# TFM

# Estudio de fraudes basados en la técnica de Ingeniería Social


- **Autor:** Julen Alzas Hernandez
- **Área:** Seguridad empresarial
- **Tutora:** Angela María García Valdés
- **Responsable:** Victor Garcia Font


- **Fecha de entrega:** 09/06/2023


Universitat Oberta
de Catalunya

## FICHA DEL TRABAJO FINAL

| | |
|---|---|
| **Título del trabajo:** | *Estudio de fraudes basados en la técnica de Ingeniería Social* |
| **Nombre del autor:** | *Julen Alzas Hernandez* |
| **Nombre del consultor/a:** | *Angela María García Valdés* |
| **Nombre del PRA:** | *Victor Garcia Font* |
| **Fecha de entrega (mm/aaaa):** | *06/2023* |
| **Titulación o programa:** | Máster universitario de Ciberseguridad y Privacidad |
| **Área del Trabajo Final:** | *Seguridad empresarial* |
| **Idioma del trabajo:** | *Castellano* |
| **Palabras clave:** | *Ingeniería social, ciberseguridad, concienciación.* |


**Resumen del Trabajo**

El Trabajo de Fin de Máster (TFM) se enfoca en la ingeniería social, una táctica utilizada por los ciberdelincuentes para obtener información confidencial de las personas. La investigación tiene como objetivo comprender los conceptos y técnicas relacionados con la ingeniería social, identificar los métodos utilizados por los ciberdelincuentes para llevar a cabo ataques de ingeniería social y analizar la información que pueden obtener mediante estas técnicas. También se investigan buenas prácticas para evitar ser víctima de estos ataques y las consecuencias legales para los infractores.

En la implementación, se instalan y configuran las herramientas necesarias para llevar a cabo pruebas de ataques de ingeniería social, se aprende a utilizarlas y se realizan simulaciones de ataques relacionados con ésta. El número de ataques simulados variará dependiendo del tiempo disponible.

La finalidad del trabajo es sensibilizar a aquellos que aún no consideran importante la ingeniería social, y que puedan juzgar por ellos mismos la importancia de tener en cuenta este tipo de ataques. La metodología empleada es investigativa y experimental, con resultados que permiten identificar las herramientas y técnicas utilizadas por los ciberdelincuentes para llevar a cabo ataques de ingeniería social.

En conclusión, el trabajo pretende ayudar en la concienciación sobre la importancia de la ciberseguridad y la necesidad de estar informados sobre los riesgos de la ingeniería social.

**Abstract**

The Master's Thesis (TFM) focuses on social engineering, a tactic used by cybercriminals to obtain confidential information from individuals. The research aims to understand the concepts and techniques related to social engineering, identify the methods used by cybercriminals to carry out social engineering attacks and analyze

the information they can obtain through these techniques. Good practices to avoid becoming a victim of these attacks and the legal consequences for violators are also investigated.

In the implementation, we install and configure the necessary tools to carry out tests of social engineering attacks, learn how to use them and perform simulations of related attacks. The number of attacks simulated will vary depending on the time available.

The purpose of the work is to raise awareness among those who still do not consider social engineering important, so that they can judge for themselves the importance of taking into account this type of attacks. The methodology used is investigative and experimental, with results that allow identifying the tools and techniques used by cybercriminals to carry out social engineering attacks.

In conclusion, the work aims to help raise awareness of the importance of cybersecurity and the need to be informed about the risks of social engineering.

# Índice


**1. Introducción** **1**

1.1. Contexto y justificación del Trabajo 1

1.2. Objetivos del Trabajo 1

1.3. Impacto en sostenibilidad, ético-social y de diversidad 2

1.4. Enfoque y método seguido 5

1.5. Planificación del Trabajo 6

1.6. Planificación detallada de estas tareas y sus dependencias 8

1.7. Análisis de riesgos 10

1.8. Estado del arte 11

1.9. Historia del arte 12

1.10. Tipologías de ataques 13

1.11. Breve descripción de los otros capítulos de la memoria 14

**2. Recolección de información** **15**

2.1. ¿Qué es la ingeniería social? 15

2.2. ¿Qué roles intervienen en la ingeniería social y cuáles son sus características? 15

2.3. ¿Cuáles son los principales tipos y métodos utilizados en la ingeniería social? 16

2.4. ¿Cuál es el modus operandi de los cibercriminales? 17

2.5. ¿Cual es la motivación de los ciberdelincuentes? 25

2.6. ¿Qué técnicas utilizan los cibercriminales, y cómo la explotan para obtener beneficios? 25

2.7. ¿Cómo podemos evitar ser engañados mediante ingeniería social? 29

2.8. ¿Qué tipo de información pueden llegar a obtener los ciberdelincuentes? 31

2.9. ¿Cómo pueden los cibercriminales obtener beneficios sobre la información obtenida? 34

2.10. A nivel legal, ¿esta serie de actuaciones están perseguidas por la Ley? 36

**3. Fase de implementación** **39**

3.1. Phishing: 39

3.2. OSINT: 51

3.3. IA: 54

**4. Conclusiones y trabajos futuros** **65**

4.1. Conclusiones Finales 65

4.2. Seguimiento de la planificación establecida 66

4.3. Problemas encontrados en la implementación del proyecto 66

4.4. Evaluación de objetivos alcanzados 67

4.5. Trabajo Futuro 67

**5. Glosario** **69**

**6. Bibliografía** **72**

**7. Anexos** **74**

# Lista de figuras

Ilustración 1: Categorización principal de la Ingeniería Social 16
Ilustración 2: Categorización según la forma de llevarlo a cabo 16
Ilustración 3: Categorización completa con ejemplos 17
Ilustración 4: Fases de la Ingeniería social 17
Ilustración 5: Estructura básica OSINT 19
Ilustración 6: Tipos de ataques de Phishing 26
Ilustración 7: Tácticas comunes de ataques phishing 26
Ilustración 8: Página web UOC clonada en local 39
Ilustración 9: Inicio de Sesión de la UOC clonada en local 40
Ilustración 10: Opciones de la interfaz gráfica de Gophish 42
Ilustración 11: Configuración de Gophish - Sending Profiles 43
Ilustración 12: Configuración de Gophish - Landing Pages 43
Ilustración 13: Email Templates - Crear Plantilla 1 44
Ilustración 14: Email Templates - Crear Plantilla 2 44
Ilustración 15: Email Templates - Editar plantilla 45
Ilustración 16: Configuración de Gophish - Users & Groups 46
Ilustración 17: Configuración de Gophish - Users & Groups 47
Ilustración 18: Mensaje de llegada a la víctima 47
Ilustración 19: Menú Phishing Zphisher 48
Ilustración 20: Zphisher elegir opción 48
Ilustración 21: Zphisher elegir servicio 48
Ilustración 22: Zphisher phishing Instagram 49
Ilustración 23: Zphisher Cloudflared 49
Ilustración 24: Zphisher Cloudflared URLs 49
Ilustración 25: Zphisher - Recolección de datos 50
Ilustración 26: QR Malicioso 50
Ilustración 27: Seeker - Atacante 51
Ilustración 28: Seeker Víctima 51
Ilustración 29: Seeker - Datos obtenidos 52
Ilustración 30: TheHarverster 53
Ilustración 31: DALL·E - Input  para perfil falso 54
Ilustración 32: DALL·E - Resultado para perfil falso 54
Ilustración 33: ChatGPT - Pie de foto para Instagram 55
Ilustración 34: Post de Instagram basado en ChatGPT 55
Ilustración 35: ChatGPT - Pretexting 56
Ilustración 36: ChatGPT - Pretexting 2 56
Ilustración 37: Video luisito editado - Deepfake 57
Ilustración 38: Video atado Anton - Deepfake 58
Ilustración 39: Resultados deepfake 1 58
Ilustración 40: Video de arma - Deepfake 58
Ilustración 41: Resultados deepfake 2 59
Ilustración 42: Deepfake entrenado 11 horas 59

Ilustración 43: Clonación de voz - Herramienta 1 61
Ilustración 44: Voice.ai - Config 1 62
Ilustración 45: Voice.ai - Config 2 62
Ilustración 46: Tortoise-TTS - Config. archivos 63
Ilustración 47: Captura FIN de entrenamiento del modelo 63
Ilustración 48: So-vits-svc-fork - Config. archivos 64

# Lista de tablas

Tabla 1: Planificación 7
Tabla 2: Diagrama gantt 8
Tabla 3: Diagrama gantt - PEC1 9
Tabla 4: Diagrama gantt - PEC2 9
Tabla 5: Diagrama gantt - PEC3 10
Tabla 6: Diagrama gantt - PEC4 10
Tabla 7: Listado de Flags de un SECTF 33
Tabla 8: Ciberdelitos en el Código Penal 38

# 1. Introducción

## 1.1. Contexto y justificación del Trabajo

La Ingeniería social es una táctica que utilizan los delincuentes cibernéticos para obtener la confianza del usuario y persuadirlo para que realice acciones bajo su influencia y engaño dónde la motivación general suele surgir del beneficio económico. Por ejemplo, esto puede incluir la ejecución de un programa malicioso, la divulgación de claves privadas o la compra en sitios web fraudulentos.

Por tanto, la ingeniería social se refiere a la manipulación de las personas para que revelen información confidencial, descarguen software malicioso, visiten sitios web peligrosos o cometan otros errores que comprometan su seguridad personal o empresarial. Los ciberdelincuentes utilizan tácticas de ingeniería social para obtener datos personales como credenciales de inicio de sesión, números de tarjeta de crédito y números de seguridad social, que luego pueden utilizar para cometer fraudes financieros. Un ataque de ingeniería social también puede ser la primera fase de un ciberataque a mayor escala. Los ciberdelincuentes prefieren este método porque les permite acceder a redes, dispositivos y cuentas digitales sin tener que pasar por los controles de ciberseguridad tradicionales. Los ataques de ingeniería social son costosos para las empresas, con un coste medio de 4,47 millones de dólares por filtración de datos según un informe de IBM de 2021.

Según el informe de KnowBe4, sobre estadísticas de ataques informáticos, los ciberdelincuentes robaron credenciales de acceso en el 85% de las infracciones relacionadas con la ingeniería social. Asimismo, entre las 23.400 organizaciones y 6.6 millones de usuarios que participaron en el estudio, el porcentaje de caer ante un ataque de phishing fué del 31.4%. Lo que deriva en que más de 2 millones de empleados (uno de cada tres) probablemente hicieron clic en un enlace o correo electrónico sospechoso o cumplió con una solicitud fraudulenta. Cabe recalcar que este dato fué obtenido con anterioridad a implantar formación anti-phishing, y que tras un año de implantarlo se redujo el porcentaje medio del 31,4% al 4,8%. Lo que demuestra la importancia y eficacia de este tipo de formaciones.

Viendo que los ataques de Ingeniería Social son tan efectivos y que la tecnología está en constante evolución, este proyecto podrá ayudar en la sensibilización de aquellos que aún no lo consideren importante. De modo que podrán ver de primera mano las pruebas realizadas y juzgar por ellos mismos la importancia de tener en cuenta este tipo de ataques.

## 1.2. Objetivos del Trabajo

Objetivos de la investigación:

- Investigar y comprender los conceptos y técnicas relacionados con la ingeniería social.
- Investigar e identificar los motivos más comunes de los ciberdelincuentes para realizar este tipo de ataques.

- Identificar e investigar los métodos más utilizados por los ciberdelincuentes para llevar a cabo ataques de ingeniería social.

- Identificar el modus operandi de los ciberdelincuentes, diferenciándolo por fases: Descubrimiento e investigación / Engaño y gancho / Ataque / Retirada.

- Analizar la información que puede ser obtenida mediante estas técnicas y cómo los cibercriminales la explotan para obtener beneficios.

- Investigar y presentar buenas prácticas para evitar ser víctima de ataques de ingeniería social.

- Investigar si las acciones relacionadas con la Ingeniería Social están perseguidas por la ley y cuáles son las posibles consecuencias legales para los infractores.

- Explorar y analizar las diferentes herramientas de Ingeniería Social existentes, para posteriormente poder seleccionar aquellas que puedan ser utilizadas en la implementación.

Objetivos de la implementación:

- Instalar y configurar las herramientas necesarias para llevar a cabo pruebas de ataques de ingeniería social.

- Aprender a utilizar las herramientas necesarias para llevar a cabo pruebas de ataques de ingeniería social.

- Implementar simulaciones de ataques phishing, spear-phishing… siendo el tiempo el único limitante sobre las pruebas a realizar.

- Simular deep fakes o ataques de ingeniería social relacionados con IA.

- Ver la capacidad del OSINT, utilizando herramientas para recopilar información online.

Objetivos de la entrega:

- Realizar las entregas pactadas con la tutora en los plazos establecidos.

- Desarrollar una memoria final que detalle los resultados de la investigación y la implementación.

- Crear un video de presentación para exponer los resultados obtenidos en el trabajo.

## 1.3. Impacto en sostenibilidad, ético-social y de diversidad

¿Crees que el resultado de este TF no tiene ningún impacto ni positivo ni negativo en aspectos de sostenibilidad medioambiental y/o huella ecológica?

Voy a realizar el TF en mi ordenador personal, utilizando los recursos disponibles. En cuanto al impacto medioambiental, debido a que no utilizaré recursos adicionales ni viajaré a un lugar específico para realizarlo, no debería haber un impacto significativo ni positivo ni negativo en aspectos de sostenibilidad medioambiental y/o huella ecológica. Sin embargo, es importante tener en cuenta que el consumo energético de mi ordenador puede generar un impacto ambiental en la medida en que requiera energía eléctrica. Por lo tanto, trataré de gestionar mi uso de energía para reducir al mínimo cualquier posible impacto negativo.

¿Ni en su desarrollo, ni durante su posible vida útil (periodo de explotación), ni tampoco en el momento de su retirada/eliminación? ¿Y en la legislación y normativas al respecto? O, visto desde otra perspectiva, ¿impacta en algunos de los ODS de esta dimensión?

El impacto de la realización del TF en un ordenador personal en aspectos de sostenibilidad medioambiental y/o huella ecológica durante su desarrollo, vida útil y retirada/eliminación debería ser casi nulo. Sin embargo, es importante tener en cuenta que cualquier dispositivo electrónico puede generar impactos ambientales durante su ciclo de vida, por lo que es importante ser conscientes de estos impactos y tomar medidas para reducirlos al mínimo. Existen legislaciones y normativas a nivel nacional e internacional que regulan la gestión adecuada de los residuos electrónicos y promueven prácticas sostenibles en la producción y uso de dispositivos electrónicos.

En cuanto al impacto de los ODS, el resultado del TF no debería tener un impacto significativo en los ODS relacionados con la dimensión ambiental. Sin embargo, cualquier pequeña contribución a la consecución de los ODS puede ser valiosa, y promover prácticas sostenibles en la producción y uso de dispositivos electrónicos puede tener un impacto positivo en la sociedad y en el medio ambiente a largo plazo. Por lo tanto, el uso eficiente de los recursos y la reducción de emisiones de gases de efecto invernadero pueden contribuir al ODS 12 y al ODS 13, respectivamente. Además, la gestión adecuada de los residuos electrónicos puede contribuir al ODS 14 y al ODS 15.

Si tiene impactos negativos, ¿cuál o cuáles son? ¿Para quién? ¿En qué ámbito geográfico? ¿Se pueden medir (recursos empleados y huella ecológic)? ¿Se han tenido en cuenta en el diseño de la solución propuesta para intentar minimizarlos?

Existen varios aspectos que pueden generar impactos en el medio ambiente, tales como:

- Extracción de materias primas: La extracción de materias primas para la fabricación de dispositivos electrónicos, como ordenadores personales, puede generar impactos negativos en la biodiversidad, el uso de agua y energía y en la emisión de gases de efecto invernadero.
- Consumo energético: Durante el uso del ordenador personal para la realización del TF, se puede generar un consumo de energía eléctrica que puede tener un impacto negativo en la huella de carbono.
- Disposición final: Una vez que el ordenador personal quede inservible, su disposición final puede tener un impacto negativo en el medio ambiente si no se realiza de manera adecuada.

Estos impactos se pueden medir a través de diferentes indicadores, como la huella de carbono y la huella ecológica, entre otros. La medida que puede estar a nuestra mano es la de intentar limitar nuestro consumo energético.

Si tiene impactos positivos, ¿cuál o cuáles son? ¿Puede mejorar o solventar alguna problemática de sostenibilidad/medioambiental existente (por ejemplo la reutilización de recursos o el impulso de la economía circular)? ¿Este impacto positivo es inherente a la propia solución o tiene que ser protagonizado por parte de los usuarios/propietarios?

La realización del TF en un ordenador personal puede tener impactos positivos, como por ejemplo:

- Ahorro de recursos: Al utilizar un ordenador personal existente para la realización del TF, se reduce la necesidad de adquirir un nuevo dispositivo, lo que implica una reducción en la extracción de materias primas y en la generación de residuos electrónicos.
- Reducción de la huella de carbono: Al reducir la necesidad de adquirir un nuevo dispositivo, se reduce la huella de carbono asociada a la extracción, producción y transporte de un nuevo dispositivo.

Del mismo modo, podemos contribuir a este impacto positivo al adoptar prácticas sostenibles al utilizar los dispositivos electrónicos, el uso eficiente de los recursos y la gestión adecuada de los residuos electrónicos.

Entre las razones que te motivan a hacer este TF, ¿hay alguna preocupación ética o de responsabilidad social?

No, ninguna de las razones que me motivan a hacer este TF tiene que ver con la sostenibilidad. Mi interés en realizar este trabajo se enfoca más en la adquisición de conocimientos y habilidades en la materia, así como en la satisfacción personal de completar un proyecto académico de calidad.

¿El resultado de este TF es tan técnico que no tiene ningún impacto ni positivo ni negativo en aspectos de género, diversidad o derechos humanos? ¿Y en alguna legislación? ¿Y en aspectos de accesibilidad, discapacidad, ergonomía y/o seguridad de los datos y las TIC? O, visto desde otra perspectiva, ¿impacta en algunos de los ODS de esta dimensión?. Si no tiene ningún impacto, ni positivo ni negativo, hay que explicar cómo se ha llegado a esta conclusión y/o justificarla.

En cuanto al impacto en aspectos de género, diversidad, derechos humanos y legislación, así como en aspectos de accesibilidad, discapacidad, ergonomía y seguridad de los datos y las TIC, no se espera que el resultado de este TF tenga impacto alguno. La solución propuesta para la realización del TF en un ordenador personal no involucra ningún tipo de discriminación o sesgo hacia ningún grupo de interés, y no tiene implicaciones en términos de protección de datos, privacidad, laboral, propiedad intelectual o seguridad de las personas.

Asimismo, se ha evaluado que el resultado del TF no impacta en los ODS de la dimensión de género (ODS 5 - Igualdad de género) ni en la dimensión de reducción de desigualdades (ODS 10 - Reducción de desigualdades). En definitiva, no se espera que este TF tenga ningún impacto, ni positivo ni negativo, en ninguno de estos aspectos o dimensiones.

| Entre las razones que te motivan a hacer este TF, ¿hay alguna preocupación sobre diversidad/género o derechos humanos? |
|---|

No, en mi caso personal no tengo preocupaciones específicas sobre diversidad/género o derechos humanos en relación con este proyecto. Mi motivación se enfoca más en la adquisición de conocimientos y la mejora de habilidades técnicas en el campo relacionado al TF.

## 1.4. Enfoque y método seguido

La estrategia más apropiada para conseguir los objetivos del trabajo parece ser adaptar herramientas y metodologías existentes, y emplear un enfoque basado en la investigación y la evaluación de la efectividad de las medidas de seguridad existentes. Esto permitiría lograr una comprensión profunda de la ingeniería social y sus técnicas, identificar las posibles debilidades y vulnerabilidades en los sistemas y procesos existentes, y proponer soluciones y recomendaciones prácticas para prevenir y evitar los ataques de ingeniería social.

En caso de que no se disponga de herramientas y metodologías adecuadas, se podrá plantear la creación de una implementación desde cero. No obstante, la intención es adaptar herramientas y metodologías ya existentes, lo que permitiría ahorrar tiempo y recursos. De manera que podremos enfocarnos en la investigación para posteriormente poder realizar una parte más práctica.

## 1.5. Planificación del Trabajo

| TAREA | INICIO | FIN | DEDICACIÓN |
|---|---|---|---|
| **PEC1 - Planificación** | | | |
| 1.1- Contexto y justificación | 3/1/23 | 3/2/23 | 4 |
| 1.2- Definir los objetivos | 3/1/23 | 3/2/23 | 4 |
| 1.3- Impacto en sostenibilidad etc. | 3/1/23 | 3/2/23 | 5 |
| 1.4- Enfoque y método seguido | 3/4/23 | 3/4/23 | 3 |
| ↓ \| 1.5- Elaborar cronograma | | | |
| 1.5.1- Definir tareas | 3/4/23 | 3/6/23 | 5 |
| 1.5.2- Calcular tiempos | 3/4/23 | 3/7/23 | 4 |
| 1.6- Análisis de riesgos | 3/8/23 | 3/9/23 | 3 |
| 1.7- Estado del arte | 3/9/23 | 3/10/23 | 3 |
| 1.8- Historia del arte | 3/9/23 | 3/10/23 | 3 |
| 1.9- Investigar sobre ingeniería social | 3/5/23 | 3/11/23 | 4 |
| **1.10- Entrega del plan de trabajo** | **3/12/23** | **3/13/23** | **Hito** |
| **PEC2 - Investigación** | | | |
| ↓ \| 2.1- Investigación sobre ingeniería social | | | |
| 2.1.1- Qué es, y los roles que intervienen | 3/14/23 | 3/16/23 | 4 |
| 2.1.2- Objetivo común de los atacantes | 3/16/23 | 3/19/23 | 5 |
| 2.1.3- Métodos, tipos y estrategias utilizadas | 3/17/23 | 3/23/23 | 13 |
| 2.1.4- Motivación de los atacantes | 3/18/23 | 3/18/23 | 2 |
| 2.1.4- Cómo se explotan y beneficios | 3/20/23 | 3/24/23 | 7 |
| 2.1.5- Cómo evitarlo y recomendaciones | 3/23/23 | 3/27/23 | 4 |
| 2.1.6- Cómo es a nivel legal | 3/28/23 | 3/31/23 | 7 |
| 2.1.7- Herramientas de Ingeniería Social | 3/31/23 | 4/4/23 | 6 |
| **↓ \| 2.2- Entrega de la PEC2** | | | 3 |
| 2.2.1- Recopilar información investigada | 3/14/23 | 4/4/23 | 10 |
| 2.2.2- Redactar la PEC2 | 3/19/23 | 4/11/23 | 15 |
| **PEC3 - Implementación** | | | |
| 3.1- Investigación de herramientas a utilizar | 4/12/23 | 4/14/23 | 6 |
| 3.2- Instalación y configuración de herramientas | 4/15/23 | 4/23/23 | 15 |
| 3.3- Realización de pruebas y registro de resultados | 4/20/23 | 4/30/23 | 25 |
| 3.4- Análisis de los resultados obtenidos en las pruebas | 5/1/23 | 5/4/23 | 8 |
| **↓ \| 3.5- Entregar la PEC3** | | | **Hito** |
| 3.5.1- Recopilar información implementada | 4/15/23 | 5/4/23 | 25 |
| 3.5.2- Redactar la PEC3 | 5/4/23 | 5/9/23 | 8 |
| **PEC4 - Repaso y documentación** | | | |
| 4.1- Repaso y elaboración de memoria final | 5/10/23 | 6/10/23 | 20 |
| 4.2- Conclusiones y trabajos futuros | 5/23/23 | 5/25/23 | 2 |
| 4.3- Elaboración del vídeo presentación | 5/26/23 | 5/31/23 | 8 |

| | | | |
|---|---|---|---|
| **4.4- Entregar la PEC4** | **6/11/23** | **6/13/23** | **Hito** |

