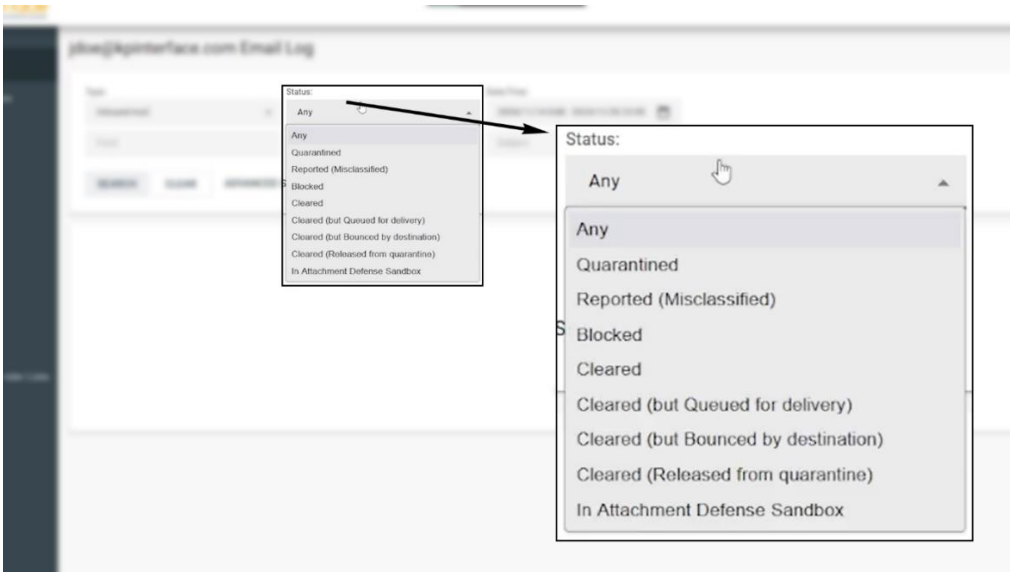


Рис. 3.8. Фільтр status для сортування електронних листів [36]

Також додаткові фільтри дозволяють деталізувати інформацію за датою та часовим діапазоном, а також за відправником, одержувачем і темою (див. рис. 3.9):

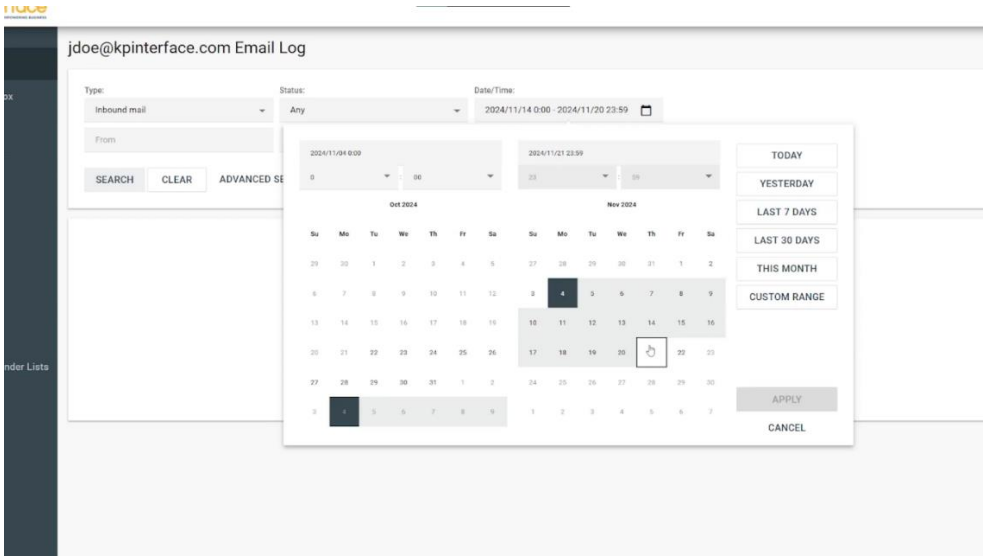


Рис. 3.9. Додаткові фільтри для детального та глибокого сортування електронних листів [36]

Примітка. Перегляд залогованих листів ЕП можуть бути доступними в системі Proofpoint лише в період 30-денної давнини.

