DOI: 10.58254/viti.6.2024.09.116

УДК 004.056

д-р філософії Марченко В. В. ORCID: 0000-0003-4271-3132 (ДУІКТ)
Чайківський В. В. ORCID: 0009-0001-4257-8893 (ДУІКТ)
Прийма О. О. ORCID: 0009-0008-6991-1773 (ВІТІ ім. Героїв Крут)

МЕТОД ПІДВИЩЕННЯ ОБІЗНАНОСТІ ОСОБОВОГО СКЛАДУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ ПРОГРАМНОГО ЗАСТОСУНКУ GOPHISH

У сучасних умовах кіберпростору, де загрози постійно еволюціонують, особливої уваги потребують фішингові атаки. Вони є одним із найпоширеніших методів соціальної інженерії, що використовуються для отримання доступу до конфіденційної інформації через маніпуляції з користувачами. Такі атаки можуть призвести до витоку даних, фінансових втрат та репутаційних ризиків.

Однією з ключових проблем є недостатня підготовка персоналу до розпізнавання фішингових загроз. Традиційні методи навчання не забезпечують належної інтерактивності та реалістичності, що знижує ефективність підвищення обізнаності. Для вирішення цього питання потрібні нові підходи, які моделюють реальні сценарії кібератак.

Інструмент Gophish дозволяє створювати персоналізовані фішингові кампанії, що імітують реальні атаки та аналізують реакції користувачів. Його функціонал включає створення шаблонів листів, відправку повідомлень та збір даних про взаємодію користувачів. Це дозволяє організаціям виявляти слабкі місця, коригувати навчальні програми та проводити додаткові тренінги.

Результати показують, що використання Gophish підвищує обізнаність персоналу щодо протидії соціальній інженерії. Інтерактивні симуляції сприяють кращому розумінню користувачами фішингових загроз та допомагають їм вчасно розпізнати небезпеку. Завдяки зібраній аналітиці керівництво може оперативно впроваджувати коригувальні заходи.

Розвиток штучного інтелекту та машинного навчання відкриває нові можливості для вдосконалення таких інструментів. Майбутні рішення зможуть адаптувати симуляції під конкретних користувачів, що зробить навчання ще ефективнішим.

Ключові слова: *фішинг, соціальна інженерія, підвищення обізнаності, Gophish, коригувальні дії, фішингові листи, симуляція.*

V. Marchenko, V. Chaikivskyi, O. Pryima Method for raising personnel awareness of information security using the Gophish software application

In today's cyberspace, where threats are constantly evolving, phishing attacks require special attention. They are one of the most common social engineering methods used to gain access to confidential information by manipulating users. Such attacks can lead to data breaches, financial losses, and reputational risks.

One of the key problems is the lack of staff training in recognizing phishing threats. Traditional training methods do not provide adequate interactivity and realism, which reduces the effectiveness of awareness raising. To address this issue, new approaches are needed that model real-life cyberattack scenarios.

The Gophish tool allows you to create personalized phishing campaigns that simulate real attacks and analyze user reactions. Its functionality includes creating email templates, sending messages, and collecting data on user interaction. This allows organizations to identify weaknesses, adjust training programs, and conduct additional training.

The results show that using Gophish increases staff awareness of social engineering. Interactive simulations contribute to a better understanding of phishing threats and help users recognize the danger in time. Thanks to the analytics collected, management can quickly implement corrective measures.

The development of artificial intelligence and machine learning opens up new opportunities for improving such tools. Future solutions will be able to adapt simulations to specific users, making training even more effective.

Keywords: *phishing, social engineering, awareness raising, Gophish, corrective actions, phishing emails, simulation.*

Вступ

Фішинг є однією з найпоширеніших форм соціальної інженерії, яка використовується зловмисниками для розсилання шахрайських електронних листів з метою впливу на користувачів. Вони намагаються змусити жертву надати чутливу інформацію, відкрити шкідливий файл або перейти за посиланням, що веде на підроблений вебсайт. Основна ціль

фішингових атак – це людський фактор, оскільки вони спрямовані на обман працівників та інших осіб, які мають доступ до інформаційних систем організації.

Такі атаки завдають значної шкоди як індивідуальним користувачам, так і великим організаціям, тому ефективне навчання персоналу є одним із ключових заходів для протидії різним методам соціальної інженерії. Проте наявні інструменти для емуляції фішингових атак мають обмежену функціональність, і їх можливості часто не відповідають вимогам сучасних сценаріїв загроз. Це створює потребу у розробці та впровадженні більш ефективних рішень, які дозволять проводити реалістичні симуляції та підвищити обізнаність користувачів. У довгостроковій перспективі такі підходи сприятимуть зниженню ризиків, пов'язаних з фішингом та іншими методами соціальної інженерії.

Згідно з рекомендаціями Національного інституту стандартів і технологій (NIST) у фреймворку NIST CSF 2.0, підвищення обізнаності персоналу щодо інформаційної безпеки має здійснюватися на регулярній основі. Навчання повинно охоплювати не лише основний персонал, а й сторонніх підрядників, які мають доступ до інформаційних систем організації [1]. Це є важливим аспектом стратегії інформаційної безпеки, оскільки людський фактор залишається однією з найвразливіших точок у захисті даних.

