UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Análisis de Phishing y Técnicas de Ingeniería Social: Estrategias de Concientización y Prevención de Ataques

AUTOR

Jorge Bryan Tomalá Domínguez

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Ing. Jorge Luis Zambrano Martínez, Ph.D.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Zambrano Martínez, Ph.D.
TUTOR

Firmado electrónicamente por:
OSCAR OMAR APOLINARIO ARZUBE

Lic. Oscar Apolinario Arzube, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

Ing. Cesar Moreira Zambrano, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Msc.
SECRETARIO GENERAL UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Jorge Bryan Tomalá Domínguez, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Luis Zambrano Martínez, Ph.D.

Santa Elena, 14 de octubre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **JORGE BRYAN TOMALÁ DOMÍNGUEZ**

DECLARO QUE:

El trabajo de Titulación, "Análisis de Phishing y Técnicas de Ingeniería Social: Estrategias de Concientización y Prevención de Ataques" previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 14 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
JORGE BRYAN TOMALA DOMINGUEZ

Jorge Bryan Tomalá Domínguez

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado "Análisis de Phishing y Técnicas de Ingeniería Social: Estrategias de Concientización y Prevención de Ataques", presentado por el estudiante, Jorge Bryan Tomalá Domínguez fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 8%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

Tesis - Final

8%
Textos sospechosos

6% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos

Nombre del documento: Tesis - Final.docx
ID del documento: 791c0ed85ca9515956712fd7e1bb306b4ddc7d0e
Tamaño del documento original: 13,89 MB
Autores: []

Depositante: JORGE LUIS ZAMBRANO MARTINEZ
Fecha de depósito: 13/10/2024
Tipo de carga: interface
fecha de fin de análisis: 13/10/2024

Número de palabras: 12.626
Número de caracteres: 87.490

TUTOR

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Luis Zambrano Martínez, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **JORGE BRYAN TOMALÁ DOMÍNGUEZ**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo de examen de carácter complexivo con fines de difusión pública, además apruebo la reproducción de este trabajo de examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 14 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
JORGE BRYAN TOMALA DOMINGUEZ

Jorge Bryan Tomalá Domínguez

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a mi tutor, le agradezco sinceramente por su valiosa guía y enseñanzas durante el desarrollo de mi propuesta tecnológica. Su disposición para resolver mis dudas y el tiempo dedicado a revisar tanto la documentación como su guía en la parte práctica han sido esenciales en este proceso.

Finalmente, quiero reconocer a los docentes de la Maestría en Ciberseguridad, que siempre estuvieron dispuestos a ayudar con sus consejos y conocimientos. Su apoyo ha sido fundamental en mi formación.

Jorge Bryan, Tomalá Domínguez

DEDICATORIA

Dedico este trabajo a mis padres, cuyo apoyo incondicional ha sido fundamental a lo largo de mis estudios. Todo lo que he logrado se lo debo a ellos, tanto por su respaldo económico como por su constante motivación para alcanzar mis metas profesionales.

A mi esposa y a mi hijo, gracias por su amor y apoyo emocional. Su aliento ha sido un pilar en este camino, motivándome a no rendirme y a seguir adelante con mis estudios.

Jorge Bryan, Tomalá Domínguez

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

Este estudio evalúa estrategias de prevención de ataques de Phishing y técnicas de ingeniería social, enfocándose en la seguridad de los usuarios finales. A través de una metodología mixta que incluyó investigación documental, simulaciones prácticas con herramientas como Kali Linux y el Social Engineering Toolkit, y encuestas, se identificaron patrones comunes de ataque y se midió la efectividad de las estrategias implementadas. Los resultados mostraron que antes de la capacitación, el 84% de los usuarios no reconocía intentos de Phishing, mientras que, tras las intervenciones educativas, este porcentaje se redujo al 4%. Esto demuestra la eficacia de simulaciones prácticas y materiales educativos como trípticos y guías prácticas. El estudio concluye que la combinación de estrategias de concientización, herramientas tecnológicas y programas interactivos de capacitación es clave para mitigar los riesgos asociados con el Phishing y la ingeniería social, fortaleciendo así la seguridad cibernética de los usuarios finales.

Palabras claves: Phishing, Ingeniería social, Seguridad cibernética, Concientización, Prevención, Tácticas de ciberdelincuentes.

ABSTRACT

This study evaluates prevention strategies for Phishing attacks and social engineering techniques, focusing on end-user security. Through a mixed methodology that included documentary research, practical simulations with tools such as Kali Linux and the Social Engineering Toolkit, and surveys, common attack patterns were identified, and the effectiveness of implemented strategies was measured. The results showed that before the training, 84% of users failed to recognize Phishing attempts, whereas after educational interventions, this percentage decreased to 4%. This demonstrates the effectiveness of practical simulations and educational materials such as brochures and practical guides. The study concludes that the combination of awareness strategies, technological tools, and interactive training programs is key to mitigating the risks associated with Phishing and social engineering, thereby strengthening the cybersecurity of end users.

Keywords: Phishing, Social engineering, Cybersecurity, Awareness, Prevention, Cybercriminal tactics.

INTRODUCCIÓN

En el panorama actual de la seguridad cibernética, el Phishing y las técnicas de ingeniería social se han consolidado como amenazas crecientes y persistentes. Estas tácticas, caracterizadas por su sofisticación y capacidad para engañar a los usuarios finales, ponen en riesgo la confidencialidad de información crítica, como contraseñas, datos financieros y credenciales de acceso a sistemas sensibles. A pesar de los avances en tecnologías de seguridad y los esfuerzos globales de concientización, el Phishing sigue siendo una de las tácticas más efectivas empleadas por ciberdelincuentes, afectando tanto a individuos como a organizaciones. Según Chiew et al. (2018), los ataques de Phishing han evolucionado durante más de dos décadas, comenzando en 1995, y sus vectores y enfoques técnicos siguen adaptándose para sortear las defensas más avanzadas.

El Phishing, uno de los mayores desafíos en el ámbito de la ciberseguridad, se caracteriza por el intento de obtener información sensible, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, mediante la suplantación de una entidad confiable en una comunicación electrónica. Estos ataques pueden manifestarse a través de diversos canales, incluidos correos electrónicos, mensajes de texto y llamadas telefónicas, todos diseñados para engañar a los usuarios y llevarlos a divulgar su información personal. Liew et al. (2019) exploran los diferentes métodos a través de los cuales se ejecutan los ataques de Phishing, resaltando la versatilidad de esta amenaza.

El principal desafío radica en la naturaleza multifacética y en constante evolución del Phishing. Los ciberdelincuentes emplean una variedad de técnicas ingeniosas para engañar a sus víctimas, desde la creación de correos electrónicos convincentes que parecen provenir de fuentes legítimas, hasta la construcción de sitios web falsos que imitan servicios auténticos. Además, la ingeniería social ha alcanzado un nivel de sofisticación que explota la psicología humana y la confianza social, manipulando a los usuarios para que realicen acciones perjudiciales. Buckley et al. (2023) analizan cómo estas tácticas de Phishing se aprovechan de la psicología humana y exploran la evolución de estas técnicas para maximizar su efectividad.

Este estudio tiene como objetivo profundizar en las tácticas empleadas en los ataques de Phishing, evaluar la efectividad de las estrategias de concientización actuales y proponer un plan de implementación con medidas de prevención. A través de este enfoque integral, se busca mejorar la protección contra estas amenazas, que continúan adaptándose a los nuevos entornos tecnológicos y humanos.

El documento se organiza en tres capítulos principales, cada uno abordando aspectos clave relacionados con la problemática del Phishing y las soluciones propuestas para su prevención.

En el capítulo 1, se profundiza sobre el problema del Phishing. Se presentan los antecedentes del proyecto, que incluyen un análisis detallado de las diversas fuentes de información utilizadas para comprender mejor cómo operan los ataques de Phishing y las estrategias actuales para su mitigación, también incluye el objetivo general y específicos del proyecto.

El capítulo 2, se presenta los conceptos clave relacionados con el Phishing y la ingeniería social, proporcionando un marco teórico que sustenta el análisis posterior. Se exploran las diferentes técnicas utilizadas por los ciberdelincuentes y se describe cómo estos ataques explotan vulnerabilidades humanas para obtener información confidencial. A nivel metodológico, se explican las técnicas de recolección de información utilizadas en el estudio, que incluyen tanto investigaciones documentales basadas en revisiones de literatura como experimentos prácticos que simulan ataques de Phishing utilizando herramientas de código abierto como Social Engineering Toolkit en el sistema operativo Kali Linux. Este enfoque metodológico busca ofrecer un análisis riguroso de cómo se pueden prevenir estos ataques a través de estrategias de concientización bien diseñadas.

El capítulo 3, se presenta el desarrollo del proyecto, mostrando ejemplos prácticos de ataques de Phishing ejecutados mediante el uso de Kali Linux y el Social Engineering Toolkit (SET), que permiten replicar escenarios reales de ataques. Se detallan los pasos seguidos para llevar a cabo estas simulaciones en un entorno controlado, destacando las vulnerabilidades más comunes que suelen ser explotadas por los ciberdelincuentes. También se presenta la propuesta, que incluye la creación de un tríptico informativo, contiene información clave, buenas prácticas y un código QR que redirige a los usuarios a una página web con contenido adicional. La página web proporcionará ejemplos prácticos, guías de detección y consejos de prevención, además de ofrecer enlaces de interés que ayudarán a los usuarios a mantenerse informados sobre las últimas amenazas cibernéticas.

CAPÍTULO I

1 FUNDAMENTACIÓN

1.1 ANTECEDENTES DEL PROYECTO

Los datos utilizados en esta investigación provienen de diversas fuentes, incluyendo literatura académica, informes de organismos gubernamentales y agencias de ciberseguridad, así como estudios empresariales. Estas fuentes ofrecen una perspectiva amplia sobre los ataques utilizando la técnica de Phishing e ingeniería social, así como sobre las estrategias de prevención utilizadas en distintos contextos.

