УДК 528.852
DOI https://doi.org/10.32782/2663-5941/2025.2.2/04

Бойко О. В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Залевський С. В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Савчук В. С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

АНАЛІЗ ЕЛЕКТРОННОГО ЛИСТА ДЛЯ ВИЯВЛЕННЯ ОЗНАК ФІШИНГУ

Розроблено практичні рекомендації щодо аналізу отриманого електронного листа для виявлення ознак фішингу, в результаті ігнорування якого здійснюється запобігання продовженню кібератаки, першим кроком якої є фішинг. З початком російської військової агресії кількість загроз у кіберпросторі України постійно збільшується, кіберзлочинці суттєво активізували діяльність у період воєнного стану в Україні та проводять фішингові кампанії з метою отримання конфіденційних даних у населення України, причому 74 відсотка фішингових атак припадає на поштовий фішинг. Слід зазначити, що фішингові листи можуть надсилатися нібито від імені державних органів, міжнародних організацій та окремих осіб, а документами-приманками можуть бути запити на отримання інформації, міжнародна кореспонденція, офіційні листи переписки державних органів України тощо. Тому користувачам, які можуть бути об'єктами майбутніх кібератак, важливо вміти розпізнавати фішинг на основі аналізу отриманого електронного поштового листа для ігнорування таких листів та припинення кібератаки. Тому необхідно розробити практичні рекомендації щодо аналізу електроного листа, застосування яких дозволить користувачам виявити ознаки фішингу у отриманому листі та, відповідно, запобігти продовженню кібератаки, першим кроком якої є фішинг та, уникнути витоку інформації, тому що метою кібератак є доступ зловмисників до конфіденційної інформації. Єдиним джерелом інформації для аналізу та встановлення факту фішинга є отриманий електронний лист, тобто адреса електронної пошти відправника та вміст повідомлення, яке включає лінк на ресурс, за допомогою якого здійснюється збір конфіденційної інформації. Тому аналіз електронного листа для визначення того, чи є цей лист фішинговим, пропонується здійснювати в такій послідовності: 1) аналіз його вмісту, 2) аналіз заголовків електронного листа, 3) аналіз та пошук інформації за електронною адресою відправника, 4) аналіз посилання на ресурс.

Ключові слова: *фішинг, кібератака, електронна пошта, електронний лист, osint.*

Постановка проблеми. З початком російської військової агресії кількість загроз у кіберпросторі України постійно збільшується, так для одночасного масового ураження великої кількості користувачів однієї організації широко використовуються методи фішингу [1]. Крім того, кіберзлочинці суттєво активізували діяльність у період воєнного стану в Україні та проводять фішингові кампанії з метою отримання конфіденційних даних у населення України [2]. Реалізація кібератаки починається з надсилання потенційним жертвам фішингових листів зі шкідливим вкладенням, після відкриття якого запускається механізм автоматичної компрометації комп'ютерної системи та створюються передумови до витоку інформації. Найчастіше фішингові листи надсилаються електронною поштою [3]. Отже, єдиним джерелом для проведення аналізу з метою встановлення початку атаки з використанням фішингу є отриманий поштовий лист, тобто адреса електронної пошти відправника та вміст повідомлення. Слід зазначити, що фішингові листи можуть надсилатися нібито від імені державних органів, міжнародних організацій та окремих осіб, а документами-приманками можуть бути запити на отримання інформації, міжнародна кореспонденція, офіційні листи переписки державних органів України тощо. Тому користувачам, які можуть бути об'єктами майбут-

ніх кібератак, важливо вміти розпізнавати фішинг на основі аналізу отриманого електронного поштового листа для ігнорування таких листів та припинення кібератаки.