Аналіз фішингових атак, проведений аналітиками Оперативного центру реагування на кіберінциденти у IV кварталі 2023 року, показав, що з 1731 зафіксованої атаки 472 мали на меті поширення шкідливих вкладень [2]. Це підтверджує, що фішинг активно використовується для розповсюдження шкідливого програмного забезпечення, який створює додаткові ризики для організацій. Відповідно до доповіді Symantec Internet Security Threat Report (ISTR), навіть невелика частка всього URL-трафіку, а саме 0,5%, є фішинговою, але її вплив на загальну безпеку залишається значним [3].

Таким чином, зростаючий рівень загроз від фішингових атак вимагає впровадження нових методів та інструментів для підвищення обізнаності користувачів. У даній статті розглядаються існуючі підходи, аналізується їх ефективність, а також пропонуються рішення, які можуть підвищити рівень підготовки персоналу та знизити ризики, пов'язані з фішинговими атаками.

Постановка проблеми. У сучасних умовах швидких змін та зростаючих загроз у кіберпросторі організаціям складно встигати за стрімкими темпами розвитку кібератак. Хоча спільнотою розроблено численні рекомендації та інструменти для підвищення рівня інформаційної безпеки, багато з них потребують адаптації під конкретні потреби організацій. У цьому мінливому середовищі особливу увагу варто приділяти людському фактору, який залишається найслабшою ланкою в системах інформаційної та кібербезпеки.

Задля зменшення ризиків організаціям рекомендовано регулярно проводити заходи з підвищення обізнаності кінцевих користувачів. Проте теоретичні знання не забезпечують належного рівня підготовки для протидії фішинговим атакам. Для цього необхідні практичні симуляції, які максимально наближають користувачів до реальних сценаріїв кібератак, що дозволяє співробітникам краще усвідомити потенційні ризики для себе та організації через неуважність або необачність.

Як правило, організації залучають зовнішніх спеціалістів для проведення таких навчань, що призводить до додаткових фінансових витрат. У зв'язку з цим виникає потреба у впровадженні внутрішніх навчальних програм, які не лише зменшать витрати, а й дозволять створювати симуляції, максимально наближені до реальних фішингових атак. Одним із таких рішень є використання інструменту Gophish, який надає можливість створення персоналізованих фішингових кампаній, аналізу реакції користувачів та визначення їх вразливих місць.

Аналіз останніх публікацій. Наукові дослідження, щодо фішингу та соціальної інженерії, підкреслюють актуальність загроз, які виникають у зв'язку з людським фактором.

Фішингові атаки залишаються одним з найпоширеніших методів соціальної інженерії, що використовуються для отримання несанкціонованого доступу до конфіденційної інформації шляхом маніпуляцій з користувачами. Перехід на дистанційну або гібридну форму роботи після пандемії COVID-19 спричинив значне зростання кількості фішингових атак, що пов’язано з більшою активністю користувачів у цифровому середовищі та їх підвищеною вразливістю до такого роду атак [4].

Результати дослідження 2023 року, проведеного компанією SlashNext, свідчать про зростаюче занепокоєння серед фахівців з кібербезпеки стосовно атак типу Business Email Compromise (BEC). У звіті вказується, що 46 % опитаних відповідальних осіб з кібербезпеки відзначили зростання кількості атак BEC на співробітників їхніх організацій. Це явище пояснюється доступністю сучасних чат-ботів на базі штучного інтелекту, які значно підвищують ефективність і масштабованість фішингових атак, що робить їх більш переконливими та складними для виявлення [5].

Аналіз публікацій також вказує на те, що електронна пошта залишається основним інструментом для здійснення фішингових атак. Згідно зі звітом IBM Security X-Force, понад 90 % успішних атак у 2023 році розпочинались саме з фішингових електронних листів. Це підтверджує значущість даного вектору загроз і необхідність приділення особливої уваги його мінімізації [6].

Дослідження, опубліковане у "Journal of Cyber Security", акцентує на зростанні ефективності фішингових кампаній завдяки впровадженню методів штучного інтелекту, які дозволяють створювати більш правдоподібні та персоналізовані атаки. Використання алгоритмів машинного навчання для аналізу поведінкових характеристик користувачів забезпечує можливість формування повідомлень, які виглядають надзвичайно переконливо, що підвищує ймовірність успішного здійснення фішингових атак [7].

Таким чином, підвищення складності та варіативності фішингових атак зумовлює необхідність впровадження комплексних рішень, які включають програмно-апаратні засоби для виявлення та блокування підозрілих електронних листів. Крім того, важливим елементом стратегії кібербезпеки залишається регулярне підвищення обізнаності співробітників, оскільки саме людський фактор продовжує залишатись найвразливішим компонентом у системах інформаційної безпеки.

Метою статті є обґрунтування та розробка методу підвищення обізнаності особового складу з інформаційної безпеки щодо готовності протидіяти соціальній інженерії, зокрема фішингу, із застосуванням програмного забезпечення Gophish.

Виклад основного матеріалу дослідження

Програмне забезпечення Gophish має відкритий вихідний код, репозиторій якого розміщено на платформі GitHub. Інструмент розроблено мовою програмування Go, а за замовчуванням він використовує базу даних SQLite, хоча є можливість підключення до MySQL при необхідності. Gophish немає вбудованого SMTP-сервера, тому для надсилання фішингових електронних листів необхідно використовувати зовнішні SMTP-рішення [8].