Singer, (2014) proporciona una visión integral de las dimensiones políticas, económicas y sociales relacionadas con la ciberseguridad, destacando la necesidad de una estrategia global para abordar los desafíos actuales y futuros en este campo en constante evolución.

La investigación académica también ha profundizado en la efectividad de las medidas de concientización en ciberseguridad. Prümmer et al. (2024) ofrecen una revisión exhaustiva de la literatura existente, subrayando la importancia de las campañas de concientización y educación para mejorar la resiliencia cibernética tanto de las organizaciones como de los individuos.

Además, la European Union Agency for Cybersecurity (ENISA) desempeña un papel clave al proporcionar informes periódicos sobre las amenazas emergentes y las tendencias en ciberseguridad, tanto a nivel europeo como global. ENISA, (2023) es una fuente valiosa que ofrece información detallada sobre las amenazas más relevantes y las áreas prioritarias de enfoque en ciberseguridad.

La investigación académica también ha profundizado en las técnicas psicológicas que utilizan los ciberdelincuentes. Gallo et al., (2024) presentan un análisis detallado de cómo los atacantes manipulan a las víctimas mediante tácticas psicológicas, lo que proporciona una comprensión fundamental para mitigar estos ataques.

Le et al., (2024) aportan una visión completa de las amenazas cibernéticas que enfrentan las pequeñas y medianas empresas, destacando la importancia de implementar medidas proactivas y estrategias de concientización adaptadas a este sector.

Estas referencias subrayan la complejidad y la importancia crítica de la ciberseguridad en la sociedad moderna. Resaltan la necesidad de implementar estrategias efectivas, marcos

sólidos de trabajo y medidas de concientización adecuadas para proteger la infraestructura digital y los datos sensibles en un mundo cada vez más interconectado.

Para abordar estos desafíos, nos basaremos en varios estándares y normativas reconocidos en el ámbito de la ciberseguridad:

- **ISO/IEC 27001**: Este estándar internacional para la gestión de la seguridad de la información cubre aspectos clave como la formación y la concientización de los empleados frente a amenazas como el Phishing y otras técnicas de ingeniería social (ISO/IEC, 2022).
- **CIS Controls**: Los Controles del Centro para la Seguridad de Internet (CIS) son una lista de prácticas recomendadas para defenderse contra las ciberamenazas. El **Control 14**, "Capacitación en habilidades de seguridad y concientización", resalta la importancia de la capacitación y concientización para prevenir ataques de Phishing (Center for Internet Security, 2024).

En la república del Ecuador el Código Orgánico Integral Penal (COIP): Tipifica delitos relacionados con el acceso e intercepciones ilegales de datos informáticos, en los artículos 230 y 234. El combate contra el Phishing y la ingeniería social demanda un enfoque multidisciplinario que integre investigación académica, colaboración intersectorial y la implementación de estrategias de concientización efectivas.

1.2 DESCRIPCIÓN DEL PROYECTO

Este estudio tiene como objetivo analizar y proponer estrategias efectivas para la concientización y prevención de ataques de Phishing y técnicas de ingeniería social, con un enfoque específico en los usuarios finales. El análisis se centrará en identificar las tácticas más comunes utilizadas por los ciberdelincuentes y en evaluar la efectividad de las estrategias actuales de concientización en diversos contextos, tales como entornos corporativos, académicos y domésticos.

En el entorno actual de la ciberseguridad, las estrategias tradicionales de concientización y prevención resultan insuficientes debido a la evolución constante de las tácticas empleadas por los atacantes. Este estudio argumenta la necesidad de un enfoque renovado y más efectivo, que combine avances tecnológicos con una comprensión profunda de la psicología y el comportamiento de los usuarios finales.

Para ilustrar la facilidad con la que los atacantes pueden llevar a cabo estos ataques, se utilizará el sistema operativo Kali Linux y la herramienta Social Engineering Toolkit (SET), lo cual permitirá demostrar la creación de sitios web maliciosos y la captura de credenciales de usuarios de manera sencilla, replicando las técnicas más comunes de los atacantes. Además, se analizarán estudios de caso para comprender los comportamientos y respuestas de los usuarios frente a intentos de Phishing.

El proyecto también incluirá un plan de implementación de estrategias de prevención basado en guías para el usuario y métodos de difusión innovadores. Se diseñará un tríptico informativo que contendrá información clave sobre el Phishing y un código QR que dirigirá a una página web dedicada, la cual ofrecerá contenido adicional, ejemplos prácticos, recomendaciones, y enlaces de interés para la detección y prevención de estos ataques.

Este enfoque no solo busca mejorar el conocimiento técnico de los usuarios, sino también abordar los aspectos psicológicos que los ciberdelincuentes explotan en los ataques de ingeniería social. Al combinar la tecnología con el comportamiento humano, el estudio permitirá un análisis integral que contribuirá a una mayor seguridad en línea.

En la parte práctica del proyecto, se utilizarán las siguientes herramientas:

- VMware Workstation Pro: Esta plataforma es ideal para usuarios individuales y proporciona una interfaz intuitiva para la creación y gestión de máquinas virtuales. Se utilizará para virtualizar Kali Linux como parte del entorno de simulación (Broadcom, 2024).
- Kali Linux: Es una distribución de Linux especializada en pruebas de penetración y auditoría de seguridad. Desarrollada por Offensive Security, Kali Linux incluye una amplia gama de herramientas que permiten analizar y evaluar la seguridad de sistemas y redes (OffSec Services Limited, 2024).
- The Social-Engineer Toolkit (SET): Integrado en Kali Linux, el SET es una herramienta de código abierto diseñada específicamente para realizar ataques de ingeniería social. Facilita la simulación de ataques de Phishing y spear-Phishing, permitiendo recrear escenarios comunes de ataque y evaluar la resiliencia de los usuarios ante tácticas de manipulación psicológica (TrustedSec, 2020).

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Analizar estrategias de prevención de ataques de Phishing y técnicas de ingeniería social mediante estudios de caso y herramientas de simulación, para la seguridad de los usuarios finales.

1.3.2 OBJETIVOS ESPECÍFICOS

- Comprender las tácticas más comunes empleadas en ataques de Phishing y las técnicas de ingeniería social utilizadas por ciberdelincuentes para manipular a los usuarios finales.
- Analizar la efectividad de las estrategias de concientización existentes a través de la revisión de literatura y estudios de caso.
- Proponer un plan de implementación para las estrategias sugeridas, que incluya métodos de difusión y guías para los usuarios.

1.4 JUSTIFICACIÓN DEL PROYECTO

Este estudio es relevante en los ámbitos social, profesional y científico:

- **Ámbito social:** El proyecto busca proteger a los usuarios finales, quienes son las principales víctimas de los ataques de Phishing y técnicas de ingeniería social, mejorando su capacidad para identificar y resistir intentos de manipulación. Al educar a los usuarios, se puede reducir el impacto de estos ataques en la sociedad.
- **Ámbito profesional:** Aporta estrategias prácticas que las organizaciones pueden implementar para reducir el riesgo de incidentes de seguridad. Las soluciones propuestas mejoran las políticas de concientización y refuerzan la seguridad dentro de entornos corporativos y otros sectores vulnerables.
- **Ámbito científico:** Contribuye al cuerpo de conocimiento existente explorando la interacción entre tecnología, psicología del usuario y las técnicas de ingeniería social. Estas áreas requieren constante actualización debido a la naturaleza cambiante y evolutiva de las amenazas cibernéticas.

El proyecto se enmarca en la línea de investigación "Tecnología y Sistemas de la Información (TSI)", abordando tres enfoques clave:

- **Redes y Seguridad de la Información:** Estudiar y desarrollar estrategias efectivas de prevención y concientización sobre el Phishing es esencial para

fortalecer la seguridad de las redes y la información. Esto minimiza el riesgo de intrusiones y brechas de seguridad causadas por errores humanos, protegiendo la integridad, confidencialidad y disponibilidad de los sistemas de información en cualquier organización.

- **Ingeniería y Gestión de TSI:** La integración de estrategias de concientización y prevención de Phishing dentro de la gestión de los sistemas de información es fundamental para garantizar que los sistemas sean no solo técnicamente robustos, sino también resilientes ante intentos de explotación mediante ingeniería social. Este estudio propone soluciones que abordan de manera integral la interacción entre los usuarios y la tecnología.
- **TSI Adaptables e Inteligentes:** Desarrollar e implementar estrategias que incrementen la concientización y la capacidad de respuesta de los usuarios frente al Phishing forma parte de un enfoque más amplio hacia sistemas adaptables e inteligentes. Este estudio no solo busca mejorar la resistencia de los usuarios, sino también proporcionar retroalimentación valiosa que permita mitigar nuevas amenazas emergentes.

1.5 ALCANCE DEL PROYECTO

Este proyecto tiene como objetivo analizar las técnicas de Phishing y las estrategias de ingeniería social mediante el uso de herramientas especializadas y la creación de recursos informativos orientados a mejorar la concienciación de los usuarios y la prevención de estos ataques. El análisis será realizado utilizando software de código abierto, como las herramientas disponibles en Kali Linux, las cuales permiten simular y estudiar ataques de Phishing en un entorno controlado.

El alcance del proyecto abarca las siguientes actividades y entregables:

Análisis de técnicas de Phishing:

Se emplearán herramientas de código abierto, específicamente el Social Engineering Toolkit (SET) de Kali Linux, para llevar a cabo simulaciones controladas de ataques de Phishing. Estas simulaciones permitirán identificar los vectores de ataque más comunes y estudiar las tácticas de ingeniería social empleadas por los ciberdelincuentes. La información obtenida a partir de estas simulaciones será analizada para comprender las vulnerabilidades de los usuarios y qué estrategias pueden ser efectivas para contrarrestar estas amenazas.