*Tabla 1: Planificación*

## 1.6. Planificación detallada de estas tareas y sus dependencias

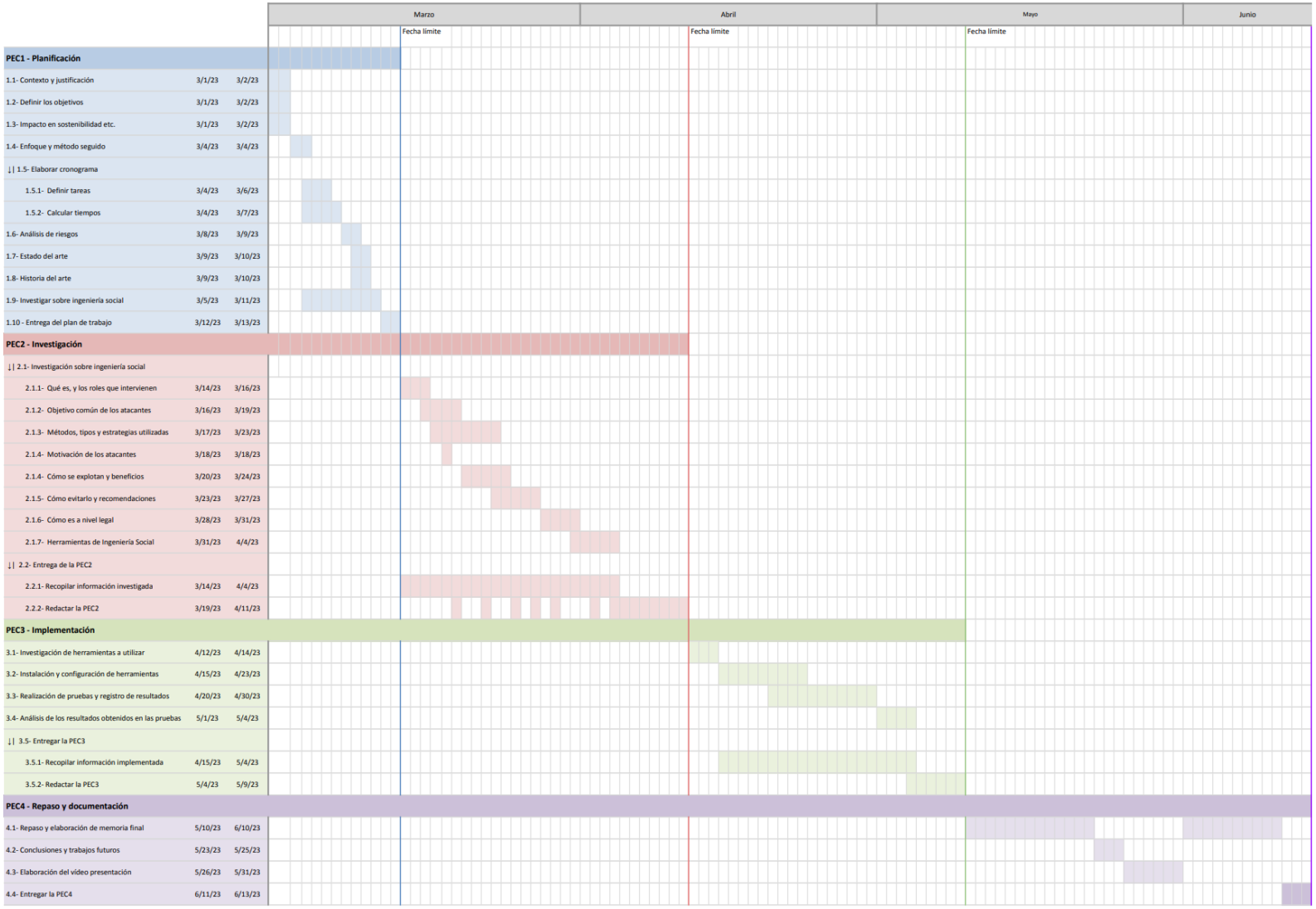


*Tabla 2: Diagrama gantt*

## PEC1

| TAREA | INICIO | FIN | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PEC1 - Planificación** | | | | | | | | | | | | | | | |
| 1.1- Contexto y justificación | 3/1/23 | 3/2/23 | | | | | | | | | | | | | |
| 1.2- Definir los objetivos | 3/1/23 | 3/2/23 | | | | | | | | | | | | | |
| 1.3- Impacto en sostenibilidad etc. | 3/1/23 | 3/2/23 | | | | | | | | | | | | | |
| 1.4- Enfoque y método seguido | 3/4/23 | 3/4/23 | | | | | | | | | | | | | |
| ↓\| 1.5- Elaborar cronograma | | | | | | | | | | | | | | | |
| 1.5.1- Definir tareas | 3/4/23 | 3/6/23 | | | | | | | | | | | | | |
| 1.5.2- Calcular tiempos | 3/4/23 | 3/7/23 | | | | | | | | | | | | | |
| 1.6- Análisis de riesgos | 3/8/23 | 3/9/23 | | | | | | | | | | | | | |
| 1.7- Estado del arte | 3/9/23 | 3/10/23 | | | | | | | | | | | | | |
| 1.8- Historia del arte | 3/9/23 | 3/10/23 | | | | | | | | | | | | | |
| 1.9- Investigar sobre ingeniería social | 3/5/23 | 3/11/23 | | | | | | | | | | | | | |
| 1.10 - Entrega del plan de trabajo | 3/5/23 | 3/11/23 | | | | | | | | | | | | | |

*Tabla 3: Diagrama gantt - PEC1*

## PEC2

| | | | Marzo | | | | | | | | | | | | | | | | | Abril | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TAREA | INICIO | FIN | 14 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **PEC2 - Investigación** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ↓\| 2.1- Investigación sobre ingeniería social | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.1- Qué es, y los roles que intervienen | 3/14/23 | 3/16/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.2- Objetivo común de los atacantes | 3/16/23 | 3/19/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.3- Métodos, tipos y estrategias utilizadas | 3/17/23 | 3/23/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.4- Motivación de los atacantes | 3/18/23 | 3/18/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.4- Cómo se explotan y beneficios | 3/20/23 | 3/24/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.5- Cómo evitarlo y recomendaciones | 3/23/23 | 3/27/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.6- Cómo es a nivel legal | 3/28/23 | 3/31/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1.7- Herramientas de Ingeniería Social | 3/31/23 | 4/4/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ↓\| 2.2- Entrega de la PEC2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.2.1- Recopilar información investigada | 3/14/23 | 4/4/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2.2.2- Redactar la PEC2 | 3/19/23 | 4/11/23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Tabla 4: Diagrama gantt - PEC2*

PEC3


*Tabla 5: Diagrama gantt - PEC3*

PEC4

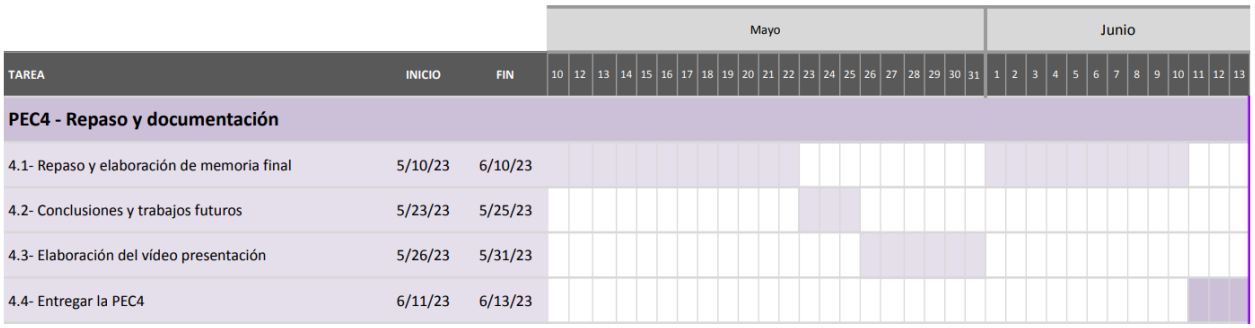


*Tabla 6: Diagrama gantt - PEC4*

## 1.7. Análisis de riesgos

La propuesta inicial para este TFM es realizar un estudio de las técnicas de ingeniería social y los métodos para obtener información, lo cual requiere una familiarización con los conceptos relacionados y el detalle de los métodos utilizados. El objetivo es descubrir qué información se puede obtener y cómo se explota con fines lucrativos. Aunque hay cierta flexibilidad en el trabajo, hay que tener en cuenta los siguientes riesgos:

| R1. Objetivo demasiado ambicioso |
|---|

El ámbito de la ingeniería social es muy amplio y complejo. Por tanto, es importante tener en cuenta que el objetivo del TFM puede ser muy ambicioso y que puede haber un riesgo de que se plantee una propuesta demasiado amplia o difícil de abarcar en el tiempo y recursos disponibles. Por ello, es necesario realizar una planificación cuidadosa y realista del trabajo a realizar, con el fin de evitar una sobrecarga de tareas y asegurar que se puedan cumplir los objetivos establecidos en el plazo previsto. En el

momento de realizar la planificación se puede concluir en que el nivel de **riesgo** es **bajo**.

R2. No encontrar herramientas útiles para las pruebas

Existe la posibilidad de que no se encuentren herramientas adecuadas para llevar a cabo las pruebas necesarias, lo que podría requerir la creación de una implementación desde cero. Sin embargo, este **riesgo** es **bajo** y se puede manejar fácilmente ya que este TF permite la flexibilidad para decidir y modificar las pruebas a realizar en función de las herramientas disponibles.

R3. Problemas o incompatibilidades entre diferentes herramientas de IS

Durante la implementación o utilización de diferentes herramientas de Ingeniería Social, puede surgir la necesidad de combinar varias de ellas para llevar a cabo las pruebas planificadas. Esto puede generar incompatibilidades entre estas herramientas, lo que puede afectar el desarrollo de las pruebas y retrasar el trabajo. Aunque a priori parezca un riesgo de nivel medio, es importante tener en cuenta esta posibilidad y estar preparado para solucionar los problemas que puedan surgir. Dado que no se especifican las herramientas a utilizar, pudiendo utilizar una gran variedad de estas, podemos deducir que el nivel de **riesgo** es **bajo**.

R4. Problemas en la propia implementación

Durante la implementación de las herramientas seleccionadas, existe el riesgo de enfrentar problemas imprevistos que puedan afectar su correcto funcionamiento. Dado que no se puede garantizar de antemano el desempeño de cada herramienta y su compatibilidad con el sistema, se podría considerar como un **riesgo** de **nivel medio**.

R5. Limitaciones de tiempo para elaborar la memoria

Durante la implementación y pruebas de las técnicas de ingeniería social, es posible que se requiera más tiempo del esperado para completar una iteración debido a la cantidad de pruebas que podrían llegar a hacerse. Sin embargo, se intentará seguir la planificación establecida, por lo que el nivel de **riesgo** es **bajo**.

## 1.8. Estado del arte

El fraude basado en la técnica de Ingeniería Social es una de las amenazas más antiguas y efectivas en el ámbito de la seguridad informática. A lo largo de los años, los ciberdelincuentes han utilizado técnicas cada vez más sofisticadas para engañar a los usuarios y obtener información confidencial o dinero. Por esta razón, es esencial que los expertos en seguridad comprendan cómo funciona la Ingeniería Social y cómo pueden prevenir estos ataques.

El estudio de fraudes basados en la técnica de Ingeniería Social es un área de investigación en constante evolución debido a la creciente sofisticación y diversidad de los ataques. La ingeniería social se ha convertido en una técnica muy común y exitosa para engañar a las personas y obtener información valiosa, lo que ha llevado a un aumento en el número de ataques y su complejidad. Por esta razón, se han llevado a

cabo numerosos estudios e investigaciones en este campo con el objetivo de comprender mejor la ingeniería social y desarrollar medidas de prevención y protección.

En el ámbito de la prevención y detección de fraudes basados en ingeniería social, existen diferentes enfoques y herramientas. Por ejemplo, algunas investigaciones se han centrado en el análisis de patrones de comportamiento y la identificación de posibles víctimas, mientras que otras se han centrado en la detección de correos electrónicos fraudulentos o en la utilización de técnicas de inteligencia artificial para detectar intentos de ingeniería social. Además, también existen diversas metodologías y técnicas utilizadas para llevar a cabo pruebas de ingeniería social y evaluar la efectividad de las medidas de seguridad existentes.

Entre las técnicas más conocidas, se encuentran el phishing o smishing, pretexting, sextorsión, baiting, vishing y dumpster diving.

En relación al avance de la inteligencia artificial, presenta un gran potencial en diversas áreas, pero también puede tener un impacto negativo, como en el caso de las estafas telefónicas basadas en la recreación de voces con software de síntesis de voz. Este tipo de estafas se están volviendo cada vez más comunes dado que ya existen programas de síntesis de voz que tan solo con una grabación de 30 segundos pueden recrear la voz y el timbre de cualquier persona de una forma realista.

## 1.9. Historia del arte

La ingeniería social es una técnica que ha sido utilizada desde hace siglos para engañar y manipular a las personas con el fin de obtener información confidencial o persuadirlas para que realicen una acción en particular. Aunque se ha convertido en una técnica popular en el mundo de la informática, sus orígenes se remontan a épocas antiguas.

Los primeros registros de la utilización de la Ingeniería Social se remontan a la antigua Grecia, donde se utilizaba para obtener información de los enemigos. Un ejemplo de ello podría ser la historia de la Guerra del Peloponeso, en la que un general espartano logró engañar a los atenienses para que permitieran el paso de su ejército mediante el uso de información falsa.

Durante la Edad Media, los reyes y nobles utilizaban la Ingeniería Social para obtener información de sus enemigos y súbditos, a menudo utilizando espías y agentes encubiertos para recopilar información. También se utilizaba la intimidación y la persuasión para conseguir información.

Con la llegada de la era moderna, la Ingeniería Social comenzó a ser utilizada por los gobiernos y militares de todo el mundo. Durante la Primera Guerra Mundial, los agentes de inteligencia utilizaron técnicas de Ingeniería Social para obtener información de los soldados y ciudadanos. En la Segunda Guerra Mundial, la Ingeniería Social se utilizó para engañar a los soldados y obtener información de los enemigos.

A medida que avanzaba la tecnología, la Ingeniería Social evolucionó y se adaptó a los nuevos medios de comunicación. Con la llegada de la era digital, la Ingeniería Social se ha convertido en una técnica popular utilizada por los cibercriminales para robar información personal, financiera y empresarial. El phishing, el smishing, el

vishing y otros tipos de ataques de Ingeniería Social se han vuelto cada vez más comunes.

Para combatir los ataques de Ingeniería Social, se han desarrollado medidas de seguridad como la educación del usuario, la autenticación multifactorial y la monitorización de la actividad del usuario. También se han llevado a cabo numerosas investigaciones y estudios para comprender mejor la Ingeniería Social y desarrollar medidas de prevención y protección.

Con la llegada de la era digital, la ingeniería social se ha convertido en una técnica popular utilizada por los cibercriminales para robar información personal, financiera y empresarial. El phishing, el smishing, el vishing y otros tipos de ataques de ingeniería social se han vuelto cada vez más comunes.

A medida que la tecnología avanza y los cibercriminales se vuelven más sofisticados, la ingeniería social sigue evolucionando. Por lo tanto, es imprescindible estar al tanto de los últimos desarrollos y técnicas utilizadas en este campo para poder protegerse contra estos tipos de ataques.

## 1.10. Tipologías de ataques

En este apartado se presentarán las herramientas y repositorios relacionados con la ingeniería social que se utilizarán en la implementación. No se incluirán aquellas herramientas que se hayan probado pero descartado para su uso.

**Phishing:**

1. Xampp
2. Gophish
3. Zphisher
4. Social Engineering Toolkit

**OSINT:**

1. Seeker
2. TheHarvester

**Inteligencia Artificial:**

1. Deepfake:
   - ➢ Faceswap.
2. Generación de Imagenes:
   - ➢ DALL·E 2
2. Chat de texto:
   - ➢ ChatGPT
3. Deepfakes:
   - ➢ FaceSwap
4. Clonación de voz:
   - ➢ Real-Time-Voice-Cloning
   - ➢ Voice.ai
   - ➢ Tortoise-TTS:
   - ➢ So-vits-svc-fork

## 1.11. Breve descripción de los otros capítulos de la memoria

- Recolección de información:

En esta sección se han abordado exhaustivamente todas las preguntas planteadas relacionadas con la ingeniería social. Se han explorado diversos aspectos, como la definición de este término, el modus operandi de los cibercriminales, los métodos que emplean y las medidas para protegerse de sus engaños. Además, se han analizado las implicaciones legales que los criminales cibernéticos podrían enfrentar, entre otros temas relevantes.

- Fase de implementación:

En esta sección se han tratado tres temas principales: el phishing, el OSINT y la aplicación de la inteligencia artificial en ataques de ingeniería social. Para cada uno de estos temas, se ha llevado a cabo la implementación o configuración de diversas herramientas, las cuales han demostrado resultados efectivos en relación a sus respectivas funciones.

- Conclusiones y trabajos futuros:

Esta sección se ha desarrollado una vez que se ha establecido el contenido central del trabajo. Como resultado, se han extraído conclusiones importantes tanto sobre los temas tratados en el trabajo como sobre su planificación, los objetivos planteados al inicio del proyecto y los desafíos encontrados durante su realización. Además, se han identificado áreas de investigación futura que podrían contribuir a mejorar el proyecto en general.

# 2. Recolección de información

## 2.1. ¿Qué es la ingeniería social?

La ingeniería social trata de utilizar técnicas de manipulación para engañar a las personas con el objetivo de que éstas expongan datos confidenciales, realicen acciones concretas o proporcionen acceso a información valiosa. Es una manera muy efectiva de saltarse la seguridad de las redes, independientemente de la solidez de un cortafuegos, las claves criptográficas empleadas, IDS, antivirus y demás herramientas de seguridad.

Es más probable que un humano confíe en otro antes que en una tecnología. Por lo tanto, podemos considerar que el eslabón más débil de la cadena de seguridad es el humano. Las actividades maliciosas realizadas a través de interacciones humanas influyen psicológicamente en una persona para que divulgue información confidencial o infrinja los procedimientos de seguridad. Debido a estas interacciones humanas, los ataques de ingeniería social son los más poderosos porque amenazan a todos los sistemas y redes. No pueden evitarse mediante soluciones de software o hardware mientras no se forme a las personas para prevenir estos ataques.

## 2.2. ¿Qué roles intervienen en la ingeniería social y cuáles son sus características?

- **El atacante**: Se trata del cibercriminal o grupo que utiliza técnicas engañosas o manipuladoras para persuadir a la víctima a realizar una acción o revelar información confidencial. Normalmente, suele hacerse pasar por una figura de autoridad real, un ejecutivo de la empresa, un representante gubernamental, o una figura ficticia, como un agente de soporte técnico. Las características comunes de un atacante pueden incluir habilidades de persuasión, conocimiento de la psicología humana, capacidad de empatía y manipulación, entre otras.

- **La víctima**: es la persona o grupo engañado o manipulado por el atacante para que revele información confidencial, realice una acción en particular o permita el acceso no autorizado a sistemas o datos. Normalmente suelen ser individuos o empresas que tienen información o activos valiosos que le podrían interesar al atacante. Las características comunes de una víctima pueden incluir una falta de conocimiento sobre los riesgos de seguridad, confianza excesiva en fuentes desconocidas, curiosidad, ingenuidad, complacencia, entre otras.

Es importante destacar que los roles de atacante y víctima pueden presentarse de manera difusa en la ingeniería social, ya que el atacante puede valerse de técnicas persuasivas o engañosas para obtener información o acciones en beneficio propio, sin que la víctima tenga conocimiento de que está siendo manipulada. En algunos casos, la persona engañada que se convierte en víctima puede transformarse en un atacante al compartir o utilizar la información confidencial obtenida. Asimismo, existen casos en los que las víctimas pueden ser conscientes de que están siendo manipuladas, pero deciden cooperar voluntariamente por diversas razones, como el miedo, la obligación o el interés económico.

Además del atacante y la víctima, también pueden intervenir otros roles en un ataque de ingeniería social, como el **empleador** y el **responsable de seguridad**. El

empleador puede tener un papel relevante en la medida en que pueda proporcionar acceso a la información y recursos que el atacante busca.

Por otro lado, el responsable de seguridad también es un actor clave en la defensa contra los ataques de ingeniería social, ya que tiene la responsabilidad de diseñar y aplicar medidas de seguridad efectivas para prevenir, detectar y responder a estos ataques. El responsable de seguridad debe ser capaz de reconocer los riesgos asociados con la ingeniería social, educar a los empleados sobre las mejores prácticas de seguridad y desarrollar políticas y procedimientos para mitigar estos riesgos. Además, es importante que el responsable de seguridad esté al tanto de las últimas tendencias en ingeniería social y esté preparado para adaptar su estrategia de seguridad en consecuencia.

## 2.3. ¿Cuáles son los principales tipos y métodos utilizados en la ingeniería social?

Los ataques de ingeniería social se pueden clasificar en dos categorías principales: ataques basados en humanos y ataques basados en ordenadores. Los ataques basados en humanos se llevan a cabo interactuando directamente con la víctima para recopilar la información deseada, mientras que los ataques basados en ordenadores se realizan utilizando dispositivos informáticos para obtener información de los objetivos.

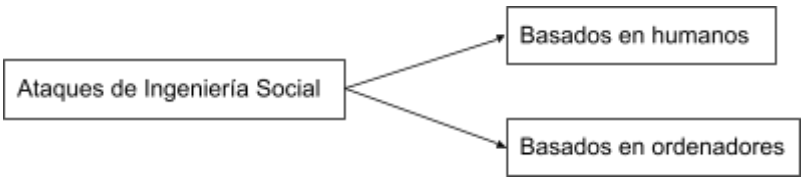


*Ilustración 1: Categorización principal de la Ingeniería Social*

Además, los ataques de ingeniería social se pueden clasificar en tres categorías según la forma en que se lleve a cabo el ataque: social, técnico y de base física. Los ataques sociales implican la manipulación psicológica y emocional de las víctimas, mientras que los ataques técnicos se llevan a cabo a través de Internet y los ataques de base física implican acciones físicas por parte del atacante.

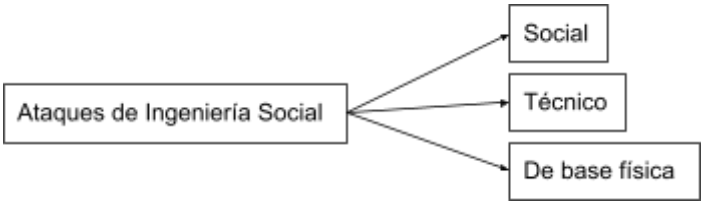


*Ilustración 2: Categorización según la forma de llevarlo a cabo*

Por lo tanto, los ataques de ingeniería social pueden combinar diferentes aspectos, como el uso de técnicas sociales, informáticas, técnicas, físicas y humanas.

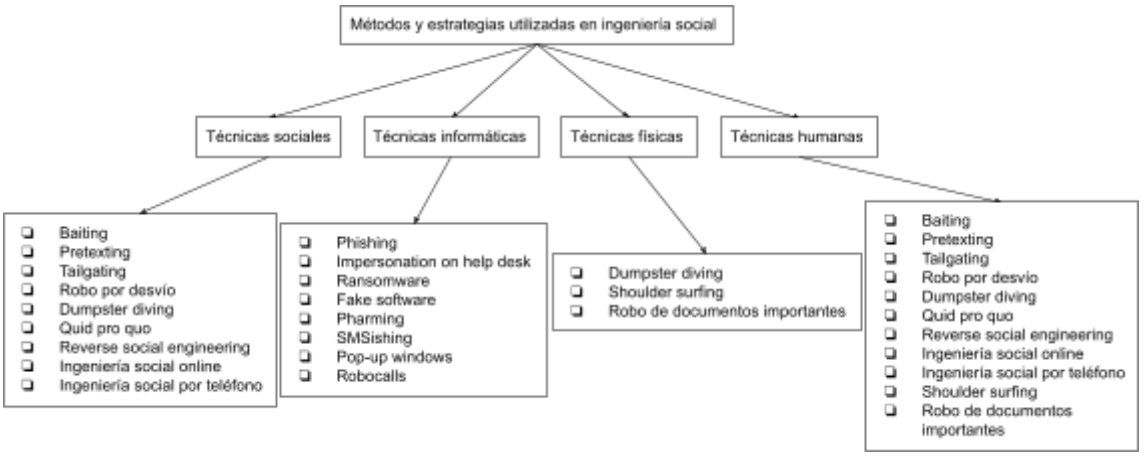


*Ilustración 3: Categorización completa con ejemplos*

Centrándonos en el tema principal, estos son los métodos más comunes utilizados por los delincuentes cibernéticos: Phishing, Pretexting, Ingeniería social inversa, Baiting, Tailgating, Spear phishing, Vishing, Smishing, Ransomware, Ataques de software falso etc .

## 2.4. ¿Cuál es el modus operandi de los cibercriminales?

Aunque los ataques de ingeniería social difieren entre sí, tienen un patrón común que implica cuatro fases: (1) recopilar información sobre el objetivo; (2) desarrollar una relación con el objetivo; (3) explotar la información disponible y ejecutar el ataque; y (4) salir sin dejar rastro.

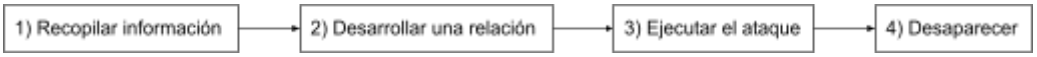


*Ilustración 4: Fases de la Ingeniería social*

### (1) Recopilar información sobre el objetivo:

Es esencial comprender que ninguna información es insignificante en el contexto de la ingeniería social. Incluso los detalles más pequeños pueden ser explotados por los cibercriminales para llevar a cabo una exitosa brecha de seguridad.

Cualquier empleado de una organización que haya dejado una huella en línea, en foros de discusión o en secciones de comentarios, puede ser contactado por un atacante con la intención de engañarlo. Además, muchas personas tienen una tendencia natural a compartir información sobre sus vidas en línea, lo que significa que esta información tiene el potencial de ser utilizada en su contra.

En la actualidad, hay diversas herramientas disponibles para recopilar información, como se puede apreciar al buscar "information-gathering" en el apartado "Temas" de Github, el cual arroja 503 repositorios públicos relacionados. Sin embargo, no solo se recopila información en línea, sino también en persona. Un ciberdelincuente podría seguirnos desde nuestra casa hasta nuestro lugar de trabajo e incluso tener una conversación casual con nosotros para obtener información personal que podríamos revelar sin darnos cuenta.