Інструмент характеризується зручним та інтуїтивно зрозумілим вебінтерфейсом, що полегшує налаштування та управління фішинговими кампаніями. Gophish дозволяє створювати шаблони електронних листів і фішингові вебсайти, а також збирати та візуалізувати дані щодо реакцій користувачів, зокрема відкриття листів, переходи за посиланнями та введення даних. Отримані аналітичні дані надають можливість організаціям оцінити рівень обізнаності персоналу з питань кібербезпеки та ідентифікувати найбільш вразливі аспекти їхньої поведінки.

Для кращого розуміння принципу роботи фішингових атак, наведено загальну концептуальну схему (рис. 1), що описує стандартний процес фішингової атаки через електронну пошту.

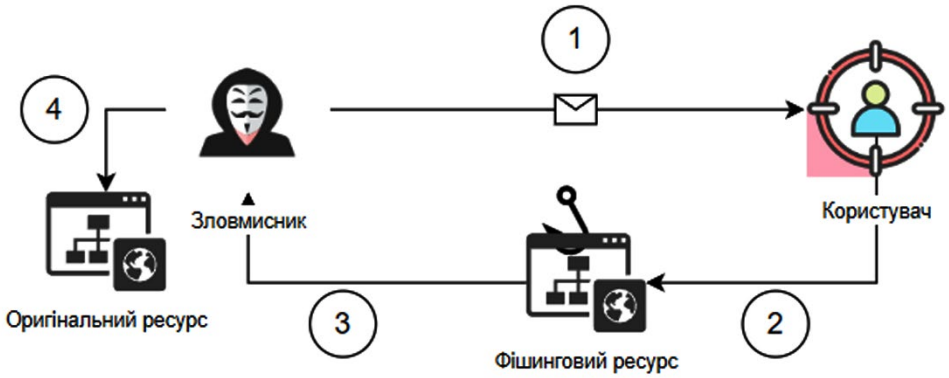

Рис. 1. Концептуальна схема фішингу

1. Зловмисник надсилає фішинговий електронний лист, маскуючи його під легітимне повідомлення (наприклад, від технічної підтримки або офіційної установи), щоб отримати від користувача чутливі дані.

2. Користувач відкриває електронний лист і взаємодіє з вкладенням або переходить за посиланням, яке веде на підроблений вебсайт.

3. На фейковому вебсайті користувач вводить свої облікові дані (логін і пароль), які стають доступними зловмиснику.

4. Зловмисник може використати отримані облікові дані для несанкціонованого доступу до оригінальних вебресурсів або зберегти їх для ініціалізації подальших атак.

Для ефективного підвищення обізнаності персоналу за допомогою Gophish необхідно встановити та налаштувати програму на внутрішньому сервері організації або в хмарному середовищі. Завдяки відкритому вихідному коду інструмент доступний для завантаження з офіційного порталу. Після інсталяції відповідальні особи можуть адаптувати Gophish для проведення реалістичних симуляцій фішингу, використовуючи можливості інструменту з копіювання інтерфейсу вебресурсів (рис. 2), що дозволяє створювати симуляції, які максимально наближені до реальних атак, на прикладі соціальних мереж.

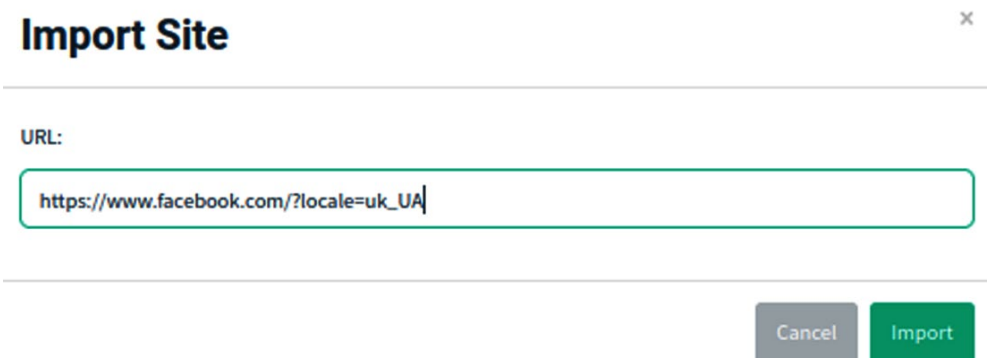

Рис. 2. Функціонал для копіювання вебресурсів

Головною метою фішингових атак є отримання чутливих даних користувача, таких як логін та пароль. Для реалізації цієї цілі в контексті підвищення обізнаності персоналу за допомогою Gophish використовуються функції «Capture Submitted Data» та «Capture Passwords» (рис. 3). Цей функціонал дозволяє фіксувати введені користувачами дані, що, у свою чергу, створює можливість для формування статистики, яка використовується для оцінки рівня обізнаності співробітників щодо фішингових загроз.

Для забезпечення максимально реалістичної симуляції та зниження ймовірності її виявлення користувачем рекомендується налаштувати автоматичне перенаправлення на

оригінальну вебсторінку після того, як користувач введе свої дані на підробленому ресурсі. Такий підхід знижує ризик виникнення підозр у користувача та зберігає природність процесу, що дозволяє отримати більш точні та достовірні результати під час проведення фішингових симуляцій.

