КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.6980
УДК 004.49

Штонда Роман Михайлович
начальник науково-дослідного відділу
Військовий інститут телекомунікацій та
інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Черниш Юлія Олександрівна
старший науковий співробітник
Військовий інститут телекомунікацій та
інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

Терещенко Тетяна Павлівна
старший науковий співробітник
Військовий інститут телекомунікацій та
інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-9659-7897
tetiana.tereshchenko@viti.edu.ua

Терещенко Катерина Володимирівна
студентка
Національний авіаційний університет, Київ, Україна
ORCID ID: 0009-0008-8469-9854
katerina60411@gmail.com

Цикало Юрій Григорович
слухач
Національний університет оборони України, Київ, Україна
ORCID ID: 0009-0006-9698-3276
ab3366bk@ukr.net

Поліщук Сергій Анатолійович
слухач
Національний університет оборони України, Київ, Україна
ORCID ID: 0009-0006-9110-7576
0988528103@ukr.net

КЛАСИФІКАЦІЯ ТА МЕТОДИ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК

Анотація. Надійна робота мереж передачі даних, комп'ютерних систем та мобільних пристроїв є обов'язковою умовою для ефективного функціонування держави і суспільства, життєдіяльності окремого індивіда. Надійність роботи ключових інформаційних систем загального користування залежить від багатьох чинників: кібератак, збою апаратного та програмного забезпечення, різного роду помилок. Стрімке розширення загроз національній безпеці у XXI ст. покладає на органи держаної влади завдання щодо їх попередження, виявлення та нейтралізації. Кібербезпека все частіше розглядається як фундаментальна проблема держави, що комплексно зачіпає її безпеку, оборону, економіку, майже всі сфери суспільного життя. Інтернет дав потужний поштовх для розвитку масової комунікації, торгівлі та обміну інформацією. Разом з тим сьогодні він є тією сферою, де здійснюється чимало правопорушень. Знеособлений характер цифрової інфраструктури зробив крадіжку ідентичності природним і надзвичайно привабливим проєктом. Кіберзлочинці активно використовують різні засоби викрадення інформації, зокрема фішинг. На сучасному етапі і у подальшій перспективі розвиток як окремих суспільств і держав, так і загалом світу буде здійснюватися відповідно до концепції інформаційного суспільства, що пов'язано з

використанням інформаційних і телекомунікаційних технологій у придбанні, зберіганні та обробці інформації у повсякденному житті. Фішинг — це серйозна проблема безпеки в мережі, яка полягає в підробці справжніх веб-сайтів, щоб обдурити користувачів в Інтернеті і вкрасти їх конфіденційну інформацію. Проводячи аналіз даних визначень можна зробити висновок, що «фішинг» можна розглядати по різному, однак основна мета його проведення залишається незмінною — викрадення даних. Практична цінність результатів полягає у можливості використання отриманого класифікатору для подальшого створення програмних рішень для розпізнавання фішингових сайтів. Він, а також набір характеристик може бути впроваджений у антифішингові розширення для браузерів або інші інструменти боротьби з фішингом.

Ключові слова: кібербезпека; кібепростір; кібератаки фішинг; фішингові повідомлення.

ВСТУП

Глобальні технологічна та інформаційна революції, як і будь-які інші соціальні явища, окрім позитивного впливу на суспільний розвиток мають і зворотній бік — негативні наслідки, які породжують чимало проблем і небажаних явищ та процесів. Йдеться не лише про виникнення глобального цифрового розриву між розвиненими країнами та рештою світу, який носить інтегральний характер і включає в себе розриви в економіці, освіті, рівні життя, доходах і т. ін. Не менш негативний, руйнівний характер мають кіберзлочинність, кібертероризм та інші явища, що становлять безпосередню загрозу національній безпеці держави. Кібербезпека все частіше розглядається як фундаментальна проблема держави, що комплексно зачіпає її безпеку, оборону, економіку, майже всі сфери суспільного життя.

Надійна робота мереж передачі даних, комп'ютерних систем та мобільних пристроїв є обов'язковою умовою для ефективного функціонування держави і суспільства, життєдіяльності окремого індивіда. Надійність роботи ключових інформаційних систем загального користування залежить від багатьох чинників: кібератак, збою апаратного та програмного забезпечення, різного роду помилок. Стрімке розширення загроз національній безпеці у XXI ст. покладає на органи держаної влади завдання щодо їх попередження, виявлення та нейтралізації.

