Ратушняк Сергій Сергійович
Національний університет «Одеська юридична академія»,
студент студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

МЕТОДИ ЗАХИСТУ ВІД ІНТЕРНЕТ-ФІШИНГУ

Фішинг – являє собою протиправне діяння, що здійснюється з метою змусити ту чи іншу особу поділитися своєю конфіденційною інформацією, наприклад паролем або номером кредитної картки. Сьогодні інформаційні технології розвинені настільки, що фішери можуть оволодіти потрібної їм інформацією практично без участі користувача. Інтерес зловмисників може викликати будь-яка інша конфіденційна інформація. Шахраї «вивуджують» дані користувачів під різними пристойними приводами: перевірка авторизації на сайті, необхідність «відписатися» від спаму в електронній пошті, оплата покупки за низькою ціною або з великою знижкою, необхідність встановити новий додаток.

Як працює інтернет-фішинг?

Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, e-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама. Користувач отримує пропозицію зареєструватися для отримання будь-якої вигоди або підтвердити свої персональні дані нібито для банківських або комерційних установ, клієнтом яких він є. Як правило, шахраї маскуються під відомі компанії, додатки соціальних мереж, сервіси електронної пошти. Електронна адреса відправника дійсно схожа на адресу знайомої користувачеві компанії. Наприклад, щоб замаскуватися під інтернет-магазин Aliexpress, шахраї шлють листи з адрес, що містять слово Alliexpress або Aliexxpress. Працює та сама схема, яка змушує людей купувати дешеві китайські кросівки таких «всесвітньо відомих брендів», як Pumma або Abibas.

Зловмисники користуються низьким рівнем обізнаності користувачів, зокрема, незнанням елементарних правил мережевої безпеки. Перш за все, організаторів фішинг-атак цікавлять персональні дані, які дають доступ до грошей, тому жертвами фішингу можуть ставати не тільки окремі люди, а й банки, електронні платіжні системи, аукціони.

Як розпізнати інтернет фішинг:

Фішингові сайти можуть ховатися за спливаючими вікнами. На них може вести таргетована реклама. Бувають ситуації, коли в графі «логін» користувач вже бачить адресу своєї електронної пошти, і йому пропонується всього лише ввести свій пароль в нижній графі.

Пропозиція залишити свої конфіденційні дані може виходити від ресурсу, який схожий на добре знайомий вам сайт, а насправді виявляється фішинговим. Шахраї створюють фішингові сайти з впізнаваним дизайном і схожим адресним рядком. Вони заманюють відвідувачів в фішингові інтернет-магазини шаленими знижками і низькими цінами. Після того, як людина вводить інформацію, необхідну для оплати товару за допомогою кредитної картки, інформація потрапляє до зловмисників.

Велика ймовірність побачити посилання на фішингових сайтів в коментарях на чужих сторінках або групах в соціальній мережі. Її також може надіслати вам друг або знайомий, чий акаунт вже зламали.

Як захиститися від інтернет-фішингу:

Захист від фішингу включає в себе дотримання кількох елементарних правил безпеки в інтернеті.

Перш за все слід пам'ятати що нікому і ні за яких обставин не можна передавати такі конфіденційні дані, як пін-код банківської картки, пароль електронної пошти або акаунтів в соціальних мережах. Ні банк, ні соціальна мережа не стануть запитувати ці дані по електронній пошті.

Установка ліцензійного програмного забезпечення. Захист від вірусів і хакерських атак на домашніх і робочих ПК може забезпечити тільки ліцензійна антивірусна програма, яку

потрібно своєчасно оновлювати. Перед установкою програм з Інтернету або реєстрацією на сервісах з введенням персональних даних слід уважно прочитати угоду користувача, оскільки одним з його умов може бути обробка та використання особистої інформації.

Слід завжди звертати увагу на дизайн сайту. Якщо сайт здається дивним, недопрацьованим, склепати нашвидкуруч або викликає якісь підозри, то дуже може бути, що це фішингових сайтів. Також слід звернути увагу на адресний рядок на засланні переходу. Незначні зміни в електронній адресі можуть привести вас на абсолютно інший сайт (наприклад, замість mail.ru може бути meil.ru).

Використання VPN при роботі з загальнодоступними точками Wi-Fi. Користуючись Інтернетом в готелі, на вокзалі або в кафе через Wi-Fi з'єднання, рекомендується включати VPN сервіс, що перенаправляє трафік на власний ресурс, видаючи «чистий» доступ, недоступний для незаконних маніпуляцій. Оскільки використання пароля не забезпечить повноцінний захист.

Правильно довіряти організацію захисту особистої інформації компаніям, що надають такі послуги. Вони володіють спеціальними методами захисту інформації і допоможуть підібрати індивідуальну систему безпеки в залежності від специфіки роботи компанії-замовника, типових загроз. Такі компанії організують захист відомостей в хмарному сховищі або на фізичному сервері.

Список використаних джерел:

1. Все о фишинге [Електронний ресурс] – Режим доступу до ресурсу: https://ru.malwarebytes.com/phishing/.

2. Острожно, фишинг [Електронний ресурс] – Режим доступу до ресурсу: https://applied-research.ru/ru/article/view?id=9077.

3. Как защититься от фишинга: 10 советов [Електронний ресурс] – Режим доступу до ресурсу: https://www.kaspersky.ru/blog/phishing-ten-tips/9744/.

4. Защита персональных данных в интернете [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/

resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-internete/.

Ключові слова: фішинг, шахрайство, фішингові сайти.
Ключевые слова: фишинг, мошенничество, фишинговые сайты.
Keywords: phishing, fraud, phishing sites.

Науковій керівник: *к.т.н., Бойко В. Д.*

Ревацкий Александр Алексеевич
Национальный университет «Одесская юридическая академия»,
студент 3-го курсу, факультета кибербезопасности
и информационных технологий

DOS/DDOS-АТАКА

Dos-атака *(Denial of Service* «отказ в обслуживании»*)* – это атака осуществлена хакерами на центральный сервер с целью довести его до отказа. Также существует **DDoS-атака** (*Distributed Denial of Service* «распределенный отказ в обслуживании») – данная атака выполняется посредством нескольких компьютеров, это могут быть сообщники, боты или даже девайсы людей, которые даже не подозревают что они, являются участником данной атаки. Также многие предпочитают этот вид атаки, чтобы было сложнее отследить атаку обратно к её источнику, так как она поступает с нескольких точек. Приведу пример на библиотеке:

Библиотекарь может помочь найти книгу за 5 минут только 1 клиенту, но если к нему обратятся еще 5 клиентов, тогда им придётся ждать. Если обратятся еще около 20 клиентов, то будет давление и он может ошибаться в выдаче книг и недовольные клиенты из-за ожидания, могут просто уйти в другую библиотеку. А библиотекарь потеряет клиентов.