ARTICLE

DOI 10.36074/grail-of-science.14.11.2025.103

СУЧАСНІ МЕТОДИ ФІШИНГУ ТА СПОСОБИ ПРОТИДІЇ

НАУКОВО-ДОСЛІДНА ГРУПА:

Радзівілов Григорій Данилович
Кандидат технічних наук, професор
Заступник начальника інституту з наукової роботи
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Артющик Андрій Борисович
науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Сайко Володимир Григорович
доктор технічних наук, професор,
професор кафедри комунікаційних систем та мереж
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Комаров Володимир Олександрович
Заслужений винахідник України
провідний науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Скляров Олексій Вікторович
провідний науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Медведь Юрій Григорович
начальник науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Радченко Микола Миколайович
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Тітаренко Андрій Володимирович
науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Бондаренко Олег Євгенійович
начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Гетьман Алевтина Вячеславівна
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

Анотація. *В роботі розглянуто сучасні методи фішингу, тенденції їх розвитку та ефективні способи протидії. Проаналізовано динаміку зростання фішингових атак у світі, зокрема еволюцію від масових електронних листів до цільового фішингу, смішингу, вішингу та використання штучного інтелекту для створення діпфейків. Висвітлено приклади реальних інцидентів, зокрема компрометацію екосистеми prt, що продемонструвала високі ризики для ланцюгів постачання програмного забезпечення. Акцентовано увагу на соціально-інженерних аспектах атак та зростанні ролі психологічного впливу на користувачів. Запропоновано комплексний підхід до протидії фішингу, який поєднує технічні, організаційні та освітні заходи. Особливу увагу приділено впровадженню механізму Trusted Sender Verification System (TSVS) — системи верифікації довірених відправників, що забезпечує багаторівневу автентифікацію електронної пошти та підвищує довіру до комунікацій. Зазначено, що поєднання криптографічних перевірок з моделлю соціальної довіри може суттєво знизити ефективність фішингових атак. Отримані результати мають практичне значення для підвищення кіберстійкості державних і корпоративних структур України.*
Ключові слова: *фішинг, кібербезпека, кіберзлочин, шахрайство, система верифікації*

За даними звіту IBM X-Force Threat Intelligence Index 2024, 41% випадків проникнення в корпоративні мережі почались саме з фішингової атаки [1]. Щорічний звіт Proofpoint також зазначає, що 75% організацій у світі стикалися хоча б з однією спробою фішингу. У глобальному масштабі фішинг вже кілька років поспіль є найпоширенішим видом кіберзлочину: лише у США в 2022 році зафіксовано понад 300 тисяч скарг на фішинг (електронний, SMS та телефонний) – більше, ніж по будь-якій іншій категорії інцидентів. Кількість атак стабільно зростає: якщо у 2019 році реєструвалось ~780 тис. фішингових інцидентів, то у 2022-му їх було вже 4,74 млн (майже у 6 разів більше), а 2023-й встановив новий піковий показник ~4,99 млн випадків [2]. Отже, проблема не зникає, а навпаки – масштаби та витонченість фішингових схем постійно збільшуються, зокрема завдяки появі нових технологій та витончених технік соціальної інженерії.

Фішинг – це різновид цифрового шахрайства, відомий уже кілька десятиліть, який і сьогодні залишається однією з найнебезпечніших кіберзагроз як для звичайних користувачів, так і для бізнесу.

Найбільш традиційний варіант фішингу здійснюється через електронну пошту. Близько 96% фішингових атак надходять саме електронними листами. Зловмисники розсилають масові повідомлення, що імітують відомі організації (банки, поштові служби, соцмережі тощо), зі шкідливими посиланнями або вкладеннями. Обсяги таких атак величезні – за оцінками, щодня глобально відправляється понад 3,4 млрд фішингових електронних листів (понад трильйон на рік.