Постановка проблеми. Інтернет дав потужний поштовх для розвитку масової комунікації, торгівлі та обміну інформацією. Разом з тим сьогодні він є тією сферою, де здійснюється чимало правопорушень. Знеособлений характер цифрової інфраструктури зробив крадіжку ідентичності природним і надзвичайно привабливим проєктом. Кіберзлочинці активно використовують різні засоби викрадення інформації, зокрема фішинг.

На сучасному етапі і у подальшій перспективі розвиток як окремих суспільств і держав, так і загалом світу буде здійснюватися відповідно до концепції інформаційного суспільства, що пов'язано з використанням інформаційних і телекомунікаційних технологій у придбанні, зберіганні та обробці інформації у повсякденному житті [1], [2]. Суттєве зростання кількості інцидентів у кіберпросторі обумовлює необхідність системного аналізу джерел виникнення загроз, на перше місце серед яких виходить фішинг.

Аналіз останніх досліджень і публікацій. Визначення терміну «фішинг» існує велика кількість. Деякі джерела визначають це поняття як спробу вкрасти інформацію про людину, використовуючи електронну пошту [3]. Інші під фішингом розуміють веб-сторінку, яка без дозволу заявляє, що діє від імені третьої сторони з метою отримання конфіденційної інформації користувачів [4]. У авторів [5] фішинг описується як кримінальний механізм, який використовує як соціальну інженерію, так і технічні

прийоми для крадіжки особистих даних користувачів та облікових даних фінансових рахунків. Проводячи аналіз даних визначень можна зробити висновок, що «фішинг» можна розглядати по різному, однак основна мета його проведення залишається незмінною — викрадення даних.

Метою статті є дослідження принципів аналізу фішингових URL, актуальні методи класифікації даних та відбір характеристик, притаманних фішинговим сайтам.

РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Згідно з [6], під фішингом розуміють процес введення в оману чи соціального примусу жертви до передачі конфіденційної інформації для зловмисного використання. Ми під «фішингом» будемо мати на увазі саме це визначення (рис. 1).

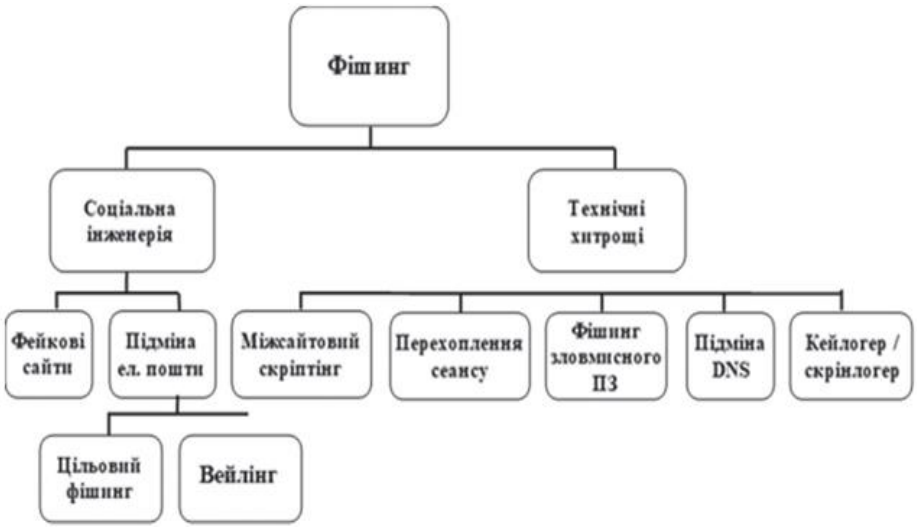

Рис. 1. Класифікація фішинг-атак

Під конфіденційною інформацією користувачів в розрізі фішингової атаки розуміють [7]:

- логін та пароль для входу в мобільні застосунки;
- номер, термін дії, CVV2/CVC2, ПІН платіжної картки;
- одноразові паролі підтвердження операцій;
- адреса електронної пошти;
- фінансовий номер телефону;
- слово — пароль до картки, відповіді на секретні питання.

