УДК 004.056
DOI: 10.31673/2409-7292.2022.014449

Алексеєнко О.А., Бурлін М.О., Кисельов О.В., Кравчук В.В., Мальгіна К.В.

МЕТОДИКИ ФІШИНГУ В МОБІЛЬНИХ СИСТЕМАХ

Швидкий розвиток мобільних пристроїв та комунікаційних технологій призвело до різкого збільшення кількості користувачів мобільних пристроїв. Мобільний пристрій замінив багато інших пристроїв і використовується для виконання багатьох завдань, починаючи від встановлення телефонного дзвінка і закінчуючи виконанням важливих та конфіденційних завдань, таких як грошові платежі. Оскільки мобільний пристрій супроводжує людину більшу частину часу, дуже ймовірно, що вона містить особисті та конфіденційні дані цієї людини. Більш широке використання мобільних пристроїв у повсякденному житті зробило мобільні системи чудовою мішенню для атак. Однією з найбільш важливих атак є атака фішинга, при якій зловмисник намагається отримати облікові дані жертви і видати себе за неї. У цій роботі проводиться аналіз різних видів фішингових атак на мобільні пристрої. Також аналізуються методи пом'якшення – методи захисту від фішингу. Дається оцінка кожної методики та короткий виклад її переваг та недоліків. Наприкінці наведено важливі кроки захисту від фішингових атак. Мета роботи – висвітлити фішингові атаки на мобільні системи, інформувати людей про ці атаки та про те, як їх уникнути.

Ключові слова: кідливе програмне забезпечення, фішинг, захист від фішингу, мобільний пристрій, мобільний додаток, безпека, конфіденційність.

Вступ

Протягом останніх 10 років технології мобільних пристроїв стрімко розвивалися завдяки щоденному збільшенню кількості користувачів і об’єктів. Згідно з даними [1], кількість користувачів мобільних пристроїв у 2021 році склала 5,3 мільярда користувачів у всьому світі. Поточні мобільні пристрої можна використовувати для багатьох приватних та фінансових програм, таких як Facebook, мобільний банк тощо. Android та iOS є двома домінуючими операційними системами з часткою ринку 99,6% розподілена як 81,7% для Android і 17,9% для iOS [2].

Згідно з Symantec, фішинг це вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Фішингове повідомлення містить фальшиве посилання на створену веб-сторінку, схожу на законну сторінку, користувача просять надати свої облікові дані для входу на сторінку, що призводить до передачі облікових даних злочинцю. Згідно [3], по всьому світу сталося не менше 255 065 унікальних атак фішингу. Зростання становить понад 10% порівняно з атаками, виявленими в 2019 році. Розподіл цих атак по галузі показано на рис. 1.

Через конфіденційність даних, що зберігаються на мобільних пристроях, ці пристрої стали чудовою мішенню для фішерів для запуску своїх програм. атаки. Мета атак - отримати доступ до облікових даних, які можуть бути корисні при використанні сервісів, у яких зареєстрований користувач. Ці послуги включають набір номера, SMS, платежі, витік конфіденційних даних та підключення. Фішер може видати себе за мобільного користувача та використовувати його мобільний телефон для виконання цих завдань без дозволу користувача. Відповідно до [4], протягом 2018 року щодня відбувалося понад 4000 атак програм-вимагачів. PhishMeInc повідомила, що програми-вимагачі та фішингові атаки працюють разом і що 97,2 фішингових електронних листів у 2016 році містять одну з форм програм-вимагачів [5]. На рис. 2 показано частоту атак програм-вимагачів на фізичних осіб у першому та третьому кварталах 2019 року. Виразно видно, що частота атак на фізичних осіб подвоїлася третьому кварталі. Дослідження, проведене доктором Зінаїдою Бененсон з Університету Фрідріха-Олександра (FAU), показало, що 78% людей продемонстрували поінформованість про фішингові атаки з невідомими посиланнями та 45% з них перейшли за посиланням [6]. Судячи з наведених цифр, ми робимо висновок, що кількість фішингових атак на мобільні пристрої різко зростає. З іншого боку, атаки поширилися на великі області послуг, як показано на рис. 1. І, враховуючи, що мобільні користувачі не знають про цю величезну загрозу, а якщо і знають, то продовжують переходити за шкідливими

посиланнями, дуже важливо звернути увагу на цей тип фішингових атак та інформувати мобільних користувачів про масштаби загрози та кроки, які вони можуть зробити, щоб запобігти подібним атакам.