Сучасні шаблони електронних листів для фішингу добре оформлені, не містять явних орфографічних помилок, та часто персоналізовані. Зловмисники активно використовують витоки даних та відкриті джерела, аби включати у повідомлення реальні імена, посадові дані чи іншу особисту інформацію, підвищуючи шанси на успіх атаки. Популярною приманкою є відомі бренди: понад 55% фішингових імейлів у світі згадують у контенті ім'я якого-небудь відомого бренду, щоб викликати довіру. Масові email-кампанії фішингу, незважаючи на невелику конверсію, залишаються вигідними за рахунок величезного охоплення – достатньо, щоб жертвою стала не велика частина отримувачів, щоб зусилля окупились.

Цільовий (прицільний) фішинг є більш небезпечною еволюцією класичного фішингу. Атаки націлені на конкретну особу або групу осіб (наприклад, співробітника певної компанії), з використанням інформації про них для підвищення правдоподібності шахрайства [3]. Особливо небезпечним різновидом є так званий whaling – «полювання на китів», коли мішенню фішингу стають особи найвищого рівня (директори, керівники підрозділів) або інші «VIP-мішені». Наприклад, шахрай може видати себе за генерального директора компанії і надіслати правдоподібний лист фінансовому директору з вимогою термінового переказу коштів. Відповідно до сучасних трендів, прицільний фішинг усе частіше доповнюється такими засобами як deepfake-відозаписи чи аудіо – про них докладніше далі.

Показовим є інцидент що стався 8 вересня 2025 року з одним з підтримувачів (maintainer) JavaScript під псевдонімом Qix- (справжнє ім'я – Josh Junon). Він отримав лист, замаскований під повідомлення служби підтримки npm. Лист нібито вимагав оновлення налаштувань двофакторної автентифікації (2FA) – і містив посилання, що вели на домен, який використовувався зловмисниками.

З отриманим доступом атакувальники в короткий час (протягом кількох годин) опублікували шкідливі версії принаймні 18 пакетів, серед яких debug, chalk, ansi-styles та інші дуже популярні пакети, що разом мають мільярди завантажень на тиждень. Шкідливий код був орієнтований на крадіжку криптовалюти: він перехоплював виклики в браузері, змінював адреси отримувачів у транзакціях, підмінював цільові адреси на ті, що контролював зловмисник, тощо. Атака також мала властивості самопоширення (worm-like behavior): код шукав токени, доступи, облікові дані на системах жертв, міг автоматично інфікувати інші пакети, якими володіє скомпрометований підтримувач або інші облікові записи.

Josh Junon повідомив, що його обліковий запис було відновлено приблизно за 8 годин після компрометації.

Хоча потенціал атаки був величезний, фактичні збитки (особливо фінансові через криптовалюту) виявилися відносно невеликими — відторгнення шкідливих версій відбулося за лічені години, а крадіжка виявилась мінімальною в порівнянні з потенційними масштабами [4].

З ростом популярності мобільних месенджерів і SMS, зловмисники активно освоїли і ці канали - через текстові повідомлення (SMS або месенджери типу WhatsApp, Telegram, Viber) (рис. 1). Приклад фішингового повідомлення показано на рис. 1.