Небезпечність фішингу обумовлена передусім прямою фінансовою шкодою, яку він завдає. Фішинг породжує «кризу довіри» до операцій в інтернеті, адже через суттєві втрати від фішинг-атак окремі фінансові інститути відмовляються від оплати і покладають відповідальність на клієнта [8]; підриває маркетингові зусилля і загальний імідж компаній (на фінансові установи (банки та кредитні спілки) зазвичай спрямовано 60–80% фішинг-атак); завдає шкоди електронній комерції. Його поширенням є занадто стрімким, унаслідок феноменальної прибутковості інвестицій у фішинг. Існує думка, що за прибутковістю глобальна кіберзлочинність випереджає навіть торгівлю наркотиками. В окремих випадках фішинг-атаки можуть нести загрозу також національним інтересам, регіональній і міжнародній безпеці. Також є ще один момент, який змушує говорити про

небезпечність даного правопорушення — кіберзлочини, зокрема фішинг, є різновидом організованої злочинності [9].

Пересічному інтернет-користувачу розпізнати фішинг-атаку буває досить складно через його довірливість і погану обізнаність з методами і тактиками фішингу, які постійно оновлюються (спам дедалі частіше поєднується зі зловмисним програмним забезпеченням) [10].

Науковці Університету Карнегі Меллон (Carnegie Mellon University) встановили наступні причини вразливості людей до фішингу. По-перше, інтернет-користувачі схильні оцінювати законність веб-сайту за його «зовнішнім виглядом», який шахраї легко дублюють. По-друге, багато користувачів не розуміють і не довіряють показникам безпеки у веб браузерах. По-третє, хоча деякі споживачі знають про фішинг, ця обізнаність не зменшує їх вразливості або не надає корисних стратегій для виявлення фішинг-атак. По-четверте, сприйняття серйозності наслідків фішингу не породжує належну поведінку користувачів [11] – [14].

Класифікація фішингових повідомлень

На даний час існує достатньо велика кількість методів реалізації фішингу. Слід відмітити, що самі методи фішингу можуть бути комбіновані, тим самим створюючи нові. В даній статті запропонована наступна класифікація фішингових повідомлень (рис. 2).