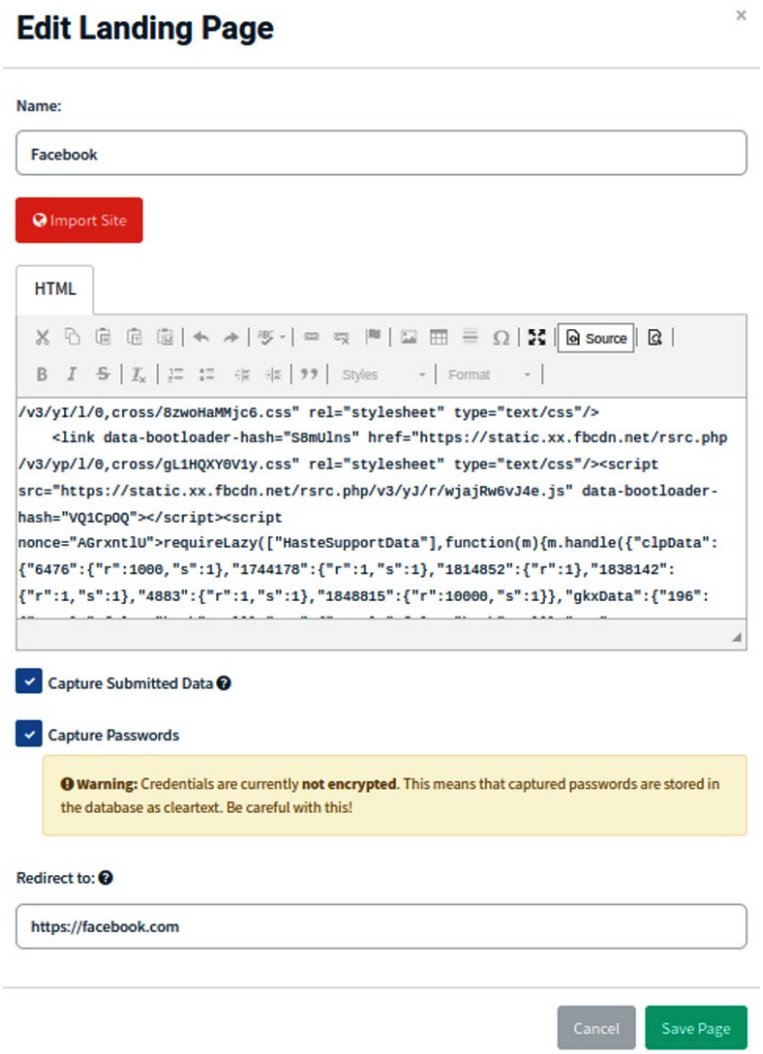

Рис. 3. Розширені функціональні можливості

Наступним ключовим етапом є налаштування шаблонів електронних листів, які будуть розсилатися співробітникам у рамках симуляцій фішингових атак. Gophish надає можливість створювати власні шаблони фішингових листів, але для досягнення максимальної ефективності ці шаблони необхідно зробити максимально схожими на легітимні повідомлення (рис. 4).

Інструмент має функцію «Import Email», яка дозволяє імпортувати електронні листи з легітимних ресурсів, адаптуючи їх до потреб конкретної організації (рис. 5). Ця можливість спрощує процес створення правдоподібних повідомлень, знижуючи час і зусилля, необхідні для розробки шаблонів. Водночас, відповідальні за навчання особи можуть створювати шаблони вручну, налаштовуючи їх під специфічні сценарії, наприклад, повідомлення щодо оновлення програмного забезпечення, зміну паролю у соціальних мережах чи корпоративних системах.

Ключовим аспектом налаштування є переконливість шаблонів. Вони повинні виглядати достатньо реалістично, щоб користувачі не могли легко відрізнити їх від справжніх

повідомлень. Це сприятиме більш природній реакції на фішингові симуляції та забезпечить отримання достовірніших результатів для подальшого аналізу та вдосконалення навчальних програм.