Електронні листи на карантині та дії з ними

Щоб переглянути лист у списку на карантині, необхідно прокрутити список праворуч, доки не буде видно стовпчик *«Actions»* (див. рис. 3.10.1). Тут можна натиснути на іконку з оком, щоб попередньо безпечно переглянути повідомлення (див. рис. 3.10.2):

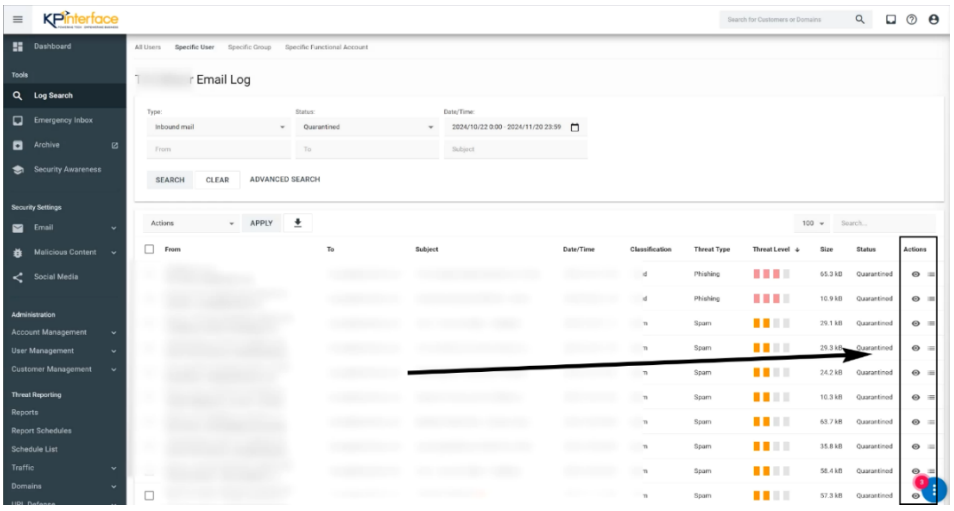


Рис. 3.10.1. Прокручуємо список електронних повідомлень вправоруч аж до функціональної панелі «Actions» [36]

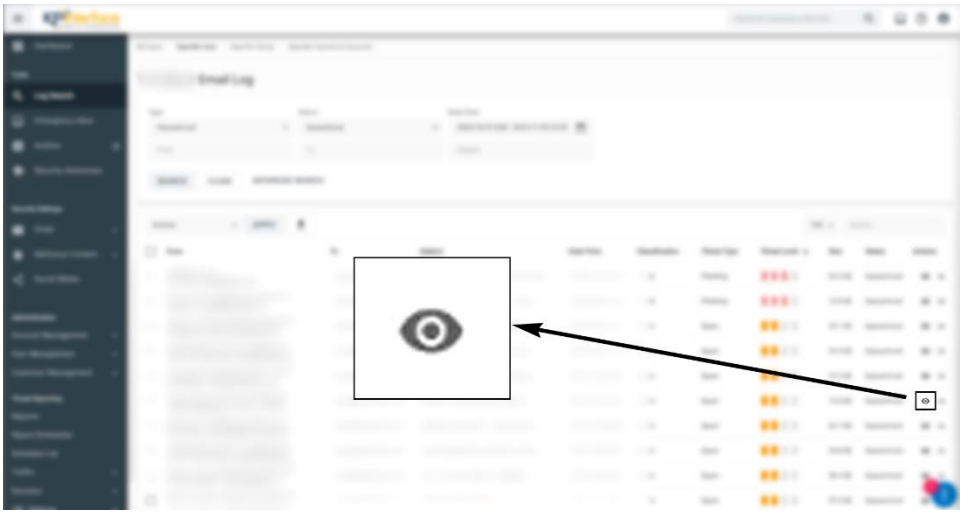


Рис. 3.10.2. Вибір піктограми з оком [36]

У нижній частині панелі попереднього перегляду є кнопки дій, які дозволяють показати зображення, повідомити про результат «false-positive», пропустити або видалити електронний лист (див. рис. 3.10.3):