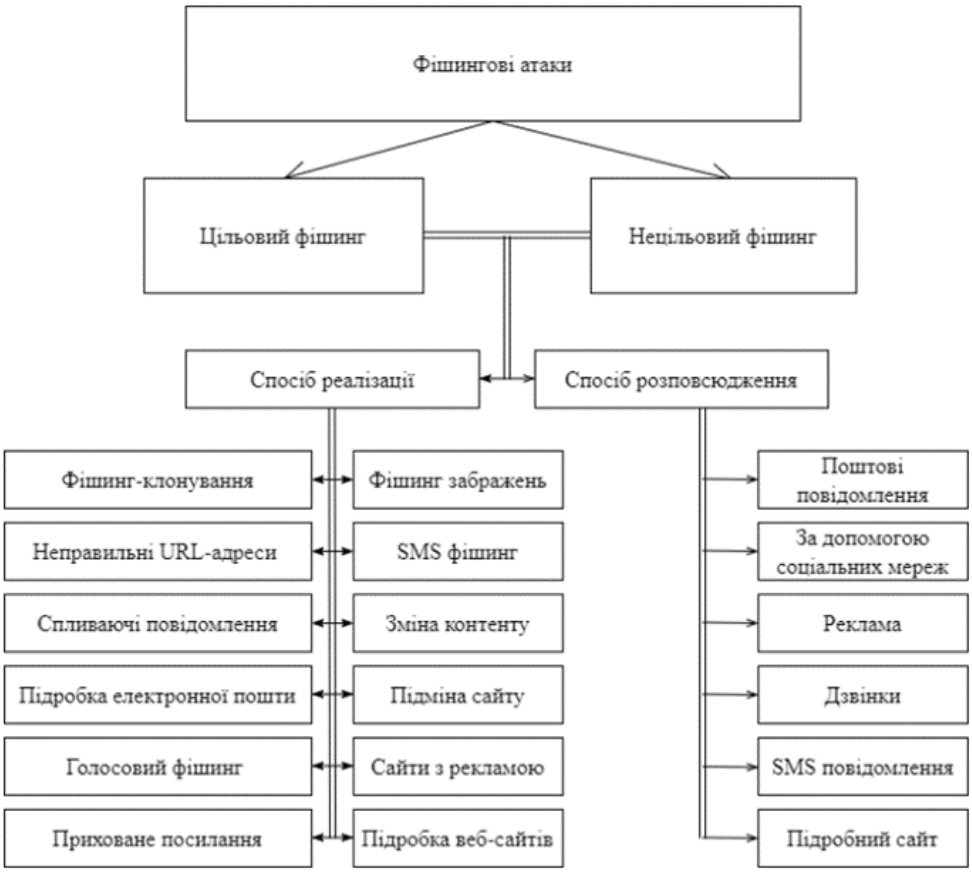

Рис. 2. Класифікація фішингових повідомлень

Першочергова класифікація фішингових повідомлень передбачає визначення того, чи була обрана зловмисником жертва. Тобто чи являється даний фішинг цільовим, чи він несе випадковий характер.

Більшість користувачів плутають спам-повідомлення з нецільовим фішингом. Варто зазначити, що ці поняття мають відмінну мету при навіть схожій реалізації. Нецільовий фішинг, хоч і не має явної жертви, все одно має на меті отримання вигоди, шляхом обману жертви та крадіжки важливої інформації.

Цільовий фішинг (Spear phishing) використовує складніші схеми, ніж нецільовий. Найчастіше він більш технологічний, а заподіяна ним можлива шкода вагоміша. Зловмисники вивчають своїх жертв та їх профілі в соціальних мережах, збирають інформацію про їх звички, використовувані сервіси, контакти та багато іншого. Якщо використовувати ці дані при складанні листа, він виглядатиме переконливим і правдоподібним. І на відміну від нецільового фішингу ймовірність жертви «потрапити на гачок» зростає.

В наведеній класифікації окремо визначено способи розповсюдження фішингових повідомлень. Спосіб, який найчастіше використовується в фішингових атаках — це поштові повідомлення. За допомогою пошти легко проводити як цільовий, так і нецільовий фішинг. Більшість сервісів та інтернет-банкінг досі використовують електрону пошту, як спосіб комунікації з користувачами. Тим самим підроблення поштових повідомлень досі є актуальною проблемою. Ще одним способом розповсюдження фішингових повідомлень є соціальні мережі. Кількість користувачів соціальних мереж зростає з кожним днем. Відповідно цільова аудиторія зловмисника може швидко розширюватися. До того ж проведення фішингових атак через соціальні мережі для зловмисника несе свої переваги. За допомогою соціальних мереж можна збирати додаткову уточнюючу інформацію про жертву, якщо зловмисника цікавить цільовий фішинг.

Використання дзвінків та SMS повідомлень актуальне для голосового та SMS фішингу відповідно. Фішинг рекламних повідомлень може бути реалізований двома способами. По-перше, на підробленому сайті розміщується реклами-приманками, для подальшого розповсюдження шкідливого контенту або обдурювання користувача при фіктивній авторизації чи реєстрації на сайті. По-друге, рекламування фішингового сайту для подальшого проведення атаки.

За способом реалізації визначені наступні види:

- фішинг-клонування (Clone phishing) — атаки клонів полягає в тому, щоб скористатися легітимними повідомленнями, які жертва, можливо, вже отримувала, і створити її шкідливу версію. Атака створює віртуальну копію законного повідомлення і відправляє повідомлення з адреси електронної пошти, яка виглядає законною. Посилання або вкладення у вихідному листі замінюються на шкідливі;
- підробка електронної пошти (Business email compromise) — характеризується отриманням даних від користувачів без їхнього відома, шляхом:
  - відправлення поштових листів через знайоме ім’я користувача;
  - відправлення поштових листів, через керівника або начальника, запитуючи важливі конфіденційні дані про користувача або про організацію;
  - видавання себе за легітимну організацію, в якій працює користувач, з метою запиту внутрішньої інформації.
- використання неправильних URL-адрес — характеризується використанням URL-адреси фішинг-сторінки для зараження цілі. Зловмисник використовує