Voy a explorar y describir las diversas técnicas que los cibercriminales pueden utilizar para recopilar información sobre un objetivo, dado que es imposible mencionar y analizar todas las herramientas disponibles para recopilar información:

1. OSINT:

El OSINT se ha visto impulsado en los últimos tiempos gracias a los avances en el IoT y el big data. Lo que ha provocado un aumento sin límites en la cantidad de datos y ha acelerado el avance de la inteligencia de código abierto.En la actualidad, la recolección de información, se está diversificando cada vez más, y los datos se analizan en función de big data. Como resultado, la obtención de inteligencia se está volviendo cada vez más importante (inteligencia se traduce como inteligencia mental, confidencialidad e información). Todos los países del mundo recopilan información sobre otros países, y la cantidad de información recopilada por estos países se llama Vigilancia y reconocimiento inteligentes (ISR, por sus siglas en inglés). Los métodos de recopilación de información como ISR se dividen en tres tipos: OSINT, inteligencia humana (HUMINT) e inteligencia técnica (TECHINT).

El OSINT es el método más básico de recolección de información, que consiste en recopilar datos a través de fuentes abiertas como Internet, transmisiones y periódicos, y procesarlos. Al utilizar información expuesta al público general, existen ventajas, como la recopilación de información en tiempo real y el acceso fácil y económico a los datos. Sin embargo, la importancia de la información es menor que la de otros métodos de recolección de información.

En la actualidad, la tecnología OSINT es la más utilizada al buscar información en línea. Sobre esta base, los usuarios obtienen información sobre los datos que buscan. Sin embargo, desde la perspectiva de la ciberseguridad, el uso de los datos recopilados por OSINT es un arma de doble filo:

- Por una parte, los datos recopilados por OSINT pueden utilizarse como medio para resolver amenazas de ciberseguridad, lo que permite localizar a los ciberdelincuentes o prevenir ciberataques antes de que se produzcan.
- Los datos recopilados por OSINT se convierten en la base para que los atacantes creen amenazas de ciberseguridad.

Dado que las directrices para las herramientas OSINT están a disposición del público, las empresas y los usuarios pueden configurar las herramientas OSINT de acuerdo con su finalidad y recopilar datos sin mucho esfuerzo.

La siguiente ilustración muestra la estructura básica de OSINT. Que consiste en recopilar, procesar, analizar y notificar datos tras identificar los datos especificados.

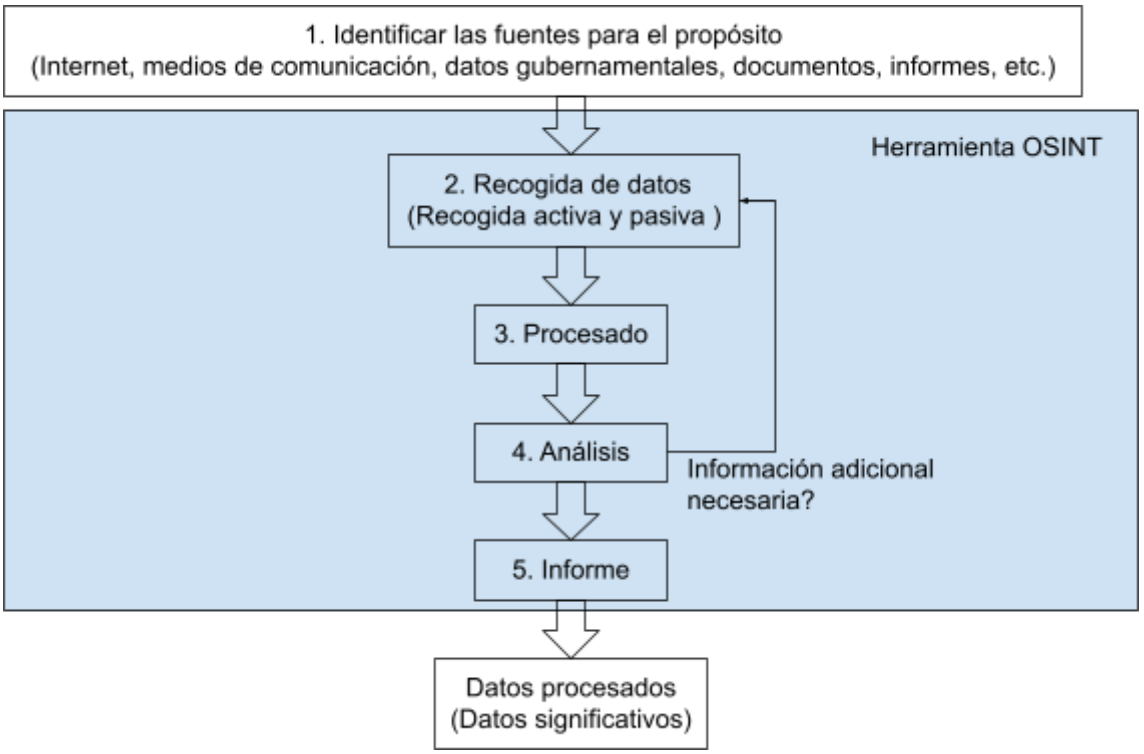


*Ilustración 5: Estructura básica OSINT*

*Paso 1. Identificar la fuente*: Se debe establecer la información que el usuario desea obtener entre numerosos datos. Por lo que hay que saber dónde y cómo obtener esta información.

*Paso 2. Recogida de datos*: Se recogen los datos obtenidos a partir de la identificación de la fuente. En la etapa de recogida activa, la información se recoge directamente mediante un programa o script en el objetivo que crea registros. En la recolección pasiva, la información se recopila utilizando Google, Netcraft, Whois, Recon-NG, Shodan, etc. por lo que deja ningún registro o log.

*Paso 3. Procesamiento:* Se trata de refinar la información obtenida en la etapa anterior. Dado que puede haber mucha información en el paso 2, la tarea de filtrado es importante en el paso de procesamiento. Además, es importante tener en cuenta la asociación entre la información, y el paso de procesamiento requiere una tarea de alta dificultad que requiere mucha experiencia y perspectivas.

*Paso 4. Análisis:* Los datos depurados en el paso anterior se procesan de acuerdo con el propósito de la investigación. Si se necesita información adicional en el paso de análisis, los pasos de recogida y procesamiento de datos se repiten continuamente para encontrar una asociación entre la información que permita obtener información significativa.

*Paso 5. Informe:* es un método para resumir los contenidos desde el primer al cuarto paso y redactarlo en forma de informe. Los informes se distribuyen y evalúan de diversas formas, e incluyen todos los datos fuente que indican la exactitud de los datos para dar credibilidad a los datos para la argumentación y las pruebas. Como resultado, gran parte de los datos generales se procesan en datos que cumplen los criterios establecidos por el usuario, lo que da lugar a datos significativos.

A continuación se presentan los principales descubrimientos que se pueden obtener mediante OSINT, organizados por su origen:

2. Metadatos:

Se pueden hallar numerosos metadatos en documentos públicos que se encuentren en lugares que deberían ser privados. Estos datos se suelen poder obtener debido a errores de configuración o a una publicación innecesaria. Algunos de los metadatos encontrados incluyen información sobre sistemas operativos, versiones de software de creación y edición de contenidos y suites ofimáticas, nombres de usuario, direcciones de correo electrónico, nombres de empleados y títulos originales de los documentos.

Es importante tener en cuenta la fecha de creación de los documentos reflejados en los metadatos, ya que esto puede indicar la vigencia de la información obtenida. En general, cuanto más reciente sea la fecha de creación, mayor será la probabilidad de que la información siga siendo relevante.

Es esencial tener en cuenta que ninguna información es irrelevante. Los títulos originales de los archivos pueden contener información valiosa que podría ser utilizada en ataques de ingeniería social. Aunque los usuarios pueden no considerarlo relevante, los atacantes pueden utilizar esta información para ganar credibilidad y engañar a los empleados utilizando la misma jerga.

3. Videos e imágenes:

Durante el análisis de videos e imágenes se puede descubrir una gran cantidad de información que pasa desapercibida para quienes las publicaron o que consideraron como irrelevante. Esta información se puede obtener de videos e imágenes publicados por visitantes o proveedores (en caso de empresas), ortofotos o fotografías de satélite y Google Street View.

Entre los hallazgos más destacados obtenidos durante el análisis de videos e imágenes que se hizo en el “INFORME SECTF 2019” de Euskalhack, se incluyen:

- Imágenes de acreditaciones de empleados y visitantes.
- Fotografías de tarjetas de acceso de los empleados.
- Información sobre el modelo y la marca de equipos informáticos.
- Software instalado en los equipos.
- Nombres de usuario utilizados.
- Versiones de sistemas operativos utilizados.
- Información sobre la marca de los navegadores web utilizados.
- Nombres de clientes de correo electrónico.
- Información sobre los sistemas utilizados para la destrucción de documentos y gestión de residuos.

4. Recopilación web:

No es de extrañar que la  web corporativas o personales y sus sitios asociados pueden ser una fuente rica en información. Gran parte de los metadatos de los documentos, así como la mayoría de los videos e imágenes, se pueden encontrar en estos sitios web. Lo primero que hará un buen ingeniero social es recolectar tantos datos como pueda de la página web de la empresa o persona. Pasando un tiempo de calidad en la página, se puede entender claramente:

- Qué hacen
- Los productos y servicios que ofrecen
- Las ubicaciones físicas
- Las vacantes de trabajo
- Los números de contacto

- Las biografías de los ejecutivos o miembros del consejo
- Los foros de soporte
- Direcciones de correo electrónico
- Las convenciones de nomenclatura de correo electrónico
- Palabras o frases especiales que puedan ayudar en la elaboración de perfiles de contraseñas
- Números de teléfono y extensiones internas
- Información jerárquica de la empresa
- Portales web obsoletos y nombres de equipos

Ver las páginas web personales de los usuarios también es sorprendente porque enlazarán casi todos los detalles íntimos sobre sus vidas: hijos, casas, trabajos y más. Esta información debería ser catalogada en secciones porque a menudo es algo de esta lista lo que se usa en el ataque.

Muchas veces, los empleados de la empresa formarán parte de los mismos foros, listas de hobbies o sitios de redes sociales. Si encuentras a un empleado en LinkedIn o Facebook, es probable que muchos más estén allí también. Tratar de recopilar todos esos datos realmente puede ayudar a un ingeniero social a elaborar perfiles tanto de la empresa como de los empleados. Muchos empleados hablarán sobre su cargo en sus medios de comunicación social, lo que puede ayudar a un ingeniero social a perfilar cuántas personas pueden estar en un departamento y cómo están estructurados los departamentos.

Es importante destacar que se pueden encontrar errores de programación o configuración de los servidores, ya que algunos de los sitios que deben estar restringidos también pueden llegar a estar indexados por los motores de búsqueda.

5. Proveedores:

Otra fuente de información valiosa se puede obtener del análisis de los proveedores. Es importante que las organizaciones consideren como un activo a fortalecer a las empresas con las que tienen una estrecha colaboración, ya que la cadena siempre es tan fuerte como su eslabón más débil. Al analizar a los proveedores, se podría destacar información relevante sobre los servicios prestados, como logística, seguridad, vending y limpieza, así como información sobre la tecnología e infraestructuras implementadas en la empresa.

6. Redes sociales:

En los últimos tiempos, muchas empresas han adoptado las redes sociales como una forma económica de hacer marketing y llegar a un amplio número de clientes potenciales. Además de ser una herramienta de promoción, las redes sociales también proporcionan a las empresas otra fuente de información valiosa en forma de publicaciones sobre eventos, nuevos productos, comunicados de prensa y noticias relacionadas con la actualidad.

Es interesante observar cómo las redes sociales han evolucionado hasta convertirse en un fenómeno en sí mismas, con nuevas plataformas emergentes constantemente. Sin embargo, es importante tener en cuenta que estas plataformas pueden proporcionar información abierta sobre la vida y la ubicación de las personas.

Es importante señalar que la información expuesta en redes sociales sobre los empleados puede permitir a un atacante diseñar un ataque dirigido con un nivel de credibilidad elevado. Los hallazgos encontrados en redes sociales pueden incluir información sobre el soporte de IT, el tiempo trabajando en la empresa, las tecnologías

específicas utilizadas, el organigrama y estructura organizativa interna, las preferencias de ocio de los trabajadores, grupos privados de Facebook sin verificación de identidad y la información sobre proveedores de servicios.

7. Leaks de credenciales:

Es relevante mencionar que durante el proceso de investigación OSINT se podrían encontrar varias cuentas de correo y credenciales pertenecientes a las empresas o usuarios objetivo en filtraciones de información publicadas en Internet. No es fácil determinar si se trata de credenciales antiguas o revocadas, pero debido a los posibles riesgos, se recomienda a las organizaciones prestar especial atención a este aspecto.

8. Buscadores:

Johnny Long escribió un famoso libro titulado “Google Hacking for Penetration Testers” y realmente abrió los ojos de mucha gente a la increíble cantidad de información que contiene Google.

Google perdona pero nunca olvida, y se le ha comparado con el Oráculo. Siempre que sepas cómo preguntarle, puede decirte casi todo lo que quieras saber.

Además, google tiene maneras avanzadas con las que poder realizar búsquedas más concretas. Por ejemplo, puedes encontrar un tipo de archivo concreto (p. ej. filetype:tipo_de_archivo) o encontrar una web que contenga una cadena exacta como por ejemplo, un título (“título_exacto”).

Existen libros dedicados exclusivamente al tema del uso de Google para buscar datos, pero lo principal que hay que recordar es que conocer los operandos de Google te ayudará a desarrollar los tuyos propios. Un sitio web como https://www.googleguide.com/advanced_operators_reference.html tiene una lista muy útil de los operandos y de cómo utilizarlos.

9. Reconocimiento Whois:

Whois es un servicio y una base de datos que contiene información de registro sobre los nombres de dominio, los propietarios y los contactos técnicos de un sitio web. Algunos de los datos que se pueden encontrar en la base de datos Whois incluyen la fecha de creación del dominio, la fecha de vencimiento, el servidor de nombres, la ubicación geográfica del servidor y la información de contacto del propietario del dominio. Es importante destacar que no toda la información que se encuentra en la base de datos Whois es pública, ya que en algunos casos se puede optar por mantener cierta información confidencial.

El acceso a la información Whois puede ser útil para investigar a una empresa y obtener detalles sobre sus servidores, pero también puede ser utilizado para lanzar ataques de ingeniería social o para recopilar más información personal. Por esta razón, algunas empresas de registro de dominios ofrecen la opción de mantener cierta información privada, como la dirección de correo electrónico y el número de teléfono del propietario del dominio, para proteger su privacidad.

10. Servidores públicos:

Los servidores de acceso público de una empresa pueden proporcionar información valiosa sobre la infraestructura de la empresa que no se encuentra en su sitio web. Al identificar el sistema operativo, las aplicaciones instaladas y la información de IP de un servidor, se puede obtener información importante sobre la empresa. Además, se puede buscar en el nombre de dominio corporativo para encontrar entradas en foros

de soporte públicos y combinar esta información con la información del servidor para obtener una imagen más completa de la infraestructura de la empresa.

Durante una auditoría, se puede utilizar distintas herramientas para buscar en la web y descubrir información valiosa sobre la empresa. Por ejemplo, en algunos casos, se han descubierto servidores públicos que albergaban cientos de documentos con información clave sobre proyectos, clientes y creadores de los documentos, lo que resultó ser muy dañino para la empresa.

Sin embargo, es importante tener en cuenta que en España, la realización de un escaneo de puertos con Nmap en un servidor público puede ser ilegal si se hace sin el consentimiento explícito del propietario del servidor o sin la autorización correspondiente de las autoridades competentes. Por ejemplo, en junio de 2003, un israelí fue acusado de intentar acceder a material informático sin autorización después de escanear el sitio web del Mossad. Aunque fue absuelto de los cargos, este tipo de acciones pueden tener consecuencias legales como veremos más adelante.

## (2) Desarrollar una relación con el objetivo:

El primer paso en el desarrollo de una relación con un objetivo en un ataque de ingeniería social es tener una comprensión clara de los objetivos que se quieren lograr. Esto implica definir objetivos específicos y medibles, que sean realistas y estén dentro del alcance de los recursos y capacidades del atacante. Una vez que se tiene esta información, el atacante recopila información sobre la víctima, como su trabajo, intereses, familia y amigos, para personalizar el ataque y crear un vínculo emocional con la víctima.

Una vez que se ha recopilado la información necesaria, el atacante comienza a desarrollar la relación con el objetivo a través de diferentes canales, como el correo electrónico, el teléfono o las redes sociales. El objetivo es crear una conexión emocional con la víctima y ganar su confianza utilizando técnicas de persuasión adecuadas.

Es importante visualizar el objetivo como ya alcanzado y establecer un plan de acción concreto con pequeñas metas que permitan avanzar gradualmente hacia el objetivo final. Además, mantener una actitud positiva y confiada durante todo el proceso es fundamental para superar los obstáculos y mantener la motivación. La actitud de gratitud y apreciación también es importante, ya que ayuda a mantener una perspectiva positiva y atractiva que puede atraer más recursos y oportunidades.

Una vez que se ha establecido la relación, el atacante puede comenzar a solicitar información o acceso a sistemas y recursos utilizando diferentes tácticas de persuasión, como la autoridad, la urgencia o la simpatía. En resumen, el desarrollo de una relación con el objetivo es un proceso en el que el atacante intenta establecer una relación de confianza con la víctima para obtener información o acceso a sistemas y recursos, y para lograrlo utiliza técnicas de persuasión y personalización del ataque.

Para entenderlo mejor, vamos a centrarnos en tres aspectos significativos:

1. Pretexto:

En el contexto de la ingeniería social, un pretexto es una excusa falsa que se utiliza para crear un ambiente propicio para persuadir a una persona con el fin de que revele información privada o lleve a cabo acciones específicas. El pretexto debe ser

cuidadosamente planeado y diseñado para ser coherente con la realidad del objetivo y con la información obtenida durante la fase de OSINT. La efectividad del pretexto se potencia al incluir pequeños detalles, como la terminología interna o las referencias a los empleados. Uno de los pretextos más efectivos ante una empresa podrían estar relacionados con el papel de un técnico de soporte de IT, ya que les permitirá a los ciberdelincuentes utilizar conocimientos propios y comportarse de manera natural para evitar levantar sospechas. Otros pretextos utilizados pueden ser la realización de una encuesta, ser asistente de un alto cargo y una entrevista de un medio digital. Los pretextos poco trabajados, incoherentes o con guiones muy rígidos suelen tener menos efectividad en un ataque de ingeniería social.

2. Llamadas en directo:

En la fase de llamadas de ingeniería social, los ciberdelincuentes tienen la oportunidad de poner a prueba sus habilidades en situaciones reales. Durante las llamadas, es importante dedicar tiempo al principio para presentarse y explicar el motivo de la llamada de forma clara y concisa. Los participantes que son más directos en la obtención de información tienden a tener más éxito en conseguir sus objetivos, siempre y cuando el pretexto utilizado sea coherente y sólido. Además, es importante convencer al destinatario de que la llamada no representa una amenaza. Con estas estrategias, se pueden hacer llamadas mucho más eficientes y lograr obtener la información necesaria.

3. Técnicas de influencia:

Las técnicas de influencia son utilizadas para persuadir a una persona a realizar una acción que de otra manera no habría hecho. El principio de obligación moral suele ser el más utilizado para persuadir a los objetivos, ya sea la obligación de asistir a alguien que solicita ayuda o la obligación de realizar correctamente su trabajo. El segundo principio más utilizado suele ser el de ejercer autoridad, representando una institución o un alto cargo. El principio de coherencia se suele utilizar como refuerzo para seguir solicitando información más allá de lo que el objetivo deseaba, aprovechando el compromiso adquirido inicialmente. También se suele utilizar el principio de afinidad o simpatía al elegir un pretexto relacionado con los gustos del objetivo o interpretar un personaje que concuerde con las preferencias personales del mismo.

En caso de querer ampliar más el conocimiento sobre estas técnicas, podemos visitar la web https://www.social-engineer.org/framework/influencing-others_/influence-tactics/ o consultar el libro "Influence, the psychology of persuasion" del profesor Robert B. Cialdini.

## (3) Explotar la información disponible y ejecutar el ataque:

En esta fase, una vez que el atacante ha establecido una relación de confianza con la víctima, empieza a utilizar diversas técnicas para obtener información sensible o lograr que la víctima realice acciones que favorezcan al atacante. Algunas de estas técnicas las podremos ver en un apartado más adelante.

Por ejemplo, el atacante puede haberse hecho pasar por una figura de autoridad o un compañero de trabajo en una fase anterior para obtener información confidencial o persuadir a la víctima para que realice una acción en particular. Al fin y al cabo, se inventan una historia creíble para obtener información o acceso a sistemas o instalaciones, sea por el medio que sea.

Es importante destacar que en esta fase, el atacante puede utilizar cualquier información obtenida en las fases anteriores para adaptar sus técnicas de persuasión y engaño y aumentar sus posibilidades de éxito en el ataque. Por esta razón, es crucial que las organizaciones y los individuos sean conscientes de los riesgos de la ingeniería social y tomen medidas para proteger su información y sistemas.

(4) Salir sin dejar rastro:

En la fase de salida, el atacante debe asegurarse de borrar o cubrir sus huellas para evitar ser detectado. Esto puede incluir eliminar cualquier registro de comunicación o transacciones con la víctima, limpiar cualquier malware utilizado en el ataque y utilizar técnicas de anonimización para ocultar su identidad. Es importante que el atacante salga sin dejar ningún rastro para evitar que se descubra su verdadera identidad y se tomen medidas legales en su contra.

## 2.5. ¿Cual es la motivación de los ciberdelincuentes?

Los motivos detrás de los ataques de ingeniería social pueden variar según el ciberdelincuente en cuestión. Algunos buscan acceder a información confidencial, como contraseñas, números de tarjetas de crédito o información financiera, para usarla en actividades ilícitas o venderla en el mercado negro. Otros utilizan la ingeniería social para introducir malware en sistemas informáticos o comprometer la seguridad de organizaciones, con el propósito de futuras extorsiones. Además, hay quienes realizan estos ataques por razones políticas o ideológicas, con la intención de obtener información o interrumpir servicios gubernamentales. No obstante, en la mayoría de los casos, el objetivo final común de los ciberdelincuentes es obtener beneficios económicos.

## 2.6. ¿Qué técnicas utilizan los cibercriminales, y cómo las explotan para obtener beneficios?

- Phishing:

Los ataques de phishing son los más comunes entre los ataques llevados a cabo por ingenieros sociales, y buscan obtener fraudulentamente información privada y confidencial de sus objetivos a través de llamadas telefónicas o correos electrónicos. Los atacantes engañan a las víctimas para obtener información confidencial, y utilizan sitios web falsos, correos electrónicos, anuncios, antivirus, scareware, sitios web de PayPal, premios y ofertas gratuitas. Estos ataques pueden ser llamadas o correos electrónicos falsos de un supuesto departamento de lotería que informa de la ganancia de un premio en efectivo y solicita información privada o hacer clic en un enlace adjunto en el correo electrónico. La información que se busca puede incluir detalles de tarjetas de crédito, datos de seguros, nombres completos, direcciones físicas, nombres de mascotas, primeros trabajos o sueños, nombre de la madre, lugar de nacimiento, lugares visitados, u otra información que la persona pueda utilizar para iniciar sesión en cuentas sensibles como banca en línea o servicios.

Existen cinco tipos de phishing: spear phishing, whaling phishing, vishing phishing, phishing de respuesta de voz interactiva y phishing de compromiso de correo electrónico empresarial. El spear phishing se dirige a personas específicas o grupos selectos utilizando sus nombres para hacer reclamos o comunicaciones, y requiere

recopilar información sobre la víctima utilizando datos disponibles en línea. El whaling phishing es un tipo de spear phishing dirigido a perfiles altos en empresas. El vishing phishing se refiere a ataques telefónicos de phishing para manipular a las personas para que proporcionen información sensible, como llamadas de un banco. El phishing de respuesta de voz interactiva utiliza un sistema de respuesta de voz interactiva para hacer que el objetivo introduzca información privada como si fuera de una empresa o banco legítimo. El phishing de compromiso de correo electrónico empresarial imita la caza de ballenas, y se dirige a los grandes "peces" de las empresas corporativas con el fin de obtener acceso a sus correos electrónicos empresariales, calendarios, pagos, contabilidad u otra información privada. Los ingenieros sociales utilizan estos datos para enviar correos electrónicos falsos, mutar correos pasados, cambiar horarios de reuniones, leer información profesional sobre la empresa y contactar con clientes o proveedores de servicios. El atacante comienza investigando a empleados de alto perfil a través de las redes sociales para conocer y comprender su información profesional, como el rango autorizado de dinero que un objetivo puede obtener del banco. Después de obtener la información deseada, el atacante envía un correo electrónico comercial muy convincente para conseguir que un empleado normal haga clic en un enlace o descargue un archivo adjunto de correo electrónico para comprometer la red de la empresa. El atacante elige una hora concreta según el calendario del objetivo e inserta un sentido de emergencia en el correo electrónico para conseguir que el empleado actúe con rapidez.