Creación de un tríptico informativo:

Como parte de las actividades de concienciación, se elaborará un tríptico en formato impreso y digital. Este material incluirá información clave sobre Phishing y las técnicas de ingeniería social, así como un código QR que enlazará a una página web informativa. El tríptico contendrá definiciones, señales de alerta, y recomendaciones de buenas prácticas para evitar ser víctima de estos fraudes. Estará diseñado de forma accesible para el público general y será distribuido en entornos organizacionales y educativos.

Desarrollo de una página web informativa:

Se creará una página web que funcionará como plataforma centralizada de recursos sobre Phishing y la ingeniería social. La web incluirá:

- Información detallada sobre estas amenazas.
- Ejemplos prácticos de ataques, cómo detectarlos y prevenirlos.
- Enlaces a recursos adicionales, como sitios de ayuda para detección de Phishing y guías de buenas prácticas.
- Un espacio interactivo que permitirá a los usuarios visualizar simulaciones de Phishing, mostrando de manera práctica cómo funcionan estos ataques.

El sitio web será diseñado tanto para usuarios individuales como para organizaciones, proporcionando contenido accesible y educativo para todos los niveles de conocimiento.

El resultado final será un proyecto integral que no solo analiza y explica los ataques de Phishing, sino que también ofrece herramientas y recursos prácticos para mejorar la prevención y la concienciación sobre estos ataques en diversos contextos. El material generado podrá ser utilizado como base para futuras campañas educativas, siendo útil tanto a nivel individual como organizacional, contribuyendo a la protección frente a amenazas en constante evolución.

Una vez presentadas las soluciones propuestas, es fundamental analizar los problemas específicos que este proyecto aborda dentro de los diferentes ámbitos. A continuación, se presenta una tabla (Tabla 1) que resume los principales problemas identificados en los ámbitos social, profesional y científico, junto con las soluciones propuestas para mitigarlos.

Ámbito	Problema Específico	Solución Propuesta
Social	Alta vulnerabilidad de usuarios a ataques de Phishing por falta de educación.	Creación de material educativo (tríptico, página web) para mejorar la concientización y la capacidad de defensa de los usuarios finales.
Profesional	Riesgo de pérdidas y daños a la reputación por incidentes de Phishing.	Estrategias de concientización que fortalecen las políticas de seguridad digital.
Científico	Evolución constante de las técnicas de Phishing.	Análisis de nuevas tácticas de Phishing y su impacto, contribuyendo al conocimiento en ciberseguridad y psicología del usuario.

Tabla 1: Detalles Problema - Propuesta

CAPÍTULO II

2 MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO CONCEPTUAL

El marco conceptual de este estudio se centra en la comprensión de los principales conceptos relacionados con el Phishing y la ingeniería social, que son tácticas empleadas por ciberdelincuentes para manipular a los usuarios y obtener acceso no autorizado a sistemas o información sensible. Este apartado proporciona definiciones clave y describe los métodos más comunes utilizados en estos ataques, con el fin de establecer una base teórica sólida para el análisis, desarrollo de estrategias de prevención y mitigación.

2.1.1 INGENIERÍA SOCIAL

La ingeniería social abarca una amplia gama de actividades diseñadas para explotar errores humanos o comportamientos con el fin de obtener acceso a información o servicios. Utiliza diversas formas de manipulación para engañar a las víctimas, llevándolas a cometer errores o a entregar información sensible. Los usuarios pueden ser inducidos a abrir documentos, archivos o correos electrónicos, visitar sitios web o conceder acceso a sistemas o servicios. Aunque algunas técnicas emplean la tecnología para engañar, su éxito depende fundamentalmente del factor humano. Entre los principales vectores de ataque de la ingeniería social se encuentran: Phishing, spear-Phishing, whaling, smishing, vishing, watering hole, baiting, pretexting, quid pro quo, honeytraps y scareware. Aunque estas técnicas se utilizan a menudo para obtener acceso inicial, también pueden emplearse en fases posteriores de un incidente o brecha de seguridad. Ejemplos relevantes incluyen la vulneración de correos electrónicos empresariales (BEC), fraudes, suplantación de identidad, falsificaciones y, más recientemente, extorsión (ENISA, 2023).

2.1.2 VECTORES DE ATAQUE

- **PHISHING**

  Tiene como objetivo robar información importante, como números de tarjetas de crédito y contraseñas, a través de correos electrónicos que utilizan tácticas de ingeniería social y engaño (ENISA, 2023).

- **SPEAR-PHISHING**

  Es una versión más sofisticada del Phishing que tiene como objetivo organizaciones o individuos específicos (ENISA, 2023).

- **WHALING**

  Es un ataque de spear-Phishing dirigido a usuarios en posiciones de alto nivel, como ejecutivos o políticos (ENISA, 2023).

- **SMISHING**

  Derivado de la combinación de “SMS” y “Phishing”, ocurre cuando el atacante recopila información sensible o convence a las víctimas de hacer clic en enlaces maliciosos compartidos a través de mensajes SMS (ENISA, 2023).

- **VISHING**

  Es una combinación de “Phishing” y “voz”, ocurre cuando se proporciona información a través del teléfono, donde actores malintencionados utilizan técnicas de ingeniería social para extraer información sensible de los usuarios (ENISA, 2023).

- **WATERING HOLE ATTACK**

  Esto ocurre cuando los hackers infectan un sitio que saben que las víctimas objetivo visitan regularmente (ENISA, 2023).

- **BAITING**

  Es un tipo de ataque de ingeniería social en el que los estafadores atraen a las víctimas para que proporcionen información sensible al prometerles algo valioso a cambio (por ejemplo, juegos gratuitos, música o descargas de películas) (ENISA, 2023).

- **PRETEXTING**

  Ocurre cuando alguien crea una identidad falsa o hace un mal uso de su rol real; esto sucede con mayor frecuencia en las violaciones de datos desde el interior (ENISA, 2023).

- **QUID PRO QUO**

  Los ataques ocurren cuando los estafadores se hacen pasar por personal del departamento de TI u otro proveedor de servicios técnicos (ENISA, 2023).

- **HONEYTRAPS**

  Son un tipo de ingeniería social en la que los estafadores crean perfiles falsos en sitios de citas en línea y redes sociales utilizando fotos robadas y atractivas (ENISA, 2023).

- **SCAREWARE**

  Asusta a las víctimas haciéndoles creer que están bajo una amenaza inminente; por ejemplo, podrías recibir un mensaje diciendo que tu dispositivo ha sido infectado con un virus (ENISA, 2023).

- **BUSINESS E-MAIL COMPROMISE (BEC)**

  Es una estafa sofisticada dirigida a empresas y organizaciones, en la que los criminales emplean técnicas de ingeniería social. El atacante puede engañar a un empleado o ejecutivo para que inicie transferencias bancarias bajo condiciones fraudulentas. Otro tipo de BEC (Business Email Compromise) es acceder a la cuenta de correo electrónico de un empleado o ejecutivo para enviar correos electrónicos que contienen código malicioso a toda la empresa (a clientes, proveedores, etc.) (ENISA, 2023).

- **FRAUD**

  Es la representación u ocultación intencional de un hecho importante en el cual la víctima debe confiar (ENISA, 2023).

- **IMPERSONATION**

  Es cuando una entidad asume ilegítimamente la identidad de otra entidad para beneficiarse de ello (ENISA, 2023).

- **COUNTERFEIT**

  Es la imitación fraudulenta de algo (ENISA, 2023).

2.2 REVISIÓN DE LITERATURA

EVOLUCIÓN Y TÉCNICAS DE ATAQUE EN EL PHISHING: UN ANÁLISIS DE VECTORES Y ENFOQUES TÉCNICOS

El estudio realizado por Chiew et al. (2018) destacan la creciente sofisticación de los ataques de Phishing, tanto en su variedad de tipos como en los vectores utilizados para comprometer a las víctimas. Los autores subrayan que los atacantes han adoptado múltiples enfoques técnicos, desde el uso de correos electrónicos maliciosos hasta la creación de sitios web falsos que imitan a organizaciones legítimas. Además, el análisis identifica que la efectividad de estos ataques radica en la capacidad de los ciberdelincuentes para explotar las vulnerabilidades humanas, aprovechando tanto la falta de conocimiento en seguridad cibernética como la urgencia psicológica inducida en las víctimas.

Uno de los aspectos más alarmantes señalados en la investigación de Chiew et al. (2018) es la evolución de los vectores de ataque, que van desde simples correos electrónicos hasta estrategias más complejas como el spear-Phishing y el whaling, diseñados específicamente para dirigirse a individuos con alto acceso a información sensible dentro de una organización. Este enfoque personalizado incrementa significativamente el éxito de los ataques, ya que las técnicas utilizadas son difíciles de detectar por los mecanismos de defensa tradicionales, como los filtros de spam o los sistemas de detección de intrusiones.

Chiew et al. (2018) también hacen énfasis en los métodos técnicos utilizados por los atacantes para evadir las barreras de seguridad. Estos métodos incluyen el uso de servidores de comando y control distribuidos, que permiten a los atacantes mantener la operatividad de sus campañas de Phishing sin ser detectados fácilmente. Los autores concluyen que, a pesar de los avances en la tecnología de seguridad, la naturaleza adaptable de los ataques de Phishing requiere soluciones más dinámicas, centradas no solo en la tecnología, sino también en la educación de los usuarios para mejorar su resistencia frente a estas amenazas.

La investigación de Chiew et al. (2018) sugiere que la prevención efectiva de los ataques de Phishing debe basarse en un enfoque multifacético, que incluya la combinación de medidas tecnológicas avanzadas con programas de concientización que eduquen a los usuarios sobre los peligros de los ataques de ingeniería social. Los autores destacan que las soluciones centradas únicamente en la tecnología pueden ser insuficientes si los usuarios siguen siendo vulnerables a las tácticas de engaño que emplean los ciberdelincuentes.