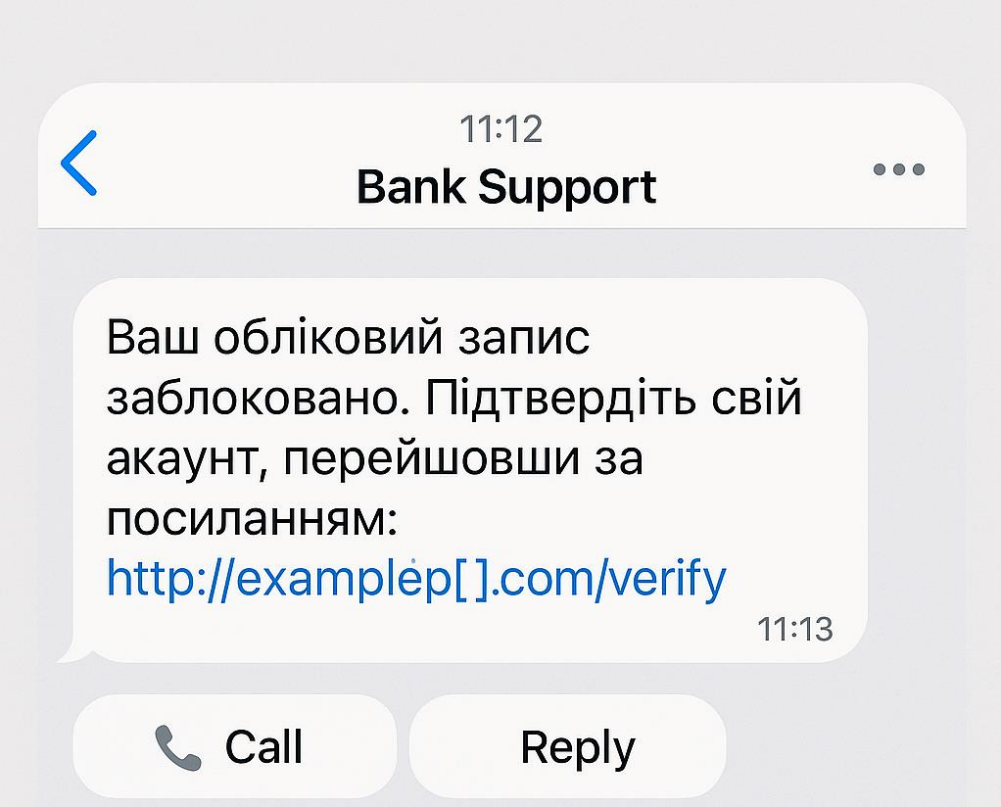

Рис. 1. Приклад фішингового повідомлення

Атакувальники розсилають повідомлення, що видають себе за банки, поштові служби, держоргани чи популярні сервіси, спонукаючи жертву перейти за посиланням або передати конфіденційні дані. За останні роки частка фішингу, що здійснюється через SMS, суттєво зросла – у 2023 році понад 28% усіх фішингових атак у світі виконувалися саме шляхом текстових повідомлень. Для порівняння, ще кілька років тому цей показник був у межах кількох відсотків. Лише за один квартал (Q3 2024) обсяг атак зріс на 22% [2]. Експерти відзначають, що з підвищенням кількості легітимних сервісних розсилок (наприклад, повідомлень від служб доставки або авторизаційних SMS від сайтів) користувачі стали більш довірливо ставитися до текстових повідомлень, і шахраї використовують це на свою користь [5].

Атаки часто виглядають переконливо: зловмисники можуть підробити поле відправника (замаскувавши номер під назву установи), включити особисті дані (ім'я користувача, інформацію про нещодавнє замовлення тощо) або надати в повідомленні "дружні" інструкції (на кшталт "Якщо це не ви намагалися

увійти в акаунт, зателефонуйте в службу безпеки за номером…" – при дзвінку жертву чекатиме фальшивий оператор).

Небезпечними також є комбіновані соціально-інженерні атаки, що здійснюються з задіянням телефонних дзвінків. Класичні сценарії атак існують вже давно: дзвінок від псевдо-співробітника банку, який "помітив підозрілу активність" і просить підтвердити дані; або дзвінок начебто від податкової/поліції з погрозою штрафів чи арешту, якщо негайно не сплатити певну суму. Шахраї можуть також представлятися техпідтримкою відомих компаній (Microsoft, провайдера інтернету тощо), заявляючи про "віруси на комп'ютері жертви" і пропонуючи допомогу, що насправді зводиться до встановлення шкідливого ПЗ. Емоційний тиск і авторитетність тону – ключові елементи такої атаки. Ілюстрація зазначеного вище показана на рис. 2.

Рис. 2. Ілюстрація атаки зловмисників на сайти користувачів

До традиційних телефонних схем останніми роками додалася нова небезпечна можливість – використання штучного інтелекту для підробки голосу. Якщо раніше жертва могла насторожитися, почувши в слухавці незнайомий акцент чи неточності, то тепер шахраї здатні синтезувати голос, практично ідентичний реальній людині. За допомогою технології deepfake audio злочинці отримують аудіозапис голосу керівника компанії або родича жертви (наприклад, зі сторінок в соцмережах чи з відео) і на його основі генерують нові фрази. У одному з резонансних випадків співробітник фінансової фірми в Гонконзі переказав шахраям $25 млн, почувши по телефону голос, що був майстерно замаскований під голос його директора. Інший приклад – злочинне угруповання у США, яке за допомогою AI-клонування голосів телефонувало літнім людям, удаючи з себе їхніх онуків, що «потрапили в біду», і виманювало гроші (цією схемою було завдано понад $5 млн збитків). Такі факти підтверджують: тепер навіть голос більше не гарантує достовірності співрозмовника.