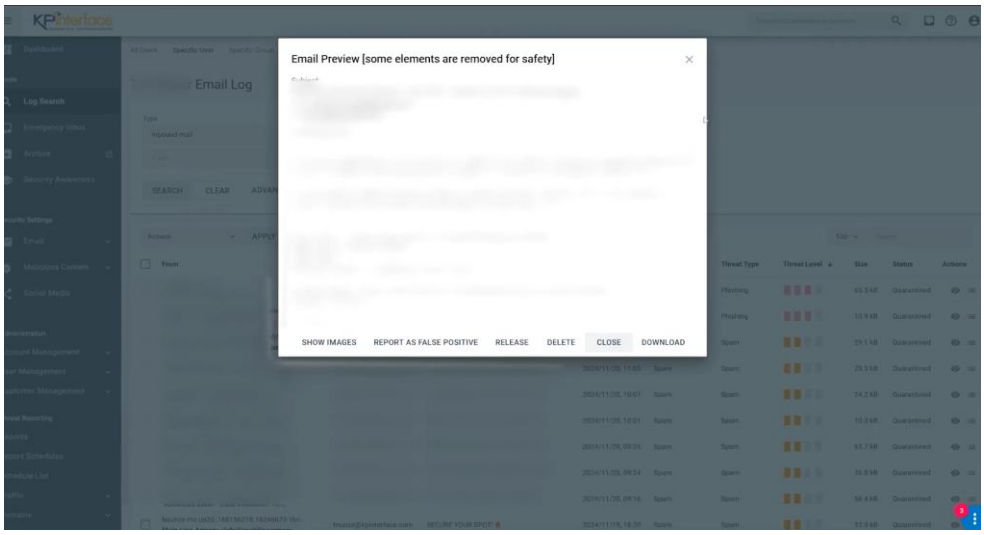


Рис. 3.10.3. Огляд можливостей попереднього перегляду електронного листа [36]

Якщо є необхідність переглянути детальний запис логування ЕП, потрібно натиснути на маркований список поруч із піктограмою ока (див. рис. 3.11.1). Тут можна внести зміни, повідомити про результат «false-positive» або роздрукувати лист (див. рис. 3.11.2):

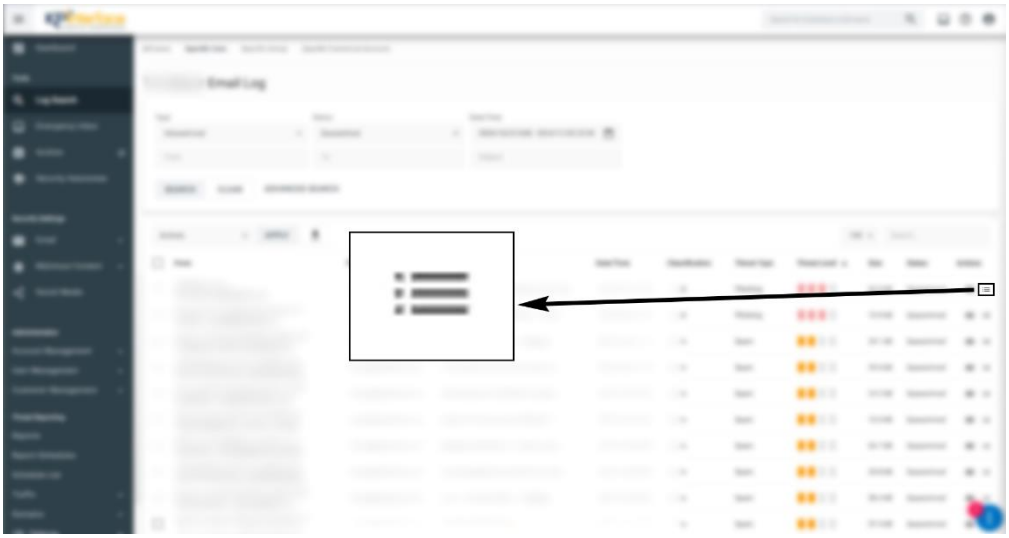


Рис. 3.11.1. Вибір маркованого списку поруч із піктограмою ока [36]

