Альтернативна практична вправа:
«Захист від фішингових атак»

Навчальна мета заняття: ознайомлення з принципами фішингових атак та протидії ним.

Час проведення: 1 год. *Місце проведення:* комп'ютерний клас.

Устаткування:
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено.**

Фішинг (англ. *fishing* – рибна ловля) – одержання доступу до конфіденційних даних користувачів, що досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Twitter, Instagram), банків (Приватбанк, Ощадбанк), інших сервісів (Google.com). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів, тощо.

Фейк (Fake) – точна копія головної сторінки (або будь-якої іншої сторінки) оригінального сайту, яка використовується для фішингу з метою отримання конфіденційних даних користувачів.

Для демонстрації техніки фішингу можуть бути використані кілька способів. Скористаємося одним з них.

1. Створити фейкову сторінку.
Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);
- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html.

2. Для розміщення сторінки в мережі слід завантажити утиліту ngrok. Для роботи з утилітою ngrok слід зареєструватися та отримати токен відповідно до інструкції (https://dashboard.ngrok.com/get-started/setup).
Запустити її з командного рядка:

ngrok http 80

Завантажити набір Uniform Server для створення та управління сайтами та привести його у готовність.

Створити в папці UniServerZ\www каталог з назвою сайту скопійованої сторінки.

Розмістити в папці www/назва_сайту скрипти сайту.
Запустити UniController (рис. 1).

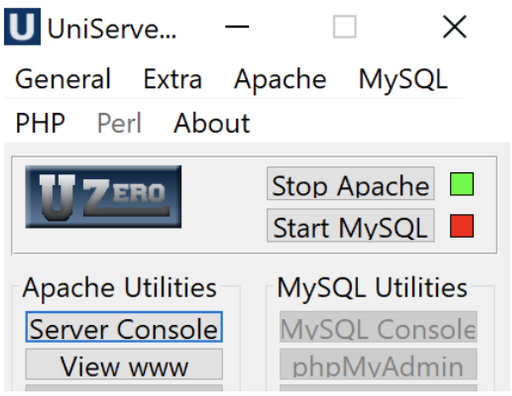

Рис. 1. Запуск Uniform Server

Перевірити роботу сайту.

Одним з додаткових інструментів фішингу може бути телефонування жертві з підміненого номера (Caller ID Spoofing), приклад налаштування та результат якого зображено на рис. 2.

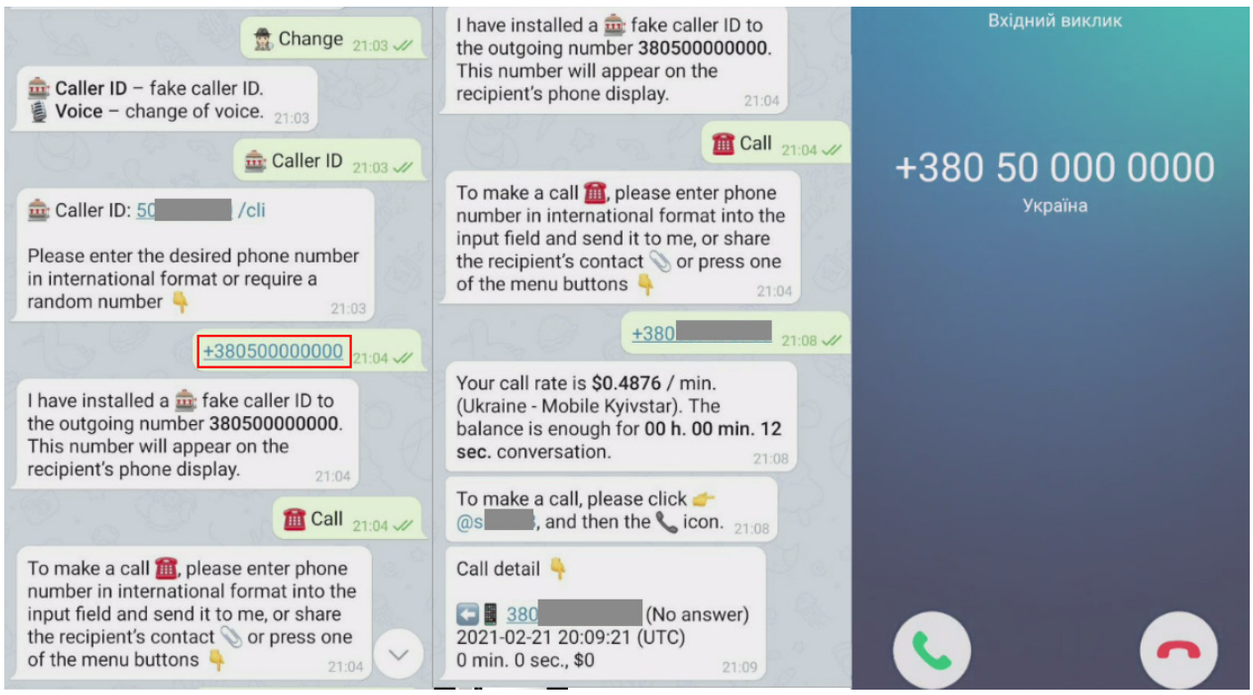

Рис. 2. Caller ID Spoofing

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти повідомлення, які надходять, та користуватись антифішинговими інструментами. Відповідні інструменти нерідко вбудовано у браузери.