Статистика відзначає стрімке зростання шахрайств із застосуванням діпфейків: за даними Всесвітнього економічного форуму, кількість інцидентів із deepfake-шахрайством зросла на 1740% з 2022 по 2023 роки [3].

Протистояння фішинговим та соціоінженерним загрозам вимагає комплексного підходу. Необхідно поєднувати технологічні рішення з підвищенням обізнаності користувачів, особливо в організаціях. Нижче перелічено ключові стратегії захисту і рекомендації:

- Регулярне навчання та перевірка співробітників. У цьому напрямку необхідно проводити для персоналу тренінги з кібергігієни та соціальної інженерії на постійній основі та ознайомлювати з новими видами атак (наприклад, демонструвати приклади реальних фішингових листів, смішинг-повідомлень, deepfake-відео). Надзвичайно ефективним є проведення фішинг-симуляцій – коли IT-відділ або запрошені фахівці час від часу імітують фішингові атаки на працівників з навчальною метою. Такі заходи дозволяють виявити слабкі місця і натренувати навички розпізнавання загроз:
- Політика верифікації критичних запитів. У цьому напрямку необхідно на рівні організацій запровадити чіткі процедури підтвердження будь-яких фінансових транзакцій або конфіденційних дій, ініційованих через електронні канали. Наприклад, правило “двох каналів”: якщо запит надійшов по email чи месенджеру, обов’язково підтвердити його достовірність іншим шляхом (телефоном керівнику за відомим номером, особисто тощо) перед виконанням. Співробітників слід навчити не боятися перевіряти навіть прохання від керівників – у компанії має бути культура, де додаткова перевірка сприймається позитивно. Багато атак могли бути зупинені, якби існував обов’язок підтверджувати фінансові розпорядження голосом або через відеозв’язок.
- Захищена багатофакторна автентифікація. У цьому напрямку необхідно використовувати 2FA/MFA для входу – це базовий механізм стримування фішингових атак, адже навіть якщо пароль викрадуть, без додаткового фактора зловмисник не отримає доступ. Важливо, щоб другий фактор був стійким до підробки: бажано застосовувати апаратні ключі безпеки (FIDO2, YubiKey) або щонайменше одноразові код-генератори, прив’язані до пристрою. Схема захищеної багатофакторної автентифікації показана на рис. 3.

Рис. 3. Захищена багатофакторна автентифікація

Якщо ж використовуються push-сповіщення в додаток (типова MFA), слід налаштувати обмеження на кількість повторних запитів і навчити користувачів ніколи не підтверджувати запити, яких вони не очікували. Для критичних систем варто впровадити політику Zero Trust щодо автентифікації: навіть з паролем і 2FA дії користувача можуть вимагати додаткових підтверджень, якщо виглядають підозріло.

- Технічні засоби проти фішингу. IT-відділи повинні розгортати сучасні рішення для фільтрації та моніторингу трафіку, що здатні автоматично блокувати відомі фішингові повідомлення. Важливо налаштувати і підтримувати протоколи автентифікації пошти – SPF, DKIM, DMARC – щоб ускладнити зловмисникам підробку доменів компанії при фішингових розсилках. Також перспективним є використання AI-алгоритмів на боці захисту – деякі сучасні системи аналізують стиль листів і поведінкові фактори, щоби помітити "нетипові" листи (наприклад, якщо з аккаунту директора раптом розсилаються запити всім підлеглим з незвичним текстом, система може заблокувати таку розсилку).