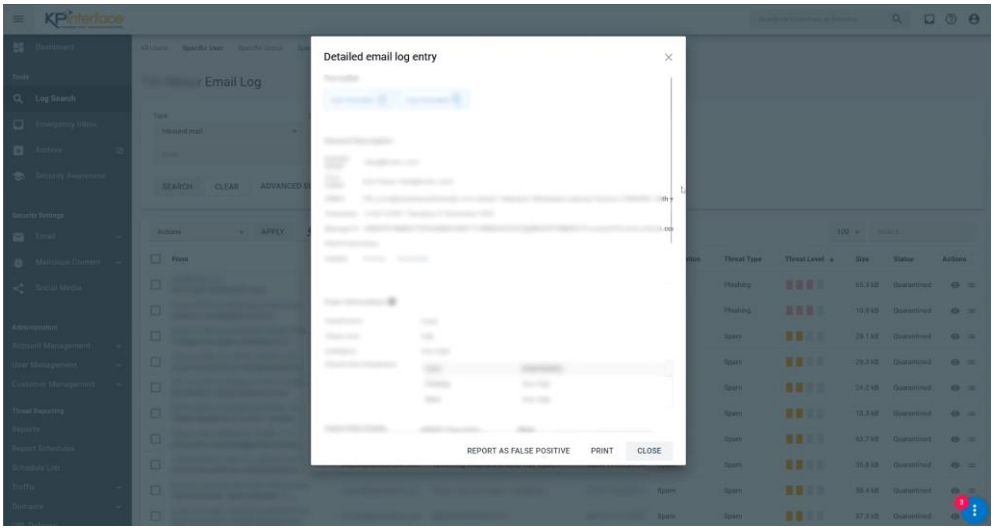


Рис. 3.11.2. Огляд розширених функцій детального логування електронних листів [36]

Щоб виконувати якісь дії із вкладеннями на карантині, необхідно встановити прапорець поруч з назвою листа та/або листами, до яких є необхідність застосувати дію (див. рис. 3.12.1). Далі потрібно вибрати дії зі спадного списку (див. рис. 3.12.2):

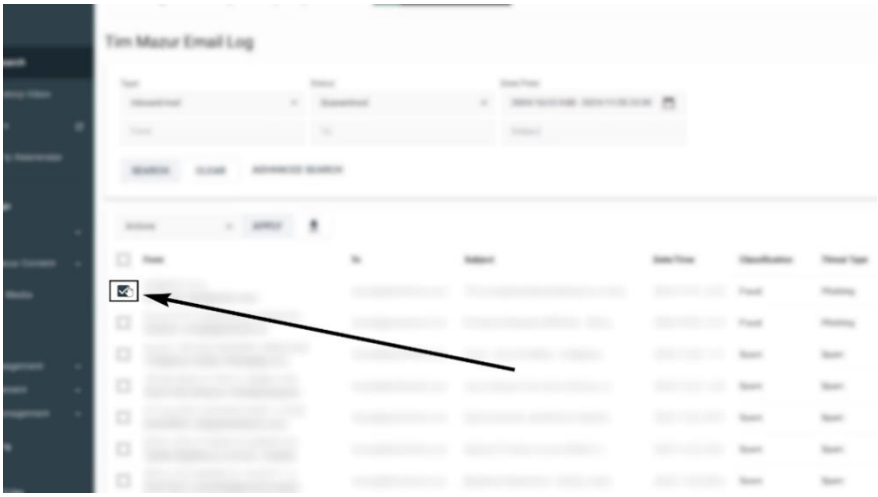


Рис. 3.12.1. Встановлений прапорець поруч з назвою листа [36]

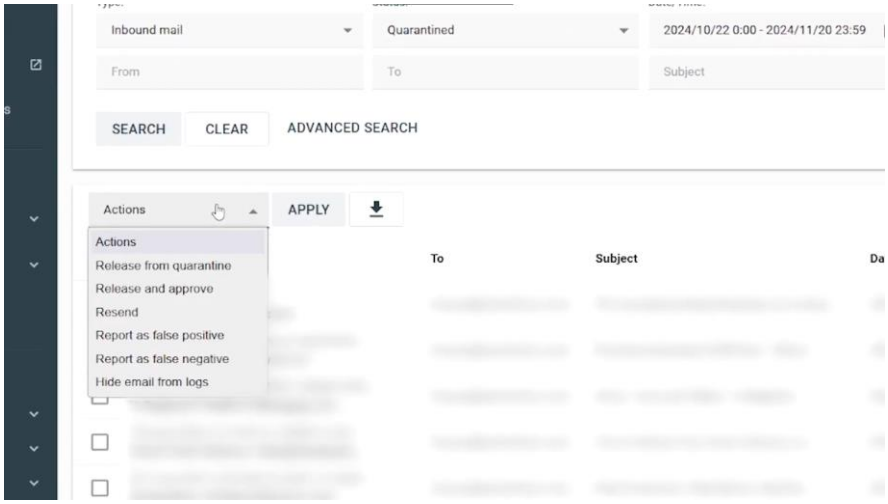


Рис. 3.12.2. Огляд розширених функцій детального логування електронних листів [36]