домени, схожі на популярні веб-сайти та створює відповідні ідентичні сайти, де просить жертву ввести свої персональні дані у визначенні поля авторизації;
- використання прихованого посилання — відрізняються наявністю фрази «Натисніть тут» і схожих на неї. Перехід на приховане посилання призводить до переходу на сторінку зловмисника;
- використання реклами — фішери підроблюють сайти з «ексклюзивними пропозиціями» в якості приманки. Прикладом даної атаки є рекламна вкладка в пошуковому браузері, де фактично коштовні послуги або додатки визначаються як ексклюзивно безкоштовні протягом певного проміжку часу, що заманює жертву з більшою можливістю скористатись пропозицією;
- підробка веб-сайтів — зловмисник публікує веб-сайт, копіюючи дизайн і вміст легітимного сайту. Для зменшення ймовірності виявлення підробки використовують інструменти для скорочення URL-адрес. За допомогою даних інструментів фейкова URL-адреса виглядає більш правдоподібно та викликає менше сумнівів у користувача;
- фішинг-зображень — фішери використовують зображення або інші мультимедійні формати для доставки шкідливого програмного забезпечення. Способами доставки таких зображень є автоматичне завантаження при переході на фішинговий сайт або використання закодованих зображень;
- голосовий фішинг — зловмисник використовує телефонні дзвінки в якості отримання конфіденційної інформації;
- SMS фішинг — фішинг з використанням SMS повідомлень, який спонукає жертву на розкриття особистої інформації шляхом переходу по зловмисним посиланням;
- використання спливаючих повідомлень — дозволяють зловмиснику отримувати реєстраційні дані, надсилаючи спливаючі повідомлення;
- зміна контенту — зловмисник змінює частину інформації на легітимному сайті з метою введення в оману жертву і переправлення її за зловмисними посиланнями;
- підміна сайту — метод, в якому шкідливий сайт видає себе за легітимний шляхом проведення атаки типу міжсайтовий скрипт чи підміною сайту;
- pharming — кібератака, призначена для перенаправлення трафіку сайту на інший, фейковий, сайт. Фармінг може проводитися або шляхом зміни файлу hosts на комп'ютері жертви, або шляхом використання вразливості в програмному забезпеченні DNS-сервера. DNS-сервери — це комп'ютери, що відповідають за перетворення імен Інтернету в їх реальні IP-адреси. Скомпрометовані DNS-сервери іноді називають «отруєними». Фармінг вимагає незахищеного доступу до цільового комп'ютера, наприклад, до зміни домашнього комп'ютера клієнта, а не корпоративного бізнес-сервера.

Відповідно до сказаного раніше, зловмисники можуть комбінувати дані способи, створювати свій власний метод проведення фішингу та вдосконалювати його. Однак, розуміння реалізації кожного з цих методів окремо зменшує ймовірність стати жертвою фішингових атак.

Виявлення фішингових атак

На сьогодні існує достатня кількість антивірусного програмного забезпечення, які пропонують різні рівні захисту для попередження фішинговим атакам. Однак, ці інструменти не мають гарантованої результативності своєї роботи. Фішингові повідомлення все одно потрапляють до жертви. Зазвичай ці захисні рішення лише блокують фішингові сайти при спробі перейти за шкідливим посиланням або просто

відправляють лист до категорії «спам», але це також відбувається далеко не завжди. Тому постає задача розробки методу аналізу фішингових повідомлень, за допомогою якого, користувачі зможуть класифікувати повідомлення на основі певних ознак.

Можливо виокремити два основних підходи до виявлення фішингу: навчання користувачів і за допомогою програмних засобів [9].

1. Навчання користувачів: користувачів можна навчити краще розуміти природу фішингових атак, що в результаті допоможе коректно розрізняти фішингові і справжні повідомлення. Це суперечить категоризації в роботі [10], де навчання користувачів розглядається як превентивний захід. Однак навчання має на меті розпізнавання користувачами фішингових атак, тому розглядається як підхід до виявлення фішингу.

2. За допомогою програмних засобів: цей підхід має на меті заповнити прогалину, яка виникає через помилку користувача або незнання, та розрізняти програмним способом фішингові та легітимні повідомлення. Цей недолік вимагає вирішення, оскільки навчання користувачів є дорожчим, ніж автоматична класифікація, та не завжди є можливим, наприклад, коли бази користувачів є завеликими (PayPal, eBay, Amazon тощо).