- Створення культури кібербезпеки. Технічні засоби ефективні, але недостатні, якщо персонал не включений у процес захисту. Потрібно формувати на підприємствах культуру, де кожен працівник усвідомлює ризики і відчуває особисту відповідальність. Корисно впровадити прості правила-нагадування: перед тим як клацнути посилання або відкрити вкладення – задумайся, чи очікував ти цей лист, чи перевірив ти адресу відправника; якщо виникає хоч найменша підозра – негайно повідом IT-відділ. Працівники мають знати, до кого звернутися в разі підозри на фішинг (окремий inbox для повідомлень про phishing, або чат з безпекою). Важливо заохочувати такі повідомлення, не карати за помилкову тривогу – навпаки, хвалити пильність. Регулярно оновлювати політики безпеки та доводити їх до колективу (наприклад, політика щодо заборони використовувати особисті пошти для робочої переписки, чи щодо порядку дій у разі отримання підозрілого листа).

- Освітні програми для користувачів. У цьому напрямку на рівні державних органів та спільнот доцільно проводити масштабні освітні кампанії для населення щодо базових принципів кібергігієни. Особливо це стосується країн, де діджиталізація відбувається швидкими темпами (наприклад Україна). Роз'яснювати широкому загалу про типові ознаки фішингу, про популярні схеми шахраїв (телефонні дзвінки про "родича в біді", фейкові SMS від банку, інтернет-розіграші, криптовалютні афери тощо) – через соціальну рекламу, сюжети на телебаченні, інформаційні брошури у банках та відділеннях пошти. Включати основи кібербезпеки в шкільну та вузівську програму, аби з молоді люди вміли критично мислити в цифровому середовищі. Проводити спеціальні тренінги для уразливих груп населення – пенсіонерів (щоб не довіряли кожному дзвінку від "служби безпеки банку"), нових інтернет-користувачів тощо.

Одним із ключових векторів фішингових атак залишається маскування відправника під легітимне джерело. Незважаючи на наявність сучасних механізмів перевірки достовірності електронної пошти (SPF, DKIM, DMARC), зловмисники продовжують ефективно використовувати схожі доменні імена, підроблені поля Display Name, або компрометовані акаунти для створення ілюзії

автентичності. Така схема фішингових атак зловмисників за допомогою електронних комп'ютерних пристроїв показана на рис. 4.

Рис. 4. Ілюстрація фішингових атак зловмисників

Цей факт вказує, що технічної перевірки доменів недостатньо — необхідна рівень персональної або організаційної довіри, подібний до концепції "білого списку" верифікованих контактів.

Для усунення зазначених вище недоліків пропонується модель Trusted Sender Verification System (TSVS) – система верифікації довірених відправників, що поєднує криптографічну перевірку (SPF/DKIM/S-MIME/PGP) з динамічною книгою контактів довіри. Її суть полягає у тому, що електронні повідомлення від невідомих або непідтверджених джерел маркуються як неперевірені, тоді як листи від контактів, які пройшли двосторонню або доменну автентифікацію, отримують статус "перевіреного відправника". Таким чином, користувач або організаційна система безпеки отримує додатковий шар контекстної фільтрації, який відокремлює потенційно шкідливі комунікації.

Система TSVS функціонує на двох рівнях:

1. Технічна автентифікація повідомлення. На цьому етапі здійснюється перевірка:

– коректності SPF та DKIM підписів,
– відповідності домену політиці DMARC (alignment check),
– наявності дійсного криптографічного підпису S/MIME або PGP,
– підтримки TLS/MTA-STS або DANE для захисту каналу передачі.

Якщо перевірки проходять успішно, повідомлення отримує базовий рівень довіри – "verified domain".

2. Соціальна/організаційна верифікація контакту. На цьому рівні формується "книга довірених відправників" (Trusted Address Book), у яку заносяться:

– адреси, з якими відбувався взаємний обмін підписаними повідомленнями (аналог принципу Trust On First Use),

– адреси, що входять до корпоративного каталогу (Active Directory, Google Directory тощо),

– адреси, підтверджені вручну користувачем або адміністратором.

Листи від адрес, відсутніх у книзі довіри, позначаються як “невідоме джерело” з відповідним візуальним попередженням у клієнті пошти.

Функціонування TSVS можна порівняти з механізмом взаємної верифікації контактів у месенджері Signal. У Signal користувач бачить повідомлення від нового співрозмовника лише після того, як відбулося взаємне підтвердження контактів (наявність номера один одного у списку контактів або ручна згода на початок спілкування).