Функціональні можливості даного модуля включають:

– *release from quarantine* (електронний лист буде надіслано в організаційний поштовий сервіс);

– *release and approve* (лист буде доставлено в організаційний поштовий сервіс, а відправника буде додано до білого списку; майбутні листи від відправників з наявного білого списку ніколи не потраплятимуть до карантину);

– *resend* (дана функція дозволяє адміністратору або кінцевому користувачеві повторно відправити лист, якщо він застряг у черзі або якщо внутрішній поштовий сервер не відповідає);

– *report as false positive* (визначає електронний лист як легітимний, гарантуючи, що майбутні листи від цього відправника будуть дозволені);

– *report as false negative* (визначає електронний лист як спам, покращуючи виявлення спаму для подібних повідомлень);

– *hide email from logs* (ця опція використовується, коли адміністратори або кінцеві користувачі не хочуть бачити конкретні спам-листи або легальні електронні листи в пошуку журналу; використання даної опції не є незворотнім).

Керування списками дозволених та заблокованих відправників

На порталі Proofpoint можна налаштувати фільтрацію ЕП, керуючи списками дозволених і заблокованих відправників (див. рис. 3.13):

Рис. 3.13. Огляд фільтрації списків дозволених та заблокованих адресатів [36]

Ця функція дає можливість дозволити використання відправників або доменів, вказавши довірені адреси ЕП (наприклад, *Joe@comp.com*) або цілі домени (такі як *enterprise.net*), щоб гарантувати, що їхні електронні листи завжди будуть доставлені до корпоративної поштової скриньки. Також ця функція дозволяє блокувати небажані адреси ЕП або домени, щоб запобігти потраплянню їхніх повідомлень до корпоративної поштової скриньки.

Примітка. Списки дозволених на рівні користувача можуть бути замінені фільтрами або правилами на рівні компанії.

Аварійна скринька

Аварійна скринька дозволяє користувачам надсилати та отримувати листи, коли поштові системи компанії не працюють в режимі офлайн (див. рис. 3.14):

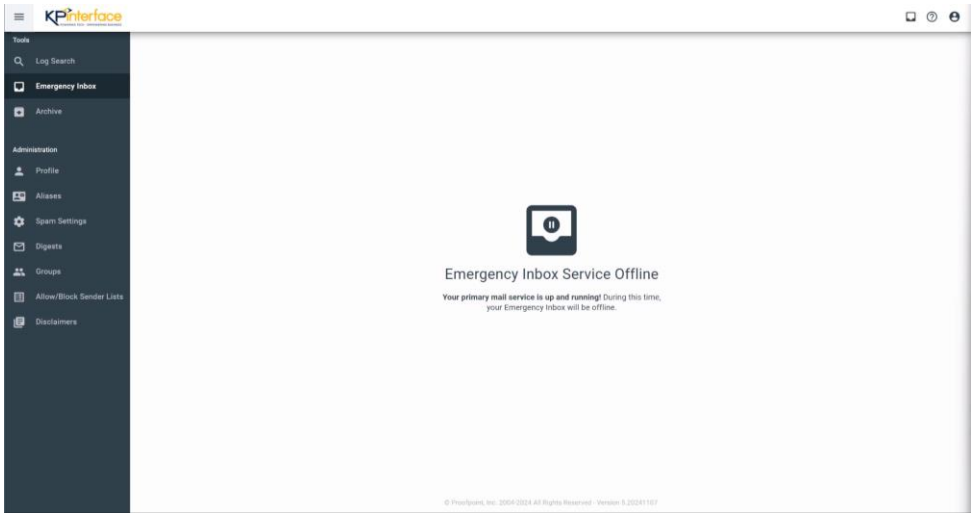


Рис. 3.14. Огляд аварійної скриньки на порталі Proofpoint [36]

Аварійна скринька автоматично почне наповнюватися електронними листами, коли організаційні поштові системи перестануть отримувати ЕП. Аварійну скриньку можна використовувати для надсилання нових повідомлень, а також для відповідей на отримані повідомлення. Як тільки доставку ЕП буде відновлено, всі надіслані повідомлення – як нові листи, так і відповіді на повідомлення – будуть автоматично доставлені на поштовий сервер [36].