Розпізнавання фішингової атаки — це початкова точка протидії фішинговим атакам. На рис. 3 показана схема алгоритму розпізнавання фішингових атак.

Рис. 3 Схема алгоритму розпізнавання фішингових атак

Ефективність виявлення може бути покращена за рахунок навчання класифікатора (як людини, так і ПЗ). У випадку з навчанням користувачів якість виявлення може бути покращена за рахунок їхнього індивідуального досвіду або за допомогою зовнішніх навчальних програм. У випадку програмної класифікації ефективність може бути підвищена в процесі «навчання» класифікатора, побудованого на алгоритмах машинного навчання, або вдосконаленням правил виявлення в системі на основі правил.

Програмний підхід до виявлення фішингових атак

Чорні списки. Це постійно оновлюванні списки, що містять раніше виявлені фішингові URL-адреси. Недоліком даної методології є затримка в оновленні списків. Для того, щоб щойно створений фішинговий сайт потрапив у список, необхідний час. Цієї затримки між відправленням даних і додаванням сайту до списку може бути достатньо для досягнення зловмисниками своїх цілей.

Білі списки. Ці списки є чимось протилежним до чорних. Якщо є певна URL-адреса, її порівнюють з легітимною адресою зі базою даних «білого списку». База даних «білого списку» здебільшого містить список популярних справжніх URL-адрес та їхні важливі дані. Як і у випадку з чорним списком, для завантаження нової відомої URL-адреси може знадобитися певний час, через який зловмисник, безсумнівно, може досягти своїх цілей.

Евристичні методи виділяють певні характеристики веб-сторінки для того, щоб визначити легітимність веб-сайту, а не залежати від будь-яких попередньо скомпільованих списків. Це перевага евристичних методів, над «списками». Більшість цих характеристик витягуються з URL-адреси та дерева об'єктної моделі документа HTML (DOM) даної веб-сторінки. Вилучені характеристики порівнюються з вже відомими, що були зібрані з фішингових та справжніх сторінок, щоб визначити їх легітимність. Деякі з цих підходів використовують евристики для обчислення оцінки підробки даної веб-сторінки, щоб перевірити її справжність. Сучасні веб-браузери та поштові клієнти побудовані з механізмами захисту від фішингу, такими як евристичні тести з метою виявлення фішингових атак. Так само евристичні тести виявлення фішингу можуть бути включені в антивіруси.

Методи візуальної схожості. Це методи розрізнення фішингових сайтів та легітимних сайтів за зовнішнім виглядом сайтів. Зазвичай фішингові сайти є майже точними копіями справжніх, щоб у користувача не виникали сумніви щодо легітимності ресурсу. З метою не бути виявленими зловмисники, як правило, вставляють зображення, Flash, ActiveX і Java-аплет замість HTML-тексту. Методи виявлення на основі візуальної схожості можуть швидко розпізнавати перераховані об'єкти на веб-сторінках фішингових сайтів. Методи, засновані на візуальній схожості, використовують підпис, щоб розрізняти фішингові сторінки. Щоб зробити підпис потрібно вибирати спільні компоненти з усього сайту, а не з окремої сторінки веб-сайту. Таким чином, одного підпису достатньо, щоб ідентифікувати різні цільові веб-сторінки окремого веб-сайту або унікальні форми веб-сайту. Даний метод використовує для порівняння дерево об'єктної моделі документа HTML (DOM), схожість каскадної таблиці стилів (CSS), візуальне сприйняття, візуальні особливості, піксельні та гібридні підходи.

Машинне навчання забезпечує спрощені та ефективні методи аналізу даних, останнім часом демонструючи багатообіцяючі результати у проблемах класифікації в реальному часі. Ключовою перевагою машинного навчання є можливість створювати гнучкі моделі для конкретних завдань, таких як виявлення фішингу. Оскільки фішинг є проблемою класифікації, моделі машинного навчання можна використовувати як потужний інструмент. Моделі машинного навчання можуть швидко адаптуватися до змін, щоб визначити моделі шахрайських операцій, які допомагають розробити систему ідентифікації на основі навчання.