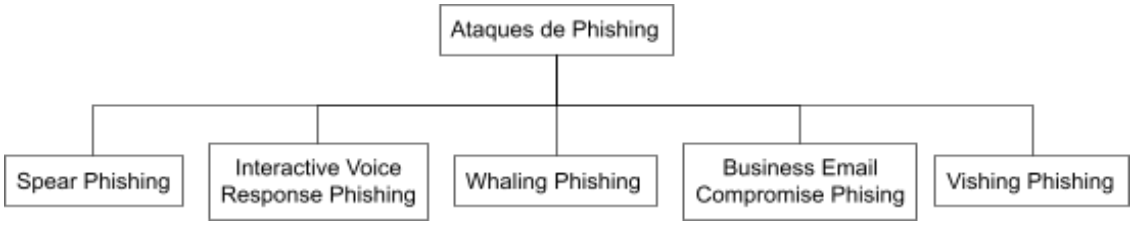


*Ilustración 6: Tipos de ataques de Phishing*

Por tanto, un ataque de Phishing sería tal que así de manera habitual:

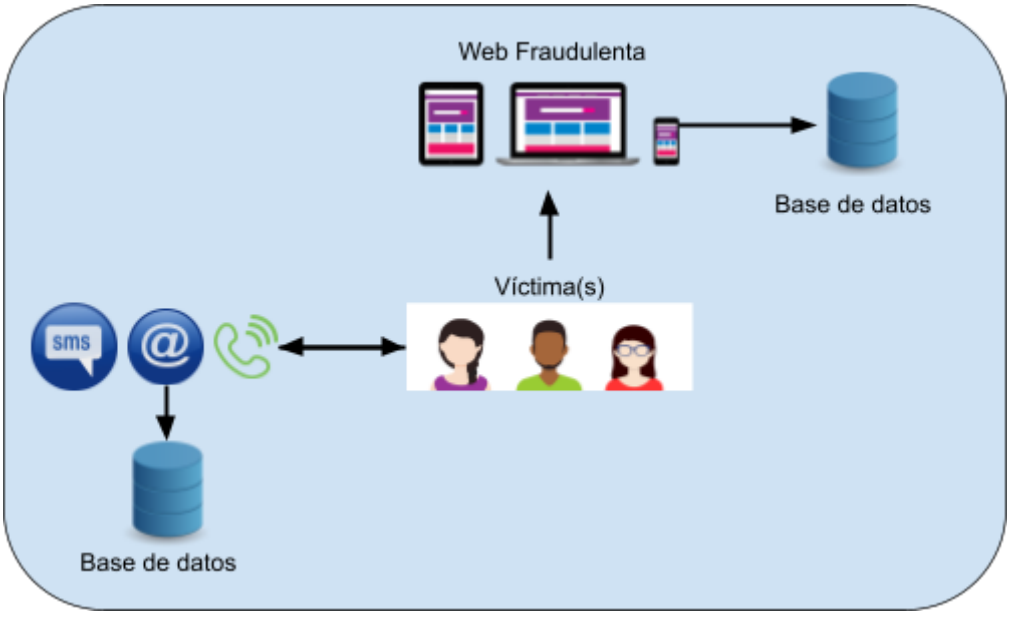


*Ilustración 7: Tácticas comunes de ataques phishing*

- Pretexting:

Los ataques de pretexto involucran crear situaciones ficticias y creíbles para obtener información personal de la víctima, aprovechándose de pretextos que hagan que ésta confíe en el atacante. Estos ataques pueden llevarse a cabo a través de llamadas telefónicas, correos electrónicos o incluso medios físicos, y suelen basarse en la información publicada en guías telefónicas, páginas web públicas o eventos en los que se reúnen profesionales del mismo ámbito. El pretexto utilizado puede ser una oferta de servicios o empleo, solicitud de información personal, asistencia a un amigo para acceder a algo o incluso una falsa promoción de lotería.

- Baiting:

El baiting es una técnica de ingeniería social que se utiliza para atraer a las víctimas y hacer que entreguen información confidencial o descarguen código malicioso, mediante la oferta de algo que resulte interesante o valioso. Esta técnica se utiliza en diversas formas de ataques de phishing, como la estafa nigeriana y los ataques de cebo, también conocidos como road apples.

Los ataques de cebo pueden ser más o menos ingeniosos, y pueden implicar dejar unidades USB infectadas con malware en lugares públicos para que alguien las encuentre y las utilice. También pueden incluir la oferta de descargas de software, música o juegos gratuitos que en realidad están infectados con malware. En algunos casos, los atacantes pueden simplemente ofrecer algo que parezca valioso para atraer a las víctimas.

Los ataques de cebo también pueden actuar como troyanos, en los que el ataque se realiza explotando material informático no seguro, como soportes de almacenamiento o unidades USB que contienen malware. Cuando las víctimas conectan la unidad USB a sus ordenadores, la unidad actúa como un troyano del mundo real y ataca el ordenador. Este tipo de ataque realiza acciones maliciosas en segundo plano sin que las víctimas se den cuenta.

- Tailgating:

Los ataques de seguimiento, también conocidos como piggybacking o acceso físico, son una técnica utilizada por los atacantes para acceder a áreas restringidas o edificios sin autorización. Esta técnica consiste en seguir a alguien que tiene autorización de seguridad para acceder a una zona o edificio, lo que permite al atacante entrar sin que se detecte su presencia. Por ejemplo, un atacante puede pedir a una persona que mantenga la puerta abierta o puede tomar prestado un dispositivo de un empleado para realizar actividades maliciosas como instalar software malicioso.

Los ataques a tarjetas RFID son un ejemplo común de ataques de seguimiento. Debido a su amplia utilización y bajo costo, los sistemas de identificación por radiofrecuencia (RFID) son la tecnología más emergente utilizada por las empresas para controlar el acceso a sus instalaciones. Sin embargo, presentan vulnerabilidades que pueden ser explotadas por los atacantes para acceder a zonas restringidas y causar graves problemas de seguridad a las empresas.

Los ataques RFID pueden realizarse en varias capas del modelo de sistema de interconexión (ISO), como la capa física y la capa de red. En la capa física, el atacante puede atacar los dispositivos RFID y la interfaz física para manipular la comunicación RFID y causar daños temporales o permanentes en las tarjetas RFID. En la capa de red, el atacante puede manipular la red RFID y la comunicación entre las entidades RFID, lo que puede permitirle acceder a inversa información confidencial o causar daños en el sistema de seguridad de la empresa.

- Otros:

Existen otros tipos de ataques de ingeniería social, entre los que se incluyen los ataques de ransomware, los ataques de software falso, los ataques de ingeniería social inversa y las ventanas emergentes.

Los **ataques de ransomware** son un tipo de ataque que se dirige a particulares y empresas. Este tipo de ataque cifra los archivos y datos de la víctima, bloqueando su acceso, y exige un rescate para desbloquearlos. Este pago se realiza con Bitcoins, una moneda digital difícil de rastrear. Los ataques de ransomware constan de seis etapas: creación del malware, despliegue, instalación, mando y control, destrucción y extorsión. Las empresas afectadas pueden sufrir los resultados del ataque de ransomware durante años debido a la pérdida de negocio, clientes, datos y productividad.

**Los ataques de software falso**, también conocidos como sitios web falsos, se basan en sitios web falsos para hacer creer a las víctimas que se trata de software o sitios web conocidos y de confianza. La víctima introduce información de inicio de sesión real en el sitio web falso, lo que proporciona al atacante las credenciales de la víctima para utilizarlas en el sitio web legítimo, como el acceso a cuentas bancarias en línea. Un ejemplo de estas amenazas es el ataque tabnabbing.

**Los ataques de ingeniería social inversa** son aquellos en los que el atacante pretende resolver un problema de la red, anunciando que es la única persona que puede solucionarlo. Una vez que se le proporciona acceso a la red, el atacante puede obtener información valiosa sin ser detectado.

Por último, los **ataques de ventanas emergentes** son aquellos en los que aparece una ventana en la pantalla de la víctima informando de que se ha perdido la conexión. El usuario reacciona volviendo a introducir la información de inicio de sesión, lo que ejecuta un programa malicioso ya instalado con la aparición de la ventana. Este programa reenvía remotamente la información de inicio de sesión al atacante.

Existen muchos otros tipos de ataques que pueden resumirse en los siguientes:

Ataques de suplantación de identidad en Help Desk: el atacante se hace pasar por alguien con autoridad o empleado de una empresa y llama al help desk solicitando información o servicios.
Ataques Dumpster Diving: consisten en recoger documentos sensibles de la basura de la empresa o de equipos desechados como material informático antiguo, unidades de disco, CD y DVD.
Ataques Quid Pro Quo: ataques de cebo que ofrecen servicios gratuitos para seducir a la víctima. Exigen un intercambio de información a cambio de un servicio o producto.
Ataques de robo por desvío: consisten en desviar a una empresa de transporte para que entregue un mensajero o un paquete en el lugar deseado.

Ataques de Shoulder surfing: consisten en observar a la víctima mientras introduce contraseñas o información sensible.
Ataques de robo de documentos importantes: consisten en robar archivos del escritorio de alguien por intereses personales.
Ataques de pharming: el atacante roba el tráfico procedente de un sitio web específico redirigiéndolo a otro sitio web falso con el fin de obtener la información transportada. Este ataque funciona pirateando el servidor del sistema de nombres de dominio (DNS) y aprovechando cualquier vulnerabilidad para cambiar la dirección del protocolo de Internet (IP) de la máquina anfitriona y del servidor.
Robocalls: son llamadas masivas automáticas con mensajes pregrabados que se dirigen a números de teléfono conocidos y utilizan el protocolo de voz sobre Internet. Cuando se responde, el número de teléfono se almacena en la base de datos del atacante y, aunque se pueden bloquear estas llamadas, los sistemas de los atacantes llaman desde otros números. Este tipo de ataque es un grave problema en muchos países y la única forma de detenerlo es no contestar a números desconocidos.

## 2.7. ¿Cómo podemos evitar ser engañados mediante ingeniería social?

Para evitar ser engañados mediante ingeniería social, es necesario tomar medidas de seguridad adecuadas y ser conscientes de las tácticas utilizadas por los delincuentes. En este apartado, se describen algunas recomendaciones:

1. Educación y concienciación:

La educación y la concienciación son fundamentales para prevenir la ingeniería social. Los usuarios deben estar informados sobre los riesgos asociados a la manipulación psicológica y conocer las técnicas de ingeniería social que se utilizan con más frecuencia. La concienciación también puede ayudar a reducir la curiosidad por hacer clic en enlaces sospechosos, descargar archivos desconocidos y compartir información personal con extraños.

2. Desconfianza por defecto:

Es importante tener cuidado con los correos electrónicos que tengan el asunto "urgente" o "confidencial" provenientes de entidades financieras o instituciones, ya que es común que los delincuentes intenten obtener información personal mediante engaños. Las entidades financieras nunca solicitan claves de acceso por correo electrónico, por lo que es mejor no ingresar a enlaces sospechosos y en caso de duda, contactar directamente a la entidad para verificar la autenticidad del correo.

3. Verificación de identidad:

La verificación de identidad es una práctica importante para prevenir la ingeniería social. Los usuarios deben comprobar la identidad de los remitentes de correos electrónicos, mensajes de texto y llamadas telefónicas antes de compartir información confidencial o hacer clic en enlaces. Es recomendable utilizar sistemas de autenticación de dos factores y preguntas de seguridad para añadir una capa adicional de seguridad.

4. Actualizaciones y parches:

Las actualizaciones y parches de seguridad son importantes para prevenir la explotación de vulnerabilidades en el software y el hardware. Los usuarios deben asegurarse de que sus dispositivos y aplicaciones estén actualizados y parcheados para protegerse contra las vulnerabilidades conocidas.

5. Contraseñas seguras:

Las contraseñas seguras son fundamentales para proteger las cuentas de los usuarios contra el acceso no autorizado. Los usuarios deben utilizar contraseñas únicas, largas y complejas, y cambiarlas regularmente. También es recomendable utilizar gestores de contraseñas para generar y gestionar contraseñas seguras.

6. Protección contra malware:

La protección contra malware es importante para prevenir la ingeniería social que utiliza archivos infectados o sitios web maliciosos. Los usuarios deben utilizar software de seguridad actualizado, como antivirus y antimalware, y evitar descargar archivos de fuentes desconocidas o hacer clic en enlaces sospechosos.

7. Protección contra el correo electrónico:

Existen diversas herramientas que pueden ayudarnos a proteger nuestros correos electrónicos de diferentes riesgos y amenazas. Por ejemplo, Abnormal es una solución en la nube que analiza más de 5.000 señales para detectar anomalías y bloquear con precisión todo el spam y los correos electrónicos de ingeniería social, tanto internos como externos. Barracuda utiliza técnicas como el análisis de virus, el análisis en tiempo real y la prevención de enlaces de URL para proporcionar la mejor protección. Su centro de operaciones de amenazas global monitorea continuamente nuevas vulnerabilidades de seguridad. Por su parte, Mimecast es un gestor de correo electrónico que protege las comunicaciones de los empleados contra amenazas específicas, como ataques de phishing, malware, ataques de ransomware y filtraciones de datos.

8. Políticas de seguridad:

Las políticas de seguridad son importantes para prevenir la ingeniería social en las organizaciones. Las empresas deben implementar políticas y procedimientos de seguridad sólidos, incluyendo la formación de los empleados sobre la ingeniería social y la implementación de medidas de seguridad física y lógica. Por ejemplo, algunas medidas incluyen la política de "Least Privilege" para limitar permisos, uso de scripts para comunicaciones, tener un punto de contacto para reportar incidentes, y crear una cultura organizacional de conciencia compartida sobre la ingeniería social.

9. Compartir información limitada:

Los usuarios deben limitar la cantidad de información personal que comparten en línea y con extraños. La información personal, como la fecha de nacimiento, la dirección y los detalles financieros, pueden ser utilizados por los delincuentes para la ingeniería social y el fraude. Por tanto, en una empresa deben existir directrices claras para evitar la publicación de información sensible en cualquier tipo de contenido, ya sean documentos, videos o imágenes corporativas. Es importante establecer pautas precisas sobre qué tipo de información se puede compartir públicamente y cómo debe ser manejada para garantizar la seguridad y privacidad de la empresa.

10. Borrado de metadatos:

Es recomendable automatizar la eliminación de metadatos en documentos donde no sean necesarios, no solo antes de su publicación, sino también en aquellos que inicialmente no fueron concebidos para su divulgación y que eventualmente puedan ser expuestos por medios alternativos.

11. Supervisión de la información:

En un entorno en el que el manejo de la información publicada se escapa de nuestro control, es fundamental establecer una supervisión continua de la información en línea. Esta supervisión debe ser constante para poder identificar la aparición de nueva

información y, en caso necesario, tomar medidas para su eliminación. Asimismo, se recomienda encarecidamente llevar a cabo una monitorización constante de posibles fugas de información que puedan aparecer en Internet. Esta tarea puede ser automatizada para poder detectar posibles vulnerabilidades de seguridad de las que no se tenía conocimiento previo.

12. Limitar medios de contacto telefónico:

Se recomienda la no publicación de números de teléfono directos de los empleados ni de extensiones internas de una empresa para evitar suplantaciones de identidad. También se sugiere centralizar las llamadas en una centralita y desviar solicitudes de información crítica al correo electrónico. Es fundamental comprobar la identidad del llamante antes de facilitar información crítica o realizar ciertas acciones. En el caso del CAU, se sugiere centralizar la gestión de solicitudes y utilizar un sistema de tickets para hacer referencia a cada solicitud. Si un técnico del CAU contacta con un empleado, siempre deberá facilitar el número de ticket. No se debe revelar información sensible o realizar acciones comprometidas sin haber verificado la identidad de la otra persona. Las empresas que externalizan el sistema de atención al usuario deben solicitar al proveedor medidas de seguridad y formación específica, y establecer una política clara sobre la información sensible.

13. Auditorías, medición y seguimiento:

Dentro de una empresa, es importante realizar pruebas de penetración periódicas por profesionales para evaluar los riesgos de ataques maliciosos, incluyendo la ingeniería social. Esto permite definir una política de seguridad adecuada y desarrollar acciones de formación y concienciación adaptadas a las necesidades de la organización.

14. Control de acceso físico:

Las empresas deben asegurarse de que sus instalaciones y equipos estén protegidos físicamente contra el acceso no autorizado. Esto incluye la implementación de medidas de seguridad, como cámaras de seguridad, tarjetas de acceso, cerraduras de puertas y otros dispositivos de seguridad.

## 2.8. ¿Qué tipo de información pueden llegar a obtener los ciberdelincuentes?

La habilidad de un experto consolidado en Ingeniería Social tiene un poder significativo que va más allá de obtener información puntual. Pueden influir en la opinión pública mediante el uso de distintas técnicas. Estas técnicas puede resultar en la obtención de diversos tipos de información, incluyendo datos financieros, credenciales privadas, perfiles de usuarios y otros datos confidenciales.

Asimismo, para realizar este apartado nos vamos a enfocar en las competiciones llamadas Social Engineering Capture the Flag (SECTF). Estas competiciones buscan demostrar el grado de amenaza que la ingeniería social representa para las empresas y cómo los concursantes se aprovechan de sus habilidades para obtener información importante de ciertas empresas.

El SECTF es una competencia en la que los participantes deben superar una serie de desafíos de seguridad informática, específicamente relacionados con la Ingeniería Social, en un formato similar al juego "Capture the Flag". Estos desafíos suelen tener un plazo límite y, después de su finalización, se publican las soluciones para que todos puedan conocer las técnicas utilizadas por los participantes.

El objetivo principal de los participantes en este tipo de competiciones suele ser obtener diferentes piezas de información, también conocidas como "flags". Para conseguirlas, los participantes suelen utilizar diferentes técnicas según la fase del concurso en la que se encuentren. En la primera fase, se suele permitir el uso de fuentes públicas de información (OSINT). En cambio, en la segunda fase, los participantes suelen realizar llamadas telefónicas en directo para obtener la información requerida. En resumen, los participantes deben utilizar diferentes estrategias y técnicas para conseguir las piezas de información necesarias, según la fase del concurso en la que se encuentren.

Además, los participantes suelen tener asignadas empresas reales a las que deben atacar y obtener información que ha sido previamente definida a través de un catálogo de preguntas. El objetivo es demostrar la cantidad de información que se puede obtener..

Es crucial destacar que los participantes en el SECTF deben cumplir con una normativa muy rigurosa, ya que es necesario garantizar la protección de las empresas que son el objetivo de la competición.

Para ejemplificar las posibilidades de obtención de información mediante ingeniería social, se presenta a continuación un conjunto de “flags” que los participantes debieron obtener durante la edición de SECTF en 2019 en la Def Con y Euskalhack:

| Lista de Flags de un SECTF |
|---|
| **Logística** |
| ¿El soporte de IT es interno o subcontratado? |
| ¿Qué empresa de paquetería utilizan? |
| ¿Cuál es el horario de recogida/entrega de paquetería? |
| ¿Tienen cafetería? |
| ¿Quién gestiona el servicio de comedor? |
| ¿Utilizan destructoras de papel? |
| |
| **Otras tecnologías** |
| ¿Bloquean sitios web? |
| En caso afirmativo ¿Cuáles? (Twitter, Instagram, etc.) |
| ¿Cuál es el nombre de la empresa VPN? |
| ¿Tienen WIFI? (sí/no) |
| En caso afirmativo ¿Cuál es el SSID? (identificador de la red inalámbrica) |
| ¿Qué marca y modelo de ordenadores utilizan? |
| ¿Qué antivirus utilizan? |

| |
|---|
| **Puede ser utilizado como pretexto in situ** |
| ¿Cuál es el nombre de la empresa de servicio de limpieza? |
| ¿Cuál es el nombre de la empresa que se encarga de las máquinas expendedoras? |
| ¿Quién se encarga de la exterminación de insectos/ plagas en la empresa? |
| ¿Quién se encarga de la gestión de los residuos / basura? |
| ¿Nombre de la empresa de guardas de seguridad? |
| ¿Qué tipo de tarjeta utilizan para acceder a la empresa? (RFID, HID, ninguna) |
| |
| **Tecnología general de la empresa** |
| ¿Qué sistema operativo utilizan? |
| ¿Cuál es la versión de service pack? |
| ¿Qué programa utilizan para abrir documentos PDF y que versión? |
| ¿Utilizan servicios como wetransfer para enviar información? |
| ¿Qué navegador utilizan? |
| ¿Qué versión? |
| ¿Qué cliente de correo utilizan? |
| ¿Utilizan algún gestor de contraseñas? |
| ¿Utilizan encriptación de disco?  En caso afirmativo ¿de qué tipo? |
| URL falsa (hacer que el objetivo visite la URL: http://www.empresa-support.es) |
| |
| **Información específica de empleados** |
| ¿Cuánto tiempo lleva trabajando para la empresa? |
| ¿Qué día del mes se cobra? |
| Información del calendario (inicio / fin de la jornada, descansos, comidas) |
| ¿Cuál es el organigrama de la organización? |
| ¿Qué operador de telefonía utilizan? |
| ¿Cuál es la última vez que han recibido una formación sobre concienciación en seguridad? |

*Tabla 7: Listado de Flags de un SECTF*

## 2.9. ¿Cómo pueden los cibercriminales obtener beneficios sobre la información obtenida?

Los cibercriminales pueden sacar provecho económico y no económico de la información obtenida tras un ataque de ingeniería social. Algunas de las posibles formas en que pueden usar la información robada incluyen:

### 1) Venta de datos:

#### a) Venta de datos personales:

Los cibercriminales pueden obtener datos personales valiosos, como nombres, direcciones, números de teléfono y direcciones de correo electrónico, mediante la realización de ataques de ingeniería social. Luego, pueden vender estos datos a otras personas que los utilizarán para el fraude de identidad, la suplantación de identidad, la creación de cuentas falsas en línea y otras actividades ilegales.

Además, es alarmante pensar que nuestra información más confidencial y privada puede ser adquirida por cualquiera que esté dispuesto a pagar por ella. A continuación, algunos de los precios por los que puedes conseguir diferentes tipos de datos personales:

**Carnets de conducir escaneados, entre 5 y 25 dólares**. Tus datos de identificación personal son sumamente valiosos para los criminales, ya que les permiten suplantar tu identidad y cometer fraudes en tu nombre. Por eso, no es sorprendente que los carnets de conducir escaneados puedan ser vendidos por unos pocos dólares.

**Servicios de suscripción**, **entre 0,5 y 8 dólares** en el mercado negro**.** Algunas personas también pueden estar vendiendo tus datos de suscripción, como tus nombres de usuario y contraseñas de sitios web y aplicaciones populares. Esto puede permitirles acceder a tus cuentas y robar información adicional, o incluso hacer compras en tu nombre.

**Pasaportes escaneados, entre 6 y 15 dólares**. Tus datos de pasaporte, como tu nombre completo, fecha de nacimiento y número de pasaporte, son también muy valiosos para los criminales. Con esta información, pueden realizar actividades ilegales en tu nombre o incluso falsificar un pasaporte falso a tu nombre.

**Selfie con documentos, entre 40 y 60 dólares.** Los criminales también pueden estar interesados en obtener imágenes de ti con tus documentos personales, como tu carnet de conducir o pasaporte. Estas imágenes pueden ser utilizadas para falsificar documentos y cometer fraudes en tu nombre.

**Historial médico, entre 1 y 30 dólares.** Tus datos de salud son también muy valiosos para los criminales, ya que pueden utilizarlos para obtener medicamentos con receta o incluso para cometer fraudes de seguros.

**Identificación, entre 0,5 y 10 dólares.** Por último, cualquier tipo de información de identificación personal, como tu nombre completo, dirección y número de teléfono, puede ser vendida por unos pocos dólares. Esto puede permitir que los criminales te contacten para intentar estafarte o incluso acosarte.

#### b) Venta de información financiera:

Mediante ataques de ingeniería social, los cibercriminales pueden adquirir información financiera valiosa como números de tarjetas de crédito, cuentas bancarias y contraseñas. Una vez que obtienen esta información, la pueden vender en el mercado negro para ser utilizada en actividades fraudulentas como compras en línea, transferencias de fondos y otros tipos de fraudes financieros.

En el cado de los **datos de tarjeta de crédito**, se pueden vender en el mercado negro **entre 6 y 10 dólares.** Sí, has leído bien, tus datos de tarjeta de crédito pueden estar siendo vendidos por unos pocos dólares en el mercado negro. Esto significa que cualquier persona puede acceder a tu información de pago y utilizarla para fines ilícitos.

### c) Venta de información empresarial:

Los ataques de ingeniería social no también pueden ser utilizados para acceder a información empresarial confidencial. Los cibercriminales pueden utilizar técnicas de ingeniería social para obtener acceso a las redes informáticas empresariales y a los correos electrónicos de los empleados. Una vez que logran acceder a esta información, pueden venderla en el mercado negro de la Deep Web. Esto quiere decir, que una vez dentro, pueden obtener información empresarial confidencial, como planes de negocio, información de clientes, propiedad intelectual y secretos comerciales.

### d) Venta de acceso a sistemas:

Los ciberdelincuentes que utilizan ataques de ingeniería social para obtener acceso no autorizado a sistemas informáticos a menudo buscan obtener beneficios financieros al vender ese acceso.

Estos delincuentes pueden vender el acceso a estos sistemas en foros clandestinos de Internet, donde pueden encontrar compradores interesados en obtener estos accesos para llevar a cabo actividades maliciosas o para obtener información valiosa de las víctimas.

La venta de acceso a sistemas puede ser una actividad muy lucrativa para los ciberdelincuentes, ya que los compradores pueden estar dispuestos a pagar grandes sumas de dinero por el acceso a sistemas valiosos. Además, los ciberdelincuentes pueden utilizar métodos sofisticados de ocultación y anonimato para evitar ser detectados por las autoridades y para mantener su anonimato en línea.

## 2) Venta de recursos:

### a) Botnets:

A menudo, los ataques de ingeniería social se centran en dejar una semilla en el ordenador infectado, pudiendo hacer cualquier ordenador parte de la botnet del atacante. Estas botnets se utilizan a menudo para enviar spam, realizar ataques de denegación de servicio (DDoS) o para minar criptomonedas. Los cibercriminales pueden vender el acceso a estas botnets a otros delincuentes para que puedan llevar a cabo sus propias actividades maliciosas y de esa manera sacar un beneficio económico.