Аналогічний підхід у TSVS передбачає, що автоматичне позначення як “достовірного” можливе лише за умови взаємної довіри — наприклад, якщо обидві сторони обмінялися підписаними листами або пройшли перевірку за іншим каналом (дзвінок, кодова фраза, захищений чат). Схема функціонування TSVS показана на рис. 5.

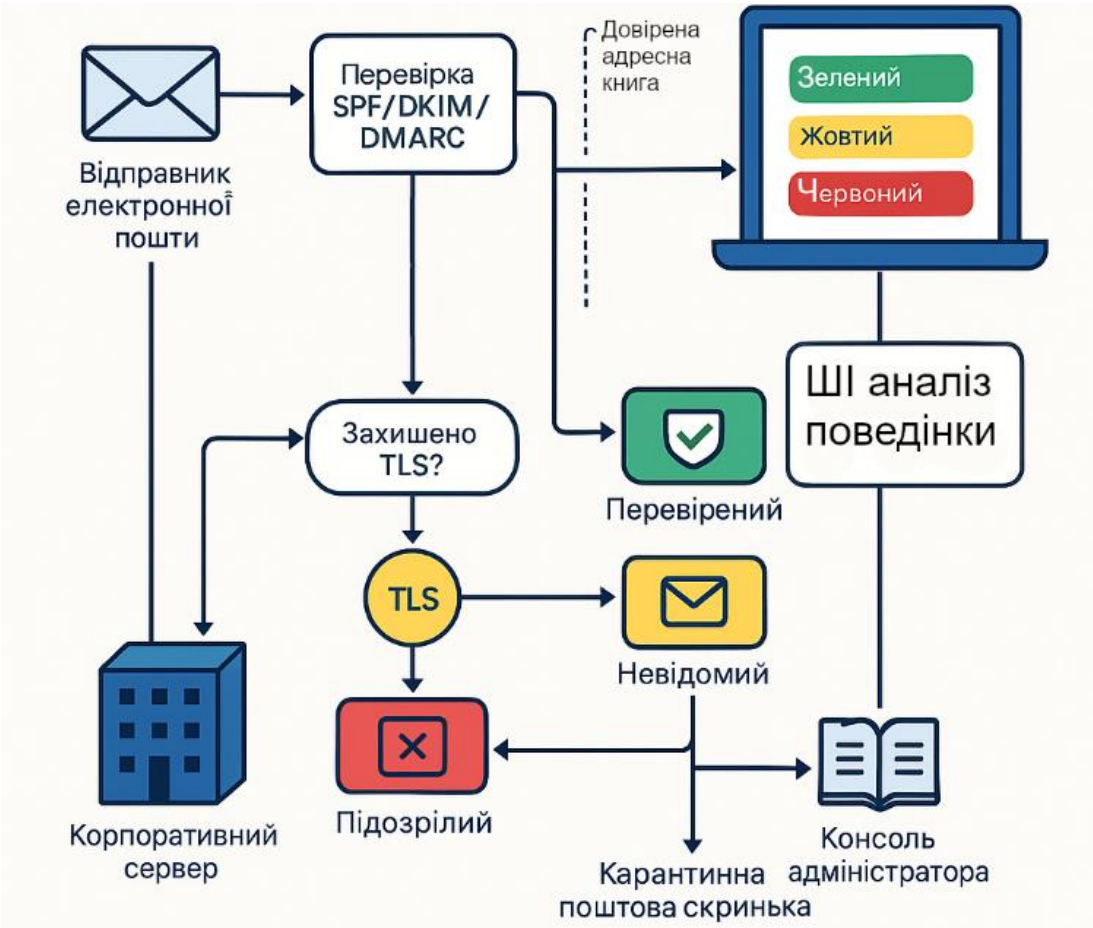

Рис. 5. Схема функціонування TSVS

Така взаємна модель значно знижує ефективність фішингових кампаній, оскільки навіть у разі успішного маскування домену або відправника лист не потрапляє у “довірений простір” користувача.