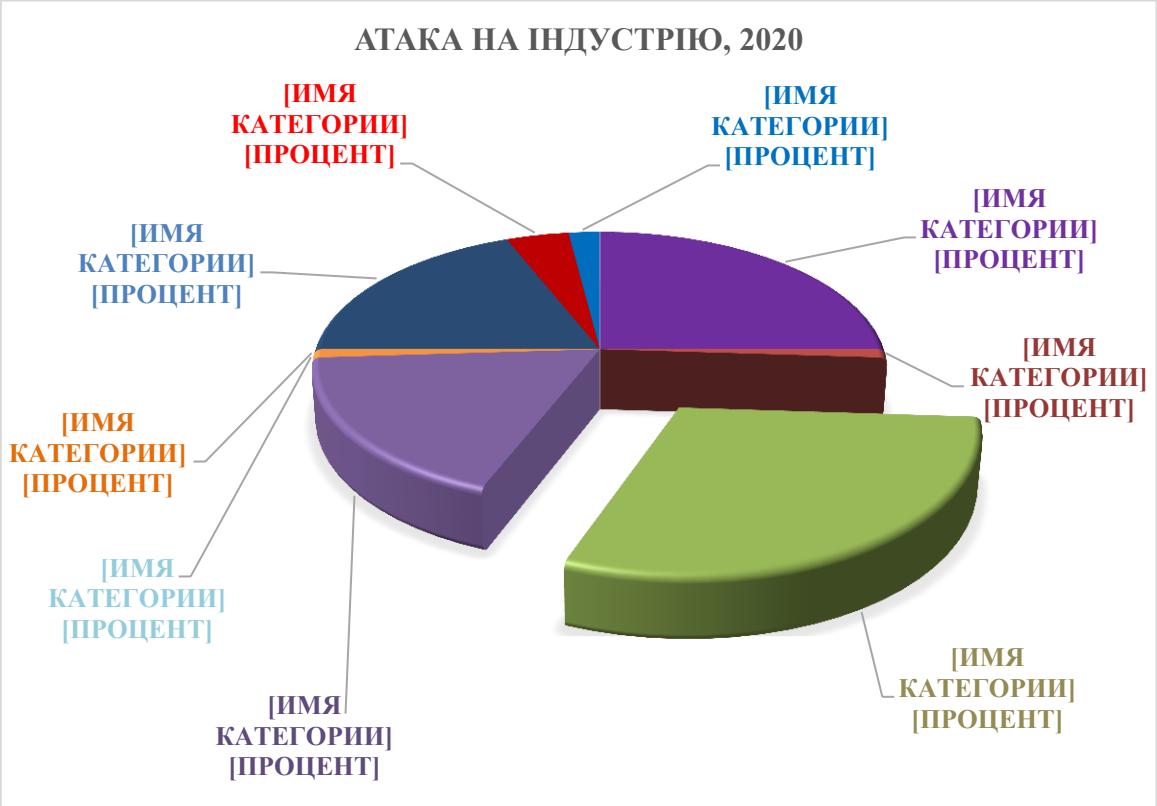

Рис. 1. Поширення фішингових атак у промисловості. Джерело: звіт APWG про глобальні тенденції фішингу та використання доменного імені 2020 року

Мобільні фішингові атаки.

Перш ніж говорити про мобільні атаки фішингу, ми повинні спочатку представити привабливі властивості мобільних пристроїв, які змусили творців шкідливих програм націлюватися на ці пристрої, визначимо типи атак фішингу. Опишемо методи розповсюдження, що використовуються в мобільних програмах, зі статистикою.