FACTORES PSICOLÓGICOS EN LA DETECCIÓN DE PHISHING

La investigación de Buckley et al. (2023) abordan las dinámicas psicológicas que influyen en el comportamiento de los empleados frente a los correos electrónicos de Phishing. En su estudio, los autores examinan factores como la intuición, la atención y la tipología de los correos electrónicos impactan en la capacidad de un empleado para identificar un ataque de Phishing. El análisis muestra que aquellos usuarios que dependen excesivamente de la intuición pueden ser más vulnerables a los ataques, en comparación con quienes dedican más tiempo a la elaboración consciente de la información contenida en el correo electrónico.

Un hallazgo clave del estudio de Buckley et al. (2023) es la influencia de la atención en la susceptibilidad a los ataques de Phishing. Los empleados que experimentan fatiga o que manejan grandes volúmenes de correos electrónicos suelen prestar menos atención a las señales de alerta, lo que aumenta la probabilidad de que caigan en el engaño. Además, la tipología del correo, es decir, su formato y estilo, juega un papel crucial. Los correos electrónicos que imitan la apariencia de comunicaciones formales y legítimas son más difíciles de detectar, lo que subraya la necesidad de enfoques más sofisticados en la capacitación y concienciación de los usuarios.

El estudio también destaca la importancia de la educación y formación continuas para mitigar el riesgo de ataques de Phishing. A través de simulaciones y análisis detallados de comportamientos, Buckley et al. (2023) sugieren que las organizaciones deben adaptar sus estrategias de ciberseguridad, enfocándose en mejorar la capacidad de los empleados para analizar cuidadosamente los correos electrónicos y no solo depender de respuestas intuitivas.

EL FACTOR HUMANO EN LOS ATAQUES DE PHISHING

En el estudio de Gallo et al. (2024) ponen de relieve la importancia del factor humano en la vulnerabilidad frente a ataques de Phishing. La investigación se centra en el análisis del comportamiento de los usuarios al leer correos electrónicos y cómo ciertos patrones pueden aumentar el riesgo de ser víctimas de Phishing. Los autores argumentan que la interacción humana con los correos electrónicos es un elemento clave que los atacantes explotan, especialmente cuando los usuarios no son capaces de identificar correctamente las señales de peligro en las comunicaciones recibidas.

El estudio recoge y analiza datos sobre cómo los usuarios evalúan los correos electrónicos, encontrando que muchos no detectan signos sutiles de engaño debido a la sobrecarga informativa y la falta de atención a detalles críticos. Gallo et al. (2024) señalan que, a menudo, los usuarios se enfocan en los aspectos superficiales del mensaje, como el remitente o el tono, y no prestan suficiente atención a enlaces sospechosos o direcciones de correo maliciosas disfrazadas como legítimas.

Además, Gallo et al. (2024) sugieren que la capacitación en ciberseguridad debe adaptarse para abordar estos comportamientos específicos, destacando la necesidad de entrenar a los usuarios en técnicas que les permitan analizar cuidadosamente cada aspecto de un correo antes de actuar. El estudio concluye que, a pesar de los avances tecnológicos

en la detección de Phishing, la conciencia y la educación de los usuarios siguen siendo la línea de defensa más importante.

ANÁLISIS DEL ENVENENAMIENTO DE LA OPTIMIZACIÓN EN MOTORES DE BÚSQUEDA

El análisis realizado por Le et al. (2024) destacan una amenaza creciente en el ámbito de la ciberseguridad conocida como envenenamiento de optimización de motores de búsqueda (SEO poisoning), la cual afecta de manera particular a las pequeñas y medianas empresas (Pymes). Esta técnica maliciosa implica la manipulación de los algoritmos de búsqueda para redirigir a los usuarios hacia sitios web fraudulentos o peligrosos, generalmente con el propósito de robar información sensible o instalar malware en los dispositivos de las víctimas. Dado que las Pymes a menudo no cuentan con los recursos necesarios para implementar medidas de seguridad robustas, se convierten en objetivos vulnerables a este tipo de ataque.

El estudio de Le et al. (2024) subraya que los ciberdelincuentes emplean técnicas avanzadas de SEO para hacer que sus sitios web maliciosos aparezcan entre los primeros resultados de búsqueda, aprovechando la confianza de los usuarios en los motores de búsqueda. Los atacantes suelen utilizar palabras clave populares o tendencias emergentes para engañar a los usuarios y lograr que visiten sitios falsificados que se presentan como legítimos. Esta amenaza no solo compromete la seguridad de los usuarios, sino que también afecta la reputación de las pymes, ya que una vez que los clientes asocian su interacción con sitios fraudulentos, la confianza en las empresas se deteriora.

En cuanto a las estrategias de mitigación, Le et al. (2024) proponen que las pymes adopten prácticas preventivas, como monitorear regularmente su presencia en línea y mejorar sus defensas técnicas, incluyendo la implementación de certificados SSL y otras medidas de autenticación en sus sitios web. También recomiendan fomentar la educación y la concientización entre empleados y clientes, con el fin de evitar que caigan en este tipo de trampas cibernéticas. Estas acciones son esenciales para proteger no solo la seguridad de la información, sino también la continuidad del negocio y su reputación en el mercado.

DETECCIÓN DE PHISHING EN REDES SOCIALES

Liew et al, (2019) presentan un enfoque innovador para la detección en tiempo real de Phishing en Twitter, una de las plataformas sociales más populares y vulnerables a la propagación de ciberamenazas. Los autores desarrollaron un mecanismo de alerta de

seguridad efectivo diseñado para identificar y mitigar ataques de Phishing que se diseminan a través de tweets maliciosos. Este enfoque aprovecha técnicas de procesamiento de lenguaje natural (NLP) y algoritmos de aprendizaje automático para analizar grandes volúmenes de datos y detectar patrones asociados con el Phishing, mejorando la capacidad de respuesta ante amenazas emergentes.

El mecanismo propuesto por Liew et al. (2019) se basa en la clasificación de tweets en tiempo real, evaluando factores como el contenido textual, la estructura de los enlaces y el comportamiento de los usuarios que publican los tweets. Este enfoque permite una detección más precisa de posibles ataques, al filtrar falsos positivos y asegurar que solo los tweets con alta probabilidad de ser maliciosos sean etiquetados y reportados. Los resultados del estudio muestran que este sistema de alertas puede ayudar a reducir significativamente el impacto de campañas de Phishing dirigidas a usuarios de redes sociales.

Además de su efectividad técnica, los autores subrayan la importancia de la colaboración entre plataformas como Twitter y las agencias de ciberseguridad para implementar estas herramientas de detección de forma más amplia. Este mecanismo no solo protege a los usuarios individuales, sino también a las empresas que dependen de las redes sociales para sus operaciones, ya que una rápida identificación de estos ataques puede evitar daños a la reputación y pérdidas financieras. Por lo tanto, la implementación de un sistema de alertas de seguridad como el descrito por Liew et al. (2019) representa un avance clave en la lucha contra el Phishing en entornos de redes sociales.

REVISIÓN SISTEMÁTICA DE LOS MÉTODOS ACTUALES DE CAPACITACIÓN EN CIBERSEGURIDAD

Prümmer et al, (2024) llevan a cabo una revisión exhaustiva de los métodos actuales de capacitación en ciberseguridad, destacando la importancia de la educación continua para fortalecer la resiliencia de individuos y organizaciones frente a las ciberamenazas. Su revisión sistemática analiza una amplia gama de técnicas de formación, desde simulaciones de ataques hasta ejercicios prácticos y campañas de concienciación, proporcionando una visión global de las mejores prácticas y los desafíos persistentes en el ámbito de la capacitación en ciberseguridad.

Uno de los puntos centrales del estudio de Prümmer et al. (2024) es la creciente adopción de simulaciones de Phishing como herramienta educativa. Estas simulaciones permiten a

las organizaciones recrear escenarios reales de ataques de Phishing, brindando a los empleados la oportunidad de enfrentarse a situaciones controladas pero representativas de amenazas reales. Este enfoque no solo mejora el reconocimiento de tácticas maliciosas, sino que también fomenta una cultura organizacional más atenta a la seguridad, donde los errores se convierten en oportunidades de aprendizaje.

Asimismo, los autores subrayan que las técnicas de capacitación deben adaptarse a los contextos específicos de cada organización y grupo de usuarios. Prümmer et al. (2024) destacan que una capacitación demasiado técnica o genérica puede perder efectividad, mientras que los métodos personalizados que consideran el perfil de riesgo, las competencias tecnológicas y las necesidades del personal resultan en una mejor retención de conocimientos y respuestas más rápidas ante incidentes de seguridad. Este enfoque refuerza la idea de que la formación en ciberseguridad no es un proceso único, sino una estrategia continua y dinámica.

DESAFÍOS GLOBALES Y ESTRATEGIAS DE DEFENSA

Singer, (2014) proporciona una visión integral sobre los desafíos actuales de la ciberseguridad y cómo estos impactan a nivel global. El libro aborda no solo los aspectos técnicos de las amenazas cibernéticas, sino también las dimensiones políticas, sociales y económicas que configuran el panorama moderno de la seguridad informática. Singer resalta que la ciberseguridad se ha convertido en una preocupación central para los gobiernos, las empresas y los individuos, subrayando la necesidad de desarrollar una comprensión amplia de sus riesgos y de las medidas necesarias para mitigarlos.