Аналіз останніх досліджень і публікацій. Приклади випадків фішингових атак з їх аналізом наведено у [4, 5], загальну класифікацію популярних напрямів фішингового атакування, які використовують кіберзлочинці під час спроб отримання доступу до конфеденційної інформації, подано у [5, 6], методи протидії фішингу розглянуто у [6, 7], але детально не розглядалися питання щодо аналізу поштового повідомлення для визначення ознак, за якими звичайний користувач мережі Інтернет може розпізнати фішинг, його проігнорувати та не реагувати на нові подібні фішингові повідомлення у майбутньому.

Постановка завдання. Метою статті є розробка рекомендацій щодо аналізу електронного листа його отримувачем для розпізнавання фішингу та, відповідно, для протидії кібератакам, метою яких є отримання доступу до конфіденційної інформації, першим етапом яких є поштовий фішинг.

Виклад основного матеріалу. Під фі́шингом (англ. phishing МФА: [‘fiʃiŋ] від fishing – риболовля) розуміють вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі їх персональних даних внаслідок самостійного розкриття конфіденційної інформації користувачами [3]. Концепцію фішингу вперше було описано в 1987 році в документі з конференції під назвою «Безпека системи: перспективи хакера», де описувалась техніка зловмисників, яка полягає в імітації авторитетних організацій або сервісів. Першими в історії вважаються систематичні фішинг-атаки, що почалися в мережі America Online (AOL) в 1995 році. Щоб викрасти легітимні облікові дані, зловмисники зв’язувалися з жертвами через AOL Instant Messenger (AIM), видаючи себе за співробітників AOL, які перевіряють паролі користувачів. Після того як AOL в 1997 році ввела контрзаходи, кіберзлочинці зрозуміли, що можуть використовувати цю методику в інших галузях, зокрема й фінансових установах. З того часу методики фішингу дедалі більше розповсюджуються серед кіберзлочинців, тому безперервно здійснюються фішингові атаки як на окремі особи, так і на організації для отримання інформації та фінансової вигоди. Як свідчить статистика за 2024 рік [3] фішинг зріс на 25 % у порівнянні з попереднім роком. У 2024 році глобальні фінансові збитки від фішингових атак оцінили в $17,4 млрд, що на 45 % більше, ніж у попередньому році. В той же час 97 % користувачів не можуть розпізнати складний фішинговий електронний лист; 95 % усіх атак, спрямованих на корпоративні мережі, спричинені успішним фішингом; 30 % фішингових листів відкривають користувачі, і 12 % цих цільових користувачів натискають шкідливе посилання або відкривають вкладення.

У світі одним з найпоширених видів фішиншу є поштовий (74 %). Саме його було використано хакерським угрупованням «Armageddon» під час його діяльності на території України [4]. Хід атаки цілеспрямованого фішингу на прикладі повідомлення електронною поштою виглядає наступним чином. Спочатку зловмисник проводить велику попередню роботу щодо пошуку інформації про майбутній об’єкт фішингу. Це може бути як адреса електронної пошти та імена підрядників або колег, так і захоплення об’єкта, нещодавні покупки тощо – будь-яка інформація, яку можна дізнатися із соціальних мереж та інших джерел та яка допоможе в тілі листа збити отримувача з пантелику і змусити повірити в його правдивість. Потім, використовуючи отримані з доступних джерел дані, атакуючий створює фішинговий лист від імені знайомої для жертви особи (колеги, члена сім’ї, друга, замовника тощо). Надіслане повідомлення має створити відчуття терміновості і переконати одержувача надіслати особисту інформацію у відповіді, ввести її, перейшовши за посиланням у листі, або скачати шкідливе програмне забезпечення з вкладень до листа. У деяких випадках, в ідеальному для зловмисника сценарії, після того як лист «спрацював», на цільовому ПК встановлюється бекдор, що дає змогу отримати доступ до необхідної інформації. Вона збирається, шифрується та надсилається особі, що здійснила атаку.

Отже єдиним джерелом інформації для аналізу та встановлення факту фішинга є отриманий електронний лист, тобто адреса електронної пошти відправника та вміст повідомлення, яке включає лінк на ресурс, за допомогою якого здійснюється збір конфіденційної інформації.