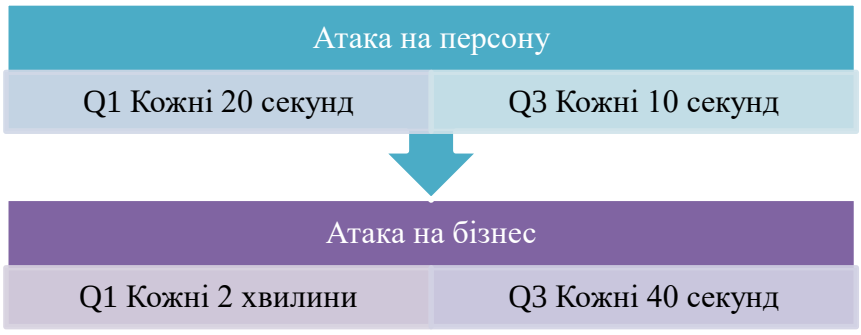

Рис. 2. Частота атак на фізичних осіб у 2020 році

Властивості використання мобільних пристроїв.

Мобільні пристрої полегшують атаки фішингу завдяки своїм наступним властивостям: Швидке зростання кількості мобільних користувачів по всьому світу, як описано в [1]. Цей перехід користувачів на мобільні пристрої спонукав фішерів перенести свої методи на

мобільні пристрої. Через обмежений розмір екрану мобільним користувачам важко відрізнити законну веб-сторінку від фішингової. Крім того, маленький розмір екрану також змушує браузери приховувати повний URL сторінки, що запитується і, отже, допомагати фішеру обманювати мобільного користувача. Через мобільність мобільного використання користувачі, як правило, реагують на взаємодію з меншою концентрацією, що може призвести до схвалення процесу фішингу. Оскільки мобільний пристрій в основному знаходиться поруч із мобільними користувачами, користувачі схильні довіряти цим пристроям. Це, у свою чергу, збільшить ймовірність злому та фішингу через цю довіру. На жаль, творці шкідливих програм та фішери знають про ці властивості і тому перенесли свої зусилля та методи на мобільні пристрої та їхні програми.

Методи мобільних фішингових атак.

Метою фішингу є отримання облікових даних, які можуть бути використані для видачі себе за людину, яка використовує облікові дані. Основна ідея успішної атаки фішингу полягає в тому, щоб обдурити користувача, щоб він надав свої облікові дані. У мобільних технологіях зловмисники використовують різні способи запуску своїх атак та обману жертв, ці способи перераховані нижче:

1) Фінансове шахрайство, як випливає з назви, спрямоване на збір фінансових даних жертви, які потім можуть бути використані для видачі себе за іншу особу та виконання фінансових операцій від його імені. Звіт MicroSave містить детальну інформацію про такі шахрайства з використанням мобільних пристроїв. У звіті йдеться, що мобільне фінансове шахрайство стає все більш поширеним у зв'язку з ширшим використанням фінансових мобільних програм для виконання електронних транзакцій. CGAP провів дослідження даного злочину у різних країнах. Ключовою ідеєю було те, що повністю захиститись від цього шахрайства неможливо. Одним із прикладів фінансового злочину може бути хибне оновлення облікового запису інтернет-банкінгу. Користувач переходить за посиланням у повідомленні, яке виглядає як законне, і він буде перенаправлений на сторінку, аналогічну сторінці входу до його банку. Щоб уникнути такого сценарію, постачальники послуг, такі як банки зазвичай використовують методи двофакторної аутентифікації, зазвичай відправляючи пін-код у вигляді SMS на мобільний телефон користувача. Якщо введений PIN-код не збігається з надісланим, вхід заборонено.