El autor también explora cómo la ciberseguridad y la ciberdefensa están estrechamente ligadas a los conceptos de guerra en la era digital. En este contexto, Singer, (2014) argumenta que los ciberataques no solo tienen el potencial de causar daños económicos significativos, sino también de desestabilizar estructuras críticas a nivel estatal y corporativo. Los ataques a infraestructuras esenciales, como redes eléctricas o sistemas financieros, son ejemplos de cómo las ciberamenazas pueden tener consecuencias devastadoras, que van más allá del ámbito tecnológico y afectan profundamente a la sociedad en su conjunto.

Además, Singer, (2014) destaca que la ciberseguridad no debe ser abordada únicamente desde una perspectiva técnica. Es crucial que los líderes gubernamentales y corporativos comprendan la interconexión entre los riesgos cibernéticos y otros desafíos globales,

como el espionaje industrial, la manipulación de la información y el terrorismo cibernético. El enfoque de Singer enfatiza la importancia de una estrategia global y colaborativa para enfrentar estos retos, incorporando tanto medidas preventivas como respuestas rápidas y coordinadas ante incidentes.

CONCLUSIONES DE ESTUDIOS RELACIONADOS CON EL PHISHING Y LA INGENIERÍA SOCIAL

En función del análisis realizado en la revisión de literatura y con el objetivo de contextualizar este estudio dentro del panorama actual de la investigación en ciberseguridad, a continuación, se presenta una tabla que sintetiza las conclusiones más relevantes de otros estudios relacionados con el Phishing y las técnicas de ingeniería social (Tabla 2). Esta tabla permite comparar las principales aportaciones de investigaciones previas y cómo se alinean o complementan las estrategias propuestas en este proyecto.

Referencia	Objetivo del Estudio	Conclusiones Principales
Chiew et al. (2018)	Analizar la evolución de los ataques de Phishing y sus vectores.	Los ataques de Phishing se han vuelto más sofisticados y personalizados, utilizando múltiples vectores de ataque.
Buckley et al. (2023)	Evaluar el impacto psicológico de los correos de Phishing en empleados.	La atención y el estado de alerta son factores clave en la detección de Phishing.
Gallo et al. (2024)	Examinar cómo los usuarios evalúan correos electrónicos fraudulentos.	El factor humano sigue siendo la mayor vulnerabilidad en los ataques de Phishing, a pesar de los avances tecnológicos.
Prümmer et al. (2024)	Revisar los métodos de capacitación en ciberseguridad actuales.	Las simulaciones de Phishing son altamente efectivas para mejorar la conciencia y las habilidades de detección.

Le et al. (2024)	Evaluar el SEO poisoning en pequeñas y medianas empresas (Pymes).	Las Pymes son vulnerables a ataques de SEO poisoning; es crucial implementar certificados SSL y medidas de autenticación.

Tabla 2: Conclusiones de estudios relacionados con el Phishing y la ingeniería social

2.3 MARCO TEÓRICO

2.3.1 LA IMPORTANCIA DE LA CIBERSEGURIDAD FRENTE AL PHISHING Y LA INGENIERÍA SOCIAL

La ciberseguridad es una disciplina esencial en la era digital actual, ya que protege los datos sensibles y la infraestructura crítica de ataques cibernéticos. En el contexto del Phishing y las técnicas de ingeniería social, esta protección se enfoca en salvaguardar la información personal y profesional de los usuarios. Los ataques de Phishing han evolucionado hasta convertirse en una de las principales amenazas para la seguridad de la información, afectando a individuos y organizaciones a nivel global (Singer, 2014).

A medida que las técnicas de Phishing y la ingeniería social se vuelven más sofisticadas, la capacidad de los usuarios para identificar y resistir estos ataques se convierte en una primera línea de defensa. Esto subraya la importancia de implementar estrategias de concientización que no solo aborden los aspectos tecnológicos, sino también los factores humanos que los ciberdelincuentes explotan para lograr sus objetivos. Al estudiar estas tácticas, se busca mitigar los riesgos y vulnerabilidades mediante el fortalecimiento de la ciberseguridad en todos los niveles (ENISA, 2023).

2.3.2 TÉCNICAS DE INGENIERÍA SOCIAL Y SU IMPACTO EN LA SEGURIDAD DE LA INFORMACIÓN

La ingeniería social es un conjunto de técnicas psicológicas utilizadas por los atacantes para manipular a los usuarios y obtener acceso a información confidencial o sistemas críticos. Estas técnicas se basan en la explotación de la confianza, la urgencia y el miedo de los usuarios, y son utilizadas en combinación con el Phishing para aumentar la efectividad de los ataques (Buckley et al, 2023).

El análisis de estas técnicas permite comprender cómo los atacantes manipulan a los usuarios finales para obtener credenciales, acceder a sistemas o realizar acciones perjudiciales. Entre las técnicas más comunes de ingeniería social se encuentran el

pretexting, el baiting, y el quid pro quo, todas diseñadas para aprovechar las vulnerabilidades humanas. Comprender estas técnicas es crucial para desarrollar estrategias de concientización que reduzcan el impacto de los ataques de Phishing y refuercen la seguridad de la información (Gallo et al, 2024).

2.3.3 ESTRATEGIAS DE CONCIENTIZACIÓN Y HERRAMIENTAS PARA LA PREVENCIÓN DEL PHISHING

La prevención de los ataques de Phishing y las técnicas de ingeniería social no solo depende de la implementación de medidas tecnológicas, sino también de la capacidad de los usuarios para identificar y evitar estas amenazas. Las campañas de concientización han demostrado ser una de las herramientas más efectivas para reducir la vulnerabilidad de los usuarios frente a estos ataques. Sin embargo, con la constante evolución de las tácticas de Phishing, es necesario actualizar regularmente las estrategias de prevención (Prümmer et al, 2024).

Este apartado explora diversas herramientas y metodologías utilizadas para la concientización y prevención de ataques de Phishing. Entre las técnicas más comunes se encuentran las simulaciones de Phishing y las capacitaciones interactivas, que permiten a los usuarios experimentar situaciones de riesgo en un entorno controlado. Además, se analizarán herramientas como el Social Engineering Toolkit (SET) (TrustedSec, 2020), que permite la simulación de ataques de ingeniería social para educar a los usuarios y mejorar su capacidad de respuesta frente a estos ataques.

2.4 METODOLOGÍA DEL PROYECTO

2.4.1 METODOLOGÍA DE LA INVESTIGACIÓN

El objetivo principal de esta investigación es analizar estrategias de prevención de ataques de Phishing y técnicas de ingeniería social mediante estudios de caso y herramientas de simulación, con el fin de mejorar la seguridad de los usuarios finales. Aunque existen investigaciones previas sobre seguridad informática y Phishing, esta propuesta busca integrar ambos elementos, proporcionando un enfoque holístico que aborde tanto los aspectos técnicos como los psicológicos.

El diseño de la investigación será analítico y explicativo, permitiendo un análisis profundo de las tácticas de Phishing y las técnicas de ingeniería social. Además, se evaluará la relación entre la concientización de los usuarios y la efectividad de las

estrategias de prevención. Con base en los hallazgos, se propondrán nuevas estrategias de concientización y prevención.

Enfoque metodológico

- **Investigación documental**

  La información primaria se recopilará mediante una revisión sistemática de artículos científicos, informes de organismos gubernamentales y publicaciones relevantes en el campo de la ciberseguridad. Se utilizarán bases de datos académicas como ScienceDirect y IEEE Xplore para obtener estudios actualizados y relevantes, como los trabajos de Gallo et al. (2024) y Le et al. (2024).

  Además, se analizarán casos documentados de Phishing extraídos de informes de ciberseguridad de instituciones como (ENISA, 2023). También se incluirán ejemplos obtenidos de plataformas como Twitter, donde se observan alertas en tiempo real de incidentes, tal como se sugiere en el trabajo de Liew et al. s2019). Esto permitirá identificar patrones de ataque y tácticas comunes empleadas por los ciberdelincuentes.

- **Investigación Experimental**

  Para validar las estrategias de prevención, se utilizarán herramientas de simulación como Kali Linux y el Social Engineering Toolkit (SET). Estas herramientas permitirán realizar simulaciones controladas de ataques de Phishing en un entorno seguro, donde se podrá observar el comportamiento de los usuarios finales ante estos ataques.

- **Investigación de Campo**

  Se realizarán experimentos directos con usuarios finales mediante encuestas y simulaciones controladas. Durante estas pruebas, se implementarán diversas estrategias de concientización (como programas de capacitación y guías prácticas) y se medirá la respuesta de los usuarios frente a intentos de Phishing. El objetivo de esta fase es determinar qué métodos de concientización son más efectivos para mejorar la capacidad de identificación y prevención de ataques.

  Los datos obtenidos se analizarán utilizando un enfoque mixto, combinando métodos cuantitativos y cualitativos. Se emplearán herramientas estadísticas para evaluar el impacto de las estrategias en términos de mejora de la tasa de éxito en la detección de ataques. A nivel cualitativo, se evaluarán las respuestas de los

usuarios para identificar patrones de comportamiento, percepción y cambios en las actitudes hacia la ciberseguridad.

- **Implementación y Evaluación de Estrategias**

  Se desarrollará e implementará un programa integral de concientización y capacitación en ciberseguridad dirigido a una muestra representativa de usuarios finales. Este programa incluirá:

  Recopilación de datos cuantitativos sobre la tasa de éxito de los ataques de Phishing antes y después de la implementación de las estrategias.

  Medición de la capacidad de los usuarios para identificar y reportar intentos de ingeniería social.

  Posteriormente, se analizarán los datos recopilados mediante técnicas estadísticas para evaluar el impacto de las estrategias en la prevención de ataques de Phishing y mejorar la resiliencia cibernética.

- **Entrevistas en Profundidad**

  Con un subconjunto representativo de los usuarios finales, se realizarán entrevistas en profundidad para comprender sus percepciones, experiencias y actitudes hacia las estrategias de concientización. Durante estas entrevistas, se explorarán las barreras y facilitadores que influyen en la adopción de comportamientos seguros en línea.