Таблиця 1

Поширені засоби виявлення фішингу

Утиліта	Опис	Переваги	Недоліки
GoldFish	Баєсова фільтрація спаму	Може бути натренований на кожного користувача; Уникає помилкових спрацювань (FP).	Нестійкий до техніки «байєсівського отруєння»; Можна обійти трохи змінюючи слова.
Браузери Site Adviser Netcraft	Чорні списки	Швидкий аналіз	Повільне оновлення списків; Хибні спрацювання (FP).
SpoofGuard PwdHash	Інтегровані в браузер рішення; Вивчає ознаки фішингу, такі як заплутані URL-адреси на веб-сторінках; Збільшує сповіщення; Метод евристики	PwdHash запобігає крадіжці паролів; SpoofGuard захищає від неавторизованих IP та MAC-адрес	Ненадійність; Захоплений пароль можна використовувати на цільовому сайті
EarthLink toolbar	Комбінація евристики, користувальницької оцінки та ручної перевірки	Перевіряє інформацію про реєстрацію домену	Не захищає від атак
eBay tool	Евристика та чорні списки	Захищає користувачів eBay	Недоліки чорних списків

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Фішинг — це серйозна проблема безпеки в мережі, яка полягає в підробці справжніх веб-сайтів, щоб обдурити користувачів в Інтернеті і вкрасти їх конфіденційну інформацію. Задачу розпізнавання фішингових сайтів можна розглядати як типову проблему класифікації в інтелектуальному аналізі даних, коли класифікатор будується на певному наборі характеристик сайту. Існують суворі вимоги до визначення найкращого набору характеристик, які при правильному виборі підвищують точність прогнозування класифікаторів. У цій роботі досліджується вибір характеристик з метою визначення ефективного піднабору з точки зору точності класифікації. Практичне значення полягає у виявленні основних переваг і недоліків нової моделі класифікації даних, яка є комбінацією декількох вже відомих та досить розповсюджених класифікаторів, це зроблено задля підвищення точності розпізнавання, а також сформовано набір характеристик, який є меншим за початковий, що збільшує швидкодію розпізнавання, при забезпеченні високого рівня точності.

Практична цінність результатів полягає у можливості використання отриманого класифікатору для подальшого створення програмних рішень для розпізнавання фішингових сайтів. Він, а також набір характеристик може бути впроваджений у антифішингові розширення для браузерів або інші інструменти боротьби з фішингом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Antonelli, C., Geuna, A., & Steinmueller, W. E. (2000). Information and communication technologies and the production, distribution and use of knowledge. *International Journal of Technology Management, 20(1/2).* https://doi.org/10.1504/ijtm.2000.002853
2. Mansell, R. (2013). The life and times of the Information Society. *Prometheus, 28(2),* 165–186. https://doi.org/10.1080/08109028.2010.503120.

3. *Fishynh (Phishing), Vishynh (vishing), Farminh — shakhraistvo v Interneti Entsyklopediia internet reklamy*. (n.d.). Entsyklopediia internet reklamy. http://vse-prosto.vestop.rf/fishing-phishingvishing-vishing-farming.html
4. Whittaker, C. (2013). Large-scale automatic classification of phishing pages. *Network and Distributed System Security Symposium.*
5. *Phishing Activity Trends Report, 1st Quarter*. (2019). APWG. http://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
6. Акулич, М. (2022). *Фишинг и маркетинг.* Litres.
7. *Що таке фішинг і як від нього захиститись.* (б. д.). Головна ФГВФО. https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html
8. Birk, D., Gajek, S., Grobert, F., & Sadeghi, Ah.-R. (2007). Phishing Phishers—Observing and Tracing Organized Cybercrime. *Second International Conference on Internet Monitoring and Protection.*
9. Brenner, S. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law and Technology, 4.*
10. Kumar, A., Chatterjee, J.M., & Díaz, V.G. (2020). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. *International Journal of Electrical and Computer Engineering (IJECE), 10(1),* 486–493. https://doi.org/10.11591/ijece.v10i1
11. Sheng, St., Holbrook, M., Kumaraguru, P., & Cranor, L. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *28th International Conference on Human Factors in Computing Systems,* 373–382. https://doi.org/10.1145/1753326.1753383
12. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *SIGCHI Conference on Human Factors in Computing Systems,* 581–590.
13. Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. *Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit, 269,* 37–44.
14. Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *SIGCHI Conference on Human Factors in Computing Systems,* 601–610.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Roman Shtonda
Head of Research Department
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Yuliya Chernish
Senior Researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

