

Огороджувальна споруда ефективна і відрізняється від попередньої тим, що захисний хвилеломний зуб встановлений від стіни на відстані, що визначається нерівністю $d/4 < l < d/2$, де d – відстань між стіною та периметром зони розміщення резервуара. До того ж, висота зуба відповідає переділу співвідношень $H/10 < H/4$, де H – висота резервуара. Зуб також може бути виконаний у вигляді ромбоподібного розсікача з кутом ромба $5 < \alpha < 80$.

1. Російські війська масово бомбардують нафтобази. Що робить Україна, щоб у фермерів, військових та населення було пальне / УЗА. URL : <https://uga.ua/meanings/rosijski-vijska-masovo-bombarduyut-naftobazi-shho-robit-ukrayina-shhob-u-fermeriv-vijskovih-ta-naselennya-bulo-palne/> (23.02.2024).

2. Удар по нафтобазі у Харкові: один із «Шахедів» влучив у захисну споруду / Укрінформ. URL : <https://www.ukrinform.ua/rubric-regions/3827312-udar-po-naftobazi-u-harkovi-odin-iz-sahediv-vluciv-u-zahisnu-sporudu.html> (23.02.2024).

3. ВБН В.2.2-58.1-94 «Проектування складів нафти і нафтопродуктів з тиском насичених парів не вище 93,3 кПа»

УДК 316.648.4

DOI: 10.31733/15-03-2024/2/509-510

Діана БОРЕЙКО

студентка ННІ права
та інноваційної освіти

Світлана НАСОНОВА

доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАСІБ ЗДІЙСНЕННЯ ПСИХОЛОГІЧНИХ АТАК

У наш час велика кількість людей несвідомо потрапляє в оману психологічних атак, здійснених методами соціальної інженерії. Адже, поняття соціальна інженерія являє собою вплив на людину за допомогою психологічних факторів, таких як маніпуляція довірою або ж людськими страхами.

Мета соціальної інженерії полягає у використанні маніпуляційних та психологічних стратегій, аби отримати від людини велику кількість інформації, яка згодом може бути використана для незаконних цілей проти особистості [1].

У соціальній інженерії використовують різноманітні техніки, спрямовані на досягнення поставлених цілей, через виявлення та використання помилок у поведінці людини. Однією з таких технік є фішинг. Його використовують для збору конфіденційної інформації (паролів, логінів, пін-кодів) шляхом розсилки листів та спаму на електронну адресу, що спонукають жертву повідомити інформацію, необхідну для шахраїв. Прекстинг поглядає в тому, щоб виглядати як інша особа або ж популярна компанія, аби отримати бажану інформацію через дзвінки або sms-повідомлення [2]. Подібним до фішингу є вішинг, але на цей раз дана афера полягає в імітуванні дзвінків на мобільний телефон, наче телефонує оператор із банку. Тобто, цей спосіб дає змогу жертві надати шахраям дані своєї картки (CVV) для списання всіх коштів з рахунку [3].

Зазначені вище психологічні атаки побудовані на вимушені жертви розкрити важливі дані або виконати дії, що згодом можуть привести до втрати коштів, секретної інформації тощо. Більшість таких махінацій розраховані на довірливих та необачних користувачів, які під впливом психологічного тиску здійснюють помилки, які дозволяють шахраям їх ошукати.

Задля того, аби не потрапити в таку ситуацію слід бути дуже уважним. Ось кілька правил, яких потрібно дотримуватись:

1. Перевірка джерел та веб-сайтів: перш ніж вводити особисті дані переконайтесь, що адреса відправника відповідає вказаній компанії в надісланому листі. Краще перевірити

SSL-сертифікат та доменне ім'я сайту на наявність будь-яких змін.

2. Уникати сумнівних ресурсів: не відкривати файли та не переходити на посилання з листів невідомих або підозрілих джерел. Це може призвести до завантаження шкідливих програм чи вірусів.

3. Використовувати різні паролі: важливо мати різні паролі для особистих аккаунтів, соціальних мереж та банківських додатків. Це допомагає захистити ваші дані у випадку злому [4].

Ці поради є лише початковою точкою для забезпечення особистої безпеки в кіберпросторі. Але при дотриманні їх під час користування Інтернетом, можна значно поліпшити свій рівень захисту від психологічних атак, здійснених методами соціальної інженерії та знати, які дії не слід виконувати, якщо жертвою кіберзлочинців стали саме ви.

Таким чином, можна сказати, що соціальна інженерія є технікою, яка демонструє всю потужність людської психології в нашому світі. Цей метод зловживання використовує людські слабкості для здійснення маніпуляцій з метою отримання конфіденційної інформації чи впливу на прийняте рішення.

Отже, вкрай важливо знати основні правила кібербезпеки, щоб не стати жертвою кіберзлочинців.

1. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті (Тетяна Савчук). URL : <https://www.radiosvoboda.org/amp/socialna-inzhenerija-shaxrajstvo/29460139.html>.

2. Соціальна інженерія – що це таке? (UKEY). URL : <https://ukeywaf.com/baza/socjalna-inzheneriya/>.

3. Соціальна інженерія: виклики та перспективи боротьби в українському контексті URL : https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/.

4. Соціальна інженерія URL : <https://blog.portmone.com.ua/uk/posts/information-posts-uk/sotsialna-inzheneriya?amp#title-10>.

УДК 614.88+351.74

DOI: 10.31733/15-03-2024/2/510-511

Катерина БОРИСОВА
курсант факультету № 4

Віталій СВІТЛИЧНИЙ
доцент кафедри протидії
кіберзлочинності факультету № 4
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОПТИМІЗАЦІЇ НАДАННЯ ПОЛІЦЕЙСЬКИМИ ДОМЕДИЧНОЇ ДОПОМОГИ

Відповідно до статті 12 Закону України «Про екстрену медичну допомогу» особами, які зобов'язані надавати домедичну допомогу людині у невідкладному стані, є поліцейські [1].

В контексті сучасних вимог до надання медичної допомоги, актуальності набуває питання оптимізації процесів надання домедичної допомоги поліцейським, адже з початком повномасштабного вторгнення росії на нашу територію, розгортанням агресії по відношенню до українців постало питання удосконалення системи захисту здоров'я населення. Інформаційні технології, що розглядаються як інструменти для підвищення ефективності та оперативності, на нашу думку, є факторами першочергової необхідності для надання допомоги. Тому ми переконані, що вчені та практики повинні зосередити увагу в цьому надважливому напрямку, та докласти зусилля до аналізу та популяризації питання використання.

Використання сучасних інформаційних засобів, таких як мобільні додатки та автоматизовані системи, може суттєво поліпшити якість та швидкість реагування