3.3. Практичні рекомендації щодо профілактики та протидії атакам соціальної інженерії

Для того, щоб організації завжди залишалися у фокусі та підготовленими до будь яких подій, потрібно знати про те, як контрзаходи можуть доповнити власні політики безпеки та загалом захиститися від схем СІ. Власне, контрзаходи проти атак СІ зосереджені на усуненні саме людських помилок.

Типи контрзаходів можна розділити на три категорії:

1. Політика та процедури. Наявність правильно налаштованих політик, протоколів і процедур гарантує, що працівники будуть готові до потенційно вразливих ситуацій. Адже, якщо існують чіткі процедури, співробітник буде більш впевнено поводитися та дотримуватися процедур компанії під час (що може бути) загрозливої ситуації.

2. Обізнаність працівників. Оскільки зловмисники постійно розвивають свою тактику, команда безпеки та навіть звичайні співробітники повинні бути навчені розпізнавати атаки (або ситуації, що відхиляються від встановлених норм).

З часом набуті навички можуть забутися. Але незважаючи на це, техніка і тактика соціальних інженерів продовжує розвиватися. Регулярні та своєчасні тренування для кожного члена команди можуть бути більш ефективними, ніж здається на перший погляд.

Комплексний навчальний план повинен включати загальну підготовку з питань безпеки, регулярні симуляції фішингових атак та повноцінні тренінги з CI. Також важливою є обізнаність працівників щодо чутливості та класифікації інформації та активів. Якщо організація має справу з критично важливою інформацією, команда повинна усвідомлювати, що до неї потрібно ставитися більш скептично, ніж до активів меншої важливості.

3. Технічні заходи. Технічні контрзаходи покликані запобігти ескалації ситуації. Мета полягає в тому, щоб зупинити суб’єкт загрози до того, як у них з’явиться можливість скористатися людською природою. Тут є кілька варіантів, зокрема утилізація відходів, яка безпечно знищує будь-яку конфіденційну інформацію, безпечні системи фізичного доступу (двері, ворота тощо), складні картки для входу, верифікація осіб, супровід гостей тощо.

Будь-які контрзаходи, які впровадила організація, повинні бути оцінені на предмет їхньої ефективності. Такі огляди можуть бути проведені власними силами або у співпраці із зовнішнім партнером.

Вони також можуть бути пасивними або активними. Пасивний огляд означає лише оцінку поверхні атаки на теоретичному рівні. Активний аналіз передбачає

активні спроби порушити конфіденційність, цілісність та/або доступність інформації.

Найважливішою частиною плану безпеки будь-якої організації є її команда. Обдумуючи, як вона буде захищати свою організацію від загроз у кіберпросторі, потрібно спілкуватися з усіма членами компанії таким чином, щоб сприяти їх залученню в загальну культуру безпеки компанії [15].

ВИСНОВКИ

У ході роботи над кваліфікаційною роботою доведено, що електронна пошта залишається одним із найбільш вразливих каналів комунікації в організаціях через постійне вдосконалення методів соціальної інженерії. Поглиблений аналіз свідчить, що традиційні технічні засоби захисту не здатні повною мірою протидіяти динамічним соціотехнічним загрозам, оскільки вони переважно орієнтовані на виявлення відомих сигнатур та правил. Отже, акцент дослідження було зроблено на комплексному підході, який поєднує технічні рішення з підвищенням обізнаності користувачів та впровадженням передових аналітичних інструментів.

Проведений аналіз архітектури та функціональних компонентів системи безпеки Proofpoint Core Email Protection показав, що рішення успішно інтегрується в корпоративну інформаційну систему на базі API, забезпечуючи сканування вхідних і вихідних повідомлень, пісочниці для вкладень та аналіз електронних листів на наявність шкідливого програмного забезпечення за допомогою штучного інтелекту в поєднанні з машинним навчанням. Такий підхід дозволяє виявляти та нейтралізувати загрози як до доставки листа, так і після неї, істотно знижуючи ризик компрометації електронної пошти.