### b) Ransomware:

El ransomware es un tipo de ataque informático en el que, una vez que el atacante ha logrado entrar al sistema mediante ingeniería social, busca encriptar la mayor cantidad posible de archivos de la empresa con el fin de bloquear el acceso a ellos. Si logra

afectar una gran cantidad de archivos o incluso el backup, la única forma de recuperarlos es pagando un rescate. Este tipo de ataques son muy lucrativos para los cibercriminales, ya que pueden obtener grandes sumas de dinero al encriptar los archivos de una empresa importante.

c) Minería de criptomonedas:

De la misma manera que una botnet, el ciberdelincuente puede decidir utilizar el dispositivo de la víctima para minar criptomonedas. Este modelo se hizo muy frecuente en la pandemia, donde este tipo de acción era bastante lucrativa dado que los cibercriminales pueden utilizar el poder de procesamiento de los dispositivos vulnerados. Estas criptomonedas pueden ser vendidas en el mercado para obtener beneficios..

3) Extorsión:

Primero, los cibercriminales buscan acceder a sistemas informáticos vulnerables, a menudo mediante técnicas como el phishing o la ingeniería social. Una vez dentro del sistema, pueden robar información confidencial como datos personales, credenciales de inicio de sesión, información financiera, documentos confidenciales, entre otros.

Luego, utilizan esta información para extorsionar a la víctima, amenazando con hacer pública la información o dañar su reputación o sus operaciones comerciales si no se les paga una cantidad de dinero. Los cibercriminales también pueden utilizar el ransomware para cifrar archivos importantes del sistema de la víctima y pedir un rescate para desbloquearlos.

## 2.10. A nivel legal, ¿esta serie de actuaciones están perseguidas por la Ley?

La Ley Orgánica 10/1995, del Código Penal, es la principal normativa en España para los ataques de ingeniería social. Sin embargo, la aplicación de la ley dependerá de la utilización de la información obtenida mediante dichos ataques. Aunque inicialmente se puede considerar una infracción del artículo 248 del Código Penal, la aplicación de otros artículos dependerá de la situación específica, dónde dependiendo la acción realizada por el ciberdelincuente, incurrirá en un tipo de sanción u otra:

- *Artículo 248:*

Este artículo establece que se considera estafa "el engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno". Los ataques de ingeniería social pueden incluir técnicas que buscan engañar a las víctimas para que realicen acciones que les perjudiquen, como proporcionar información confidencial o realizar transferencias de dinero.

Asimismo, aquellos que cometan el delito de estafa serán sancionados con una sentencia de prisión que puede variar entre seis meses y tres años. La gravedad de la infracción se valorará teniendo en cuenta varios factores, como el importe defraudado, el impacto económico sufrido por la víctima, la relación entre la víctima y el delincuente, los métodos utilizados por el delincuente y cualquier otra circunstancia relevante.

Los siguientes artículos son relevantes en situaciones de ataques de ingeniería social, aunque su aplicación dependerá de cada caso particular:

- Artículo 264:

El artículo regula el sabotaje informático y aunque no hace referencia explícita a los ataques de ingeniería social. Castiga las acciones que provocan la inutilidad de datos informáticos, programas informáticos o documentos electrónicos ajenos sin autorización y de manera grave. Por tanto, el sabotaje informático es perseguido por la ley en España, y podría ser aplicado en ataques de ingeniería social.

- Artículo 197:

Este artículo establece que comete este delito "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación". Este artículo puede ser aplicable en aquellos casos en los que se obtiene información privada de manera ilícita a través de técnicas de ingeniería social.

- Artículo 270:

El artículo castiga con prisión de seis meses a cuatro años y multa de doce a veinticuatro meses a quien, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. Este artículo se aplicaría en un ataque de ingeniería social porque castiga la explotación económica de obras sin autorización, lo que puede incluir el engaño de personas para obtener información o acceso a dichas obras.

Cabe recalcar que estos artículos no hacen referencia explícita al término "ingeniería social", sino que se refieren a delitos informáticos relacionados con la obtención fraudulenta de información, datos personales a través de medios electrónicos o situaciones que podrían darse en un ataque de ingeniería social.

Dentro del Código Penal Español, existen varios artículos que pueden estar relacionados con la ingeniería social, debido al uso inapropiado de la información obtenida o las acciones realizadas. La tabla proporcionada muestra diferentes tipos de ciberdelitos que se encuentran contemplados en la legislación española, aunque no todos ellos serán aplicables a ataques de ingeniería social. Puede ser interesante saber sobre ellos dado que pueden estar relacionados entre sí.

| DESIGNACIÓN | CÓDIGO PENAL ESPAÑOL | TIPO DE HECHO |
|---|---|---|
| Acceso e interceptación ilícita | Art. 197 a 201. Descubrimiento y revelación de secretos | Descubrimiento/revelación de secretos |
| | | Acceso ilegal informático |
| | Art. 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial) | Otros relativos al mercado/consumidores |
| Interferencia en los datos y en el | Arts. 263 a 267 y 625.1. Daños y daños informáticos | Daños |

| sistema | | Ataques informáticos |
|---|---|---|
| Falsificación Informática | Arts. 388-389, 399 bis, 400 y 401 | Falsificación de moneda, sellos y efectos timbrados |
| | | Fabricación tenencia de útiles para falsificar |
| | | Usurpación del estado civil |
| Fraude Informático | Arts. 248 a 251 y 623.4 | Estafa bancaria |
| | | Estafas con tarjetas de crédito, débito y cheques de viaje |
| | | Otras estafas |
| Delitos Sexuales | Arts. 181, 183.1,183.bis,184, 185, 186, 189 | Exhibicionismo |
| | | Provocación sexual |
| | | Acoso sexual |
| | | Abuso sexual |
| | | Corrupción de menores/incapacitados |
| | | Pornografía de menores |
| | | Delito de contacto mediante tecnología con menor de 13 años con fines sexuales |
| Contra la propiedad industrial e intelectual | Arts. 270 a 277 y 623.5 (Contra la propiedad intelectual y contra la propiedad industrial) | Delitos contra la propiedad industrial |
| | | Delitos contra la propiedad intelectual |
| Contra el Honor | Arts. 205 a 210 y 620.2 | Calumnias |
| | | Injurias |
| Delitos contra la salud pública | Arts. 359 a 371 | Tráfico de drogas |
| | | Otros contra la salud pública |
| Amenazas y coacciones | Arts. 169 a 172 y 620 | Amenazas |
| | | Amenazas a grupo étnico cultural o religioso |
| | | Coacciones |

*Tabla 8: Ciberdelitos en el Código Penal*

# 3. Fase de implementación

Es importante señalar que en esta sección se busca llevar a cabo la puesta en marcha o implementación de las herramientas que el autor del TFM considere necesario. Si bien hay algunos aspectos específicos que se investigarán como el phishing o temas relacionados a la inteligencia artificial, estos no son esenciales y, por lo tanto, existirá una amplia variedad de herramientas o implementaciones que el autor podrá utilizar para este apartado.

## 3.1. Phishing:

### 3.1.1. Clonación manual:

Con el fin de llevar a cabo este apartado, se pretendía clonar la página web de la universidad para luego simular un ataque de phishing local. Para llevar a cabo este proceso, se instaló XAMPP para la ejecución local del sitio clonado.
Es importante destacar que no se usó ninguna herramienta para realizar la clonación. En su lugar, se hizo clic derecho en la página web original y se seleccionó la opción "Guardar como". Posteriormente, se modificó el código para asegurarse de que todos los recursos cargaran correctamente.

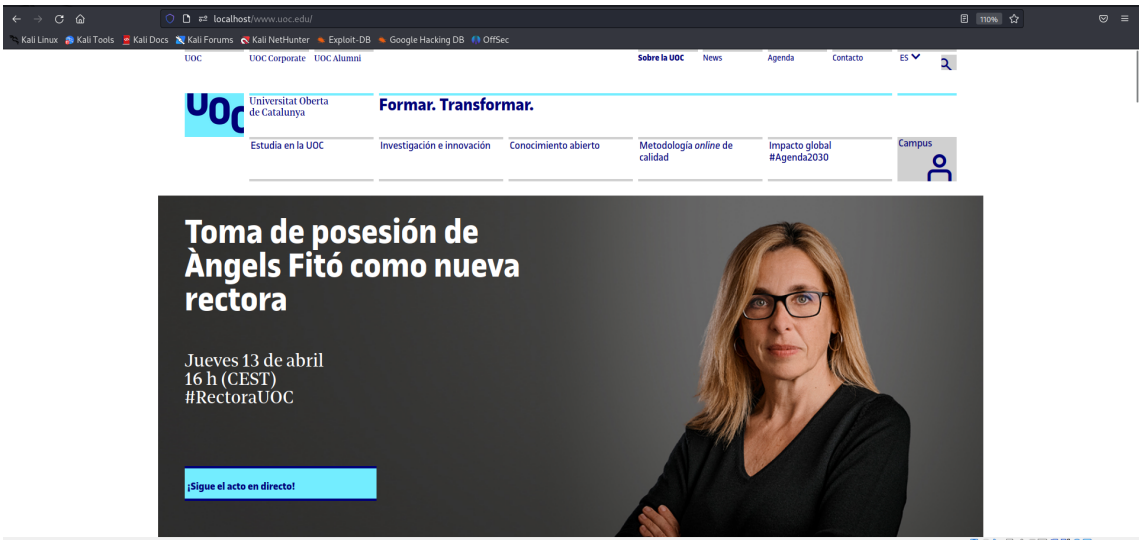


*Ilustración 8: Página web UOC clonada en local*

Tras la clonación del índice, nos interesaba que el apartado “Campus” redireccione a nuestro login local malicioso por lo que cambiamos el redireccionamiento.

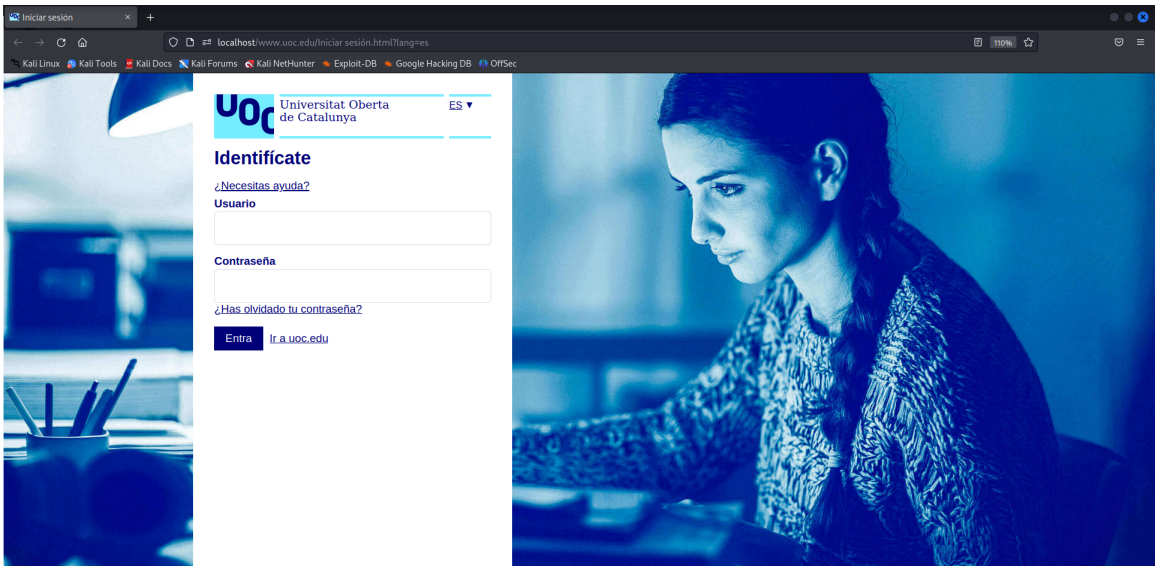


*Ilustración 9: Inicio de Sesión de la UOC clonada en local*

Se han implementado modificaciones en el código de inicio de sesión que permiten guardar el nombre de usuario y la contraseña una vez que el usuario ha hecho clic en el botón "Entra". Luego, estos datos se almacenan en una base de datos antes de redireccionar al usuario a la página oficial de inicio de sesión. Si no se proporcionan las credenciales adecuadas, se mostrará un mensaje de error.

También se han realizado modificaciones en el código debido a problemas que surgieron al llamar a Google Analytics, lo que resultaba en una URL confusa al intentar iniciar sesión. El código importante que recoge los datos del usuario en nuestra base de datos es el siguiente:

```
// Iniciar sesión.html
// Obtener elementos del DOM
const usernameInput = document.getElementById('username');
const passwordInput = document.getElementById('password');
const submitButton =
document.getElementById('identification-form').querySelector('button
[type="submit"]');

// Agregar evento de clic al botón de enviar
submitButton.addEventListener('click', function (event) {
// Prevenir que el formulario se envíe automáticamente
   event.preventDefault();

   // Obtener valores de usuario y contraseña
   const username = usernameInput.value.trim();
   const password = passwordInput.value.trim();

   // Validar campos vacíos
   if (username === '' || password === '') {
```

```
      alert('Por favor, ingresa tu usuario y contraseña.');
      return;
   }

   // Enviar datos a PHP usando AJAX
   const xhr = new XMLHttpRequest();
   xhr.open('POST', 'guardar_datos.php', true);
   xhr.setRequestHeader('Content-type',
'application/x-www-form-urlencoded');
   xhr.onreadystatechange = function () {
      if (xhr.readyState === 4 && xhr.status === 200) {
         // Redirigir a la URL deseada
         window.location.href =
'http://cv.uoc.edu/auth?campus-nplincampus';
      }
   };
   const data = `username=${username}&password=${password}`;
   xhr.send(data);
});
```

```
// guardar_datos.php
<?php
// Obtener valores de usuario y contraseña
$username = $_POST['username'];
$password = $_POST['password'];

// Conectar a la base de datos
$mysqli = new mysqli('localhost', 'root', '', 'basedatos');

// Verificar la conexión
if ($mysqli->connect_error) {
  die('Error de conexión (' . $mysqli->connect_errno . ') ' .
$mysqli->connect_error);
}

// Preparar y ejecutar la consulta SQL
$sql = "INSERT INTO usuarios (username, password) VALUES
('$username', '$password')";
if ($mysqli->query($sql) !== TRUE) {
  echo 'Error al guardar los datos: ' . $mysqli->error;
}

// Cerrar la conexión a la base de datos
```

```
$mysqli->close();
?>
```

Se ha realizado un vídeo para poder ver de manera dinámica el funcionamiento y no llenar este apartado de imágenes innecesarias.

- URL: https://youtu.be/k0WKNSSdorw

Observación: Aunque se probaron diversas herramientas para realizar la clonación automática, como Social-Engineering-Toolkit, goclone y wget, llevar a cabo la clonación manualmente proporcionó una impresión más completa que las herramientas automáticas.

### 3.1.2. Campaña de correos:

Para este apartado, vamos a utilizar la herramienta **Gophish**. Esta herramienta se utiliza para crear y ejecutar campañas de phishing de manera controlada con el fin de evaluar la seguridad y concienciar a los usuarios sobre las técnicas de phishing.

Gophish nos permite a los usuarios enviar correos electrónicos de phishing y simular ataques de phishing para medir la capacidad de los usuarios para detectar y responder a estas amenazas. La herramienta también permite personalizar los correos electrónicos de phishing y el contenido de la página de inicio de sesión falsa para que se adapten a un objetivo específico.

Para emplearla, descargamos el software, otorgamos los permisos de ejecución correspondientes y lo ejecutamos. Con estos tres sencillos pasos, accedemos a una interfaz gráfica fácil de utilizar para llevar a cabo nuestras campañas de phishing.

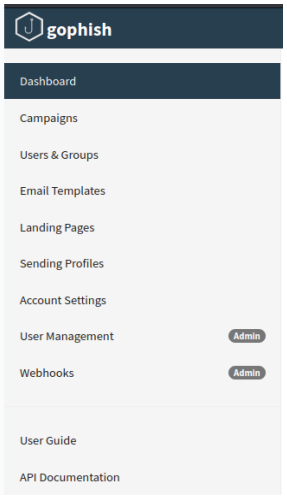


*Ilustración 10: Opciones de la interfaz gráfica de Gophish*

En este caso, nos vamos a centrar en 5 apartados: “Sending Profiles”, “Landing Pages”, “Email Templates”, “User & Groups” y “Campaigns”.

El **apartado de Sending Profiles en Gophish** es donde se configura el servidor de correo electrónico utilizado para enviar correos electrónicos de phishing durante la campaña.

Requiere que se configure una cuenta de correo electrónico válida para enviar correos electrónicos de phishing. Para ello, se ha creado una nueva cuenta de hotmail llamada “c.ontacto_c.liente_a.dmin@hotmail.com”.

En esta sección, configuraremos el servidor SMTP, el puerto, el protocolo de seguridad y las credenciales de autenticación para la cuenta de correo electrónico.

La configuración de Sending Profiles es importante ya que permite a Gophish enviar correos electrónicos de phishing desde una cuenta de correo electrónico válida y de confianza, lo que aumenta las posibilidades de que los correos electrónicos de phishing lleguen a la bandeja de entrada de los destinatarios y se abran.

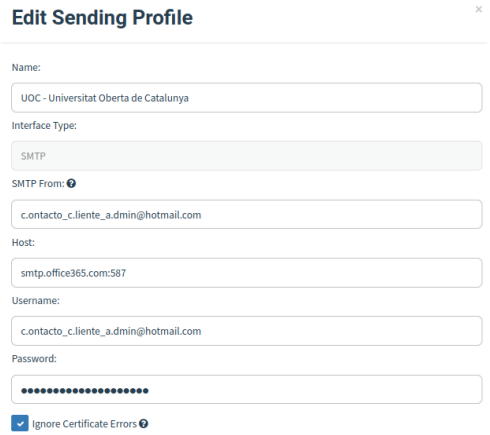


*Ilustración 11: Configuración de Gophish - Sending Profiles*

El **apartado de Landing Pages en Gophish** se utiliza para crear y personalizar las páginas de inicio de sesión falsas que se utilizan en una campaña de phishing.

Las páginas de inicio de sesión falsas son una técnica común utilizada en los ataques de phishing, donde los atacantes crean páginas web que se asemejan a la página de inicio de sesión real de un sitio web legítimo. En nuestro caso, ya hemos realizado esto en el apartado de “Clonación manual”. Por tanto, sólo tendremos que importar nuestra web clicando en “Import Site”.

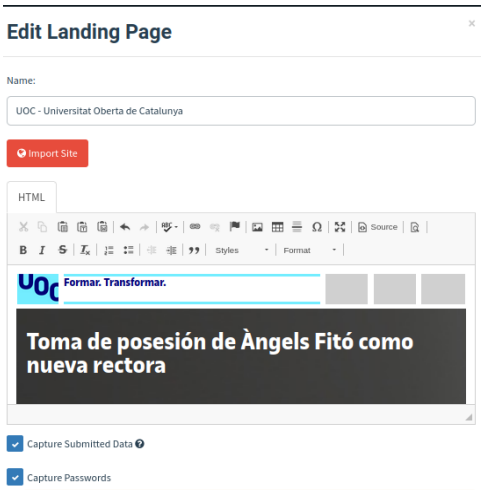


*Ilustración 12: Configuración de Gophish - Landing Pages*

El **apartado de Email Templates en Gophish** se utiliza para crear y personalizar plantillas de correo electrónico que se utilizan en una campaña de phishing.

Las plantillas de correo electrónico son la base de una campaña de phishing exitosa, ya que deben ser convincentes y persuasivas para que los destinatarios abran y respondan al correo electrónico. En Gophish, el apartado de Email Templates permite a los usuarios crear plantillas de correo electrónico personalizadas que se adaptan a un objetivo específico.

En nuestro caso, lo más realista sería crear nuestra propia plantilla de correo electrónico personalizada utilizando el editor de HTML integrado de Gophish. Ya que tenemos mensajes de la UOC por el hecho de ser estudiantes, sería apropiado aprovecharse de eso para realizar nuestra plantilla. Para ello, clicamos en cualquier mensaje de la UOC => Mostrar original => Copiar en portapapeles.

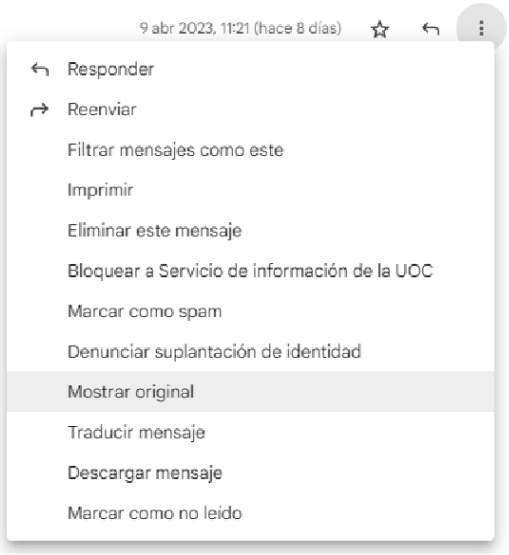


*Ilustración 13: Email Templates - Crear Plantilla 1*

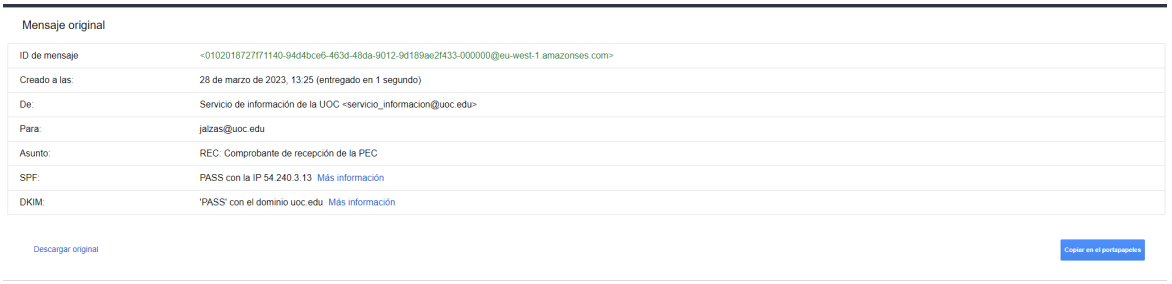


*Ilustración 14: Email Templates - Crear Plantilla 2*

Además, el apartado de Email Templates también permite a los usuarios configurar los detalles del correo electrónico, como el asunto, el cuerpo del mensaje, los archivos adjuntos y los enlaces. Estos detalles son importantes para hacer que el correo electrónico parezca lo más auténtico posible y engañar a los usuarios.

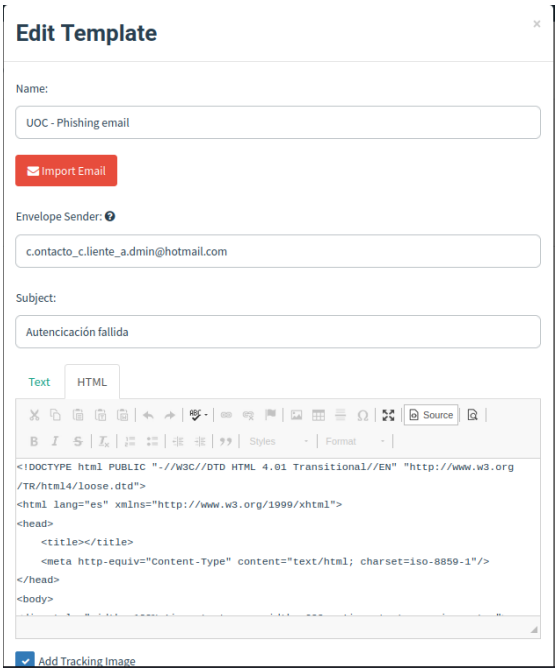


*Ilustración 15: Email Templates - Editar plantilla*

El **apartado de Users & Groups en Gophish** se utiliza para agregar y administrar usuarios y grupos que se incluirán en una campaña de phishing.

En Gophish, los usuarios y grupos representan los destinatarios a los que se enviarán los correos electrónicos de phishing durante una campaña. El apartado de Users & Groups permite a los usuarios agregar manualmente destinatarios individuales o importar una lista de destinatarios a través de un archivo CSV.

Además, el apartado de Users & Groups también permite a los usuarios crear grupos de destinatarios basados en características similares. Estos grupos permiten a los usuarios enviar correos electrónicos de phishing personalizados a un grupo específico de destinatarios y evaluar la efectividad de la campaña en un subconjunto específico de usuarios.

En el apartado de Users & Groups, los usuarios también pueden ver el estado de los destinatarios, como si han abierto el correo electrónico de phishing, si han hecho clic en el enlace o si han ingresado sus credenciales de inicio de sesión. Esta información es importante para evaluar la efectividad de la campaña de phishing y realizar mejoras para futuras campañas. En este caso, la página de inicio de sesión no se encuentra enlazada directamente, por lo que sabremos que los destinatarios han hecho clic en el enlace cuando accedan al apartado "Campus" y proporcionen sus credenciales de inicio de sesión.