  Los datos obtenidos de estas entrevistas serán analizados cualitativamente para identificar posibles áreas de mejora en las estrategias implementadas, así como ajustar el contenido de los programas de concientización para aumentar su efectividad.

Hipótesis

La implementación de programas de concientización y capacitación en seguridad cibernética reducirá la tasa de éxito de los ataques de Phishing y aumentará la capacidad de los usuarios finales para identificar y reportar intentos de ingeniería social.

Condiciones para comprobar la hipótesis:

Para evaluar esta hipótesis, se diseñará e implementará un programa integral de concientización y capacitación en seguridad cibernética dirigido a los usuarios finales. Se medirá la tasa de éxito de los ataques de Phishing antes y después de la implementación del programa, con el fin de evaluar su efectividad en la prevención de estos ataques.

Asimismo, se realizarán pruebas y encuestas para evaluar la capacidad de los usuarios finales de identificar y reportar intentos de ingeniería social, tanto antes como después de la implementación del programa. Estas mediciones permitirán llevar a cabo una evaluación exhaustiva del impacto del programa en la resiliencia cibernética de la organización y en la capacidad de los usuarios para protegerse frente a amenazas en línea.

Variables

Variable Independiente: Implementación de programas de concientización y capacitación en seguridad cibernética.

Variable Dependiente: Tasa de éxito de los ataques de Phishing y capacidad de los usuarios finales para identificar y reportar intentos de ingeniería social.

Población

La población objetivo para esta investigación estará constituida por los usuarios finales que residen en los Departamentos de la Comuna San Pablo. Estos usuarios representan individuos que utilizan dispositivos electrónicos y están expuestos a posibles ataques de Phishing y técnicas de ingeniería social en su día a día. La población incluirá a personas de diferentes edades, niveles de educación, ocupaciones y niveles de experiencia en tecnología, ya que la concientización y la prevención de estos ataques son relevantes para todos los usuarios de la comunidad. La muestra para este estudio estará conformada por 50 personas seleccionadas de esta población, representando una diversidad de perfiles en cuanto a experiencia tecnológica y exposición a riesgos cibernéticos.

2.4.2 METODOLOGÍA DE DESARROLLO DEL PROYECTO

El desarrollo del proyecto se centrará en la creación de dos productos principales: un tríptico informativo y una página web interactiva. Ambos elementos estarán diseñados para facilitar la concientización sobre Phishing y proporcionar a los usuarios finales herramientas útiles para evitar caer en este tipo de estafas.

Desarrollo del Tríptico:

- **Fase de Investigación y Contenido:** Se recopilará información clave sobre el Phishing y las técnicas de ingeniería social, enfocándose en ejemplos claros y sencillos para el usuario final. El contenido incluirá definiciones básicas, ejemplos de ataques comunes, y buenas prácticas para evitar ser víctima de estas estafas.

Las fuentes de información incluirán artículos académicos, como Buckley et al, (2023) y estudios técnicos como Singer, (2014).

- **Diseño Gráfico:** Utilizando herramientas de diseño, se diseñará el tríptico con una estructura visualmente atractiva que sea fácil de leer y comprender. Se incluirán infografías que expliquen cómo identificar un mensaje de Phishing y las acciones correctas a tomar en caso de recibir uno.

Desarrollo de la Página Web:

- **Fase de Planificación y Estructura:** La página web estará organizada en secciones que proporcionen información detallada sobre el Phishing, enlaces a fuentes confiables, ejemplos de buenas prácticas, y herramientas interactivas como tests para que los usuarios puedan evaluar su nivel de conocimiento sobre el tema. El contenido será dinámico y actualizado regularmente con las últimas amenazas y soluciones.
- **Tecnologías Utilizadas:** El desarrollo de la página web se llevará a cabo utilizando tecnologías open source. También se aprovecharán herramientas de seguridad proporcionadas por Kali Linux para realizar pruebas de simulación de Phishing, utilizando kits como el Social Engineering Toolkit (SET).

CAPÍTULO III

3 PROPUESTA

3.1 DESARROLLO

En esta sección, se detallan los pasos seguidos durante la implementación del proyecto. El enfoque principal es demostrar, mediante ejemplos prácticos, cómo los ciberdelincuentes ejecutan ataques de Phishing y cómo los usuarios pueden ser vulnerables a ellos. Utilizando herramientas especializadas, se replican escenarios de ataques de Phishing para analizar su impacto y las tácticas empleadas. A partir de estos ejemplos, se propuso una serie de estrategias de concientización, diseñadas para educar a los usuarios finales en la detección y prevención de estos ataques. Este desarrollo tiene como objetivo final proporcionar soluciones prácticas y accesibles que mejoren la seguridad cibernética en diferentes contextos.

3.1.1 ENCUESTA

La encuesta realizada a los usuarios finales (Ver Anexo 1) está diseñada para evaluar la experiencia de los usuarios con mensajes sospechosos y Phishing. Se les ha asignado una codificación a las opciones de respuesta (Ver Anexo 2), permitiendo un análisis más estructurado y cuantificable de los resultados. Los datos recolectados muestran las respuestas obtenidas antes de llevar a cabo la capacitación (Ver Anexo 3) y, posteriormente, tras la implementación de las estrategias formativas (Ver Anexo 4).

En base a los datos de la encuesta inicial, se detallan las siguientes inferencias:

Experiencia con mensajes sospechosos: Una pequeña proporción de encuestados ha experimentado mensajes sospechosos en alguna medida, mientras que otra gran porción indica no estar seguro lo que resalta la prevalencia de este problema (Ilustración 1).

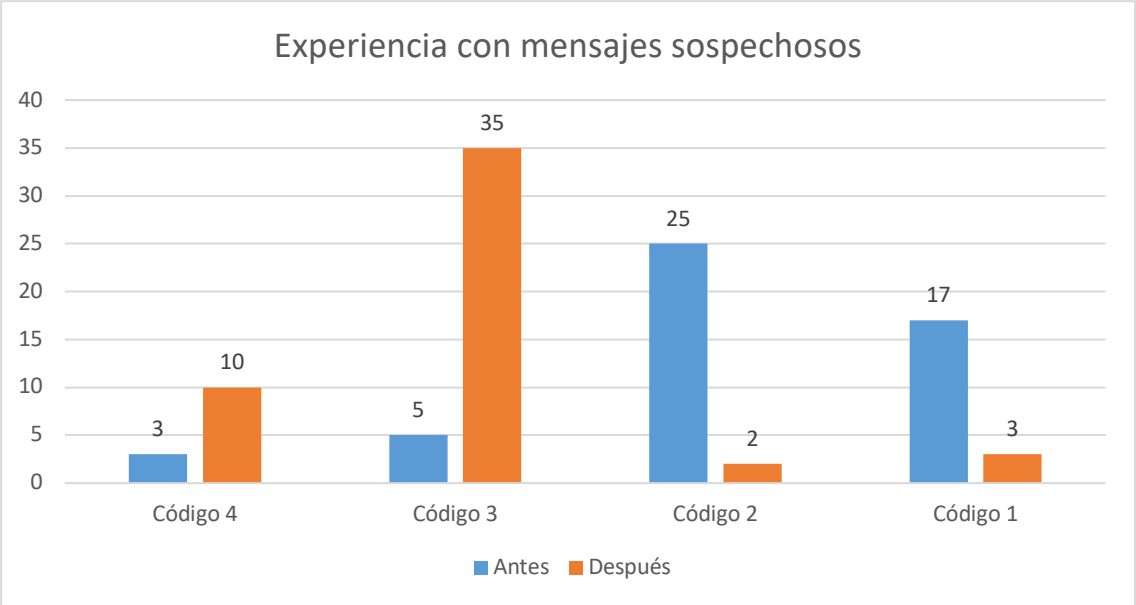

Ilustración 1: Experiencia con mensajes sospechosos

Capacidad para identificar mensajes de Phishing: Hay una gran división entre aquellos que se sienten seguros en identificar mensajes de Phishing y aquellos que no están seguros o no saben cómo hacerlo, lo que sugiere la necesidad de educación y concientización (Ilustración 2).

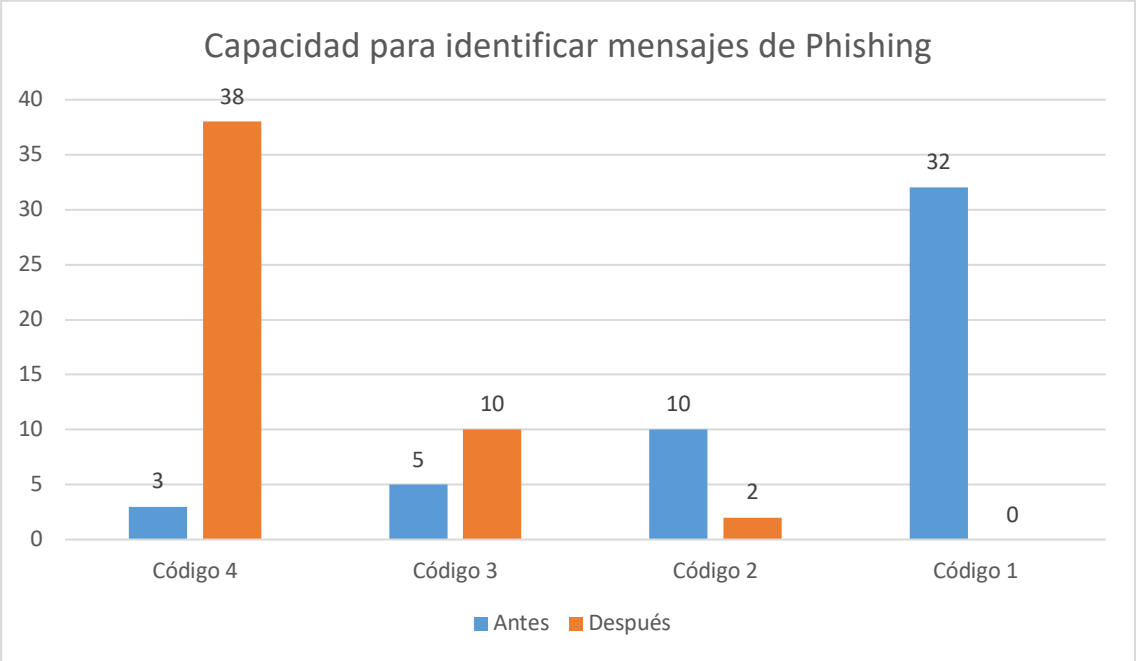

Ilustración 2: Capacidad para identificar mensajes de Phishing

Participación en programas de concientización sobre seguridad informática: La mayoría de las personas encuestadas no han participado en programas de concientización sobre

seguridad informática, lo que indica una posible área de mejora en la educación de seguridad cibernética (Ilustración 3).

