УДК 004.056

Гаць Д.М.
Куперштейн Л.М.

ПОПЕРЕДЖЕННЯ ФІШИНГОВИХ АТАК НА ОСНОВІ ГЕЙМІФІКАЦІЇ

Вінницький національний технічний університет

Анотація

Проведено аналіз різних видів фішингових атак та їх статистику. Проаналізовано відомі підходи захисту від фішингових атак та розглянуто засіб попередження фішингових атак на основі гейміфікації.

***Ключові слова**: фішинг, кібербезпека, захист, навчання, гейміфікація.*

Abstract

This report analyzes different types of phishing attacks and their statistics. Known approaches to protection against phishing attacks are analyzed and means of preventing phishing attacks based on gamification are considered.

***Keywords**: phishing, cyber security, protection, learning, gamification.*

Вступ

У сучасному цифровому світі, де шахраї намагаються використовувати різноманітні маніпуляції для отримання доступу до особистої інформації та фінансових ресурсів, захист від фішингових атак є критично важливим завданням. Кожен день мільйони людей використовують Інтернет для здійснення операцій з банківськими рахунками та обміну особистими даними. Але разом зі зручністю та доступністю мережі з'являються й загрози, зокрема фішингові атаки, які можуть призвести до крадіжки інформації та фінансових втрат. Одним із способів забезпечення безпеки інтернет-користувачів є навчання за допомогою засобу попередження фішингових атак на основі гейміфікації.

Результати дослідження

В сучасному світі термін “фішинг” є дуже поширеним. Власне фішинг – це вид кіберзлочину метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних [1]. Шахраї виманюють у користувачів конфіденційну інформацію: від логінів та паролів поштових скриньок до інформації про банківські картки. При цьому можуть використовуватись різні способи: електронні листи, посилання в месенджерах та SMS, підроблені сторінки популярних онлайн-сервісів.

Варто зауважити те, що фішинг є найпоширенішою формою кіберзлочинності. Використання вкрадених облікових даних є найпоширенішою причиною витоку даних. За статистикою 91% всіх кібератак припадають на фішингові розсилки, а 70 % кібератак використовують комбінації фішингу та злому [2]. Також щодня надсилається 3,4 мільярда спам-повідомлень. Щодня Google блокує близько 100 мільйонів фішингових листів. Крім того понад 48% листів, надісланих у 2022 році, були спамом [2].

Фішингова атака може приймати різні форми, і хоча вона часто відбувається електронною поштою, існує багато інших підходів, які шахраї використовують для виконання своїх схем. Це особливо актуально сьогодні, коли фішинг продовжує розвиватися, часом дивуючи своєю різноманітністю та ступенем поширеності.

Фішинг електронною поштою – це найпоширеніший тип фішингової атаки. Кіберзлочинці

видають себе за компанії чи благодійні організації в електронному листі, пропонуючи потенційним жертвам клацнути посилання та ввести особисту інформацію або заплатити за щось [3].

Smishing – це коли кіберзлочинці відправляють текстові (SMS) повідомлення, видаючи себе за компанію чи благодійну організацію. Ці повідомлення працюють так само, як фішинг електронною поштою.

Vishing – це коли кіберзлочинці дзвонять своїм жертвам і намагаються отримати від них інформацію, таку як облікові дані або дані кредитної картки, по телефону [3].

Angler phishing – це коли кіберзлочинці використовують соціальні мережі для отримання інформації, щоб змусити цілі відвідати підроблений веб-сайт або завантажити зловмисне програмне забезпечення.

Китобійний фішинг - це форма цільового фішингу, при якому атаки спрямовані на керівників вищої ланки та високопоставлених менеджерів.

Фішингові атаки можуть завдати надзвичайні збитки як простим людям так і великим компаніям. Візьмемо для прикладу кілька відомих фішингових атак.

Наприкінці 2015 року FACC, аерокосмічна компанія, що спеціалізується на авіаційних компонентах і системах, втратила 47 мільйонів доларів після успішної китобійної атаки [2]. Кіберзлочинці видали себе за генерального директора FACC Волтера Стівена, надсилаючи електронного листа іншому співробітнику з проханням про переказ коштів для «проекту придбання». Фішингова атака була успішною, оскільки хакерам вдалося відтворити стиль написання Стівена, надавши повідомленню легітимність, щоб нічого не підозрюючий співробітник виконав його.

Сумнозвісна кібератака на Sony у 2014 році призвела до витоку 100 терабайт даних із великої індустрії розваг, а також завдала значної шкоди серверам і робочим можливостям [2]. У той час як зловмисне програмне забезпечення використовувалося для ексфільтрації даних та очищення серверів Sony, початковий доступ було надано через фішингові електронні листи, надіслані керівникам Sony.

І тому постає питання, як захистити себе чи свою компанію від фішингових атак?

Оскільки фішингові атаки активно застосовують соціальну інженерію, навчання користувачів (персоналу) є найважливішою стратегією захисту компанії. Якщо навчити персонал виявляти ознаки фішингових атак та час від часу проводити тренінги на цю тему або таємні імітації фішингових атак, то це забезпечить набагато кращий захист, ніж спеціалізовані програмні рішення.