Tetiana Tereshchenko
Senior Researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-9659-7897
tetiana.tereshchenko@viti.edu.ua

Katerina Tereshchenko
Student
National Aviation University, Kyiv, Ukraine
ORCID ID: 0009-0008-8469-9854
katerina60411@gmail.com

Yurii Tsykalo
Listener
National Defence University of Ukraine, Kyiv, Ukraine
ORCID ID: 0009-0006-9698-3276
ab3366bk@ukr.net

Serhiy Polishchuk
Listener
National Defence University of Ukraine, Kyiv, Ukraine
ORCID ID: 0009-0006-9110-7576
0988528103@ukr.net

CLASSIFICATION AND METHODS OF DETECTION OF PHISHING ATTACKS

Abstract. The reliable operation of data transmission networks, computer systems and mobile devices is a mandatory condition for the effective functioning of the state and society, and the life of an individual. The reliability of key information systems for public use depends on many factors: cyber attacks, hardware and software failures, and various types of errors. Rapid expansion of threats to national security in the 21st century. entrusts state authorities with the tasks of their prevention, detection and neutralization. Cyber security is increasingly viewed as a fundamental problem of the state, which comprehensively affects its security, defense, economy, and almost all spheres of public life. The Internet gave a powerful impetus to the development of mass communication, trade and information exchange. However, today it is the area where many crimes are committed. The impersonal nature of digital infrastructure has made identity theft a natural and highly attractive project. Cybercriminals actively use various means of stealing information, including phishing. At the current stage and in the future, the development of both individual societies and states, as well as the world in general, will be carried out in accordance with the concept of the information society, which is connected with the use of information and telecommunication technologies in the acquisition, storage and processing of information in everyday life Phishing is a serious online security problem that involves spoofing genuine websites to trick online users and steal their

confidential information. Analyzing these definitions, we can conclude that "phishing" can be considered in different ways, but the main purpose of its conduct remains unchanged—stealing data. The practical value of the results lies in the possibility of using the obtained classifier for further creation of software solutions for recognizing phishing sites. It, as well as a set of characteristics, can be implemented in anti-phishing browser extensions or other anti-phishing tools.

Keywords: cyber security; cyberspace; phishing cyberattacks; phishing messages.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Antonelli, C., Geuna, A., & Steinmueller, W. E. (2000). Information and communication technologies and the production, distribution and use of knowledge. *International Journal of Technology Management, 20(1/2).* https://doi.org/10.1504/ijtm.2000.002853
2. Mansell, R. (2013). The life and times of the Information Society. *Prometheus, 28(2),* 165–186. https://doi.org/10.1080/08109028.2010.503120
3. *Fishynh (Phishing), Vishynh (vishing), Farminh — shakhraistvo v Interneti Entsyklopediia internet reklamy*. (n.d.). Entsyklopediia internet reklamy. http://vse-prosto.vestop.rf/fishing-phishingvishing-vishing-farming.html
4. Whittaker, C. (2013). Large-scale automatic classification of phishing pages. *Network and Distributed System Security Symposium.*
5. *Phishing Activity Trends Report, 1st Quarter*. (2019). APWG. http://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
6. Akulych, M. (2022). *Fyshynh y marketynh*. Litres.
7. Shcho take fishynh i yak vid noho zakhystytys. (n.d.). https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html
8. Birk, D., Gajek, S., Grobert, F., & Sadeghi, Ah.-R. (2007). Phishing Phishers—Observing and Tracing Organized Cybercrime. *Second International Conference on Internet Monitoring and Protection.*
9. Brenner, S. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law and Technology, 4.*
10. Kumar, A., Chatterjee, J.M., & Díaz, V.G. (2020). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. *International Journal of Electrical and Computer Engineering (IJECE), 10(1),* 486–493. https://doi.org/10.11591/ijece.v10i1
11. Sheng, St., Holbrook, M., Kumaraguru, P., & Cranor, L. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *28th International Conference on Human Factors in Computing Systems*, 373–382. https://doi.org/10.1145/1753326.1753383
12. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *SIGCHI Conference on Human Factors in Computing Systems*, 581–590.
13. Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. *Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit, 269*, 37–44.
14. Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *SIGCHI Conference on Human Factors in Computing Systems*, 601–610.