Для практичного застосування TSVS пропонується триступенева система маркування повідомлень у клієнті:

Рівень	Статус	Умови автентифікації
Перевірений	Відомий контакт, пройдено DKIM/DMARC + взаємна історія або підпис S/MIME	Зелене маркування, дозволений активний контент
Невідомий	Новий відправник або без криптопідпису	Попередження “Невідомий відправник”, обмеження кліків
Підозрілий	DKIM/DMARC fail, look-alike домен, різниця між From і Reply-To	Червоний банер, автоматичний карантин листа

Сповіщення клієнтів - двигун продажів багатьох бізнесів. Швидко повідомити сотні людей про знижки, розпродажі, статус замовлення або доставки просто необхідно, щоб забезпечити високий рівень сервісу. Чим більше клієнтська база, тим складніше знайти універсальний спосіб інформування - одні вважають за краще смс, інші читають повідомлення в месенджерах, третім зручніше отримати лист по електронній пошті.

Автоматичні оповіщення відправляються в режимі реального часу або за заданим графіком. Це означає, що незалежно від кількості контактів в базі, всі передплатники отримають повідомлення практично одночасно. Сервіс автоматичних повідомлень дозволяє економити час співробітників - більше не потрібно відправляти особисті листи клієнтам, система сама відправить повідомлення по шаблону.

Сервіс миттєвих автоматичних повідомлень - це економія робочого часу співробітників і засобів компанії. Система дозволяє говорити з клієнтом замість продавця. Перевага повідомлень в тому, що клієнт може ознайомитися з повідомленням у зручний для нього час (під час перерви або після роботи). У той час як дзвінок від менеджера з продажу в робочий час може сприйматися як дратівливий чинник.

Впровадження системи автоматичних повідомлень дозволяє підвищити лояльність клієнтів. Інформування про статус замовлення або доставки, зміни робочого графіка, знижки, розпродажі дає можливість нагадати про себе і підтримувати зв'язок з клієнтом. Використовуйте систему оповіщень, щоб привітати клієнтів з днем народження або святом, пропонуючи особливі умови обслуговування.

Автоматичні оповіщення можна використовувати для отримання зворотного зв'язку про товари і послуги або відвідуванні закладу. Надішліть клієнту повідомлення з опитуванням, щоб дізнатися про його враження і поліпшити сервіс. Інтеграція чат-бота в Telegram дозволяє налаштувати відповіді на актуальні питання та консультувати клієнтів цілодобово, навіть коли офіс закритий.

Функціонал автоматичних повідомлень можна інтегрувати з програмою лояльності. Система автоматично проінформує клієнта про наявність балів або

бонусів, коли їх кількість досягне певного рівня. Можлива відправка повідомлень через задані проміжки часу (щомісяця, квартал або раз на рік).

Додатково інтегрована можливість регулювання кількості повідомлень. Клієнт сам вибирає, скільки повідомлень він хоче отримувати і як часто. Якщо послуга більш не актуальна, одержувач може відмовитися від розсилки - відповідний маркер з'явиться в картці клієнта в CRM.

Розсилка SMS повідомлень, що інтегрована в CRM-системи, дозволяє створити та налаштувати під потреби свого бізнесу автоматичну систему комунікації з постійними клієнтами та замовниками. При цьому для того, щоб ця система почала функціонувати, керівнику компанії або розробнику, який виконував створення CRM-системи, потрібно лише один раз налаштувати автоматичні сценарії та шаблони, після чого програмне забезпечення самостійно виконуватиме відправлення повідомлень певній групі клієнтів.

Цей механізм надає користувачу візуальні сигнали безпеки, аналогічні до “verified” позначок у месенджерах або соціальних мережах.

Перевагами методу є:

– зменшення ризику атак із підміною відправника (spoofing, look-alike domains).

– можливість інтеграції з існуючими протоколами автентифікації (SPF/DKIM/DMARC/S-MIME).

– проста для сприйняття користувачем модель “дружній/чужий лист”.

– підвищення ситуаційної обізнаності – користувач бачить рівень довіри до повідомлення.

Обмеженнями є:

– складність підтримки в середовищах з великою кількістю зовнішніх контактів.

– ризик компрометації “довіреного” акаунта – якщо справжній відправник зламаний, система позначить його як безпечного.

– необхідність централізованого керування політиками довіри та оновлення сертифікатів.