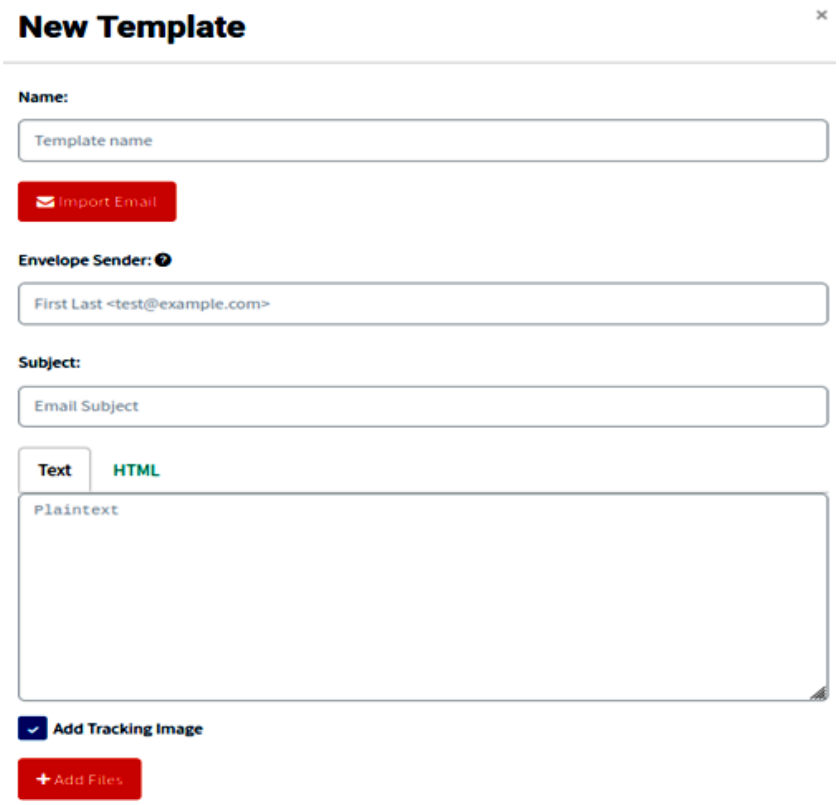

Рис. 4. Діалогове вікно створення нового шаблону

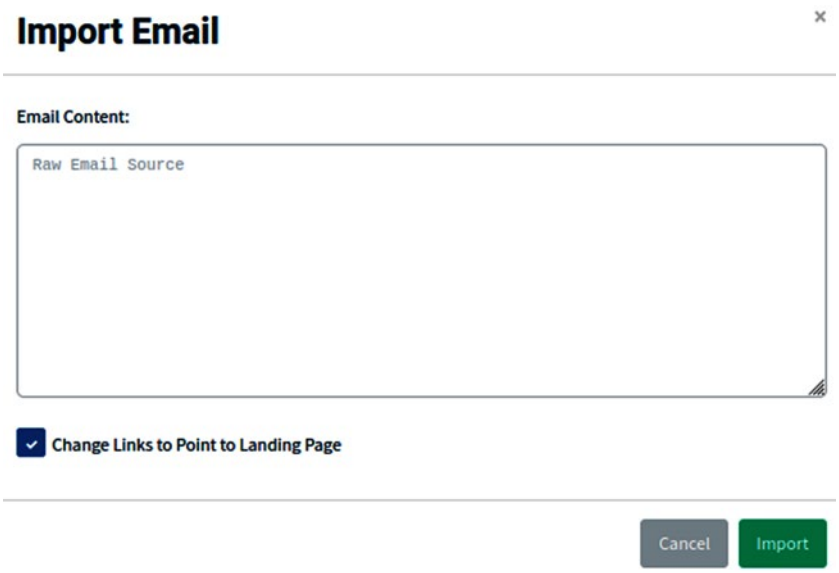

Рис. 5. Діалогове вікно з можливістю копіювання легітимного листа

Важливим елементом, що дозволяє впроваджувати коригувальні дії після проведення практичних навчань з фішинговими симуляціями, є моніторинг показників та формування звітності (рис. 6). Відповідно до рекомендацій компанії Terranova Security, яка спеціалізується на навчанні співробітників з питань кібербезпеки, відстеження таких показників, як відкриття

електронних листів, завантаження вкладень, розкриття облікової інформації та загальна кількість кліків під час фішингових симуляцій, є основою для складання звітів. Ці звіти містять інформацію про кількість користувачів, які стали жертвами фішингових атак, а також про те, скільки співробітників повідомили про підозрілу активність [9].

Інструмент Gophish забезпечує можливість детального аналізу поведінки кожного користувача, залученого до фішингових тестувань. Серед показників, які відстежуються під час кампаній, можна виділити:

час відкриття електронного листа: дозволяє отримати інформацію про те, коли користувач відкрив фішингове повідомлення, що може свідчити про швидкість його реакції на подібні повідомлення;

час і дата відкриття посилання: допомагає визначити, наскільки швидко користувачі реагують на фішингові атаки, переходячи за підозрілими посиланнями;

введення облікових даних: фіксується, чи ввів користувач свої облікові дані на підробленій вебсторінці, що дозволяє оцінити реальний ризик витоку інформації.

Такий детальний аналіз допомагає організаціям ідентифікувати слабкі місця в поведінці співробітників і розробляти подальші навчальні програми, спрямовані на підвищення рівня обізнаності та готовності до протидії фішинговим атакам. Звітність також сприяє оцінці загальної ефективності проведених симуляцій та дозволяє оперативно вживати заходів для усунення виявлених проблем.