Порівняльний аналіз з іншими наявними платформами підтвердив унікальні переваги Proofpoint: використання власної лінгвістичної моделі Nexus для виявлення BEC-атак, застосування комп’ютерного зору для розпізнавання візуальних загроз і глибоке машинне навчання для адаптації до нових тактик зловмисників. Це забезпечує високу точність виявлення та мінімізацію хибних спрацьовувань, що істотно підвищує ефективність роботи відділу безпеки та скорочує час реагування на інциденти

Розроблені рекомендації щодо впровадження Proofpoint Core Email Protection передбачають налаштування політик фільтрації, карантинування підозрілих листів та регулярний перегляд звітів користувачів через щоденні дайджести. Практичний

сценарій включає створення централізованого процесу моніторингу, призначення відповідальних осіб за аналіз логів та проведення навчальних сесій для підвищення кібергігієни співробітників.

Отже, результати роботи мають достатній практичний потенціал для будь-якої організації, що прагне підвищити стійкість корпоративної електронної пошти до соціотехнічних атак. Запропонована стратегія дає змогу поєднати технологічні засоби захисту зі зміною поведінкових паттернів користувачів, створюючи багаторівневий бар’єр проти сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Email Reporting and Remediation – eBook. *Proofpoint*. URL: https://www.proofpoint.com/us/resources/e-books/email-reporting-and-remediation (date of access: 23.03.2025).
2. How Emails Can Manipulate: The Rise of Social Engineering. URL: https://emailauth.io/blog/email-social-engineering (date of access: 23.03.2025).
3. Q4 2024 Cyber Threat Landscape Report. *Kroll*. URL: https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q4-2024-threat-landscape-report-phishing (date of access: 23.03.2025).
4. 12 Types of Social Engineering Attacks to Look Out For. *Copado: AI-Powered DevOps for Business Applications*. URL: https://www.copado.com/resources/blog/12-types-of-social-engineering-attacks-to-look-out-for (date of access: 30.03.2025).
5. Phishing Email Examples. *NordVPN*. URL: https://nordvpn.com/blog/phishing-email-examples (date of access: 30.03.2023).
6. Різноманітний арсенал соціальної інженерії: види атак та способи їх запобігання. *HackYourMom*. URL: https://hackyourmom.com/kibervijna/riznomanitnyj-arsenal-soczialnoyi-inzheneriyi-vydy-atak-ta-sposoby-yih-zapobigannya (дата звернення: 30.03.2025).
7. Що таке Spear Phishing та як від нього захиститися? *HackYourMom*. URL: https://hackyourmom.com/kibervijna/shho-take-spear-phishing-ta-yak-vid-nogo-zahystytysya (дата звернення: 30.03.2025).
8. Що таке фішинг? Методи атак та приклади. *ТОВ «Грідінсофт»*. URL: https://gridinsoft.ua/phishing (дата звернення: 23.03.2025).
9. What Is Spear Phishing?. *Palo Alto Networks*. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-spear-phishing (date of access: 30.03.2025).

10. The Dark Side of AI: A New Era of Cyber Threats. *CommSec Cyber Security*. URL: https://commsec.ie/the-dark-side-of-ai-a-new-era-of-cyber-threats (date of access: 30.03.2025).

11. What is a Whaling Cyber Attack? Examples and Prevention. *IdentityTheft*. URL: https://identitytheft.org/attacks/whaling (date of access: 30.03.2025).

12. Laptiev S. THE ADVANCED METHOD OF PROTECTION OF PERSONAL DATA FROM ATTACKS USING SOCIAL ENGINEERING ALGORITHMS. *Cybersecurity: Education, Science, Technique.* 2022. Vol. 16, no. P. 45–62. URL: https://doi.org/10.28925/2663-4023.2022.16.4562 (дата звернення: 30.03.2025).

13. Siddiqi M. A., Pak W., Siddiqi M. A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences.* 2022. Vol. 12, no. 12. P. 6042. URL: https://doi.org/10.3390/app12126042 (date of access: 30.03.2025).

14. Що таке фішинг і чому він небезпечний для компаній. *Український телекомунікаційний портал.* URL: https://portaltele.com.ua/news/internet/shho-take-fishyng-i-chomu-vin-nebezpechnyj-dlya-kompanij.html (дата звернення: 30.03.2025).

15. Werner K. Social Engineering Countermeasures. RangeForce Cloud-Based. *Cyber Range.* URL: https://www.rangeforce.com/blog/social-engineering-countermeasures (date of access: 14.05.2025).