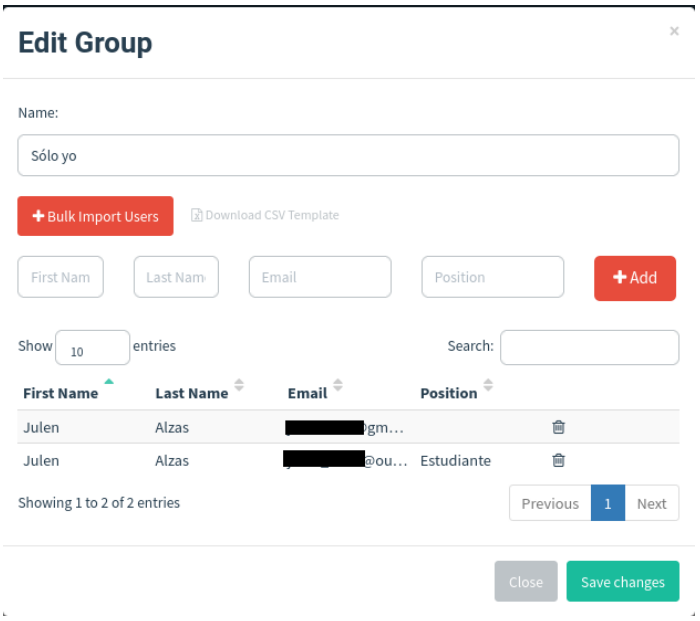


*Ilustración 16: Configuración de Gophish - Users & Groups*

El **apartado de Campaigns en Gophish** se utiliza para crear, configurar y lanzar una campaña de phishing.

Una campaña de phishing se refiere al proceso de enviar correos electrónicos de phishing a un grupo de destinatarios, con el objetivo de engañarlos para que hagan clic en un enlace o proporcionen información confidencial. El apartado de Campaigns permite a los usuarios configurar y personalizar los detalles de una campaña de phishing, incluyendo los correos electrónicos, las páginas de inicio de sesión falsas, los destinatarios y los informes.

La configuración de los apartados anteriores nos permitirá  crear una nueva campaña de phishing o modificarla a nuestro antojo.De esta manera, podremos  seleccionar los destinatarios de la campaña, el template utilizado como mensaje, agregar usuarios individuales o grupos previamente creados o utilizar distintas web “malintencionadas”.

Además, el apartado de Campaigns también permite a los usuarios configurar los detalles de la campaña, como el nombre, el asunto del correo electrónico, el horario de inicio y finalización y los intervalos de envío de correos electrónicos. También pueden configurar los informes de la campaña, como la frecuencia de actualización y el formato del informe.

Una vez que se ha configurado la campaña de phishing, los usuarios pueden lanzarla y realizar un seguimiento del progreso en el apartado de Campaigns.

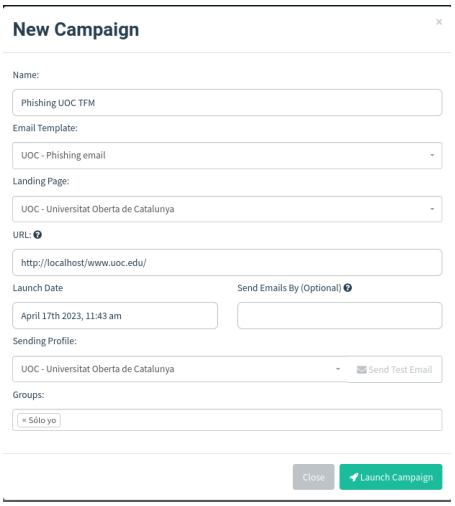


*Ilustración 17: Configuración de Gophish - Users & Groups*

Por tanto, el mensaje que le llegaría a la víctima sería el siguiente:


*Ilustración 18: Mensaje de llegada a la víctima*

En el siguiente vídeo se puede observar que el despliegue de la campaña funciona perfectamente: https://youtu.be/9h_2cDhbUAc

### 3.1.3. Clonaciones ya realizadas por herramientas:

**Zphisher** es una herramienta automatizada de phishing con más de 30 plantillas que nos ofrece una posibilidad de realizar phishing sin tener ningún tipo de conocimiento. Además, de manera predeterminada ofrece la ejecución en localhost, Cloudflare y LocalXpose. La amplia variedad que proporciona se puede ver en la siguiente imagen:


*Ilustración 19: Menú Phishing Zphisher*

Cada una de las plataforma a elegir ofrece una variedad de opciones distintas, en nuestro caso vamos a realizar la prueba con el inicio de sesión de Instagram:

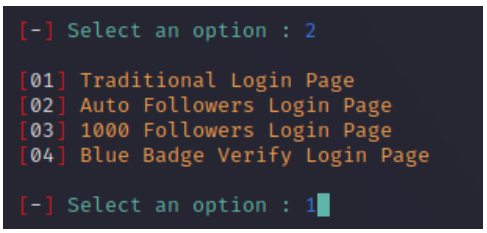


*Ilustración 20: Zphisher elegir opción*

Elegimos la opción localhost:


Ilustración 21: Zphisher elegir servicio

Ya lo tenemos de manera local:

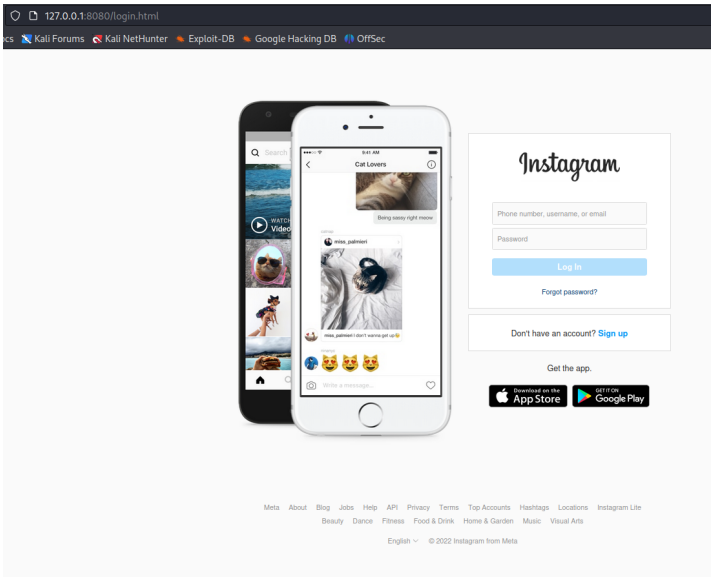


*Ilustración 22: Zphisher phishing Instagram*

En caso de querer tener una URL accesible por cualquiera en internet, simplemente tendríamos que utilizar la opción Cloudflared o LocaXposet. En este caso lo realizamos con Cloudflare:

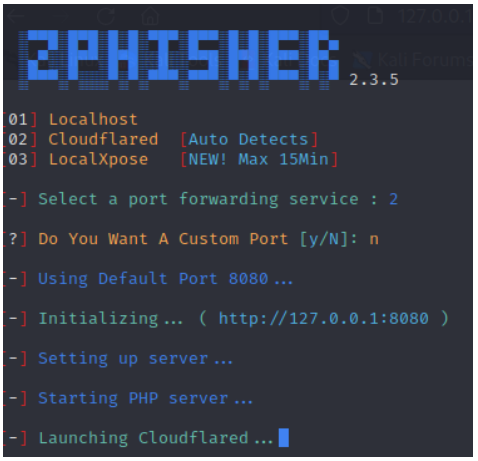


*Ilustración 23: Zphisher Cloudflared*


Ilustración 24: Zphisher Cloudflared URLs

La recolección de información se guarda en archivos locales de la máquina cómo “ip.txt” o “usernames.dat”:


*Ilustración 25: Zphisher - Recolección de datos*

Se ha realizado un vídeo en el que se prueban varias plataformas distintas. Se puede observar en éste enlace:

- URL: https://youtu.be/NUgVHxvm57k

### 3.1.4. QR Maliciosos:

"**Social Engineering Toolkit**" es una herramienta que se centra en la ingeniería social, tal como lo sugiere su nombre. Entre sus funciones, incluye la capacidad de generar códigos QR maliciosos que pueden dirigir a los usuarios a una página web comprometida:

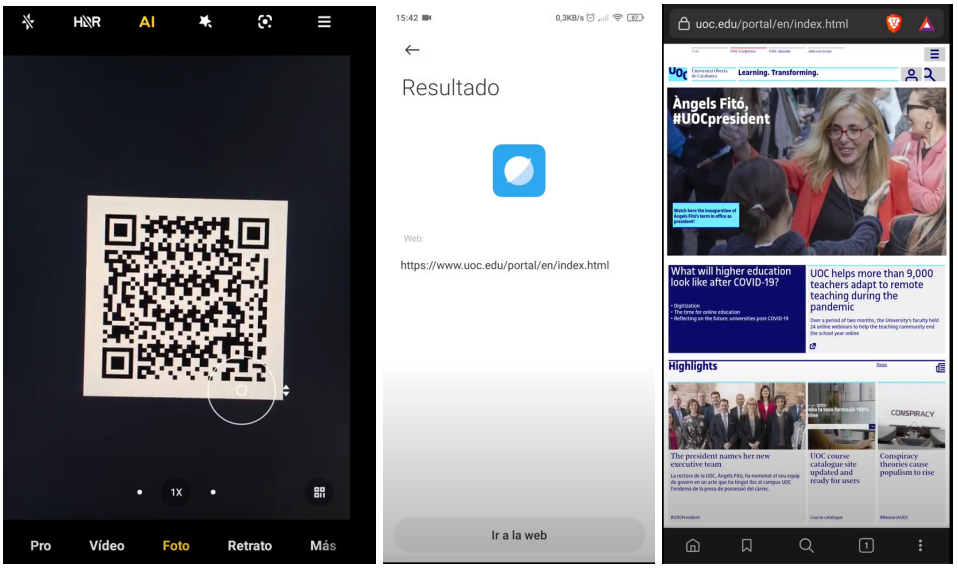


*Ilustración 26: QR Malicioso*

Un ciberdelincuente podría utilizar un código QR en múltiples contextos. Por ejemplo, podrían colocar el código en una tarjeta de presentación para dirigir a los usuarios a una página web falsa que les pida sus credenciales de inicio de sesión. O podrían poner el código en un cartel en una calle muy transitada, promocionando un falso concurso con un gran premio. Los usuarios que escaneen el código serían dirigidos a una página web que solicite información personal, como su nombre completo y número de teléfono, y esto se utilizaría para llevar a cabo actividades maliciosas, como el robo de identidad o el fraude.

## 3.2. OSINT:

Realizar un apartado general de OSINT puede resultar poco efectivo si no se tiene un objetivo concreto en mente. La búsqueda de información puede variar muchísimo dependiendo de la situación o el propósito que se tenga. Por esta razón, en lugar de enfocarme en una lista predefinida de herramientas, prefiero utilizar aquellas que me aporten información relevante y de interés según lo que busque en ese momento.

Cada situación requiere un enfoque distinto, por lo que siempre es importante tener claro el objetivo y adaptarse a las herramientas que mejor se ajusten a él. La clave del éxito en OSINT radica en saber cómo utilizar las herramientas adecuadas para cada situación y estar en constante búsqueda de nuevas fuentes de información.

### 3.2.1. Localizar a la víctima

Nuestro objetivo será obtener la ubicación de la víctima, para lo cual utilizaremos la herramienta "**seeker**". Al hacer clic en un enlace, la víctima será redirigida a una plataforma que le solicitará permisos de ubicación. Una vez que la víctima acepte el uso de la ubicación, será redirigida a la URL de destino sin sospechar nada fuera de lo común, ya que la solicitud de ubicación parecerá legítima:

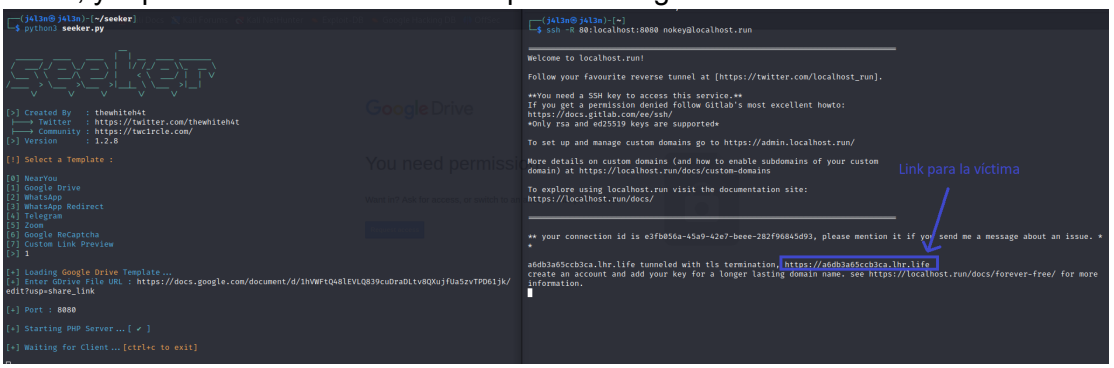


*Ilustración 27: Seeker - Atacante*

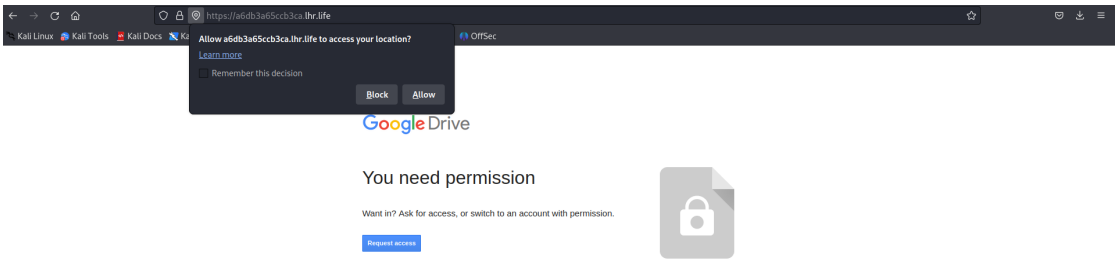


*Ilustración 28: Seeker Víctima*

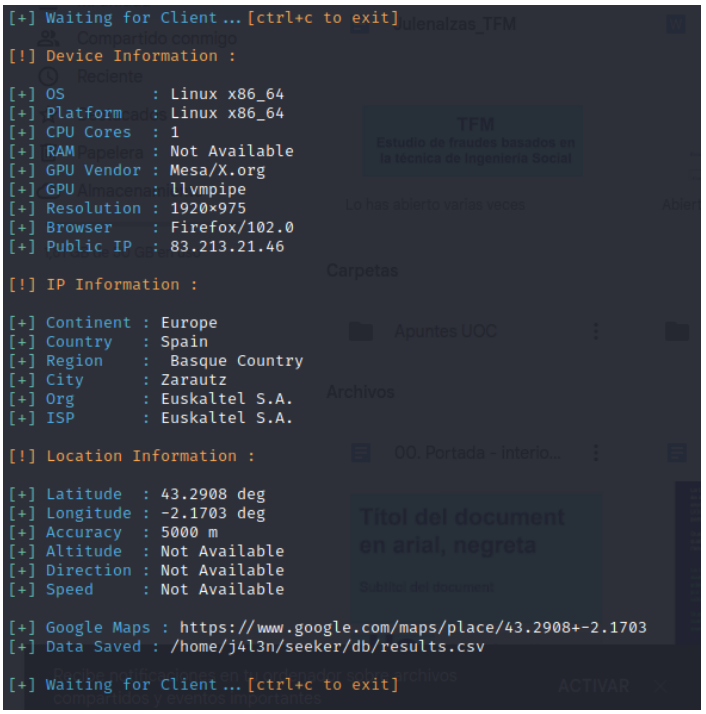


*Ilustración 29: Seeker - Datos obtenidos*

Como podemos observar, la herramienta ofrece una plantilla de posibles plataformas con las que se nos pedirán los permisos de ubicación. En el siguiente vídeo podemos observar el funcionamiento tanto con Drive como Whatsapp:

- URL: https://youtu.be/QAX87ZJ-sa0

### 3.2.2. TheHarvester:

Es una herramienta que se caracteriza por ser fácil de utilizar y al mismo tiempo potente. Su propósito es proporcionar información valiosa durante la etapa de reconocimiento de una evaluación de “red team” o una prueba de penetración. La herramienta se enfoca en la recopilación de inteligencia de fuentes abiertas (OSINT), con el fin de determinar el panorama de amenazas externas de un dominio en particular.

Para probarla, simplemente vamos a intentar que la herramienta recopile información de “www.uoc.edu”, realizando un comando en el que se iteren todos los recursos públicos que no necesiten una clave API para obtener resultados:

```
shell> for i in anubis baidu bevigil bing bingapi bufferoverun
certspotter crtsh dnsdumpster duckduckgo hackertarget omnisint otx
qwant rapiddns sublist3r threatcrowd threatminer urlscan yahoo; do
theHarvester -d www.uoc.edu -b $i; done
```

En la siguiente imagen se pretende mostrar una imagen editada de todos los resultados:

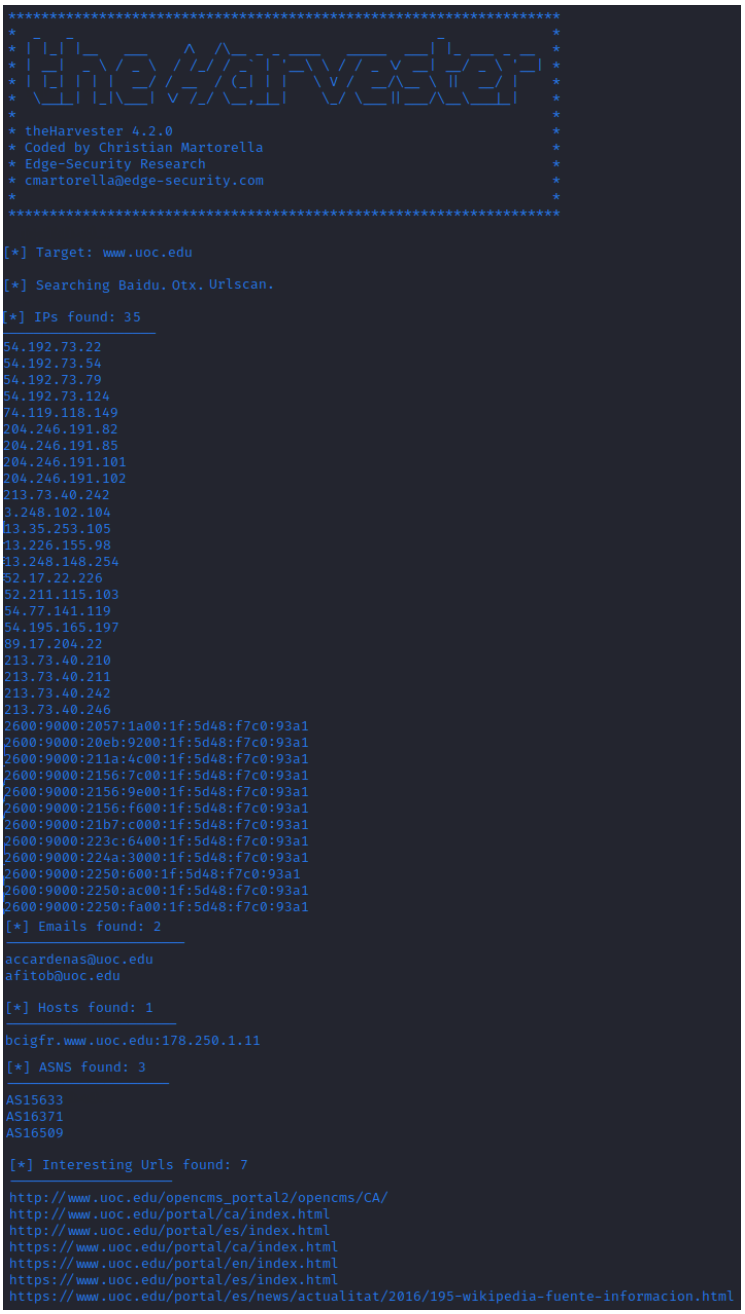


*Ilustración 30: TheHarverster*

Con tan solo unos minutos, un ciberdelincuente que quisiera atacar a alguien de la UOC habría obtenido 35 IPs, 2 emails, 1 host, 3 ASN (Autonomous System Number) asociados con el dominio objetivo y 7 URLs interesantes. Por tanto, aunque no todo el contenido obtenido sea de calidad para el cibercriminal, con tan solo un comando ya tendría información con la complementar su ataque de ingeniería social.

En caso de desear ver la ejecución cicar en el siguiente enlace. Resumidamente, es lo que aparece en la imagen anterior:

- URL: https://youtu.be/Sf3-VrAiEq0

## 3.3. IA:

En los últimos tiempos, la inteligencia artificial ha estado en constante desarrollo y puede convertirse en el mejor aliado de un ciberdelincuente. En este trabajo, nos enfocaremos en algunos aspectos que resultan interesantes. Debido a que la IA no es determinista, los resultados obtenidos pueden ayudarnos a inferir si las herramientas utilizadas son aptas para ser usadas en ataques de ingeniería social.

Aunque no se buscará entrenar modelos en detalle, ya que esto podría requerir demasiado tiempo y exceder el alcance del proyecto, en ciertos casos podría ser interesante realizar este tipo de entrenamiento para evaluar su utilidad. Además, se abordarán conceptos como ChatGPT, DALL·E 2, deepfakes y clonación de voz con el objetivo de determinar si las herramientas utilizadas son viables en un ataque de ingeniería social.

### 3.3.1. DALL·E 2

DALL·E 2 es una herramienta de inteligencia artificial creada por OpenAI que tiene la capacidad de generar imágenes a partir de descripciones de texto. Esta tecnología utiliza un modelo de aprendizaje profundo que es capaz de crear representaciones visuales detalladas de objetos, animales y escenas complejas, a partir de simples descripciones de texto.

Sin embargo, al igual que ocurre con otras tecnologías de IA, DALL·E 2 también puede ser utilizada con fines maliciosos. Los ciberdelincuentes podrían utilizar esta herramienta para crear perfiles falsos con fotos creadas por IA, lo que les permitiría ocultar su verdadera identidad en línea y llevar a cabo actividades ilegales sin ser detectados.

Por lo tanto, crear perfiles falsos es más fácil que nunca, tan solo tengo que decirle a la inteligencia artificial que cree una imágen de una chica sevillana muy guapa y éste es uno de los resultado:

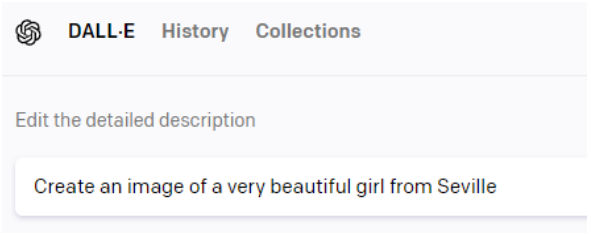


*Ilustración 31: DALL·E - Input para perfil falso*

*Ilustración 32: DALL·E - Resultado para perfil falso*

### 3.3.2. Chat Gpt

ChatGPT es un modelo de lenguaje natural basado en inteligencia artificial que tiene la capacidad de generar respuestas coherentes y contextuales a preguntas y conversaciones en diferentes idiomas. Debido a su habilidad para procesar y comprender el lenguaje humano, ChatGPT se ha convertido en una herramienta muy útil en una amplia variedad de situaciones relacionadas con la ingeniería social. Desde la generación de correos electrónicos persuasivos y engañosos hasta la simulación de conversaciones en línea con la intención de obtener información confidencial, este modelo de IA puede ser utilizado para llevar a cabo una amplia variedad de ataques de ingeniería social de manera efectiva.

Perfiles Falsos:

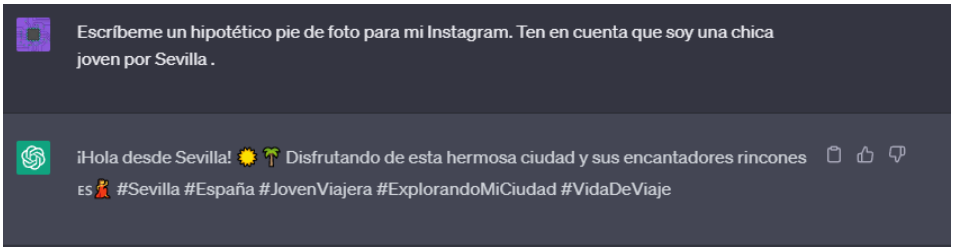


*Ilustración 33: ChatGPT - Pie de foto para Instagram*

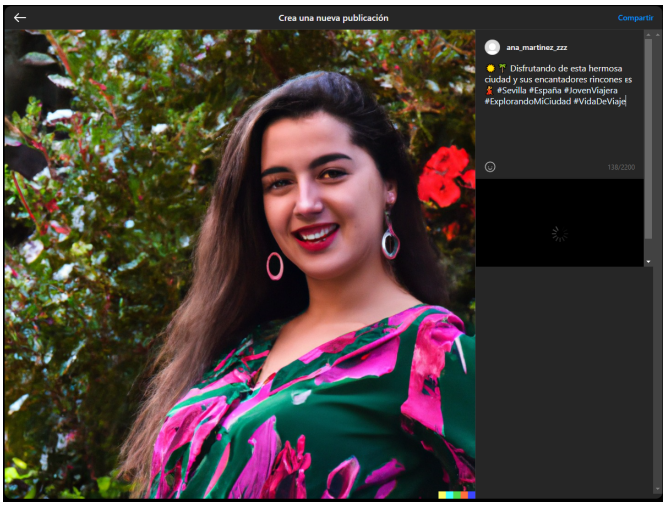


*Ilustración 34: Post de Instagram basado en* ChatGPT

Pretexting:

ChatGPT es capaz de generar tres situaciones de pretexting que podrían ser utilizadas por los ciberdelincuentes con tan solo un par de líneas. Por cuestiones de brevedad, solo se presentará la primera.