2) Оновлення служб. У цьому методі атак злочинці використовують зареєстровані служби для користувачів, щоб збирати їх облікові дані і, отже, видавати себе за законних користувачів і замість цього використовувати служби, включаючи Drop Box, Google Drive, обліковий запис Microsoft і т.д. необхідності оновлення служби, для цього користувач повинен надати свої облікові дані. На цей час облікові дані, пов'язані з цією службою, обробляються для злочинця. Як і у випадку фінансового шахрайства, деякі постачальники послуг використовують двофакторну автентифікацію. Однак, шахрай може обійти це, перебуваючи в мережі під час запуску атаки, а також отримати PIN-код.

3) Реклама. Шахрай автоматично надсилає підроблені рекламні пропозиції ряду користувачів, вони представлені у формі купівлі купонів, квитків, подарунків тощо. Користувачеві пропонується створити обліковий запис, щоб отримати цю пропозицію. Потім злочинець використовує надані облікові дані, щоб спробувати увійти в інші системи, сподіваючись, що користувач використав ту саму вказану інформацію.

4) Цей тип атаки більше націлений на людину чи організацію. Цей тип атаки вимагає соціальної інженерії, щоб зібрати правильні дані, а потім обдурити цільову людину. У 2010 році в ході спрямованої атаки було зламано код на багатьох машинах з використанням шкідливого ПЗ для доступу до систем Google, Adobe та інших систем США. Атака була спрямована на крадіжку інтелектуальної власності виконавчого редактора https://www.darkreading.com/.

5) Whaling Whaling 2.2.5. Китобійний промисел – це особливий вид фішингу. Жертва нападу – відома особистість. Хакер витрачає багато часу на збирання інформації про свою мету, коли буде зібрано потрібну кількість інформації, зловмисник використовуватиме її для

запуску атаки. Зловмиснику може знадобитися деякий час, щоб завоювати довіру своєї жертви, перш ніж почати. Приклад нападу такого злочину був, коли Leoni AG, найбільший у Європі виробник проводів та електричних кабелів, втратила 44,6 млн. доларів внаслідок шахрайства, під час якого фінансовий персонал обманом змусили переказати гроші не на той банківський рахунок.

Методи розповсюдження.

Під методом поширення ми маємо на увазі походження мобільного трафіку, що використовується для фішингу. iOS більш схильна до фішингових атак, ніж Android. Відсоток фішингових атак для iOS становить 63%, а для Android – лише 37%. Обґрунтування полягає в тому, що користувачі Apple більш престижні і, отже, є кращими фішинговими об'єктами, ніж інші. Існує безліч методів поширення, які використовуються для фішингу. У таблиці 1 нижче наведено дані про популярність методів розширення згідно. Як видно з сьогодення, методи мобільного фішингу стають все більш цілеспрямованими та технічно добре організованими. Цілі стають все більш конкретними і ретельно вибираються. Інтенсивно використовується соціальна інженерія, щоб зробити фішинг ефективнішим. У наступному розділі ми поговоримо про методи захисту від фішингу на мобільних пристроях, їх переваги та недоліки.

Мобільний антифішинг. Методи.

Тут варто згадати, що методи фішингу в мобільних програмах можуть бути реалізовані через веб-браузер або з використанням сторінки входу в певний мобільний додаток. Метод захисту повинен виявляти атаки фішинга через браузери або програми.

Були запропоновані різні методи веб-антифішингу, ці методи ґрунтуються на контенті, чорних та білих списках. У методах, що базуються на контенті, вміст веб-сайту використовується для визначення того, є він фішинговим сайтом чи ні. У той час як чорні списки та білі списки порівнюють запитану URL-адресу або з чорним списком фішингових URL-адрес, або з білим - нефішингових.

Існує метод, що базується на реєстрації користувачів на веб-сайті, після чого для кожного користувача генерується унікальний код. Користувача просять ввести кілька цифр унікального коду, і веб-сайт повинен відповісти повним кодом. Правильний код означає, що веб-сайт є справжнім. Цей метод вимагає, щоб користувачі зареєструвалися та запам'ятали свій код для різних веб-сайтів, але після зламування коду фішинг буде легко запущений.

