**Оксана Плигань**

**(Біла Церква, Україна)**

**СОЦІАЛЬНА ІНЖЕНЕРІЯ: ЯК ШАХРАЇ МАНІПУЛЮЮТЬ ЛЮДЬМИ В КІБЕРПРОСТОРІ**

У сучасному цифровому світі технології розвиваються швидше, ніж засоби їхнього захисту. Попри складні системи шифрування, антивіруси та фаєрволи, кіберзлочинці знайшли спосіб облаштувати навіть найсучасніші засоби захисту — через людину. Саме людський фактор є найвразливішою ланкою в системах безпеки, і методи соціальної інженерії спрямовані на його використання.

Соціальна інженерія — це мистецтво маніпуляції людьми з метою отримання конфіденційної інформації, доступу до систем або ресурсів без необхідності застосування технічного злочину. Це одна з найефективніших форм кібератак, після чого вона не вимагає складних програмних засобів або технічних знань. Достатньо лише переконати людину надати доступ або розкрити важливі дані, і хакер може отримати контроль над системою. [1]

На відміну від традиційних методів злому, соціальна інженерія використовує не слабкі місця програмного забезпечення, а психологічні особливості людини: довіру, страх, цікавість, поспіх, бажання допомогти або навіть жадібність. Наприклад, працівник може отримати лист від нібито керівника з проханням надіслати важливі файли або перейти за посиланням для "термінового оновлення пароля". Довіряючи авторитету, він виконує запит, що може призвести до витоку даних або компрометації у всій системі. [1]

Методи соціальної інженерії активно застосовуються не лише проти окремих користувачів, а й проти великих компаній, банківських установ, урядових організацій. Масштабні кібератаки починаються з простих дій — шахраї можуть зателефонувати в IT-відділ компанії, представити технічного спеціаліста і попросити надати тимчасовий доступ до серверів. Також досвідчені фахівці можуть стати жертвами, якщо не будуть обережними.

У цій статті ми розглянемо найпоширеніші методи соціальної інженерії, реальні приклади атаки, причини їх ефективності та основні способи захисту від подібних загроз.

Соціальна інженерія включає широкий спектр тактик, спрямованих на маніпуляцію людьми для отримання конфіденційної інформації або доступу до системи. Розглянемо найпоширеніші методи, які задають кіберзлочинці.

Фішинг — це шахрайський метод, коли зловмисник віддає себе за довірену особу або організацію, щоб змусити жертву розкрити паролі, банківські реквізити або інші особисті дані. Також реалізується через електронні листи, підроблені вебсайти або повідомлення в месенджерах. [4]

**Як же це працює?**

* Жертва отримує лист, який виглядає як офіційне повідомлення від банку поштової служби, соціальної мережі або користувача.
* Список містить посилання на підроблений сайт або вкладений файл із вірусом.
* Користувач вводить свої дані або відкриває завантажений файл, після чого зловмисник отримує доступ до його електронного запису чи пристрою.

Щоб захиститися, потрібно завжди перевіряти адресу відправника та URL-посилання, не відкривати негативні вкладення, використовувати багатофакторну автентифікацію (2FA).

Наступні - с**мішинг (Smishing) і вішинг (Vishing).**  
Це різновиди фішингу, але через інші канали зв'язку:

* **Смішинг (SMS-фішинг)** — шахрайство через SMS або месенджери.
* **Вішинг (Voice-phishing)** — телефонне шахрайство.

**Наприклад, л**юдині телефонує «співробітник банку» й повідомляє, що з її рахунку намагаються списати гроші. Щоб «заблокувати» операцію, жертва має продиктувати SMS-код, який фактично використовується для входу в її акаунт.

Щоб не стати жертвою, слід дотримувався простих правил:

* Не довіряти незнайомим номерам.
* Передзвонювати в банк чи компанію самостійно через офіційний номер.
* Не повідомляти коди підтвердження навіть банкам.

### **Байтінг - це** атака, що використовує цікавість або жадібність жертви. Шахраї розповсюджують заражені файли або фізичні носії (наприклад, флешки) з привабливими назвами.

**Можливий алгоритм атаки:**

* Жертва містить USB-накопичувач із записом «Зарплатна інформація» або «Конфіденційно».
* Вставляє його в свій комп'ютер, після чого шкідливе програмне забезпечення отримує доступ до системи.
* Або ж людина завантажує «безкоштовний» фільм, програму, музику, разом із якими встановлено вірус.