Тому аналіз електронного листа для визначення того, чи є цей лист фішинговим, пропонується здійснювати в такий послідовності: 1) аналіз його вмісту, 2) аналіз заголовків електронного листа, 3) аналіз та пошук інформації за електронною адресою відправника, 4) аналіз посилання на ресурс. Розглянемо детально ці етапи.

1. Аналіз вмісту повідомлення. Відомо, що поштові фішингові листи містять термінову

інформацію, щоб своєю терміновістю викликати необдуману, але певну дію від жертви, наприклад натиснути на зловмисне посилання, яке веде на підроблену сторінку авторизації або завантажує шкідливе програмне забезпечення. Тому на основі аналізу доступних фішингових листів визначено ознаки, за якими можна розпізнати фішингові повідомлення. До них віднесено:

загальні або неофіційні привітання. Листи без персоналізації та формальностей, мають викликати підозри (наприклад, «Шановний клієнт»);

запит на особисту інформацію часто використовують кіберзлочинці, але банки, фінансові установи та більшість онлайн-сервісів намагаються цього уникати;

некоректна граматика. Орфографічні або друкарські помилки, а також незвичайні фрази часто можуть означати небезпеку, але брак помилок не є доказом легітимності;

несподівані повідомлення або будь-який незапланований контакт з банком має викликати підозри;

терміновість. За допомогою фішингових повідомлень часто намагаються викликати відчуття терміновості дій, залишаючи жертвам менше часу на роздуми;

пропозиція, від якої складно відмовитися.

Приклад фішингового повідомлення з відповідними ознаками наведено на рис. 1.

2. Аналіз заголовків електронного листа. Для виключення можливості, що адреса електронної пошти відправника адреса була підроблена треба переглянути заголовок електронного листа, тому що саме там містяться ознаки підробки адреси. Заголовок складається з серії рядків [8]. Кожне поле заголовка складається з одного рядка тексту ASCII із зазначенням назви поля, двокрапки та значення. Основні поля заголовків, пов'язані з транспортуванням повідомлень: To: (вказує адресу DNS основного одержувача); Cc: (визначає адресу вторинного одержувача); BCC: (визначає адресу копії третій стороні, про яку не знають основний та додатковий одержувач) ; From: (вказує ім'я особи, яка написала повідомлення); Sender :: (вказує адресу електронної пошти особи, яка надіслала повідомлення); Received: (стосується ідентифікації відправника, даних, а також часу отримання повідомлення. Також містить інформацію, яка використовується для пошуку помилок у системі маршрутизації); Return-Path: (цю інформацію додає агент передачі повідомлень. Ця частина використовується для вказівки способу повернення до відправника); Date: (дата і час відправлення повідомлення); Reply-To: (адреса електронної пошти, на яку слід надсилати відповіді); Message-Id: (посилається на унікальний номер для посилання на це повідомлення пізніше); In-Reply-To: (Message-Id повідомлення, на яке лист є відповіддю); References: (містить інші відповідні ідентифікатори повідомлень).

В залежності від операційної системи та поштового клієнту для відображення заголовків можуть використовуватися різні команди. Так в Gmail в акаунті Google це команда «Показати