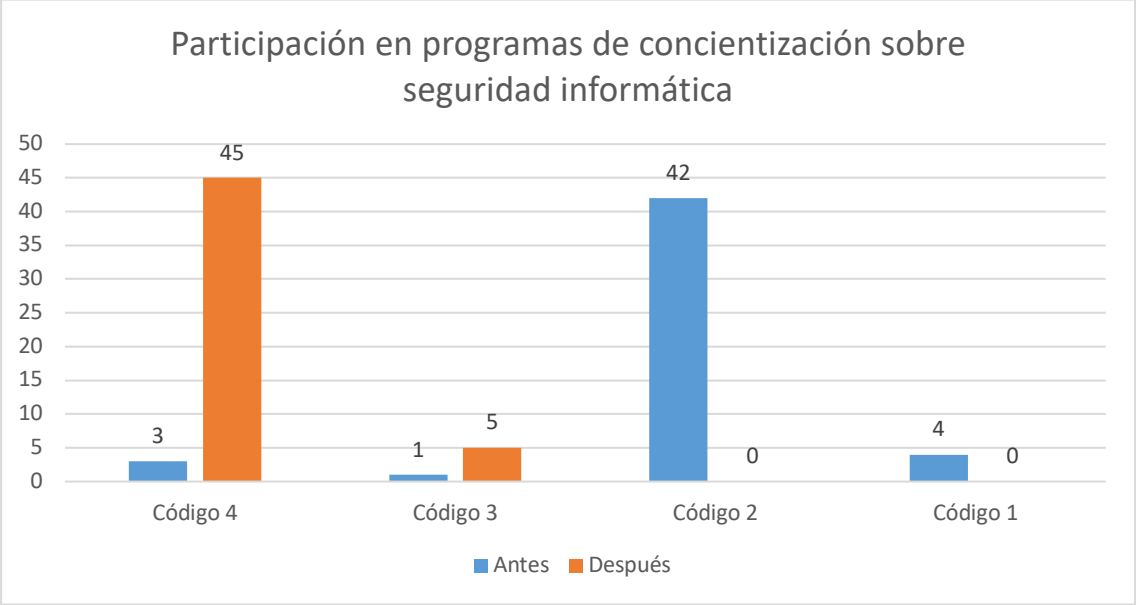

Ilustración 3: Participación en programas de concientización sobre seguridad informática

Medidas de seguridad al recibir un mensaje sospechoso: La respuesta más común es lo abro, pero no hago clic en ningún enlace y una pequeña parte en eliminar el mensaje de inmediato, lo que muestra una actitud cautelosa pero no necesariamente informada (Ilustración 4).

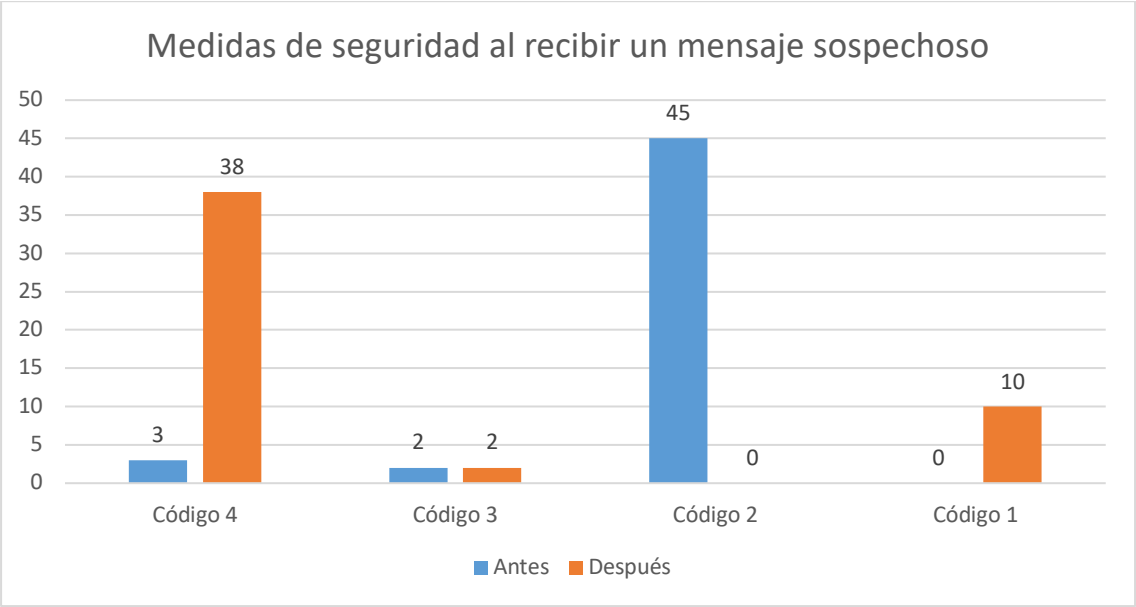

Ilustración 4: Medidas de seguridad al recibir un mensaje sospechoso

En general, estas inferencias sugieren que existe una necesidad de aumentar la educación y concientización sobre seguridad cibernética, así como mejorar las habilidades de identificación y respuesta a mensajes de Phishing entre los usuarios.

Basándonos en los resultados de la encuesta posterior a la capacitación, podemos realizar varias inferencias:

- Experiencia con mensajes sospechosos: La mayor parte de encuestados ha experimentado mensajes sospechosos en alguna medida, lo que resalta la prevalencia de este problema, pero con la capacidad del usuario de analizar los mensajes (Ilustración 1)
- Capacidad para identificar mensajes de Phishing: La mayoría de las personas (76%) afirma que siempre pueden identificar mensajes de Phishing, lo que indica un alto grado de confianza en su capacidad para reconocer este tipo de amenaza (Ilustración 5).
- Participación en programas de concientización sobre seguridad informática: La mayoría de las personas (90%) afirma participar regularmente en programas de concientización sobre seguridad informática, lo que sugiere un alto nivel de conciencia y educación en este tema (Ilustración 6).
- Medidas de seguridad al recibir un mensaje sospechoso: La mayoría de las personas (76%) indica que reporta como spam y bloquea al remitente, mientras que el resto indaga más sobre el mensaje antes de tomar una acción, lo que muestra una respuesta rápida y efectiva ante posibles amenazas (Ilustración 7).