Ідея TSVS узгоджується з тенденцією розвитку протоколів Verified Mark Certificates (BIMI) та концепції Zero Trust Email Framework, але доповнює їх персональним рівнем довіри. Надалі можливе розширення механізму через використання:

– AI-моделей поведінкової автентифікації, які аналізують стиль листування і попереджають при нетиповому тексті,

– двоетапної верифікації контактів між організаціями (наприклад, підтвердження доменів через DNS challenge),

–інтероперабельності з месенджерами, де вже реалізовано механізм взаємної верифікації (Signal, Matrix, WhatsApp).

Висновки. Таким чином, система верифікації довірених відправників може стати одним з ключових елементів сучасної стратегії захисту від фішингу, забезпечуючи не лише технічну, а й соціально-контекстну перевірку достовірності повідомлень. Створення шаблонів повідомлень для кожного виду повідомлень дозволяє виключити помилки і людський фактор. Можливе створення необмеженої кількості шаблонів для кожного етапу воронки продажів - інформаційні, що залучають, продають повідомлення. Для

керівництва компанії доступна наскрізна аналітики по всьому розсилок і кожному каналу окремо.

Список використаних джерел:

[1] Фішинг трансформується: які головні загрози існують у 2025 році та як їм протидіяти. *DATAMI.* URL: https://datami.ee/ua/blog/how-phishing-is-changing-in-2025-analysis-by-datami/ (дата звернення: 06.10.2025)
[2] 99 Global Phishing Statistics & Industry Trends (2023–2025). *CONTROL D.* URL: https://controld.com/blog/phishing-statistics-industry-trends/ (дата звернення: 06.10.2025)
[3] Understanding Social Engineering Fraud: From Psychological Traps to AI-Driven Fraud. *feedzai.* URL: https://www.feedzai.com/blog/what-is-social-engineering-fraud/ (дата звернення: 06.10.2025)
[4] Атака на ланцюг постачання npm: компрометація Qix, заражені пакети та наслідки для веб3. *CyberSecureFox.* URL: https://cybersecurefox.com/uk/ataka-lantsiug-postachannia-npm-chalk-strip-ansi/ (дата звернення: 06.10.2025)
[5] Why the Twilio Breach Cuts So Deep. WIRED. URL: https://www.wired.com/story/twilio-breach-phishing-supply-chain-attacks/ (дата звернення: 06.10.2025)

MODERN PHISHING METHODS AND COUNTERMEASURES

SCIENTIFIC RESEARCH GROUP:
Grygoriy Radzivilov
Candidate of Technical Sciences, Professor
Deputy Head of the Institute for Scientific Work
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Andrii Artiushchyk
Researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Volodymyr Sayko
Doctor of Technical Sciences, Professor, Professor of the Department of Telecommunication Systems and Networks
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Volodymyr Komarov
Honored Inventor of Ukraine
Leading researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Oleksii Skliarov
Leading researcher of the research laboratory
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Yurii Medved
Head of scientific-researching laboratory
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Mykola Radchenko
Senior researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Andrii Titarenko
Researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine

Oleg Bondarenko
Head of research department
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
Alevtyna Hetman
Senior researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine

Summary. *This work examines modern phishing methods, current development trends, and effective countermeasures. The dynamics of phishing attack growth worldwide are analyzed, highlighting the evolution from mass email campaigns to targeted phishing, smishing, vishing, and AI-driven deepfake-based attacks. Real-world incidents are discussed, including the npm supply chain compromise, which demonstrated the high risks to software distribution ecosystems. Particular attention is given to the social-engineering dimension of phishing and the increasing role of psychological manipulation. A comprehensive approach to phishing mitigation is proposed, combining technical, organizational, and educational measures. The paper introduces the Trusted Sender Verification System (TSVS) — a trusted-sender verification model that integrates multi-level authentication and dynamic trust management in email communication. The proposed method combines cryptographic verification with social trust mechanisms to significantly reduce the effectiveness of spoofing and phishing campaigns. The research results have practical importance for enhancing cyber resilience in governmental and corporate structures of Ukraine.*
Keywords: *phishing, cybersecurity, cybercrime, fraud, verification system*