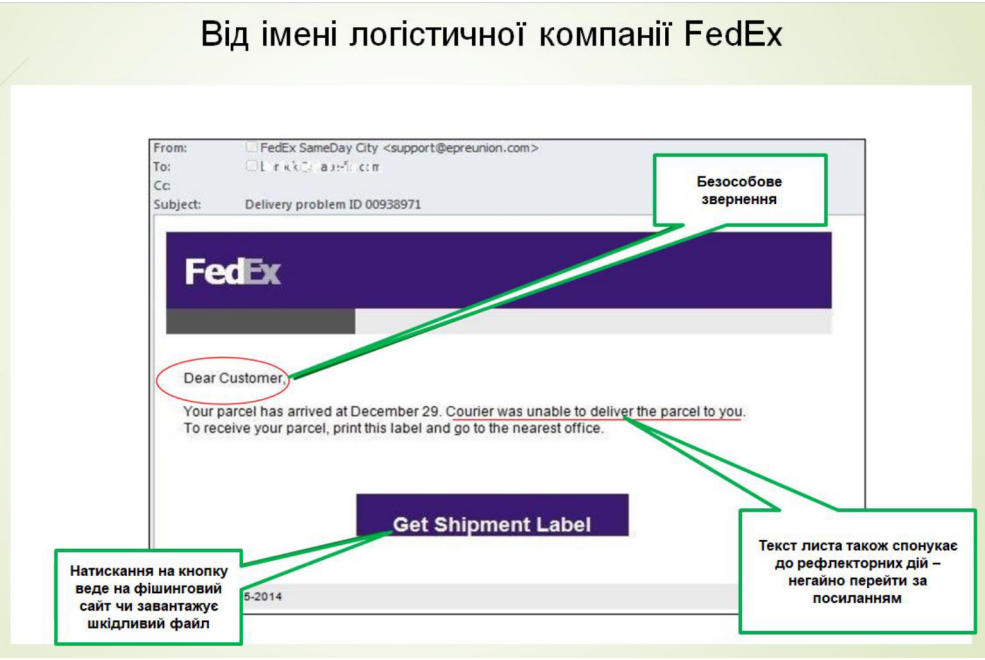

Рис. 1. Приклад фішингового листа

оригінал». В інших поштових службах це можуть бути команди такі як «Переглянути джерело повідомлення», або «Всі заголовки», або «Заголовки Інтернету» тощо. В [9] можна знайти інструкції щодо отримання даних заголовка з різних поштових клієнтів. Для зручності аналізу заголовків доцільно використовувати аналізатор – онлайн додаток, що на основі обробки заголовків з електронної пошти здійснює аналіз серверів, через які виконувалося надсилання листа. Збирається можлива інформація за цими серверами: IP адреса, географічне розташування, коли і на ім'я якого зареєстрований сервер, інколи номер телефону і поштова адреса власника сервера, тощо. Прикладами аналізаторів є Mxtoolbox,, Headers.aspx.

Під час аналізу заголовків треба звертати увагу на наступні аспекти:

• Received From: вказується ім'я хоста сервера-відправника, та якщо воно не збігається з заявленою адресою відправника, що це може бути ознакою нелегітимності;

• Return-Path: показує адресу, на яку буде повернений лист в разі невдалої доставки. Деякі підроблені електронні листи будуть містити підроблено поле «From» але не це поле, тому якщо у полі «Return-Path» та «From» містяться різні адреси, то це є ознакою підробки адреси відправника;

• X-Originating IP: Це поле може містити вихідну IP-адресу для поштового сервера відправника. Для отримання більш детальної інформації цій адресі для подальшого аналізу можна використовувати інструменти OSINT, наприклад набір інструментів IntelTechniques.

• Received-SPF: розшифровується як Sender Policy Framework чи інфраструктура політики відправника – це запис, який забезпечує взаєморозуміння між поштовими серверами відправника та одержувача. Він містить інформацію про те, з яких IP-адрес може надсилатися пошта від вказаного домену. За його допомогою можна знизити загальну кількість спаму, зменшити ймовірність того, що домен буде скомпрометований та захиститися від спаму. Тому якщо в цьому заголовку у отриманому листі вказано «pass», значить домен, використаний для відправки пошти, автентифіковано та можна буди впевненим у легітимності відправника електронного листа;