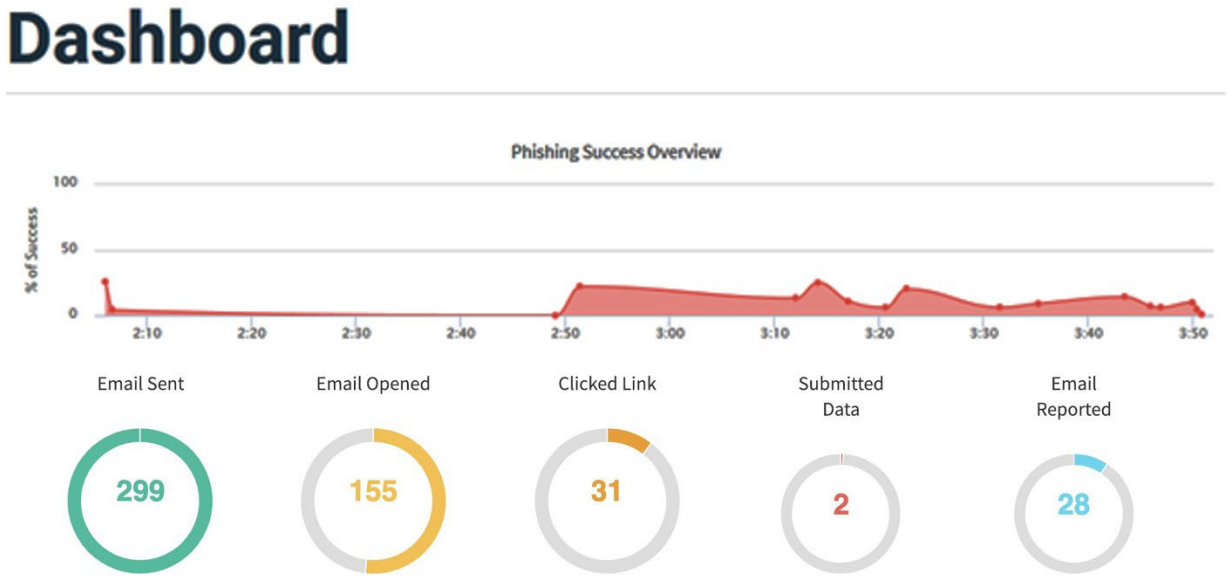

Рис. 6. Візуалізація результатів фішингової кампанії Gophish

Варто підкреслити, що проведення заходів із практичного тестування користувачів, зокрема симуляцій фішингових атак, є ключовим елементом для оцінки рівня обізнаності персоналу щодо кіберзагроз. Такий вид тестувань дозволяє реально оцінити, наскільки співробітники готові виявляти та ефективно протидіяти атакам соціальної інженерії в умовах, максимально наближених до реальних. Проте самих лише тестувань недостатньо для підтримки високого рівня інформаційної безпеки в організаціях. Важливо не тільки виявити слабкі місця, але й впроваджувати коригувальні дії на основі отриманих результатів.

Одним із ключових коригувальних заходів є регулярне навчання співробітників, яке охоплює як звичайних працівників, так і керівний склад. Воно має включати роз'яснення потенційних наслідків успішних кібератак, що дозволяє співробітникам краще усвідомлювати серйозність можливих загроз (рис. 7). Практичні тестування допомагають ідентифікувати тих

співробітників, які потребують додаткового навчання, та дозволяють керівництву адаптувати навчальні програми відповідно до потреб організації.

Порівняння результатів до і після проведення навчальних заходів дає розуміння на скільки знизилась вразливість компанії до фішингових атак. Наприклад, якщо до навчання 40 % користувачів вводили дані на фейкових сайтах, а після – лише 10 %, це свідчить про 75 % зниження вразливості, що можна обчислити за формулою:

$$\Delta P = \frac{P_{before} - P_{after}}{P_{before}} \times 100\%,$$

де ΔP – зниження рівня вразливості персоналу до фішингових атак (відсоток зменшення вразливості);

P_{before} – кількість користувачів, які піддалися фішинговій атаці до навчання (до проведення тренінгів);

P_{after} – кількість користувачів, які піддалися фішинговій атаці після навчання (після проведення тренінгів).

Такі показники демонструють значне підвищення обізнаності та рівня кібергігієни серед працівників. Також, завдяки використанню Gophish, вдається оптимізувати витрати на зовнішні послуги, оскільки інструмент дозволяє проводити навчання внутрішніми ресурсами організації. Це підтверджується розрахунками рентабельності інвестицій (Return On Investment):

$$ROI = \frac{B - C}{C} \times 100\%,$$

де ROI – рентабельність інвестицій у навчання;

B (Benefits) – сума потенційно зекономлених коштів від зменшення кількості інцидентів;

C (Costs) – загальна вартість проведення навчання (інвестиції у тренінги та навчальні програми).

Для аналізу швидкості реакції користувачів на фішингові атаки важливим показником є середній час відкриття листа:

$$T_{avg} = \frac{\sum T_{open}}{N},$$

де T_{avg} – середній час реакції користувачів;

$\sum T_{open}$ – сума часу між моментом відкриття листа і здійсненням першої дії користувачами (наприклад, кліком на посилання або закриття листа);

N – загальна кількість користувачів, які отримали фішинговий лист.

Після навчання цей час реакції користувачів може зрости, що буде свідчити про обережніше ставлення до електронних повідомлень.

Таким чином, комплексний підхід, що поєднує регулярні симуляції та постійне навчання, сприяє підвищенню загального рівня обізнаності в організації, дозволяє зменшити ризики, пов'язані з фішинговими атаками, і формує культуру інформаційної безпеки.

Процес формування та впровадження програм навчання має базуватися на результатах попередніх тестувань, що дозволяє адаптувати підхід до конкретних потреб організації та виявлених вразливостей. Навчальні заходи можуть включати спеціалізовані зовнішні програми для певних груп співробітників, які мають доступ до критичних даних та систем. Крім того, рекомендується регулярно проводити загальні тренінги, які організовує внутрішній підрозділ інформаційної безпеки для всіх працівників, з метою підвищення загального рівня обізнаності щодо базових принципів кібергігієни [10].