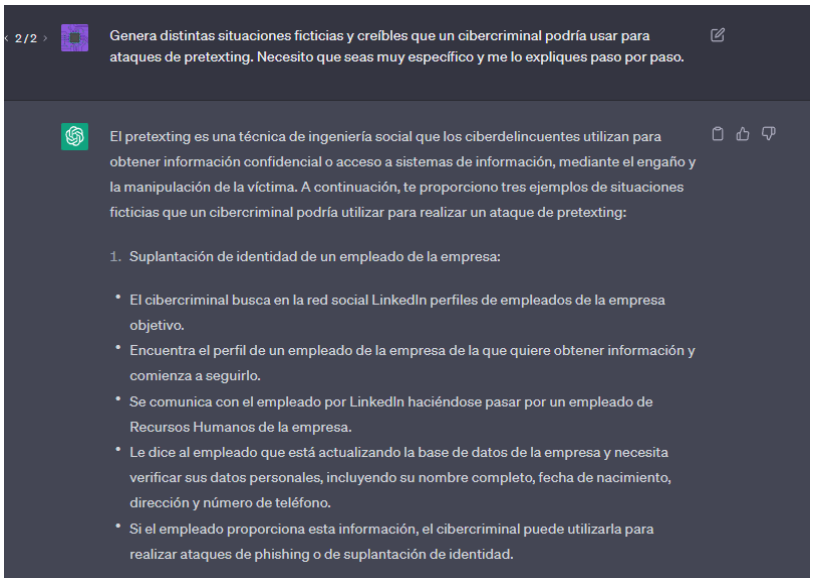


*Ilustración 35: ChatGPT - Pretexting*

Sobre la situación elegida, podemos especificar que sea aún más concreto en cómo podemos desarrollar el mensaje que debemos mandar. Por tanto, ya no es necesario para el atacante romperse la cabeza en la mayoría de situaciones.:

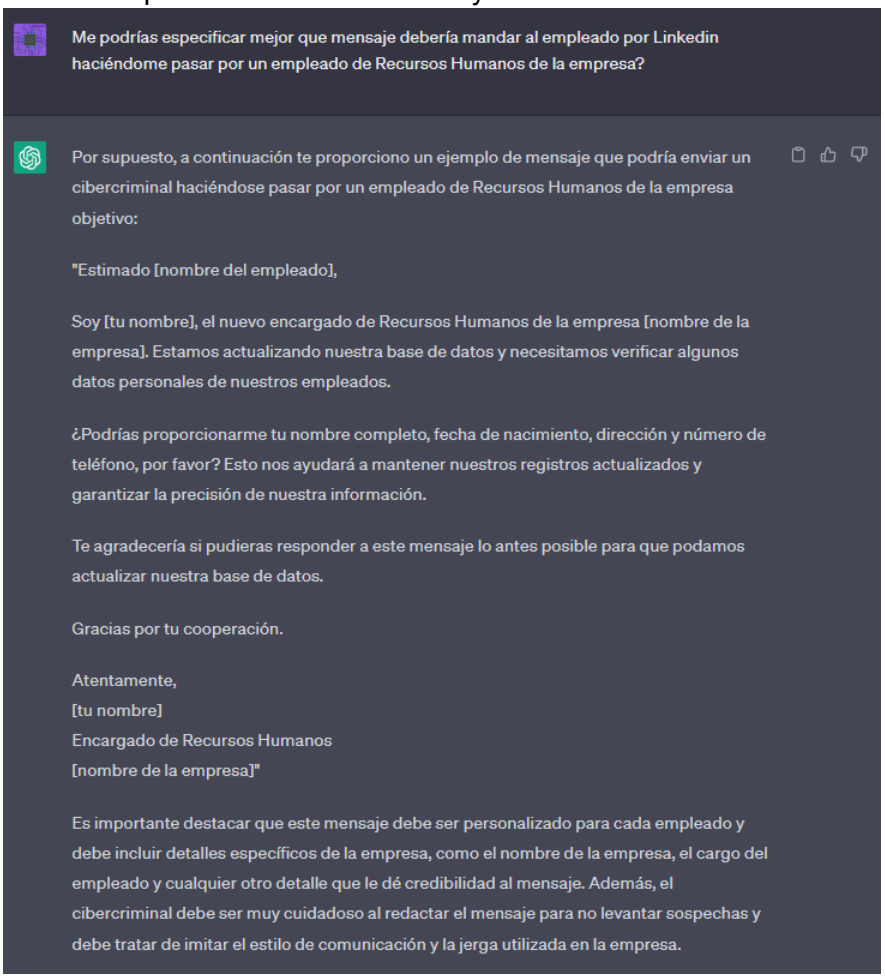


*Ilustración 36: ChatGPT - Pretexting 2*

OSINT:

Al igual que con la sección anterior, explorar todas las posibilidades de ChatGPT podría llevarnos a un sinfín de opciones. Por lo tanto, en su lugar, me limitaré a recomendar el artículo "103 OSINT ChatGPT Prompt Ideas", que ofrece una amplia variedad de ideas que pueden ser experimentadas con ChatGPT relacionadas al OSINT.

### 3.3.3. Deep fakes

En un mundo en el que la inteligencia artificial puede suplantar a cualquier persona mediante medios comunes como un ordenador en casa, podríamos pensar que existen diversas formas en que los deepfakes pueden ser utilizados para la ingeniería social:

- Suplantación de identidad: Se puede utilizar el Deepfake para crear videos falsos de una persona y hacer que parezca que está diciendo algo que nunca dijo. Esto puede utilizarse para difundir información falsa, manipular a la gente o difamar a alguien.
- Fraude financiero: Se puede utilizar el Deepfake para crear videos falsos de un CEO de una empresa y hacer que parezca que está autorizando una transacción financiera importante. Esto puede engañar a los empleados de la empresa y llevar a cabo una transferencia fraudulenta de fondos.
- Extorsión: Los delincuentes pueden utilizar el Deepfake para crear videos falsos de alguien en una situación comprometida y amenazar con hacerlo público si la víctima no cumple con sus demandas.
- Manipulación política: Los videos Deepfake pueden ser utilizados para crear discursos falsos de políticos o líderes mundiales y manipular la opinión pública.

En mi caso, tenía la intención de realizar pruebas prácticas de Deepfake utilizando un video de cinco minutos de duración de una persona con la herramienta FaceSwap. Para lograrlo, tenía pensado utilizar un video de Luisito Comunica (Top 5 MIS POLÉMICAS 2019) hablando frente a la cámara, el cual podría simular una entrevista ficticia con cualquier persona o cualquier otro método para conseguir el vídeo. Se había editado y acortado el vídeo para que la IA sólo reconozca la cara de Luisito. En la siguiente imagen se puede apreciar cómo se desenfocan varias partes del vídeo dado que la IA las reconocía cómo caras.


*Ilustración 37: Video luisito editado - Deepfake*

Tras esto, sólo necesitaba saber cuál era el video a suplantar. Parecía una buena idea utilizar el vídeo de Anton Fomenko llamado “How To Escape Being Held Hostage”.

Aquí, Anton escapa de estar atado en una silla, por lo que podría ser un buen contexto para un deepfake de ingeniería social.


*Ilustración 38: Video atado Anton - Deepfake*

Tras entrenar el modelo hasta 4 horas, el resultado fué completamente insatisfactorio. Aunque el vídeo fué recortado en muchas ocasiones, el hecho de tener una persona que no estuviera de frente hacia la cámara hacía que muchas veces ni siquiera captase bien el lugar donde realizar el “cambio de cara”.


*Ilustración 39: Resultados deepfake 1*

Posteriormente, decidí hacer un cambio radical, cambiaría el vídeo de Anton, por uno mucho más corto, de tan solo unos segundos. De manera que el entrenamiento sobre menos cantidad de fotogramas podría dar mejores resultados. Consiguientemente, pensando en un posible ataque de ingeniería social, busqué un vídeo corto relacionado a un arma de fuego para ponerle la cara de Luisito.

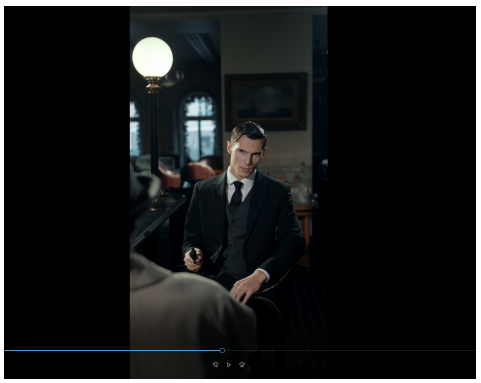

*Ilustración 40: Video de arma - Deepfake*

Tras entrenar el modelo 10 horas, los resultados fueron sorprendentemente peores o al menos parecidos.

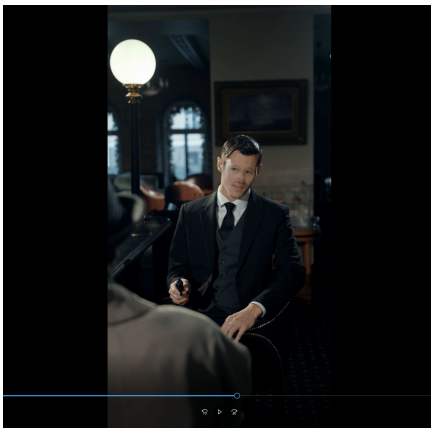

*Ilustración 41: Resultados deepfake 2*

Para finalizar y decidir si valía la pena seguir probando, decidí utilizar dos vídeos en el que el protagonista estuviera frente a la cámara, sin movimientos bruscos etc. Para ello, utilicé dos vídeos que no tienen nada que ver con el TFM, pero sirven como referencia para ver el tipo de resultado que aportan. Por un lado el vídeo de Luisito ya mencionado y otro llamado “PREGUNTAS Y RESPUESTAS DE CHILL #6 | IBAI LLANOS”. Podéis ver el resultado por vosotros mismos:

- URL: https://youtu.be/hNwkNDL2Qkw

| Graphs | # | Start | End | Elapsed | Batch | Iterations | EGs/sec |
|---|---|---|---|---|---|---|---|
| | 1 | 04/26/23 19:09:43 | 04/26/23 20:45:39 | 01:35:56 | 16 | 65426 | 363.7 |
| | 2 | 04/27/23 14:40:23 | 04/27/23 15:21:33 | 00:41:09 | 16 | 25262 | 327.4 |
| | 3 | 04/27/23 15:22:20 | 04/27/23 15:23:24 | 00:01:04 | 16 | 656 | 328.0 |
| | 4 | 04/27/23 16:02:41 | 04/27/23 16:55:49 | 00:53:08 | 16 | 23199 | 232.9 |
| | 5 | 04/27/23 17:11:01 | 04/27/23 18:44:24 | 01:33:23 | 16 | 53641 | 306.4 |
| | 6 | 04/27/23 19:25:15 | 04/27/23 21:57:08 | 02:31:52 | 16 | 104240 | 366.1 |
| | 7 | 04/28/23 14:44:34 | 04/28/23 15:25:24 | 00:40:49 | 16 | 25751 | 336.5 |
| | 8 | 04/28/23 15:27:24 | 04/28/23 15:56:48 | 00:29:24 | 16 | 16441 | 298.2 |
| | 9 | 04/28/23 16:07:31 | 04/28/23 16:08:59 | 00:01:27 | 16 | 791 | 290.9 |
| | 10 | 04/28/23 16:11:22 | 04/28/23 17:00:02 | 00:48:40 | 16 | 30315 | 332.2 |
| | 11 | 04/28/23 17:00:44 | 04/28/23 17:07:36 | 00:06:52 | 16 | 3316 | 257.6 |
| | 12 | 04/28/23 17:08:23 | 04/28/23 18:07:40 | 00:59:17 | 16 | 38870 | 349.7 |
| | 13 | 04/28/23 18:21:04 | 04/28/23 19:35:28 | 01:14:23 | 16 | 50772 | 364.0 |
| | Total | 04/26/23 19:09:43 | 04/28/23 19:35:28 | 11:37:24 | 16 | 438680 | 335.5 |

*Ilustración 42: Deepfake entrenado 11 horas*

## Conclusión deepfakes:

Después de llevar a cabo algunas pruebas en el campo del deepfake, he llegado a la conclusión de que para obtener los mejores resultados, los videos utilizados para el entrenamiento deben tener ciertas características específicas. En primer lugar, es recomendable que los videos se enfoquen de frente y que no tengan muchos cambios de cámara ni movimientos bruscos. Estas condiciones proporcionan estabilidad en la información de entrenamiento, lo que es esencial para que los algoritmos de deepfake produzcan resultados precisos y realistas.

Sin embargo, es importante tener en cuenta que el proceso de entrenamiento del modelo de deepfake puede ser muy lento, incluso con una tarjeta gráfica de alta gama como la RTX 3080 (que es mi caso). Esto se debe a que los modelos de deep learning son muy complejos y requieren mucho procesamiento para funcionar correctamente.

Además, existen otros factores que pueden afectar la calidad de los resultados obtenidos, como la calidad de los datos de entrenamiento y el modelo utilizado. Es posible que se requieran ajustes adicionales en el proceso de entrenamiento para obtener los mejores resultados posibles.

Cabe mencionar que los resultados obtenidos en estas pruebas pueden verse afectados por la herramienta utilizada, aunque se utilizó el repositorio de GitHub con más estrellas relacionadas al deepfake para asegurar la calidad de la herramienta. Sin embargo, esto no garantiza la perfección en los resultados, y puede requerir un proceso de prueba y error para obtener los mejores resultados posibles. En resumen, la experimentación y exploración continua en el campo del deepfake es crucial para lograr resultados más precisos y realistas. En nuestro caso, el entrenamiento no ha sido suficiente para conseguir un resultado realista.

Los ciberdelincuentes deben considerar la complexión física de la persona, así como el color de piel, cabello y otros detalles, ya que el parecido con la persona real es lo que hace que el deepfake sea más realista y convincente. Además, crear un deepfake puede llevar mucho tiempo y esfuerzo en comparación con otros tipos de ataques que pueden lograr resultados similares con menos dedicación y horas invertidas.

En cuanto a la calidad de los resultados, es fundamental considerar que los algoritmos de deepfake requieren una gran cantidad de datos de entrenamiento para producir resultados precisos y realistas, por lo que es necesario asegurarse de que los videos utilizados para el entrenamiento sean de buena calidad y cumplan con los requisitos necesarios.

Por último, es importante tener en cuenta que, incluso utilizando herramientas de alta calidad, los resultados obtenidos pueden no ser perfectos y pueden requerir ajustes adicionales en el proceso de entrenamiento para obtener resultados óptimos.

### 3.3.4. Clonado de voz

En esta sección se tiene en cuenta que un atacante podría obtener la voz de su víctima mediante una llamada telefónica, lo que podría permitir la creación de audios malintencionados y deepfakes con la voz de la víctima. Esto representa una posible vía de ataque que los ciberdelincuentes podrían utilizar para engañar o manipular a otros mediante el uso de la voz de la víctima.

Por consiguiente, se han grabado siete archivos de audio con el fin de evaluar si es posible llevar a cabo una clonación de voz precisa. Los archivos de audio servirán para determinar si la clonación de voz es satisfactoria o si el resultado es significativamente diferente al original. Este sería el contenido de los audios:

- Audio 1: No estoy seguro de que deba proporcionar esta información por teléfono.
- Audio 2: No entiendo por qué necesita esta información personal.

- Audio 3: Cómo puedo estar seguro de que usted realmente es quien dice ser.
- Audio 4: Lo siento, pero no puedo ayudarte con eso.
- Audio 5: No tengo autorización para proporcionar esa información.
- Audio 6: |No estoy cómodo compartiendo esa información por teléfono.
- Audio 7: Lo siento, pero no puedo tomar una decisión sobre eso en este momento.

Real-Time-Voice-Cloning

Después de hacer las configuraciones necesarias, se agregó una carpeta que contiene los archivos de audio mencionados anteriormente para que la herramienta pueda reconocerlos y tratar de clonarlos. Desafortunadamente, en este caso el resultado no fue satisfactorio y la herramienta no pudo producir una clonación de voz precisa.

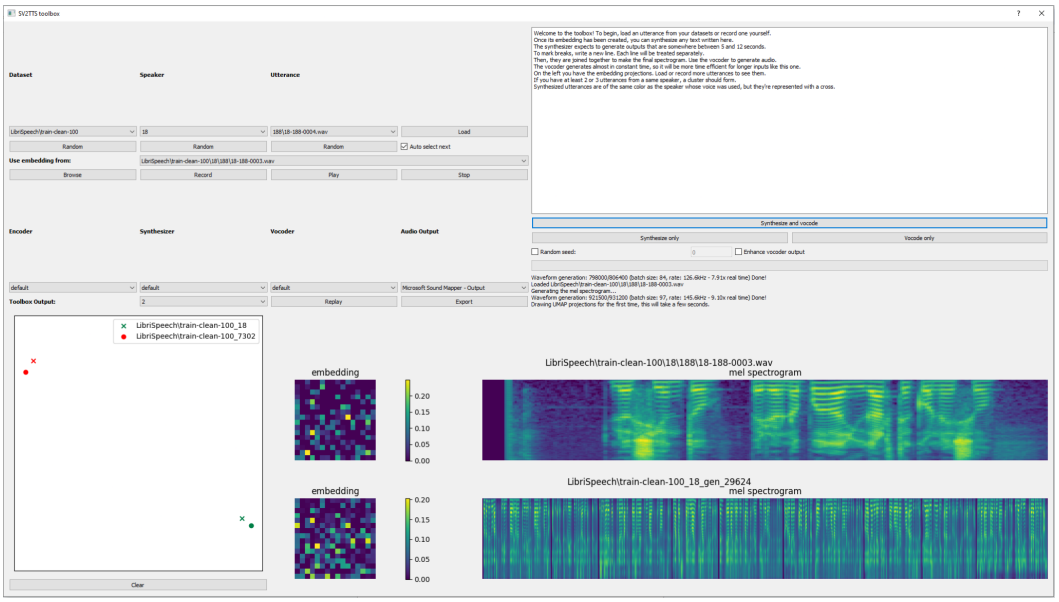


*Ilustración 43: Clonación de voz - Herramienta 1*

En caso de querer ver el resultado, en este vídeo se muestra la ejecución de la herramienta. Aunque el repositorio esté pensado para clonación de voces inglesas, no parece merecer la pena indagar en variaciones a castellano por el resultado obtenido :

- URL: https://youtu.be/XQNxjDMtt8A

Voice.ai

Para poder clonar una voz utilizando esta herramienta, se requiere un mínimo de 15 minutos de grabación de audio. En el caso de querer hacerlo de manera similar a la herramienta previa, se han utilizado los 7 audios mencionados anteriormente y se han reproducido en bucle hasta llegar a los minutos requeridos. La herramienta tiene sus limitaciones de manera gratuita, pero simplemente ha de arrastrarse el audio y rellenar unos pocos campos:

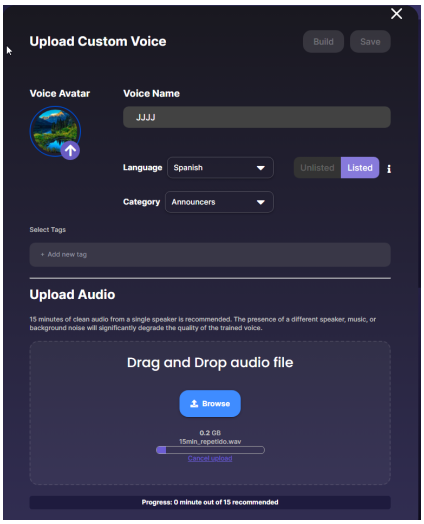


*Ilustración 44: Voice.ai - Config 1*

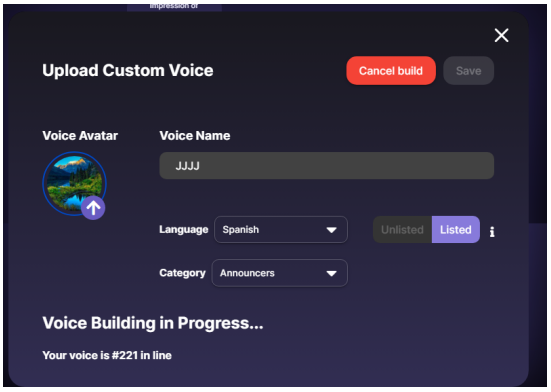


*Ilustración 45: Voice.ai - Config 2*

En la siguiente URL, se puede observar que el resultado tampoco llega a ser satisfactorio. Dado que la voz de la víctima es la mía, se debe añadir un audio con el contenido que queremos hacer que la voz clonada diga. Para eso, he utilizado un modelo ya entrenado de Coqui TTS con más de 5000 audios. De esta manera, la voz clonada intentará decir lo mismo que el audio añadido:

- URL: https://youtu.be/jA0MANPR-kk

## Tortoise-TTS:

Este repositorio, al igual que "Real-Time-Voice-Cloning", ha sido desarrollado para el idioma inglés, sin embargo, se puede notar una mejora significativa en la similitud del tono de voz con el original. En este caso, simplemente se ha tenido que añadir los audios mencionados anteriormente a la carpeta “JulenDataset” y referenciar esa nueva voz al realizar el comando de ejecución:

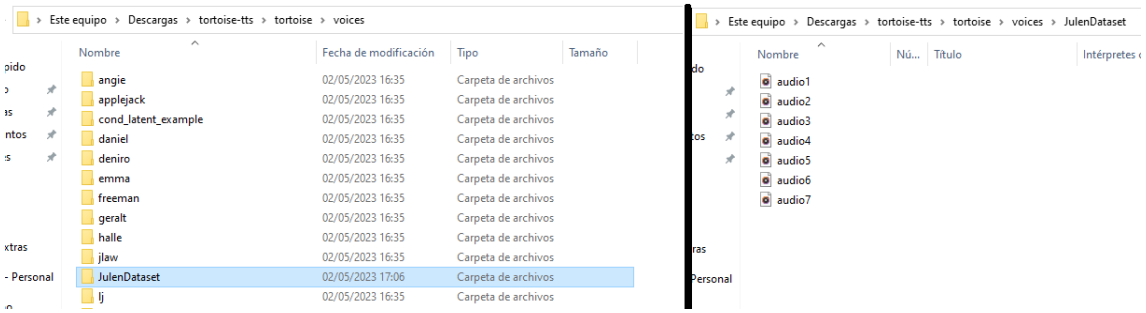


*Ilustración 46: Tortoise-TTS - Config. archivos*

En el siguiente enlace podemos observar la ejecución y resultado. Aunque la tonalidad se parezca más que las anteriores veces, no parece suficiente para un ataque de ingeniería social:

- URL: https://youtu.be/3CmOM1fMnGk

So-vits-svc-fork:

En este caso, el modelo fue entrenado durante aproximadamente 40 minutos, ya que los pasos predefinidos en el repositorio se completaron en ese tiempo. Esta herramienta tampoco ha ofrecido resultados destacables.

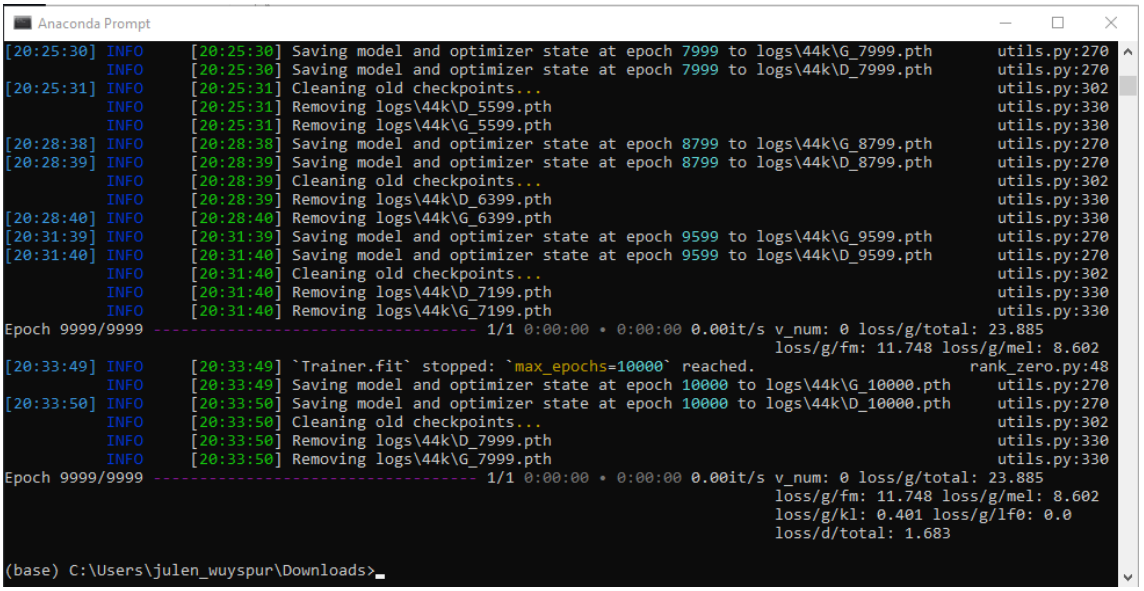


*Ilustración 47: Captura FIN de entrenamiento del modelo*

Además, los audios utilizados se colocan de la siguiente manera “\dataset_raw\JulenDataset\Julen”:

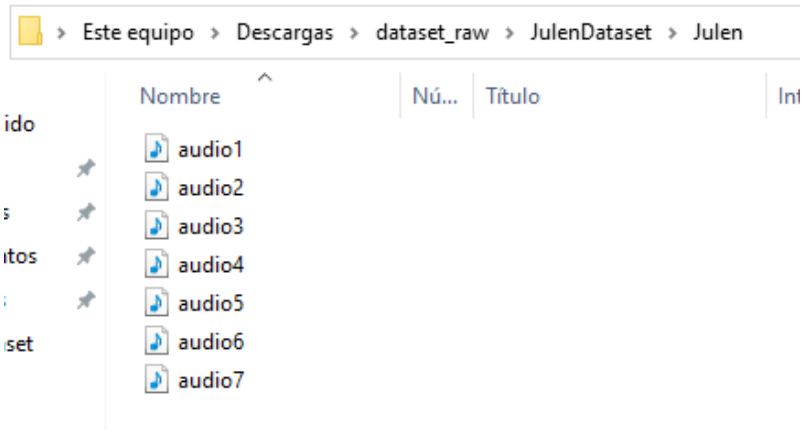


*Ilustración 48: So-vits-svc-fork - Config. archivos*

Una vez que el modelo está entrenado, los resultados los podemos observar en el siguiente vídeo. Utilizamos el mismo audio de entrada que en el apartado de "Voice.ai" :

- URL: https://youtu.be/pYAAyxcoCWU

Conclusión clonación de voz:

Clonar una voz de manera creíble parece requerir una gran cantidad de audios, lo que puede dificultar la tarea de los ciberdelincuentes en muchos casos. Además, estos audios deben tener una calidad mínima y el modelo necesita un largo tiempo de entrenamiento para lograr una clonación más realista. A partir de las pruebas realizadas con el tiempo y los pocos audios disponibles, no se puede concluir que la clonación de voz sea factible para los ciberdelincuentes. Es importante tener en cuenta que pueden existir herramientas mejores que pueden producir mejores resultados y que, en muchos casos, las herramientas de pago pueden ser más útiles para este tipo de situaciones.
Es importante destacar dos herramientas de pago que, aunque no se han evaluado en profundidad, parecen ofrecer resultados excelentes en la clonación de voz con un tiempo de entrenamiento mínimo. La herramienta principal que ha mostrado una mayor cantidad de videos de clonación exitosa es "elevenlabs.io", mientras que la segunda herramienta recomendada es "resemble.ai".