• DKIM (DomainKeys Identified Mail) – другий ступінь захисту під час передачі даних між поштовими серверами. Це механізм, який працює через ключі шифрування. Для того, щоб його активувати, створюються два ключі шифрування: приватний та публічний. Два ключі працюють у зв'язці. Коли сервер отримувача бачить лист, він запитує публічний ключ відправника. З його допомогою він розшифровує прихований підпис, який підтверджує авторство відправника. Отже, це спосіб авторизації, який не можна ігнорувати, тому якщо в цьому заголовку є «pass» то ймовірність що відправник не був підроблений – збільшується;

DMARC (Domain-based Message Authentication, Reportingand Conformance) – третій етап захисту. Це технологія, яка визначає, що робити з повідомленнями відправника, якщо вони не пройшли аутентифікацію за допомогою SPF та DKIM. Це правила, які встановлює відправник для листів, надісланих від його імені. Так відправник захищає своїх одержувачів від зловживань його репутацією, використання його домену шахраями. Тобто сам факт існування таких правил є ознакою легітимності відправника електронного листа. Тому треба звертати увагу на існування в цьому заголовку є «pass» в цьому заголовку.

3. Наступний етап аналізу отриманого електронного листа – це дослідження електронної адреси. Обов'язково треба звернути увагу на домен, з якого надіслано лист. Зрозуміло, що викликає підозру той факт, що, наприклад, американський чи німецький банк надсилатиме електронний лист з китайського домену. Обовязково треба перевірити, що адреса, з якої надіслано лист, дійсно існує. Для цього можна застосувати інструмент Hunter.io. У разі позитивного результату треба переглянути історію використання електронної пошти за допомогою відповідних інструментів, наприклад Emailrep.io. Це система сервісів, сканерів і служб накопичення, які збирають дані про адреси електронної пошти, домени та Інтернет-користувачів на основі даних з профілів соціальних мереж, професійних мережевих сайтів, витоків облікових даних даркнета, інших витоків даних, фішингових наборів, фішингових електронних листів, списків спаму, відкритих поштових ретрансляторів, віку та репутації домену, інформації про ризиковані адреси електронної пошти, тощо. Тому інформація, яку можна отримати з використанням цього сервісу може бути корисною для розуміння цілей відправника на основі аналізу попередніх дій, що відбувалися з використанням відповідної електронної адреси та свідчити про те, що лист – фішинговий.

Для більш глибокого аналізу адреси електронної пошти відправника у разі необхідності можна використовувати технології OSINT, розро-

блені, наприклад, Майклом Базелем, який працював 18 років як державний експерт розслідування комп'ютерних злочинів у робочої групи ФБР з кіберзлочинів. Його книги з відповідної тематики користуються популярністю у Сполучених Штатах, в Європі та використовуються державними установами як навчальні посібники зі збору розвідувальних даних та захисту особистої інформації. Так, у [10] можна знайти детальні рекомендації М. Базела щодо здійснення дослідження за технологіями OSINT за відомою електронною адресою для деанонімізації відправника. Саме їх можна використовувати у разі необхідності для встановлення реального відправника.

Також є можливість формулювання запиту до постачальника електронної пошти, якщо є юридичне обґрунтування. Відповідні запити формулюються згідно з діючим законодавством. Слід зазначити, що порядок доступу до таких даних регулюється законодавством тієї країни, де вони перебувають фізично. Так, наприклад, під час проведення кримінального провадження треба враховувати підстави та умови надання правової допомоги та процедуру написання запитів, яка детально розглянута в [11].

4. Аналіз посилання на ресурс, на який пропонується перейти у надісланому поштовому листі. Треба контролювати адреси сайтів та сторінок, на яких треба перейти та ввести будь-які дані, а саме знайти точну адесу відповідного сайту та порівняти з посиланням, яке було надіслано в листі. Різниця лише в одну літеру в адресі відповідного сайту вже є ознакою фішингу.