Наприклад, компанія помічає витік даних після того, як один із співробітників підключив знайдену флешку в офісі.

**Щоб захиститися, не** використовуйте незнайомі флешки або файли з ненадійних джерел, слід встановити антивірус і заблокувати автозапуск носіїв.

Передтекст — це маніпуляція, коли шахрай створює правдоподібну легенду, щоб отримати інформацію.

**Як працює?**

* Зловмисник може представити співробітника компанії, журналісту або навіть колезі.
* Використовує знання про жертву, щоб витягти довіру.
* Просити розкрити пароль, особисті дані або виконати певну дію.

**Приклад:**  
Шахрай телефонує в компанію, видаючи себе для ІТ-адміністратора, і просить співробітників назвати пароль для оновлення системи.

**Як захиститися?**

* Перевіряти особу співрозмовника через офіційні канали.
* Не розголошувати конфіденційну інформацію телефоном або через email.

### **Підйом і контрейлерний транспорт -** це методи фізичного доступу до об'єктів.

* **Tailgating** — шахрай проходить за працівником у захищену зону, не маючи доступу.
* **Piggybacking** — працівник сам дозволяє шахраю ввійти, думаючи, що це колега або відвідувач.

**Як працює?**

* Зловмисник може нести коробки або каву, щоб людина ввічливо відчинила двері.
* Віддає себе за кур'єра, ремонтника, нового працівника.

**Наприклад:** шахрай проходить в офіс, користуючись відкритими дверима, і краде документи або підключається до мережі.

**Як захиститися?**

* Використовувати картковий доступ.
* Не відкривати двері незнайомцям [3].

Соціальна інженерія залишається однією з найнебезпечніших загроз у сфері інформаційної безпеки. На відміну від традиційних кіберзагроз, що базуються на вразливостях програмного забезпечення, вона використовує людські емоції, довіру та неважливість. Саме тому такі атаки є ефективними та часто навіть успішними проти добре захищених систем [2].

Розглянуті методи — фішинг, смішинг, вішинг, байтінг, передтекстинг, tailgating та piggybacking — демонструють, наскільки легко шахраї можуть змусити людей добровільно передавати конфіденційну інформацію або надавати доступ до важливих ресурсів. Кіберзлочинці постійно вдосконалюють свою тактику, використовуючи соціальні мережі, підроблені сайти, телефонні дзвінки та навіть фізичні методи проникнення [2].

Основний захист від соціальної інженерії — це не лише технічні засоби, а й підвищення обізнаності користувачів. Навчання безпечної поведінки в цифровому середовищі, критичне мислення та постійна перевірка будь-яких запитів на конфіденційність значно знижують ризики атак.

Компанії та організації повинні впроваджувати політику інформаційної безпеки, проводити тренінги для співробітників, використовувати багатофакторну автентифікацію та суворо контролювати доступ до важливих даних.[5]

Загалом, соціальна інженерія доводить, що безпека в цифровому світі залишається не лише від технологій, а й від рівня обізнаності кожного користувача. Тільки поєднання технічних рішень і людської пільги може забезпечити ефективний захист від цієї загрози.

**Література:**

1. Г**рей Джо** «Соціальна інженерія та етичний хакінг на практиці». – Видавництво: Book-Shop, 2023. – 228 с.

2. . **А. А. Мельниченко** «Соціальна інженерія як фактор забезпечення стійкого розвитку соціальної системи» // Вісник НТУУ «КПІ». Політологія. Соціологія. Право. – 2012. – № 1. – С. 35-40.

3. **Є.І. Суіменко** «Соціальна інженерія. Експериментальний курс лекцій: навчальний посібник». Київ, Україна: Науково-видавнича рада НАНУ, 2011- 224 с.

4. М. О. Шатковський, (2015). Вплив соцiальної iнженерiї на iнформацiйну безпеку організацій. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. Київ : НТУУ «КПІ», 216-219.

5. Ю. М Якименко, Д. І Рабчун, М. М. Запорожченко, (2021). Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти. Кібербезпека: освіта, наука, техніка, 1 (13). DOI 10.28925/2663-4023.2021.13.615