УДК 159.922.7:004.056(043.2)

ПСИХОЛОГІЧНІ ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА СПРИЯТЛИВІСТЬ ДО ФІШИНГОВИХ АТАК

Олексій Жеребко

Національний авіаційній університет, Київ

Науковий керівник – Людмила Сидорчук, д-р. пед. наук, проф.

Ключові слова: фішингові атаки, кіберпсихологія, соціальна інженерія, психологічні тактики.

В епоху цифровізації, зі збільшенням числа користувачів інтернету, актуальність кіберпсихології суттєво зростає, особливо у контексті боротьби з кіберзагрозами, такими як фішингові атаки, які представляють собою вид соціальної інженерії з метою отримання конфіденційної інформації. Значущість дослідження психологічних аспектів фішингових атак обумовлена не тільки зростаючою кількістю таких інцидентів, але й розширенням спектра їх впливу на індивідів та організації.

Фішингові атаки – це оманливі спроби отримати конфіденційну інформацію, таку як імена користувачів, паролі та дані кредитної картки, видаючи себе за надійну особу в електронних комунікаціях [1]. Класифікація фішингових атак залежить від способів взаємодії з жертвою: від електронних листів і повідомлень до веб-сайтів, що імітують легітимні сервіси. Психологічні механізми, які лежать в основі успіху фішингових атак, включають маніпуляції з такими факторами, як довіра, цікавість, страх, жадібність та соціальний тиск, що спонукає індивідів до імпульсивних дій. Зловмисники активно використовують ці елементи, намагаючись впливати на психологію та емоції жертв, щоб спонукати їх виконати певні дії, часто на шкоду власним інтересам.

Серед найбільш поширених психологічних тактик, які використовуються в фішингових атаках, можна виділити:

1. Довіра та авторитет: спроби фішингу часто використовують людську схильність довіряти авторитетним особам або установам. Видаючи себе за законні організації, зловмисники маніпулюють цією довірою на свою користь [2].

2. Цікавість і терміновість: фішингові повідомлення можуть викликати відчуття терміновості або викликати цікавість через тривожні заяви чи пропозиції, які надто гарні, щоб бути правдою. Це може затьмарити судження та призвести до натискання шкідливих посилань або надання конфіденційної інформації [3].

3. Звикання: із збільшенням частоти цифрових комунікацій люди можуть звикнути, що призведе до менш критичного оцінювання кожного отриманого повідомлення. Це підвищує ймовірність попастися на фішингові афери [4].

4. Емоційна маніпуляція: емоції відіграють вирішальну роль у процесі прийняття рішень. Фішингові атаки часто використовують такі емоції, як страх, хвилювання чи цікавість, щоб переважити логічне мислення [5].

Психологічний вплив фішингових атак на жертв може бути глибоким і тривалим. Відчуття зради довіри, втрати контролю над особистою інформацією, а також потенційні фінансові втрати можуть спричинити розвиток стресових станів, анксіозності, а іноді й депресії. Важливою є робота з психологами для відновлення психологічного стану жертв, а також розробка стратегій відновлення довіри до цифрового простору.

Таким чином, до методів протидії фішинговим атакам можна віднести:

1. Освітні програми: систематична освіта користувачів щодо загроз кібербезпеки та методів їх виявлення є критично важливою. Освітні програми можуть включати інформацію про типові прийоми фішингу, способи розпізнавання підозрілих повідомлень та веб-сайтів, а також кроки, які слід вжити при виявленні фішингової спроби.

2. Розробка технічних засобів: технологічні рішення, такі як фільтри спаму, системи розпізнавання фішингу та безпечні браузери, можуть зменшити кількість фішингових атак, що досягають користувача. Однак жодна система не може бути абсолютно надійною, тому поєднання технічних засобів з освітніми програмами забезпечує кращий захист.

3. Підвищення кібергігієни: кібергігієна включає в себе набір простих правил поведінки в інтернеті, які можуть значно знизити ризик стати жертвою фішингу. Це включає не натискання на підозрілі посилання, використання двофакторної аутентифікації, регулярну зміну паролів та утримання від передачі конфіденційної інформації через незахищені канали.

4. Психологічна підтримка: важливою є психологічна підтримка жертв фішингових атак. Розробка програм підтримки та відновлення може допомогти людям подолати негативний вплив, який такі атаки можуть мати на їхнє емоційне становище та довіру до цифрового простору.

Кіберпсихологія відіграє ключову роль у розумінні та протидії фішинговим атакам, оскільки багато з цих атак спираються на психологічні механізми. Комбінування освітніх програм, технічних засобів, зміцнення кібергігієни та психологічної підтримки може створити більш безпечне цифрове середовище. Однак, враховуючи постійну еволюцію кіберзагроз, важливо продовжувати дослідження та розробку нових методів захисту та освіти для адаптації до змінюваного ландшафту кібербезпеки.

Список використаних джерел:

1. Botelho, Christopher M., and Joseph A. Cazier. "Guarding Corporate Data from Social Engineering Attacks." In Handbook of Research on Information Security and Assurance, 423–32. IGI Global, 2009. URL: http://dx.doi.org/10.4018/978-1-59904-855-0.ch037(Last accessed:14.03.2024).

2. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails / M. Butavicius et al. AIS eLibrary. URL: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1097&context=acis2015 (Last accessed:15.03.2024).

3. Jayatilaka A., Ali Babar M., Arachchilage N. Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors. https://www.ndss-symposium.org/wp-content/uploads/usec2024-72-paper.pdf. URL: https://www.ndss-symposium.org/wpcontent/uploads/usec2024-72-paper.pdf (Last accessed:15.03.2024).

4. Baki S., Verma R. Sixteen Years of Phishing User Studies: What Have We Learned?. ResearchGate. URL: https://www.researchgate.net/publication/354542932_Sixteen_Years_of_Phishing_User_Studies_What_Have_We_Learned (Last accessed:15.03.2024).

5. Jari M. An Overview of Phishing Victimization: Human Factors, Training and the Role of Emotions. Computer Science and Information Technology. 2022. Vol. 12, no. 13. URL: https://aircconline.com/csit/papers/vol12/csit121319.pdf (Last accessed:16.03.2024).