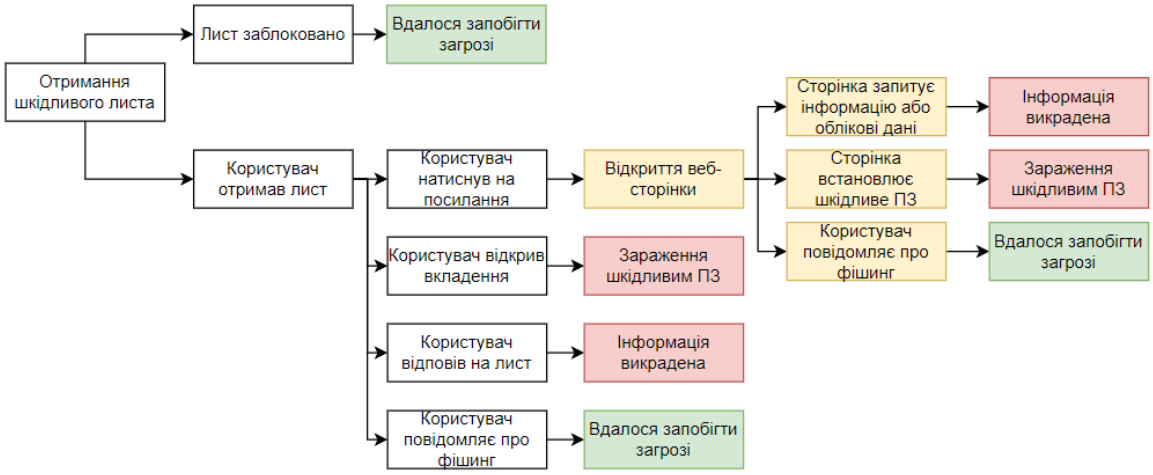

Рис. 7. Поширені шляхи фішингових атак на електронну пошту [9]

Відповідно до міжнародних стандартів, зокрема ISO/IEC 27002, підвищення рівня обізнаності співробітників має бути постійним і регулярним процесом [11]. Для цього доцільно використовувати цикл Шухарта-Демінга (PDCA), що забезпечує безперервний розвиток та вдосконалення навчальних програм (рис. 8).

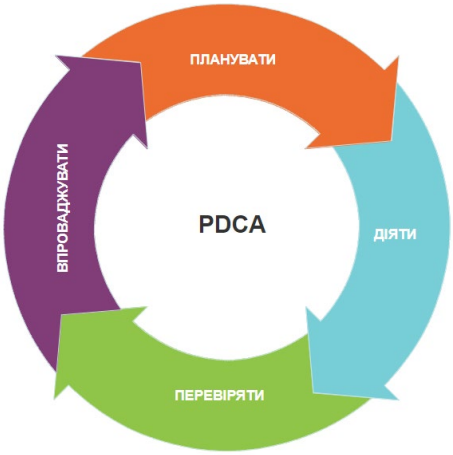

Рис. 8. Цикл Шухарта-Демінга

У контексті використання Gophish, процес підвищення обізнаності персоналу органічно поєднується з принципами циклу PDCA:

планувати (Plan) – визначення потреби у проведенні навчань, враховуючи сучасні тенденції атак, що базуються на методах соціальної інженерії. На цьому етапі аналізується, які вразливості виявлено під час попередніх тестувань, та формуються відповідні навчальні сценарії;

діяти (Do) – реалізація розроблених навчальних програм за допомогою Gophish, що дозволяє організувати симуляції фішингових атак. Під час цього етапу користувачі проходять практичне тестування в умовах, наближених до реальних кібератак;

перевіряти (Check) – аналіз результатів симуляцій, зокрема, оцінка показників взаємодії користувачів з фішинговими листами, часу реакції, частоти введення даних на фейкових ресурсах. Це дозволяє оцінити ефективність проведених заходів;

впроваджувати (Act) – на основі отриманих результатів розробляються плани коригувальних дій, що включають проведення додаткових внутрішніх або зовнішніх навчань

для тих, хто виявився менш підготовленим. Визначаються напрямки подальшого вдосконалення рівня кібергігієни організації.

Таким чином, використання циклу PDCA дозволяє створити структуру навчання, що сприяє постійному розвитку навичок співробітників та підвищує загальний рівень інформаційної безпеки в організації.

На додаток до Gophish, доцільно розглянути Phishing Quiz від Google – безкоштовний інтерактивний онлайн-інструмент, призначений для навчання користувачів розпізнавати фішингові атаки. Цей сервіс імітує реалістичні сценарії електронних листів, дозволяючи користувачам відпрацьовувати навички виявлення загроз без необхідності попереднього технічного налаштування [12].

Перевага Phishing Quiz полягає в простоті використання: достатньо мати доступ до інтернету, що робить його зручним для організацій без значних технічних ресурсів. На відміну від Gophish, який потребує розгортання на внутрішніх серверах або в хмарі, а також технічних знань для налаштування, Phishing Quiz не вимагає додаткових інвестицій і може бути швидко інтегрований у процес навчання.

Однак, функціональні можливості Phishing Quiz є обмеженими, оскільки він не підтримує масштабні кампанії з детальним аналізом поведінки користувачів. Водночас Gophish надає інструменти для комплексного навчання з можливістю збору статистики та подальшого вдосконалення програм безпеки.

