УДК 004.056

О. В. Кухарець
О. П. Войтович

ЗАСІБ ДЛЯ ІДЕНТИФІКАЦІЇ ФІШИНГОВИХ САЙТІВ

Вінницький національний технічний університет

Анотація

Розглянуто проблему викрадення конфіденційних даних користувачів в інтернеті. Як саме вдається здійснювати атаку. Як усунути дану проблему.

Ключові слова: фішинг, атака, логін, пароль, кредитні дані, шахрайство, хакер, викрадення даних, конфіденційні дані, захист.

Abstract

The problem of stealing confidential user data on the Internet is considered. How exactly do you manage to carry out an attack. How to fix this problem..

Keywords: phishing, attack, login, password, credit data, fraud, hacker, data theft, confidential data, protection.

Вступ

З появою інтернету людське життя стало значно простішим, проте з’явилась нова проблема – викрадення конфіденційних даних користувачів. За останні декілька років проблема фішингу стала глобальною, з кожним днем число жертв зростає. Саме тому необхідно дослідити дану проблему та знайти спосіб її вирішення.

Результати дослідження

В першу чергу необхідно визначити, яким чином працює фішинг – атака [1]. Першим етапом є електронний лист на пошту.

Для початку зловмисники знаходять електронну адресу жертви (купують бази з адресами). Створюють поштову скриньку, маскуючи її під оригінальну. Наприклад можуть замінити одну літеру або ж покластися на те, що користувач не знає якою має бути адреса в дійсності і створити на свій лад, також вік доменного імені не має бути меншим 30 днів. Далі йде важлива частина – створення змісту листа [1-3]:

- жертва обов’язково має перейти за посиланням. В своїх листах зловмисники використовують яскраві заклики перейти за посиланням (виділяють червоним кольором);
- вказане посилання може перенаправляти на інший сайт;
- в тексті листа можлива наявність граматичних та орфографічних помилок;
- зазвичай сервіси, в яких зареєстровані користувачі, мають їх персональні дані (прізвище, ім’я, номер телефону і тд), тобто якщо в листі немає звернення по імені, його можна вважати підозрілим;
- часто зловмисники можуть просити ввести логін і пароль, проте ці дані є конфіденційними і ні один сервіс не може їх запитувати;
- наявність фраз типу «останнє попередження», «термінова перевірка», «швидке блокування» спонукають перестати думати і терміново діяти;
- наявність в електронних листах JavaScript.

Якщо ж жертва перейшла за посиланням, то вона потрапляє на фішинговий сайт, який зазвичай є копією оригінального, проте не клікабельним. Зловмисники або копіюють існуючий сайт, або створюють лише необхідну їм сторінку. Так як адресу оригінального сервісу вони не можуть використати, це дозволяє помітити атаку. Ознаками за якими можна визначити фішинговий сайт (табл. 1) [1-4]:

Таблиця 1 – Ознаки фішингового сайту

1.	Відсутність політики інформаційної безпеки та контактних даних
2.	Наявність IP-адреси в посиланні
3.	Використання піддоменів, щоб зробити посилання законними.
4.	Використання небезпечного протоколу http
5.	Відсутність маркування конфіденційних даних
6.	Спосіб оплати лише за допомогою банківського переказу

Провівши дослідження того як працює зловмисник, можна будувати захист від фішингу. В першу чергу необхідно провести захист на рівні електронного листа. Поштові сервери допомагають у цьому, вони відправляють підозрілі листи від підозрілих доменів в спам. Проте необхідно передбачити випадок коли користувач прочитає повідомлення.

Для виявлення фішинг атаки створено браузерне розширення, яке на основі певних критеріїв робить висновки про безпечність листа та сайту і виводить повідомлення, якщо можлива небезпека. Критерії за якими відбувається перевірка листа:

- наявність таких фраз: «останнє попередження», «термінова перевірка», «швидке блокування», а також виділених червоним кольором слів;
- наявність JavaScript;
- наявність граматичних та орфографічних помилок;
- перевірка доменного імені на вік.

Критерії за якими перевіряється сайт:

- наявність IP-адреси в посиланні або декількох піддоменів;
- створено базу даних з адресами найпопулярніших сервісів, тому відбуватиметься перевірка на наявність адреси в базі;
- наявність протоколу https;
- маркування конфіденційних даних (пароль, CVV);
- наявність контактних даних.

Засіб включає систему підтримки прийняття рішень, оскільки, щоб виявити фішинг атаку не завжди достатньо одного критерію із вище перерахованих.

Висновки

Проаналізувавши таку вагому проблему сучасності як фішинг, було визначено декілька критеріїв за якими можна визначити чи є лист або ж сайт безпечними та розроблено засіб для ідентифікації фішингових сайтів. Проте основним захистом є сама людина. Оскільки тільки вона вирішує чи варто надавати свої конфіденційні дані.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, *106, 1–20.* doi:10.1016/j.eswa.2018.03.050
2. Basnet R., Mukkamala S., Sung A. H. (New Mexico, 2008) Detection of Phishing Attacks: A Machine Learning Approach, с. 373–383.
3. 7 ознак фішингових листів: веб-сайт. URL: https://www.belinvestbank.by/individual/page/7-priznakov-fishingovyh-pisem (дата звернення: 02.03.2021).
4. RAMZAN, Zulfikar. Phishing attacks and countermeasures. Handbook of information and communication security, 2010, 433-448.

Кухарець Оксана Володимирівна — студентка групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kukharets1bs.17b @gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** — доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Kukharets Oksana V. — Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : kukharets1bs.17b @gmail.com

Supervisor: ***Voitovych Olesya P.*** — docent of the department of information security, Vinnytsia National Technical University, Vinnytsia