*Список використаних джерел*

1. *https://coderlessons.com/articles/java/5-prichin-ispolzovat-jpa-hibernate*
2. *https://ru.bmstu.wiki/ORM_(Object-Relational_Mapping)#.D0.94.D0.BE.D1.81.D1.82.D0.BE.D0.B8.D0.BD.D1.81.D1.82.D0.B2.D0.B0*
3. *https://habr.com/ru/post/667078/*

**УДК 004.056.53:159.9**

*Діденко М.М., здобувачка 4 курсу*
*спеціальності 125 «Кібербезпека»*
*Крижановський В.Г., д.т.н., професор*
*кафедри інформаційних технологій*

## ПСИХОЛОГІЧНІ РИСИ ЛЮДИНИ, ЯКІ СПРИЯЮТЬ ЇЇ ВІДГУКУ НА ФІШИНГ

*Донецький національний університет імені Василя Стуса, м. Вінниця*

Чим швидше людство розвивається, чим більше новітніх пристроїв створюється – тим більше з’являється різноманітної цікавої інформації, до якої не кожна людина може мати доступ. Саме через це все частіше з’являються нові варіанти соціальної інженерії. Один з найпопулярніших методів являється фішинг.

Фішинг – техніка інтернет-шахрайства, що є спрямована на отримання конфіденційної інформації користувачів. Головним видом фітингових атак є підроблений лист, відправлений жертві по електронній пошті, який виглядає як лист від офіційної структури(платіжної системи, банку, компанії, тощо). У листі міститься форма для введення персональних даних (пін-код, логін і пароль і т.п.) або посилання на web-сторінки, де розташовується така форма [1-2]. Коли користувач вводить той же пароль і логін, щоб отримати доступ до «псевдо-сайту», шахрай отримує доступ до даних користувача, після чого може користуватись ними як забажає, в той час, як користувач може навіть і не подозрювати.

З метою захисту своїх користувачів від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування людей про те, що той чи той сайт є підозрілим та може належати шахраям. Найновіші версії браузерів уже мають функцію «Антифішинг». Не дивлячись на всі існуючі наразі застережні заходить величезна кількість сучасних інтернет-користувачів та користувачів соцмережами, месенджерами продовжує «вестися» на різноманітні підступні фішингові прийоми та стратегії

[3]. Тому виникає питання, які саме люди схильні до того, щоб відкрити той самий лист?

Психологічною передумовою застосування методів фішингу є така особливість людської психіки, як когнітивні упередження, а саме когнітивні упередження викривлення. Саме через це надійність комп'ютерної системи є не вищою, ніж надійність її оператора. Зловмисники проникають навіть у добре спроектовані, захищені комп'ютерні системи, скориставшись неуважністю довірених користувачів або умисно вводячи їх в оману [4]. Є низка упереджень, які «допомагають» витягнути шахраю інформації:

- Ефект неоднозначності — коли на вибір впливає нестача інформації, або «неоднозначність»;
- Якорування— упередження, яке описує звичайну схильність людей при прийнятті рішень надто сильно покладатися на перший запропонований шматок інформації;
- Евристика доступності— «скорочення шляху», яке спирається на безпосередні приклади, які приходять на думку певної людини при оцінці конкретної теми, концепції, методу або рішення;
- Ефект прокляття знання — упередження, коли краще поінформованим людям надзвичайно важко думати про проблему з точки зору менш поінформованих людей.

Не виключається й те, що людина могла відкрити даного листа через втому чи необачність (але вірогідність цього досить мала). Тому хто все ж таки відкриє даного листа притаманні такі риси: безвідповідальність, жадібність, байдужість, істеричність, неуважність, незнання, невпевненість(як у собі, так і в отриманій інформації), скупість, підступність, легковажність, невпевненість, егоїзм.

Неможливо, щоб всі ці риси характеру чи когнітивні упередження будуть присутні у цієї людини, але певна низка з них буде наявна. І саме завдяки цій певній низці соціальний інженер зможе отримати «доступ» до людини та таємної інформації. Всі організації зобов’язані мати захищені поштові та веб-шлюзи, які будуть сканувати електронні листи і фільтрувати їх, зменшуючи ймовірність того, що співробітник натисне на нього. Також необхідно стежити за оновленнями програмного забезпечення, відстежувати співробітників, які працюють з конфіденційною інформацією і забезпечити складнішу систему їх аутентифікації, проводити регулярні курси або тренінги з персоналом.

Варто пам’ятати, що для того, щоб не стати жертвою фішингу, слід дотримуватись наступної низки правил:

1. Завжди звертати увагу на адресу відправника. Одна неправильна літера, слово чи навіть крапка має насторожити отримувача і змусити стати уважним і не відкривати даного листа;
2. Якщо лист було отримано від офіційної структури, необхідно в першу чергу перевірити її домен;
3. Потрібно зачекати, оскільки більшість фінигових атак дезактивуються за 12 годин, у той час як дійсні листи залишаються набагато довше;

4. Якщо випадково з листа ви завантажили файл, то ні в якому разі неможна його відкривати і потрібно звернутись до фахівців;
5. Не варто переходити за підозрілими адресами. Вони можуть містити віруси та "спливаючі" вікна, які автоматично завантажують шкідливі програми на комп'ютер.

*Список використаних джерел*

1. *Махницький О.В. Використання соціальної інженерії для крадіжки особистих даних, 6 с.*
2. *Т. В. Нескородєва, В. Ю. Грущенко Детектування фішингових посилань Матеріали наукової конференції (2019–2020 рр.). URL:* ***https://jpvs.donnu.edu.ua/article/view/10424/***
3. *Фішинг. URL: https://cutt.ly/fN9jPpX (дата звернення: 06.11.2022)*
4. *Перелік когнітивних упереджень. URL: https://cutt.ly/qN1AAcJ (дата звернення: 06.11.2022)*

**УДК 004.056.5:343.97](477)**

*Єрмак Д.М., здобувач вищої освіти*
*Зелінська О.В., доцент,*
*доцент кафедри інформаційних технологій*

## ЗАХОДИ УКРАЇНИ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НАЦІОНАЛЬНОЇ ІНФОСФЕРИ ТА ПРОТИДІЇ ПРОЯВАМ КІБЕРЗЛОЧИННОСТІ

*Донецький національний університет імені Василя Стуса, м. Вінниця*

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи: Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки».

Сьогодні фахівці з кіберзахисту від ДССЗЗІ, СБ та МВС України стикаються у своїй роботі з численними труднощами, не маючи змоги самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному та кіберпросторі. Через це їм доводиться дедалі активніше шукати шляхи співробітництва з аналогічними організаціями світового співтовариства, використовуючи для цього всі наявні можливості й механізми, які є в розпорядженні кожної з країн [1].