Висновки і перспективи подальших досліджень

Відповідно до представленої інформації, метод підвищення обізнаності персоналу є важливим елементом загальної стратегії кібербезпеки, оскільки людський фактор залишається однією з найвразливіших ланок захисту. Практичні тренінги та симуляції, зокрема за допомогою Gophish, дозволяють ознайомити співробітників з реалістичними сценаріями, що імітують дії зловмисників, тим самим підвищуючи їхню готовність до виявлення фішингових атак.

Наукові дослідження свідчать, що симуляції, які відтворюють реальні фішингові сценарії, дозволяють співробітникам краще розпізнавати ознаки шахрайства в майбутньому, оскільки вони створюють умови для активного навчання. Це важливо, оскільки активні методи навчання, які включають практичний досвід, значно перевершують пасивні методи (лекції, брошури) за ефективністю запам’ятовування і застосування знань у реальних умовах. Зокрема, дослідження показують, що після практичних тренінгів зростає рівень обізнаності співробітників щодо фішингових загроз, що значно знижує кількість успішних атак.

Розглянутий метод, заснований на використанні Gophish, є ефективним інструментом для підвищення рівня обізнаності завдяки його функціональних можливостей:

Персоналізовані фішингові кампанії: Gophish дозволяє створювати сценарії, які максимально наближені до реальних атак, з урахуванням специфіки діяльності організації та її співробітників. Це забезпечує кращу підготовку користувачів до виявлення фішингу, оскільки вони стикаються з прикладами, подібними до тих, які можуть зустрітися у їхній повсякденній роботі.

Відстеження реакцій користувачів у реальному часі: завдяки можливості моніторингу дій співробітників під час симуляцій, керівництво може ідентифікувати слабкі місця та визначити, які аспекти безпеки потребують додаткового навчання. Це дозволяє адаптувати підходи до навчання і зосередити увагу на найбільш критичних питаннях.

Зручна візуалізація результатів: Gophish надає звіти, які включають детальну аналітику щодо дій користувачів (відкриття листів, кліки на посилання, введення облікових даних). Це дозволяє ефективно оцінювати результати тренінгів і визначати подальші коригувальні дії, що підвищує загальну кібергігієну в організації.

Завдяки цим функціям метод, заснований на використанні Gophish, не тільки навчає співробітників розпізнавати фішингові атаки, але й забезпечує інтерактивний підхід до навчання, який підвищує ефективність запам’ятовування інформації та практичного застосування навичок. Відповідно, це дозволяє організаціям вчасно реагувати на виявлені слабкі місця та адаптувати свою стратегію кібербезпеки до нових викликів, що постійно з’являються в динамічному кіберпросторі.

Подальші дослідження будуть спрямовані на вдосконалення існуючих методів підвищення обізнаності шляхом інтеграції технологій штучного інтелекту та машинного навчання. Це відкриває можливості для розробки адаптивних симуляцій, які зможуть підлаштовуватися під індивідуальні особливості користувачів, що зробить процес навчання більш ефективним та персоналізованим. Враховуючи динамічний розвиток кіберпростору, де методи атак постійно еволюціонують, такі інноваційні підходи забезпечать організаціям необхідну гнучкість у протидії новим загрозам та дозволять вчасно адаптувати стратегії кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The NIST Cybersecurity Framework (CSF) 2.0. *National Institute of Standards and Technology*. URL: https://doi.org/10.6028/NIST.CSWP.29 (date of access: 08.10.2024).

2. Звіт за четвертий квартал 2023. *Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України*. URL: https://scpc.gov.ua/uk/articles/341 (дата звернення: 08.10.2024).

3. Gray J. Practical Social Engineering: A Primer for the Ethical Hacker. San Francisco: No Starch Press, 2022. 240 p.

4. Phishing Attacks in Social Engineering: A Review / K. Sarpong Adu-Manu et al. *Journal of Cyber Security*. 2023. P. 1–29. URL: https://doi.org/10.32604/jcs.2023.041095 (date of access: 08.10.2024).

5. The State of Phishing 2023. Slashnext. URL: https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf (date of access: 08.10.2024).

6. IBM Security X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/security/services/ (date of access: 08.10.2024).

7. Advances in AI-based Phishing Detection and Prevention: A Review / R. Singh, A. Sharma. Journal of Cyber Security and Privacy, 2023. P. 32–45. URL: https://doi.org/10.3390/cybersecurity-2023-01234 (date of access: 08.10.2024).

8. Gophish – Open Source Phishing Framework. *Gophish*. URL: https://getgophish.com/ (date of access: 08.10.2024).

9. Why Is Phishing Awareness Training Important? *Terranova Security | Partner of Choice in Security Awareness*. URL: https://www.terranovasecurity.com/blog/why-is-phishing-training-so-important (date of access: 08.10.2024).

10. Enhancing Cybersecurity Through Phishing Simulation Training. Journal of Information Security & Privacy, Rouse, M., & Field, R. (date of access: 08.10.2024).

11. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2017, IDT; ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015, IDT).

12. Can you spot when you’re being phished? *Jigsaw | Google*. URL: https://phishingquiz.withgoogle.com/?hl=en (date of access: 08.10.2024).