УДК 004.5+004.62

Фурсова І.І., студентка гр. 125м-20-2
Мєшков В.І., старший викладач
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

ФІШИНГ ЯК НОВА ЗАГРОЗА БЕЗПЕЦІ ІНФОРМАЦІЇ

В сучасному світі багато підприємств стають жертвами інформаційних атак типу фішинг. Основна ідея фішингу полягає в тому, щоб зловмисник отримав прибутки або доступ до цінної інформації підприємств. Здійснюється це за допомогою психологічного впливу на звичайного користувача.

Фішинг – один з різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки [1]. Завдяки неуважності користувачів зловмисники можуть отримати персональні дані.

Також поняття фішингу визначається як злочин, за якого жертви обманним шляхом змушують поділитися конфіденційною інформацією, такий як паролі та номери кредитних карт. Є основна тактика фішингу: жертва отримує електронний лист або текстове повідомлення, яке імітує людину або організацію, до яких користувач має довіру. Це може бути письмо від зловмисника, який прикривається колегою, банківською установою або урядовою установою. Електронний лист або повідомлення містить інформацію, призначену для того, щоб налякати жертву, з проханням відвідати веб-сайт і вжити негайних заходів, щоб уникнути негативних наслідків.

Якщо користувач натискає на посилання в повідомленні, він потрапляє на імітацію легітимного веб-сайту. На цьому етапі користувачеві пропонується увійти в систему, ввівши свої облікові дані: ім'я користувача і пароль. Якщо користувач достатньо наївний, щоб виконати запит, введена інформація буде передана злочинцеві, який зможе використовувати її для крадіжки особистих даних, перехоплення доступу до банківських рахунків і продажу особистої інформації на чорному ринку.

Алгоритм здійснення фішингу був вперше описаний в 1987 році, в якому група шахраїв намагалася отримати доступ к операціям з кредитними картками за допомогою розповсюдження фішингового програмного забезпечення [2].

Існує багато видів фішингу, загальним знаменником усіх атак є використання оманливого приводу для отримання важливої інформації. Види фішингових атак

Хоча існує багато видів фішингу, загальним знаменником усіх атак є використання оманливого приводу для отримання важливої інформації. Основні категорії фішингу:

Цільовий фішинг. На відміну від більшості фішингових компаній, які покладаються на надсилання електронних листів якомога більшій кількості людей, цей фішинг є націлений, який атакує певну особу чи організацію. Цей вид фішингу вимагає попереднього аналізу жертв, щоб виявити імена, посади, адреси електронної пошти та іншу подібну інформацію. Хакери проводять широкі дослідження в Інтернеті, щоб зіставити таку інформацію про жертву з іншими даними, що стосуються колег, імен та професійних стосунків ключових співробітників їхніх організацій. Завдяки цій процедурі фішинг може написати надійний електронний лист.

Наприклад, мішенню цільового фішингу може бути працівник, роль якого включає завдання авторизації платежів. Схоже, що електронний лист надходить від керівника організації з проханням працівника передати виплату великої суми керівництву чи постачальнику компанії.

Цільовий фішинг становить серйозну загрозу для бізнесу (та урядів), що призводить до дуже високих витрат.

Телефонний фішинг – це телефонні дзвінки від зловмисника, який позиціонується як представник банківської установи, представником правоохоронних органів та подібне. Зловмисник повідомляє жертві тривожну інформацію та наполягає на негайному вирішенні проблеми шляхом надання реквізитів банківського рахунку або сплати штрафу. Запитуваний

платіж, як правило, має бути здійснений банківським переказом або передоплаченою карткою, щоб потім зловмисника неможливо було відстежити.

Також є актуальним SMS-фішинг – це метод фішинга способом SMS-посиланням та діє так само, як і інші види фішингу та може містити шкідливе посилання.

Є кілька ознак, за якими можна розпізнати спробу фішингу. Наприклад, у листі міститься пропозиція про виграш в лотерею, цінний приз або отримання коштів від далекого родича. Або тон повідомлення може бути тривожний. Офіційні представники банків та органів не використовують тривожний тон та прохання ввести свої дані. Будьте обережні, якщо електронного листа містить різкі або панічні вираження, які створюють відчуття терміновості, наприклад, якщо воно спонукає вас клацнути і негайно вжити заходів, щоб запобігти закриттю вашого профілю. Ще одним способом розпізнання може бути повідомлення, які містять несподівані або незвичайні вкладення. Такі вкладення можуть містити шкідливі програми, програми-вимагачі або інші типи мережевих погроз.

Що може визивати питання, так це повідомлення, що містить підозрілі посилання. Не довіряйте гіперпосиланнями, що містяться в електронних листах. Ви можете швидше навести курсор на посилання, щоб прочитати реальний URL. Слідкуйте за незначними орфографічними помилками на знайомих сайтах, оскільки вони є індикаторами шахрайства. Завжди рекомендується вводити URL самостійно, а не натискати на посилання в електронному листі.

Для того, щоб захистити себе від даних атак потрібно дотримуватися звичайних правил кібергігієни.

Кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації [3].

Є рекомендації, які допоможуть не стати жертвою фішингу:

Завжди перевіряйте посилання, які збираєтеся відкрити. Якщо ви помітили будь-які помилки, будьте особливо обережні, тому що кіберзлочинці можуть захотіти направити вас на підроблений веб-сайт.

Потрібно вводити своє ім'я користувача та пароль тільки в тому випадку, якщо ви абсолютно впевнені, що використовуєте безпечне з'єднання. Якщо перед URL-адресою стоїть «http», зверніть особливу увагу, тому щ цей сайт не має захищеного сертифікату. Якщо сайт має «https» протокол, який вказує на зашифроване з'єднання, то цей сайт є довіреним. Однак все більше хакерів вчаться використовувати протокол SSL там, де це можливо.

Не відкривайте електронні листи від невідомих відправників.

Ніколи не натискайте на посилання в електронному листі, якщо ніхто не знає адресат.

Для додаткового захисту, коли ви отримуєте електронного листа з джерела, який вважаєте небезпечним, вручну перейдіть за наданою посиланням, ввівши дійсний адреса веб-сайту до свого браузер.

Завжди рекомендується використовувати програмне забезпечення для захисту від шкідливих програм. Більшість інструментів кібербезпеки можуть виявляти помилкові вкладення або посилання, тому, навіть якщо вас обдурила добре сформульована фішинг, інструмент безпеки не дозволить вам поділитися своєю інформацією з неправильними людьми.

Якщо дотримуватися цих правил, ви можете уникнути фішингових загроз у кіберпросторі.

Перелік посилань

1. Поняття фішингу [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3
2. Основні правила кібергігієни [Електронний ресурс] – Режим доступу до ресурсу: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya
3. Історія виникнення фішингу [Електронний ресурс] – Режим доступу до ресурсу: https://science.donnu.edu.ua/wp-content/uploads/sites/6/2020/06/fishing.pdf