Система виявлення фішингу представлена в [17]. Запропонована структура отримує функції веб-сайту і порівнює їх з вихідними функціями справжнього сайту. Однак більшість сторінок фішингу дуже схожі на справжні, і, отже, це може призвести до помилкових спрацьовувань. Система також потребує великих обчислень для отримання тексту, зображень та колірних характеристик веб-сайту. Метод використовує вилучення скріншотів для обчислення візуальної подібності, метрику, яка називається коефіцієнтом обману, для розрахунку подібності. Цей метод призначений для екранів входу до мобільних програм і не працює для веб-входів.

Bayesian метод заснований на побудові моделі навчання на основі збору даних про дозволи та ключові журнали. Після вивчення модель використовується для відповідної перевірки програм. Проте система вимагає доробок щодо пам'яті і схеми управління, після чого її можна буде оцінити на предмет практичного використання.

Ще одна техніка, використовувати деякі функції URL-адрес для визначення легітимності веб-сторінки на основі частотного аналізу вилучених функцій фішингових URL-адрес. Метод не може виявляти для фішингових сайтів нову поведінку щодо фішингового URL-сховища.

Візуальна криптографія як метод для виявлення фішингу. Пропонована структура є інтерактивним методом, що використовує схему перевірки капча, засновану на візуальній криптографії. І користувач, і сервер володіють частиною капча, і працюють разом, щоб відновити повне зображення. Час, що витрачається на відновлення капчі, фіксується та використовується у процесі виявлення фішингу.

Метод MP-щита заснований на пошуку в Google URL-адрес із чорного списку, крім того, він витягує характеристики URL-адрес і передає їх у відповідну модель класифікатора. Цей метод може генерувати помилкові спрацьовування і покладатися на Google для пошуку в Інтернеті, а не спеціальний довірений чорний список.

Уникнення фішингу

Аби уникнути фішингу, користувач повинен знати URL, який може індитифікувати ціль фішингової атаки. Але, як ми відмічали раніше, невеликий екран мобільного пристрою робить перевірку на наявність URL-адрес значно важкішим. Для цього ми пропонуємо декілька порад, котрі можуть бути корисними для мобільних користувачів.

1) Найбільшим питанням є встановлення та використання справжніх додаткив, що надаються довіренними постачальниками. Це дозволить користувачам бути впевненим у тому, що їх додатки не є частиною фішингової атаки. Відповідно до даних [23], компанія PhishLabs повідомила, що 11 злоякісних додатків, які запевняють, що вони є справжніми мобільними платіжними додатками, були в офіційному магазині додатків Google.

2) Користувач може використовувати засоби захисту від фішингу довіренних компаній, які дозволять йому виявляти фішингові атаки та уникати їх.

3) Ніколи не відповідати на будь-які підозріли повідомлення та листи. Якщо ви підозрюєте, чому вам їх надсилають, то ви у ризику стати ціллю фішингової ататки. Не відповідайте на ці листи.

4) Хорошою практикою для уникнення фішингу є використання закладок веб-браузеру, які ви часто відвідували. Це ускладнить реєстрацію небажанних веб-сторінок, які можут бути фішинговим сайтами.

5) Користувач повинен слідкувати за записами безпеки та вивчати безпечне використанні мобільних пристроїв.

6) Важливо забезпечувати високий захист мобільного пристрою за допомогою паролю та інших методів контролю. Це захистить від крадіжки персональних даних після втрати мобільного пристрою.

7) Використовуйте служби анти-крадіжки в захисті мобільного пристрою, як Remote Lock, Remore Wipe, аби знайти та захистити дані на ньому.

8) Використовуйте безпечні методі перегляду, аби уникнути відвідування шкідливих веб-сайті.