16. 50 відтінків фішингу, або Руки геть із клавіатури!. *Петр и Мазепа.* URL: https://petrimazepa.com/ru/50_vidtinkiv_fishingu_abo_ruki_get_vid_klaviaturi (дата звернення: 30.03.2025).

17. Тенденції у розвитку фішингу та протидія йому. *IT Specialist.* URL: https://my-itspecialist.com/trends-in-phishing-development-and-countermeasures (дата звернення: 10.04.2025).

18. What Is Email Scanning?. *CheckPoint.* URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-scanning

(date of access: 10.04.2025).

19. What is Attachment Sandboxing and Why Do You Need It?. *VIPRE*. URL: https://vipre.com/blog/attachment-sandboxing-important (date of access: 10.04.2025).

20. What is EDR vs. XDR?. *Palo Alto Networks.* URL: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-xdr (date of access: 10.04.2025).

21. EDR vs XDR – What Is the Difference?. *Trend Micro.* URL: https://www.trendmicro.com/en_gb/what-is/xdr/edr-vs-xdr.html (date of access: 10.04.2025).

22. The DNA Behind UEBA. *CheckPoint.* URL: https://emailsecurity.checkpoint.com/blog/the-dna-behind-ueba (date of access: 10.04.2025).

23. Proofpoint Core Email Protection. *Cybersecurity Excellence Awards.* URL: https://cybersecurity-excellence-awards.com/candidates/proofpoint-core-email-protection-2025 (date of access: 15.04.2025).

24. Proofpoint Core Email Protection. Decision Guide for Choosing a SEG or API-based Deployment. *Proofpoint.* URL: https://www.proofpoint.com/sites/default/files/solution-briefs/pfpt-us-sb-core-email-protection-decision-guide.pdf (date of access: 07.05.2025).

25. Tech Win Cyber. API Email Security Gateway VS Secure Email Gateway Comparison, 2024. *YouTube.* URL: https://www.youtube.com/watch?v=T43iKDWTP5c (date of access: 07.05.2025).

26. Understanding Core Email Protection: API and Adaptive Email DLP – White Paper. *Proofpoint.* URL: https://www.proofpoint.com/us/resources/white-papers/understanding-core-email-protection-api-and-adaptive-email-dlp (date of access: 15.04.2025).

27. Secure Email Gateway (SEG) vs. API-Based Email Security. *Proofpoint.* URL: https://www.proofpoint.com/us/blog/email-and-cloud-threats/secure-email-gateway-seg-vs-api-based-email-security (date of access: 07.05.2025).

28. Proofpoint Core Email Protection – Solution Brief. *Proofpoint.* URL: https://www.proofpoint.com/sites/default/files/solution-briefs/pfpt-us-sb-core-email-protection.pdf (date of access: 15.04.2025).

29. Proofpoint Email Protection vs. ProtonMail vs. Trend Vision One vs. ePrism Email Security. *SourceForge.* URL: https://sourceforge.net/software/compare/Proofpoint-Email-Protection-vs-ProtonMail-vs-Trend-Vision-One-vs-ePrism-Email-Security (date of access: 19.04.2025).

30. Proton: Privacy by default. *Proton.* URL: https://proton.me (date of access: 19.04.2025).

31. Trend Vision One™ – A Single & Unified Cybersecurity Platform. *Trend Micro*. URL: https://www.trendmicro.com/en_us/business/products/one-platform.html (date of access: 19.04.2025).

32. Edgewave ePrism Email Security. *Webservio Inc.* URL: https://www.webservio.com/email-security/edgewave-eprism-email-security.html (date of access: 19.04.2025).

33. Proofpoint, Inc. Form 10-K for the fiscal year ended December 31, 2013. URL: https://www.sec.gov/Archives/edgar/data/1212458/000121245814000004/proofpoint-12312013x10k.htm (date of access: 15.04.2025).

34. 5 Reasons Proofpoint Is a Leading Choice for Augmenting Microsoft 365 Email Security via API – eBook. *Proofpoint.* URL: https://www.proofpoint.com/uk/resources/e-books/proofpoint-top-choice-augmenting-microsoft-365-email-security-via-api (date of access: 19.04.2025).

35. KPInterface Inc. How to Use Proofpoint Email Protection: A Complete Guide, 2024. *YouTube*. URL: https://www.youtube.com/watch?v=v68N_R_fOFk (date of access: 17.05.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)