Observación: También se ha intentado trabajar con Coqui TTS, uno de los mejores repositorios dedicados a la clonación de voz. Aun así, aunque he sido capaz de poner el repositorio en marcha sobre los modelos de voces que ya tiene creados, no se ha podido utilizar para entrenar modelos con voces propias. Por eso, la falta de tiempo y por comentarios del repositorio de Coqui TTS donde se afirma resultados electrónicos y distorsionados tras más de 70 horas de entrenamiento, se ha decidido dejar este repositorio de lado. Más información en el anexo.

# 4. Conclusiones y trabajos futuros

## 4.1. Conclusiones Finales

Los ciberdelincuentes utilizan diversas técnicas para engañar a sus víctimas y lograr sus objetivos malintencionados. Para ello, recopilan información sobre su objetivo y establecen una relación con él antes de llevar a cabo el ataque. En la actualidad, Internet ha ampliado las posibilidades de obtener información y ha proporcionado herramientas muy poderosas para los delincuentes. Por lo tanto, es lucrativo para ellos utilizar estos métodos ya que les permiten obtener información valiosa y realizar ataques con éxito.

Es fundamental que las personas sean conscientes de los métodos y pretextos que pueden utilizar los ciberdelincuentes para atacar y aprendan a protegerse. La educación y la concienciación son herramientas esenciales para evitar ser engañados y desarrollar los conocimientos necesarios para prevenir los ataques. De esta manera, podrán evitar ser víctimas de los ciberdelincuentes y proteger su información personal y financiera.

Asimismo, después de analizar y probar diversas herramientas para llevar a cabo ataques de ingeniería social, se ha observado que muchas de ellas no ofrecen los resultados deseados. Por ejemplo, algunas herramientas para la clonación de webs, como goclone o Social Engineering Toolkit, han ofrecido una clonación peor que la realizada manualmente. Además, en el ámbito del deepfake y la clonación de voz, se han presentado múltiples problemas para poner en marcha distintos repositorios, y algunos de ellos han aportado inconsistencias entre la documentación y la implementación, como es el caso de Coqui TTS.

Sin embargo, a pesar de estos contratiempos, existe una gran variedad de herramientas en el mercado, tanto gratuitas como de pago, por lo que es solo cuestión de tiempo para que los ciberdelincuentes lleguen a ellas. En el caso del phishing, es muy fácil clonar una web y existen plantillas realizadas por otros desarrolladores que permiten realizar una campaña completa de phishing en cuestión de unos clics, sin necesidad de tener conocimientos de programación. Herramientas como Gophish y Zphisher, que se han utilizado en el apartado de implementación, son ejemplos de ello.

La inteligencia artificial (IA) también juega un papel importante en la ingeniería social. Aunque OpenAI ofrece herramientas bien diseñadas y que arrojan muy buenos resultados, fuera de ahí, las herramientas gratuitas pueden generar mayores dolores de cabeza. Sin embargo, en el caso específico de la clonación de voz, parece haber una mayor viabilidad debido a los tiempos de entrenamiento menores que se han obtenido en las pruebas. Entrenar una IA para clonar una voz o realizar deepfakes puede llevar muchas horas y aun así, el resultado puede ser decepcionante. No obstante, es probable que estas herramientas mejoren en el futuro y alcancen el nivel de las que ofrece OpenAI. O que en su caso, otras herramientas no probadas ofrezcan mejores resultados.

En conclusión, realizar ataques de ingeniería social es más fácil que nunca para un ciberdelincuente. En este trabajo, nos hemos centrado en algunas herramientas gratuitas, pero existen muchas más herramientas gratuitas y de pago en el mercado con las que probablemente se obtengan mejores resultados. Además, con herramientas como ChatGPT, los ciberdelincuentes ni siquiera tienen que pensar demasiado para crear situaciones de “pretexting efectivas”. Es importante que las empresas y los usuarios tomen medidas preventivas para protegerse contra estos ataques cada vez más sofisticados y fáciles de realizar.

## 4.2. Seguimiento de la planificación establecida

Se propusieron 4 iteraciones en la planificación inicial del proyecto. La primera iteración se dedicó a la planificación, la segunda se enfocó en investigar cuestiones específicas relacionadas con la ingeniería social, y la tercera se centró en implementaciones y pruebas relacionadas con la ingeniería social. Esto nos permitió dejar la última iteración para revisar y finalizar la documentación, así como para la elaboración del video.

Siguiendo el plan establecido, logramos realizar la planificación dentro de los plazos establecidos, entregando la documentación esperada en cada entrega. Aunque surgieron algunas variaciones en cada iteración debido a problemas encontrados durante la implementación, pudimos probar diferentes herramientas en diferentes áreas para llegar a conclusiones relevantes

## 4.3. Problemas encontrados en la implementación del proyecto

A continuación, se presentan algunos problemas identificados durante la implementación.

| P1. Errores sobre los repositorios y herramientas |
|---|

Durante la implementación, se han detectado varios problemas relacionados con diversas herramientas. Encontramos que muchos de los repositorios que utilizamos no están siendo actualizados, lo que ha causado errores inesperados y ha retrasado las pruebas de dichas herramientas. Además, hemos descubierto discrepancias entre la documentación y la realidad del proyecto, lo que ha generado demoras en las pruebas o incluso ha imposibilitado su realización.

| P2. Resultados inesperados sobre las herramientas |
|---|

Se han encontrado dificultades con varias herramientas utilizadas, lo cual ha generado resultados que no cumplen completamente las expectativas. Aunque se ha logrado obtener conclusiones a partir de las pruebas realizadas, el factor limitante ha sido el tiempo, tal y como se estableció en la planificación inicial.

En primer lugar, la clonación automática de sitios web no ha cumplido con las expectativas planteadas, ya que las herramientas automáticas han demostrado ser menos eficaces que la clonación manual. Además, tanto los deepfakes como la clonación de voz no han producido los resultados esperados. No se han obtenido suficientes resultados para considerarlos efectivos en ataques de ingeniería social.

P3. Implementación muy ambiciosa

Es posible que incorporar los elementos de deepfake y clonación de voz al TFM pueda brindar una perspectiva innovadora. Sin embargo, es importante considerar que inicialmente se planificó llevar a cabo la implementación en la tercera iteración, lo cual podría haber resultado en una fase demasiado ambiciosa. La fase actualmente se resume en 4 semanas para llevar a cabo las pruebas necesarias y evaluar una amplia gama de herramientas (de las cuales algunas han sido descartadas y otras no). Esto puede haber dado lugar a una fase excesivamente ambiciosa.

## 4.4. Evaluación de objetivos alcanzados

La evaluación de los objetivos alcanzados revela un notable grado de cumplimiento en relación a las metas establecidas inicialmente para el proyecto. En general, todos los objetivos planteados han sido exitosamente abordados y realizados con éxito. Sin embargo, es importante destacar que los resultados obtenidos en los apartados de Deepfake y Clonación de voz han presentado ciertas limitaciones que impiden considerarlos plenamente satisfactorios.

## 4.5. Trabajo Futuro

Una vez alcanzados los objetivos didácticos establecidos en este trabajo, se presentan a continuación diversas áreas de investigación futura que podrían contribuir a mejorar el proyecto:

- Aunque se ha logrado avanzar en el desarrollo de técnicas de deepfake y clonación de voz, las pruebas realizadas han arrojado resultados que no alcanzan el nivel óptimo deseado. Esto indica que aún existen desafíos por superar en la implementación de estas tecnologías y que se requiere un trabajo adicional para mejorar y perfeccionar los resultados obtenidos. Por tanto, podría ser interesante como trabajo futuro mejorar los resultados obtenidos y centrarse únicamente en estas dos cuestiones enfocadas en ataques de ingeniería social.
- Se plantea la posibilidad de investigar e implementar herramientas capaces de detectar eficientemente casos de Phishing, clonación de voz y deepfakes. Sería necesario llevar a cabo rigurosas evaluaciones para determinar si estas herramientas realmente cumplen con sus promesas.
- Dado que ha sido un tema no muy detallado en el TFM, se podría realizar un estudio más profundo sobre la psicología detrás de los ataques de ingeniería social: Comprender la psicología humana involucrada en los ataques de ingeniería social puede proporcionar información valiosa para la prevención y mitigación de tales ataques. Un trabajo futuro podría involucrar investigaciones

sobre la persuasión, la influencia social y los factores cognitivos que hacen que las personas sean más susceptibles a los intentos de manipulación.

- Para combatir los ataques de ingeniería social, es fundamental que los usuarios estén bien informados y sean conscientes de las tácticas utilizadas por los atacantes. Un trabajo futuro podría implicar el desarrollo de herramientas y software interactivos que eduquen y concienticen a los usuarios sobre los riesgos asociados con la ingeniería social y les enseñen cómo protegerse adecuadamente. También se podrían probar las herramientas ya creadas para este fin y evaluarlas.
- Una área de investigación futura fascinante podría centrarse en examinar las técnicas empleadas por los ciberdelincuentes para desaparecer. Este estudio exploraría cómo los ciberdelincuentes se aseguran de borrar o encubrir meticulosamente sus huellas, evitando ser detectados. Investigaríamos cómo eliminan cualquier rastro de comunicación o transacciones con sus víctimas, cómo limpian el malware utilizado en los ataques y cómo emplean técnicas de anonimización para ocultar su identidad.

# 5. Glosario

**Phishing:** Es un tipo de fraude en línea en el que se suplanta la identidad de una persona o empresa legítima con el objetivo de obtener información confidencial del usuario, como contraseñas, información bancaria o números de tarjeta de crédito.

**Ingeniería social:** Es el uso de técnicas de manipulación para engañar a las personas y obtener información confidencial o acceso a sistemas o recursos.

**Malware:** Software diseñado para dañar o interrumpir sistemas, redes o dispositivos informáticos.

**SMSishing:** Es una técnica de ingeniería social en la que se utiliza el mensaje de texto para engañar a los usuarios para que compartan información confidencial.

**Pretexting:** Es una técnica de ingeniería social en la que el atacante se hace pasar por alguien de confianza para obtener información privada, como información financiera o de cuentas de usuario.

**Sextorsión:** Es una forma de extorsión en línea en la que un atacante utiliza información comprometida (como fotos o videos sexuales) para chantajear a la víctima para que realice acciones específicas.

**Baiting:** Es una técnica de ingeniería social en la que el atacante ofrece algo atractivo (como una descarga gratuita) para que la víctima haga clic en un enlace malicioso o proporcione información confidencial.

**Vishing:** Es una técnica de ingeniería social que utiliza llamadas telefónicas de voz en lugar de mensajes de texto o correo electrónico para engañar a las personas para que compartan información confidencial.

**Dumpster diving:** es una técnica de ingeniería social que implica buscar información confidencial en la basura de una organización o individuo.

**Deepfake:** Es una técnica de inteligencia artificial que se utiliza para crear videos o imágenes manipuladas, en los que se sustituyen los rostros o las voces de las personas por otros, a menudo con el fin de engañar o difundir información falsa. Estas manipulaciones pueden ser muy realistas y difíciles de detectar, lo que las convierte en una herramienta potencialmente peligrosa para la desinformación y el engaño.

**Tailgating**: técnica de ingeniería social que consiste en seguir a una persona para acceder a un edificio o zona restringida sin identificación adecuada.

**Robo por desvío:** técnica de ingeniería social que consiste en distraer al objetivo para robar sus pertenencias o información sin que se dé cuenta. Suele consistir en desviar a una empresa de transporte para que entregue un mensajero o un paquete en el lugar deseado, con la intención de robarlo.

**Quid pro quo:** técnica de ingeniería social que consiste en ofrecer una compensación a cambio de información del objetivo.

**Reverse social engineering:** técnica de ingeniería social que consiste en que el atacante se hace pasar por un objetivo para recopilar información de la organización o empresa.

**Ingeniería social online:** técnica de ingeniería social que se realiza a través de la red, como por ejemplo, el phishing o el pharming.

**Ingeniería social por teléfono:** técnica de ingeniería social que se realiza a través de una llamada telefónica, como por ejemplo, los robocalls.

**Impersonation on help desk:** técnica de ingeniería social que consiste en hacerse pasar por personal del servicio de soporte para obtener información o acceso no autorizado.

**Ransomware:** técnica de ingeniería social que consiste en cifrar los archivos del objetivo y exigir un rescate para recuperarlos.

**Fake software:** técnica de ingeniería social que consiste en ofrecer un software falso para obtener acceso no autorizado al equipo del objetivo.

**Pharming:** técnica de ingeniería social que consiste en redirigir el tráfico de un sitio web legítimo a un sitio web falso para obtener información sensible.

**Ventanas emergentes o pop-up**: técnica de ingeniería social que consiste en mostrar ventanas emergentes falsas para obtener información del objetivo.

**Robocalls:** técnica de ingeniería social que consiste en realizar llamadas automáticas para obtener información o acceso no autorizado.

**Shoulder surfing:** técnica de ingeniería social que consiste en observar “por encima del hombro” del objetivo para obtener información.

**Robo de documentos importantes:** técnica de ingeniería social que consiste en robar documentos importantes del objetivo.

**OSINT:** El método común de recolección de información, que consiste en recopilar datos a través de fuentes abiertas como Internet, transmisiones y periódicos, y procesarlos. OSINT es la abreviatura de "Open Source Intelligence".

**Vigilancia y Reconocimiento Inteligentes (ISR):** La recopilación de información por parte de los gobiernos sobre otros países y su actividad, que se divide en tres tipos: OSINT, inteligencia humana (HUMINT) e inteligencia técnica (TECHINT).
**Humint**: La recopilación de información mediante la utilización de personas que se infiltran en organizaciones o entidades con el fin de obtener información.

**Techint:** La recopilación de información mediante el uso de técnicas y herramientas técnicas como la vigilancia de redes, la recolección de datos forenses y la recuperación de datos de discos duros.

**Metadatos:** Información adicional que se encuentra en los documentos, archivos o imágenes que se puede obtener a través de la configuración del dispositivo o del software utilizado. Pueden incluir información sobre la fecha de creación, autor, título original, versión de software, sistema operativo, entre otros.

**Ortofotos:** Imágenes aéreas de alta resolución que se utilizan para cartografía, planeamiento urbano y gestión del territorio.

**Spear phishing:** Ataque dirigido a personas específicas o grupos selectos utilizando sus nombres para hacer reclamos o comunicaciones, y requiere recopilar información sobre la víctima utilizando datos disponibles en línea.

**Whaling phishing:** Tipo de spear phishing dirigido a perfiles altos en empresas.

**Phishing de respuesta de voz interactiva:** Utiliza un sistema de respuesta de voz interactiva para hacer que el objetivo introduzca información privada como si fuera de una empresa o banco legítimo.

**Social Engineering Capture the Flag (SECTF):** Es una competición en la que los participantes deben superar una serie de desafíos relacionados con la ingeniería social para obtener información de empresas asignadas.

**Flags:** Son piezas de información que los participantes en una competición SECTF deben obtener.

**SSID:** Siglas de "Service Set Identifier", se refiere al nombre de la red inalámbrica.

**RFID:** Siglas de "Radio-Frequency Identification", se refiere a un sistema de identificación por radiofrecuencia.

**Botnet:** Una botnet es una red de dispositivos infectados por malware que se controlan remotamente para realizar actividades maliciosas en línea.

**Deep Web:** Parte de la internet que no se puede encontrar a través de los motores de búsqueda comunes y que a menudo se utiliza para actividades ilegales.

# 6. Bibliografía

## Libros consultados:

Para el apartado de investigación:


- Christopher Hadnagy / Paul Wilson, Social Engineering: The Art of Human Hacking, ISBN: 978-0-470-63953-5,Wiley, Indianapolis, IN y ©2011, 2010.
- Gustavo E. Aboso, "Ciberdelitos: Análisis doctrinario y jurisprudencial" ISBN: 978-987-47138-8-9, Editorial Albremática S.A., 2022.


## Trabajos académicos consultados:

Para el apartado de investigación:


- Leydi Dayana Tamayo Argoti, "Técnicas de ingeniería social aplicada en los estudiantes de grado 11° de la ciudad de san juan de pasto", universidad nacional abierta y a distancia, escuela de ciencias básicas tecnologías e ingeniería, especialización en seguridad informática, san juan de pasto, 2020. URL: https://repository.unad.edu.co/bitstream/handle/10596/37622/ldtamayoar.pdf?sequence=1&isAllowed=y
- Tobar Alvarez Juana Del Rocio, "ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse, 2022. URL: http://dspace.utb.edu.ec/bitstream/handle/49000/13062/E-UTB-FAFI-SIST-000396.pdf?sequence=1&isAllowed=y
- Lucía Do Nascimento Fernández, "Phishing: aspectos técnicos y procesales del delito estrella en tiempos de pandemia", Universidad Rey Juan Carlos, 2020-2021. URL: https://burjcdigital.urjc.es/bitstream/handle/10115/17989/TFG%20VERSI%c3%93N%20FINAL.pdf?sequence=1&isAllowed=y


## Páginas web y artículos online consultados:


- INCIBE: "El engaño como arma del delito". URL: incibe.es/aprendeciberseguridad/ingenieria-social, 01/03/2023.
- INCIBE: "TemáTICas Ingeniería social". URL: incibe.es/protege-tu-empresa/tematicas/ingenieria-social, 03/03/2023.
- IBM: "¿Qué es la ingeniería social?". URL:ibm.com/es-es/topics/social-engineering, 01/03/2023.
- Helpransomware: "PHISHING BY INDUSTRY 2021" URL: helpransomware.com/wp-content/uploads/2022/05/KnowBe4-HelpRansomware.pdf, KnowBe4, 01/03/2023.
- Social-Engineering: "The Social Engineer Blog". URL: https://www.social-engineer.org/blog/, 05/03/2023.
- Social-Engineering: "Influence Tactics". URL: https://www.social-engineer.org/framework/influencing-others/influence-tactics/, 07/03/2023
- Aura: "The 12 Latest Types of Social Engineering Attacks (2023)". URL: https://www.aura.com/learn/types-of-social-engineering-attacks, 08/03/2023.
- EnRedAndo: "EnRedAndo 769". URL:https://www.euskadigital.eus/programas/enredando/enredando-769/, 10/03/2023
- Euskalhack: "INFORME SECTF 2019". URL: https://www.euskalhack.org/securitycongress2019/SECTF/EuskalHack_SECTF_2019.pdf, 15/03/2023.

- DEFCON: “The 2019 Social Engineering Capture the Flag Report” . URL: https://www.social-engineer.org/wp-content/uploads/2019/11/SECTF-DEFCON27-SECOM-2019.pdf, 16/03/2023.
- Mdpi: “Social Engineering Attacks: A Survey”, Escuela de Ingeniería Eléctrica e Informática, Universidad de Dakota del Norte, Grand Forks, ND 58202, EE.UU, 2019. URL: https://www.mdpi.com/1999-5903/11/4/89
- Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, “Advanced social engineering attacks”, ScienceDirect, 2014. URL: https://reader.elsevier.com/reader/sd/pii/S2214212614001343?token=85FAAF0AD26CA8A65811C93EAE3E3B11D70EBC9D1933932E73D7F130F05EAF867CBD574C09AF32E1ED511590176E3E0B&originRegion=eu-west-1&originCreation=20230317121435.
- Yong-Woon Hwang, Im-Yeong Lee, Hwankuk Kim,Hyejung Lee, Donghyun Kim, “Current Status and Security Trend of OSINT”, Wiley, 2021. URL: https://downloads.hindawi.com/journals/wcmc/2022/1290129 .pdf.
- Cltr: “INFLUENCE, THE PSYCHOLOGY OF PERSUASION”. URL: https://cltr.nl/wp-content/uploads/2020/04/Robert-P-Cialdini-Influence-The-Psychology-of-Persuasion.pdf, 20/03/2023.
- Oedi: “Ciberdelitos”. URL: https://oedi.es/ciberdelitos/, 04/04/2023.
- Kaspersky:https://www.kaspersky.es/blog/valor-datos-darkweb/24602/, 06/04/2023.

Para el apartado de implementación:

- Mdn web docs: https://developer.mozilla.org/en-US/docs/Web/API/XMLHttpRequest/readystatechange_event, 13/04/2023.
- Php.net: https://www.php.net/docs.php,13/04/2023.
- Getgophish: https://getgophish.com/documentation/, 15/04/2023.
- JAN ČERNÝ: https://noticias.ai/wp-content/uploads/2023/03/103-osint-chatgpt-prompt-ideas.pdf, 03/05/2023.


## Videos consultados:


Para el apartado de implementación:

- Azaze Shari. “Phishing Attack using GOPHISH Demonstration Tutorial” URL: https://www.youtube.com/watch?v=sfjQ4KIfL-U.
- Ernes cybersecurity. “Cómo obtener la ubicación EXACTA de una persona usando seeker”. URL: https://www.youtube.com/watch?v=mAdvvl0a5D0.
- Hey, Let's Learn Something. “Clone your voice | How to install Real-Time Voice Cloning toolbox Python?”. URL: https://www.youtube.com/watch?v=xQtVO0GxJ14
- P3tro. “So-Vits-SVC: Local Training Tutorial”. URL: https://www.youtube.com/watch?v=MDCXJY2zAmE
- UnitedShoes. “so-vits-fork Installation Tutorial for Windows 10”. URL: https://www.youtube.com/watch?v=kdMpB2YCqqU
- El Pingüino Tech. “Cómo INSTALAR y UTILIZAR theHarvester en LINUX”. URL: https://www.youtube.com/watch?v=g9mQzg0Yxbw

# 7. Anexos

## Clonación de voz  - Problemas

En algunos de los repositorios de código abierto gratuitos, he encontrado una documentación muy deficiente. Aunque parezca completa en un principio, muchas veces no es suficiente para clonar una voz personalizada. Afortunadamente, Coqui-ai/TTS proporciona algunos modelos pre-entrenados de buena calidad, incluyendo dos en castellano. Uno de los modelos no produce ningún audio, pero el otro genera una voz bastante realista, teniendo en cuenta que proviene de un modelo pre-entrenado en castellano con más de 5000 audios originales.

El repositorio de Coqui ofrece una opción de "fine-tuning", que propone utilizar un modelo ya pre-entrenado para agregar nuestros propios audios o conjuntos de datos. Sin embargo, los pasos a seguir son bastante vagos, y se encontraron errores en el código e inconsistencias entre secciones sobre los modelos pre entrenados. Por ejemplo, el código solicita un archivo de transcripciones llamado "metadata.txt" con un formato específico, pero al depurar errores en diferentes secciones, se descubrió que en realidad se buscaba el archivo "metadata.csv" (con una extensión diferente) o el formato de los audios sin agregar automáticamente la extensión ".wav". Después de muchos intentos, no se logró realizar la clonación de audio personalizada.

También se probó la clonación de audio en proyectos de Google Collab tanto para el proyecto anterior como para Tortoise y otros, sin encontrar resultados sorprendentes ni similares al original.

Por lo tanto, la clave para utilizar la clonación de voz es la cantidad de audios que se tengan de una persona. Se podrían necesitar una gran cantidad de audios para entrenar un modelo que pueda producir buenos resultados. Sin embargo, una gran cantidad de audios no siempre se traduce en un buen resultado.

Asimismo, cabe recalcar que se instaló COQUI TTS sobre un ordenador Windows 10 y un ordenador Kali Linux, consiguiendo reproducir voces de modelos ya creados pero en ningún caso poder entrenar los modelos.