Висновки

У цій статті ми представили короткий опис методів боротьби з фішингом, які використоуються на мобільних приладах. Ці метод базувалися на деяких особливостях мобільни пристроїв, через які фішингові атаки на них були більш вирогіднішими. Деякі з цих функцій були невелики розміри екрану та велике відчуття довіри користувачів до мобільних пристроїв. Ми розібрали методи боротьби з фішингом, які були запропоноані для мобільних користувачів. Наше вивчення показало, що всі ці методи мають деякі недоліки, що роблять їх меньш ефективними перед виявленням фішингових атак. Слідуючи з цього, найбільша задача перекладається на користувачів мобільних пристроїв, які мають виконувати деякі кроки безпееки, які можуть допомогти уникати фішинг. Ці кроки та методики було викладено в останньому розділі цієї статті.

Ціль статті заключається в освітленні фішингових атак на мобільні пристрої, а також в інформуванні людей про такі атаки і способом їх уникнення.

Перелік посилань

1. https://wearesocial.com/special-reports/digital-in-2017-global-overview
2. http://www.gartner.com/newsroom/id/3609817
3. Aijaz Ahmad, S., et al. (2013) Smartphone: Android vs IOS. The SIJ Transactions on Computer Science Engineering & Its Applications (CSEA), 1, 141-148.
4. US Government (2016) How to Protect Your Network from Ransomware. Technical Guidance Interagency Document. US Government, Washington, DC.

5. PhishMe, Inc. (2016) Malware Review Q3. PhishMe, Inc., Leesburg, VA.
6. https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-fro m-unknown-senders/
7. Luminzu Mudiri, J. (2012) Fraud in Mobile Financial Services. MicroSave, Lucknow.
8. Buku, M.W. and Mazer, R. (2015) Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System. CGAP, Washington, DC.
9. http://resources.infosecinstitute.com/spear-phishing-real-life-examples/#gref
10. https://www.scmagazineuk.com/leoni-ag-suffers-34-million-whaling-attack/article/ 530694/
11. WANDERA (2017) Mobile Data Report: Focus on Phishing.
12. Yoon, J.W., et al. (2010) Hybrid Spam Filtering for Mobile Communication. Computers and Se-curity, 29, 446-459. https://doi.org/10.1016/j.cose.2009.11.003
13. Memon, I.K. and Khan, M.K. (2013) Anti Phishing for Mid-Range Mobile Phones. International Journal of Computer and Communication Engineering, 2, 115-119.
14. Singh, D., et al. (2011) Telephony Fraud Prevention. US Patent.
15. Mahmoud, T.M. and Mahfouz, A.M. (2012) SMS Spam Filtering Technique Based on Artificial Immune System. IJCSI International Journal of Computer Science Issues, 9, 589-597.
16. Mishra, M., et al. (2012) A Preventive Anti-Phishing Technique using Code Word. International Journal of Computer Science and Information Technologies, 3, 4248-4250
17. Archana, M., et al. (2011) Architecture for the Detection of Phishing in Mobile Internet. Interna-tional Journal of Computer Science and Information Technologies, 2, 1297-1299.
18. Malisa, L., et al. (2015) Technical Report: Detecting Mobile Application Spoofing Attacks by Leveraging User Visual Similarity Perception.
19. Kumar, N. and Chaudhary, P. (2017) Mobile Phishing Detection using Naive Bayesian Algo-rithm. International Journal of Computer Science and Network Security, 17, 142-147. [20] Orunso-lu, A.A. (2017) A Lightweight Anti-Phishing Technique for Mobile Phone. Acta Informatica Pra-gensia, 6, 114-123.
20. Yenurkar, B. and Zade, S. (2014) An Anti-Phishing Framework with New Validation Scheme Using Visual Cryptography. International Journal of Computer Science and Mobile Computing, 3, 739-744.
21. Bottazzi, G. (2015) MP-Shield: A Framework for Phishing Detection in Mobile Devices. IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Com-puting, Liverpool, 26-28 October 2015, 1977-1983.
22. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.293
23. http://onlinesecurity.trendmicro.com.au/blog/2016/06/22/phishlabs-warns-of-malw are-posing-as-legit-apps-on-google-play/

Надійшла: 15.01.2022 Рецензент: д.т.н., професор Вишнівський В.В.