**PRÁCTICA N°4**

**TEMA: “PREVENCIÓN DE ATAQUES DE INGENIERIA SOCIAL Y SEGURIDAD EN EL ACCESO”**

**1. OBJETIVOS**

1.1 Personalizar y configurar una simulación de ataque de phishing en un entorno controlado.

1.2 Implementar una campaña de concientización y entrenamiento para prevenir ataques de phishing.

1.3 Establecer factores adicionales de autenticación.

**2. PREPARATORIO**

***2.1 Consultas que es la Ingeniería Social y como se aplica hacia las personas?***

La ingeniería social es un método utilizado por atacantes para manipular de manera psicológica a las personas con el único fin de obtener información confidencial, acceso a sistemas o realizar acciones específicas. La ingeniería social explota la confianza de los individuos [1].

A las personas se aplica de diferentes maneras como:

**Manipulación:** Los atacantes se hacen pasar por figuras de autoridad, técnicos de soporte o incluso amigos para engañar a las victimas y que estas revelen información sensible [1].

**Persuasión:** Utilizan métodos de persuasión como la creación de un sentido de urgencia o miedo para que actúen sin pensar [1].

**Engaño:** Envían correos o mensajes falsos que parecen legítimos para obtener credenciales, información personal o acceso a sistemas [1].

***2.2 Investigar que es un ataque de phishing y como afecta a los usuarios finales?***

El phishing es un tipo de ataque de ingeniería social usando la técnica de engaño donde los atacantes envían correos electrónicos que parecen ser de fuentes confiables con el único objetico de engañar a la victima y obtener datos bancarios, usuarios o contraseñas [2].

Esta clase de engaño afecta a los usuarios de manera económica o confidencial dado que tiene accesos a cuentas bancarias, a sistemas confidenciales o a datos sensibles [2].

***2.3 Enumerar que tipos de factores de autenticación existen y porque son importantes? (mínimo 3)***

Al utilizar los factores de autenticación se puede tener el control de acceso a sistemas, permitiendo al usuario comprobar su identidad para tener autorización de ingreso a dicho sistema [3].

Esto reduce el riesgo de accesos no autorizados y evita el robo de información confidencial o de explotación de ataques dentro de un sistema [3].

Se puede tener varios factores de autenticación como:

1. El conocimiento de algo como PINs, contraseñas, tokens entre otros.
2. Posesión: Tokens Físicos, Celulares, entre otros.
3. Inherencia: características biológicas, huellas dactilares reconocimiento facial, etc [3].