Аргумент на користь навчання співробітників з питань кібербезпеки простий: якщо співробітники не знають, як розпізнати загрозу безпеці, то вони і не зможуть її уникнути чи повідомити про неї. Статистично 90-95% порушень кібербезпеки спричинені людськими помилками [4]. І це зовсім не означає, що співробітники, які потрапили в пастку, безвідповідальні. Вони роблять звичайні людські помилки — довіряють фальшивим особистостям, спокушаються “наживкою”, вразливі до інших тактик, які використовуються злочинцями для отримання доступу до інформації компанії. Але це трапляється, якщо вони не підготовлені до подібного, не брали участь у тренінгах та навчальних програмах з кібербезпеки.

Одним із перспективних способів захисту від фішингу може бути засіб попередження фішингових атак на основі гейміфікації. Він використовує елементи гри, щоб навчати користувачів розпізнавати фішингові атаки і вчасно виявляти шахраїв. Цей підхід залучає людей до активної взаємодії з інформацією про фішинг і надає їм навички, які допомагають уникнути шахрайства [5].

Засіб попередження фішингових атак на основі гейміфікації може включати різноманітні вправи, завдання і виклики, які користувачі повинні виконувати. Це може включати віртуальні симуляції фішингових атак, де користувачам потрібно розпізнавати підозрілі повідомлення електронної пошти або веб-сторінки. Такі симуляції можуть надавати навички аналізувати вміст, перевіряти URL-адреси, виявляти фальшиві доменні імена та інші ознаки фішингу.

Засоби попередження фішингових атак на основі гейміфікації мають кілька переваг порівняно з іншими методами [6]:

- можуть бути адаптовані для різних вікових категорій користувачів. Основний принцип гейміфікації полягає в тому, щоб зробити процес навчання та участі цікавим та захоплюючим для користувачів;
- Гейміфікація може зробити процес навчання та попередження фішингових атак більш захоплюючим і цікавим для користувачів. Шляхом використання гейміфікаційних елементів, можна створити відчуття конкуренції, співпраці та досягнення мети, що збільшить інтерес користувачів до процесу та їх бажання брати участь у ньому;
- Гейміфікаційні інструменти можуть забезпечити систему моніторингу та оцінки процесу навчання та захисту від фішингу. Адміністратори можуть отримувати дані про активність користувачів, їхні досягнення та слабкі місця, що дозволяє здійснювати аналіз та покращувати програму безпеки.

Враховуючи ці переваги, засоби попередження фішингових атак на основі гейміфікації можуть бути ефективним і привабливим варіантом для навчання користувачів та забезпечення їх захисту від фішингу.

Висновки

Під час дослідження було розглянуто проблему фішингових атак і розглянуто різні засоби захисту, спрямовані на попередження цих атак. Було проаналізовано статистику, яка свідчить про широке поширення фішингу в сучасному цифровому світі. Також представлено методи боротьби з фішингом, одним з яких є попередження фішингових атак на основі гейміфікації. На основі проведення дослідження можна зробити висновок, що використання такої технології, як гейміфікація забезпечує ефективну комбінацію освіти та розваги, що сприяє залученню уваги користувачів та активному навчанню. Крім того, гейміфікація може бути адаптована до потреб різних вікових груп, що робить її універсальним інструментом захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Phishing | What Is Phishing?. Phishing | General Phishing Information and Prevention Tips. URL: https://www.phishing.org/what-is-phishing (date of access: 15.06.2023).
2. The Latest Phishing Statistics (updated May 2023) | AAG IT Support. AAG IT Services. URL: https://aag-it.com/the-latest-phishing-statistics/ (date of access: 15.06.2023).
3. 20 types of phishing attacks + examples and prevention tips. Official Site | Norton™ - Antivirus & Anti-Malware Software. URL: https://us.norton.com/blog/online-scams/types-of-phishing (date of access: 15.06.2023).
4. Dakpa T., Augustine P. Study of Phishing Attacks and Preventions. International Journal of Computer Applications. 2017. Vol. 163, no. 2. P. 5–8. URL: https://doi.org/10.5120/ijca2017913461
5. Game-Based Learning, Gamification in Education and Serious Games. MDPI, 2022. URL: https://doi.org/10.3390/books978-3-0365-3809-9 (date of access: 15.06.2023).
6. Why Gamification is Important & Its Benefits. Spinify. URL: https://spinify.com/blog/why-gamification-is-important/#:~:text=You%20see,%20gamification%20increases%20user,and%20works%20for%20different%20industries. (date of access: 15.06.2023).

Гаць Дмитро Миколайович – студент групи 1БС-19Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: natzu.natzu2016@gmail.com

Dmytro Hats M - Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : natzu.natzu2016@gmail.com

Купершmейн Леонід Михайлович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: kupershtein@vntu.edu.ua

Kupershtein Leonid M — PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, kupershtein@vntu.edu.ua