Висновки. Розроблено практичні рекомендації щодо аналізу отриманого електронного листа для виявлення ознак фішингу, в результаті ігнорування якого здійснюється запобігання продовженню кібератаки, першим кроком якої є фішинг. Що дозволяє, відповідно, уникнути витоку важливої інформації, тому що метою кібератак є доступ зловмисників до конфіденційної інформації. Перспективою подальших досліджень є більш глибоке дослідження кожного виду фішингу та розроблення методики протидії та деанонімізації зловмисників.

Список літератури:

1. Cyber Digest. *Огляд подій в сфері кібербезпеки*. НКЦК. Липень 2023. URL: https://surl.li/qlmafy (дата звернення: 12.02.2025).

2. Стартував проєкт із протидії кібершахрайству у фінансовому секторі. *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/6103.html (дата звернення: 12.02.2025).

3. 2024. Phishing statistics and trends: What you need to know URL: https://nordvpn.com/pl/blog/phishing-statistics/ (дата звернення: 19.03.2025).

4. Хакерське угруповання Armageddon/Gamaredon. Технічна сторона кібератак ФСБ РФ проти України. ДКІБ СБУ. Київ, 2021. URL: https://ssu.gov.ua/uploads/files/DKIB/Технічний звіт діяльності Армагедон.pdf (дата звернення: 12.02.2025).

5. What is Phishing? Types of Phishing Attacks. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ (дата звернення: 12.02.2025).

6. The anatomy of a phish. URL: https://iwebtechnology.net/the-anatomy-of-a-phish/ (дата звернення: 12.02.2025).

7. How to prevent phishing attacks URL: https://nordvpn.com/pl/blog/how-to-prevent-phishing/ (дата звернення: 12.02.2025).

8. E-mail-format. URL: https://www.geeksforgeeks.org/e-mail-format/ (дата звернення: 12.02.2025).

9. How to Get Email Headers. URL: https://mxtoolbox.com/Public/Content/EmailHeaders/ (дата звернення: 12.02.2025).

10. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. *Paperback*. 2022. By Michael Bazzell. 480 p.

11. Методичні рекомендації щодо виконання вимог міжнародних договорів та КПК України про міжнародну правову допомогу при проведенні процесуальних дій – К. : Генеральна прокуратура України; Національна академія прокуратури України, 2017. – 60 с.

Boiko O. V., Zalevsky S. V., Savchuk V. S. ANALYSIS OF AN EMAIL FOR SIGNS OF PHISHING

Practical recommendations have been developed for analyzing a received email to identify signs of phishing, as a result of which ignoring it prevents the continuation of a cyberattack, the first step of which is phishing. Since the beginning of Russian military aggression, the number of threats in Ukraine's cyberspace has been constantly increasing, cybercriminals have significantly intensified their activities during the period of martial law in Ukraine and are conducting phishing campaigns in order to obtain confidential data from the population of Ukraine, with 74 percent of phishing attacks falling on email phishing. It should be noted that phishing emails can be sent allegedly on behalf of state bodies, international organizations and individuals,

and decoy documents can be requests for information, international correspondence, official correspondence letters of state bodies of Ukraine, etc. Therefore, it is important for users who may be the objects of future cyberattacks to be able to recognize phishing based on the analysis of a received email in order to ignore such emails and stop the cyberattack. Therefore, it is necessary to develop practical recommendations for analyzing an email, the application of which will allow users to detect signs of phishing in the received email and, accordingly, prevent the continuation of a cyberattack, the first step of which is phishing, and avoid information leakage, because the goal of cyberattacks is for attackers to access confidential information. The only source of information for analyzing and establishing the fact of phishing is the received email, i. e. the sender's email address and the content of the message, which includes a link to a resource through which confidential information is collected. Therefore, analyzing an email to determine whether this email is phishing is proposed to be carried out in the following sequence: 1) analyzing its content, 2) analyzing the email headers, 3) analyzing and searching for information by the sender's email address, 4) analyzing the link to the resource.

Key words: *phishing, cyberattack, email, email, osint.*