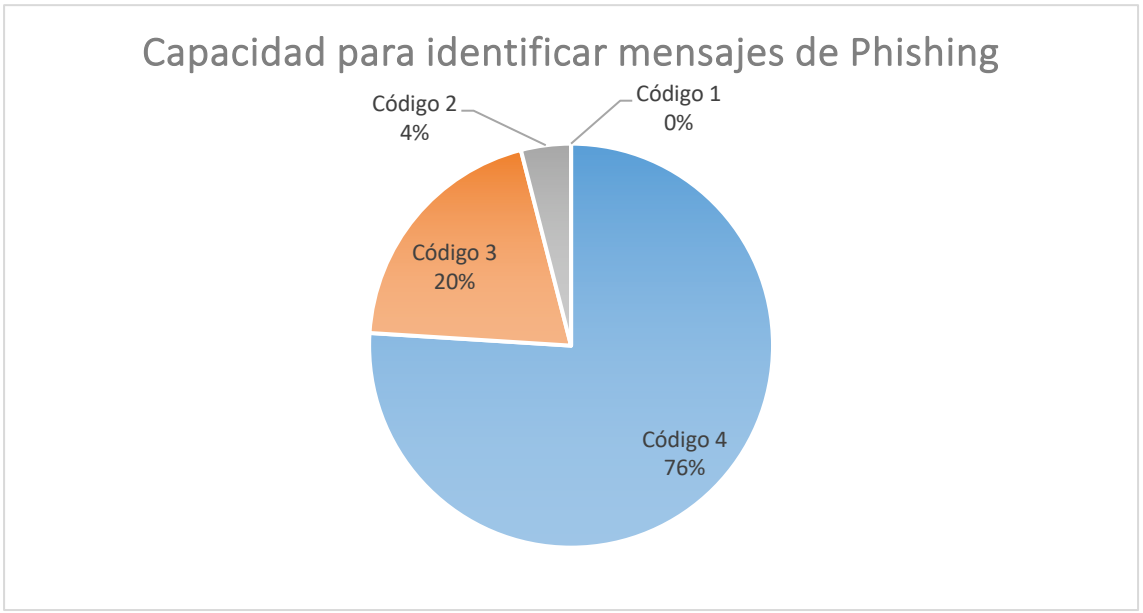

Ilustración 5: Porcentaje de capacidad para identificar mensajes de Phishing

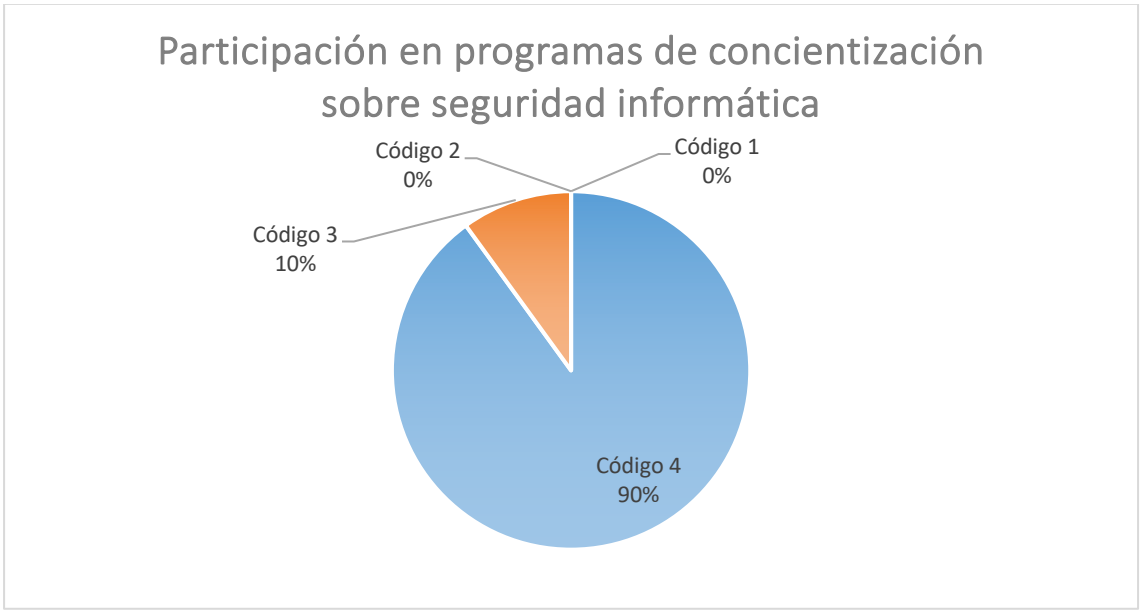

Ilustración 6: Porcentaje de participación en programas de concientización sobre seguridad informática

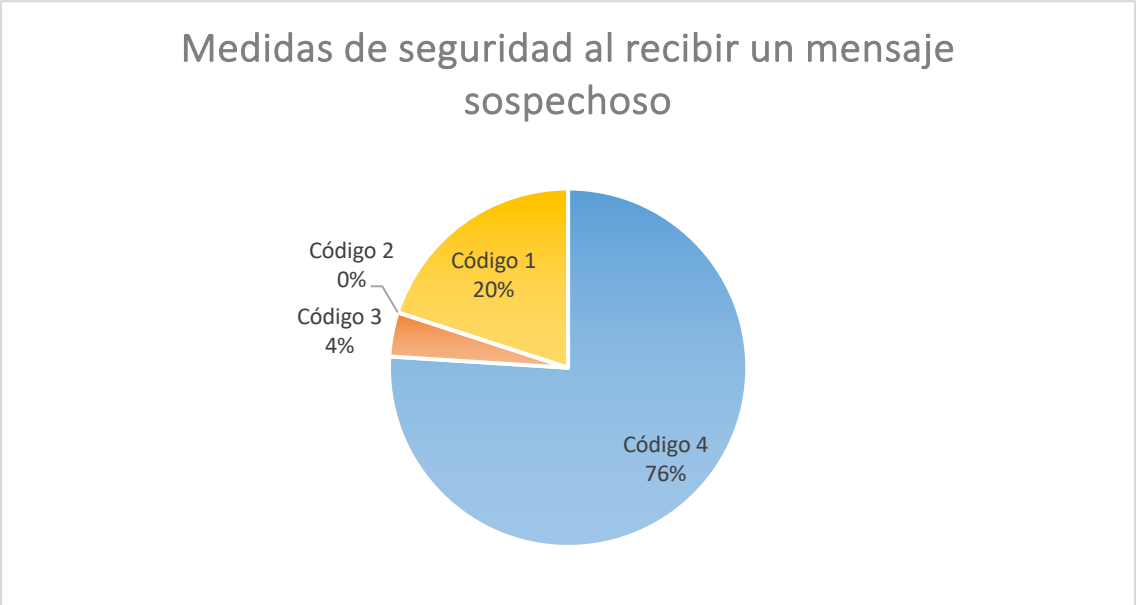

Ilustración 7: Porcentaje de medidas de seguridad al recibir un mensaje sospechoso

Estos resultados sugieren que existe un alto nivel de conciencia y preparación entre los encuestados en lo que respecta a la seguridad informática y la identificación de mensajes de Phishing. La participación regular en programas de concientización y la rápida respuesta ante mensajes sospechosos indican un enfoque proactivo hacia la protección contra amenazas cibernéticas.

Efectividad de las estrategias de concientización y capacitación en la reducción de la tasa de éxito de los ataques de Phishing en el futuro: Con base en la mejora observada en la capacidad de los usuarios para identificar mensajes de Phishing tras la capacitación, se prevé una disminución en la tasa de éxito de los ataques de Phishing en el futuro.

Relación entre la integración de estrategias de concientización y capacitación y la resistencia al Phishing por parte de los usuarios finales: Se encontró una asociación positiva entre la participación en programas de concientización y capacitación y la resistencia al Phishing por parte de los usuarios finales. Aquellos que recibieron capacitación muestran una mayor capacidad para identificar y evitar mensajes de Phishing, lo que sugiere que la educación desempeña un papel crucial en la protección contra estos ataques.

De la hipótesis planteada: “La implementación de programas de concientización y capacitación en seguridad cibernética reducirá la tasa de éxito de los ataques de Phishing y aumentará la capacidad de los usuarios finales para identificar y reportar intentos de ingeniería social” se puede corroborar con la encuesta posterior, donde se observa un

aumento en la cantidad de personas que afirman poder identificar mensajes de Phishing con mayor seguridad. Por lo tanto, este resultado respalda la hipótesis de que la educación y concientización pueden mejorar significativamente la capacidad de detección del Phishing.

3.1.2 ENTREVISTA

A continuación, se detalla lo más relevante de la entrevista a los usuarios finales (Ver Anexo 5)

Experiencia personal con Phishing:

Algunos de los participantes mencionan haber recibido mensajes de Phishing en algún momento, compartieron experiencias específicas sobre cómo identifican y manejan correos electrónicos, mensajes de texto de Phishing en el pasado.

Varias personas expresan preocupación por la sofisticación creciente de los ataques de Phishing y la dificultad para distinguir los mensajes legítimos de los fraudulentos.

Medidas de seguridad utilizadas:

Los participantes discutieron las medidas de seguridad que implementan al recibir mensajes sospechosos, como no hacer clic en enlaces desconocidos o verificar los datos del remitente.

Algunos mencionan haber recibido capacitación sobre cómo identificar mensajes de Phishing y qué hacer en caso de sospecha.

Otros admiten no tener protocolos claros para manejar mensajes sospechosos y expresan interés en recibir más educación sobre el tema.

Participación en programas de concientización:

Pocos participantes mencionan haber participado en programas de concientización sobre seguridad informática en el pasado, pero expresan que la capacitación era limitada o insuficiente.

Algunos sugirieron que los programas de concientización deberían ser más interactivos y personalizados para abordar mejor las necesidades individuales.

Hubo una solicitud generalizada de más oportunidades de capacitación y concientización sobre seguridad informática en el lugar de trabajo.

Sugerencias para mejorar la concientización sobre Phishing:

Los participantes ofrecieron una variedad de sugerencias para mejorar la concientización sobre Phishing, que incluían sesiones de capacitación más frecuentes, ejercicios prácticos de Phishing simulado y campañas de sensibilización en curso.

Algunos sugirieron la implementación de programas de recompensas o reconocimientos para empleados que demuestren un buen conocimiento y prácticas de seguridad informática.

Varios participantes expresan la necesidad de una comunicación clara y regular sobre las amenazas de seguridad informática y las mejores prácticas para mitigarlas.

3.1.3 DESARROLLO DEL TRÍPTICO

Dado el análisis de los conceptos clave y las técnicas de Phishing desarrolladas en el Capítulo 2, se recopiló información para definir una guía simplificada pero concisa sobre el Phishing, destinada a educar a los usuarios sobre cómo identificar y prevenir estos ataques. Esta guía se presenta bajo el eslogan "¡PROTEGE TU IDENTIDAD DIGITAL!" y está diseñada para ser accesible y práctica, facilitando la comprensión de los riesgos y las medidas de seguridad necesarias.

El tríptico interior se subdivide en tres partes (Ver Anexo 6):

- ¿Qué es el Phishing?
  En esta sección se colocó información relevante sobre el Phishing y ejemplos más comunes y los medios en los cuales se pueden presentar.
- ¿Cómo detectar un intento de Phishing?
  En esta sección se colocó consejos puntuales y una breve descripción.
- ¿Qué hacer si encuentras un intento de Phishing?
  En esta última sección se colocó las recomendaciones si el usuario detecta un intento de Phishing.

El tríptico exterior (Ver Anexo 7) contiene el eslogan, al igual que una sugerencia de mantenerse al día respecto a los temas de ciberseguridad. Además, se muestra información de contacto cómo el logo de la Universidad, y un código QR (Ver Anexo 8) que es un enlace a la página web que forma parte de este estudio.

3.1.4 DESARROLLO DE LAS PRUEBAS DE PHISHING

Para la parte de la página web se inició sobre el análisis de las herramientas respecto al Phishing que tenemos en la plataforma Kali Linux, con el fin de mostrar a los usuarios la facilidad de poder caer en este engaño, y poder puntualizar los consejos para detectarlos.

A continuación, se detallan los pasos que se realizaron en la parte práctica:

Se descargó el sistema operativo del portal web oficial (Ilustración 8).

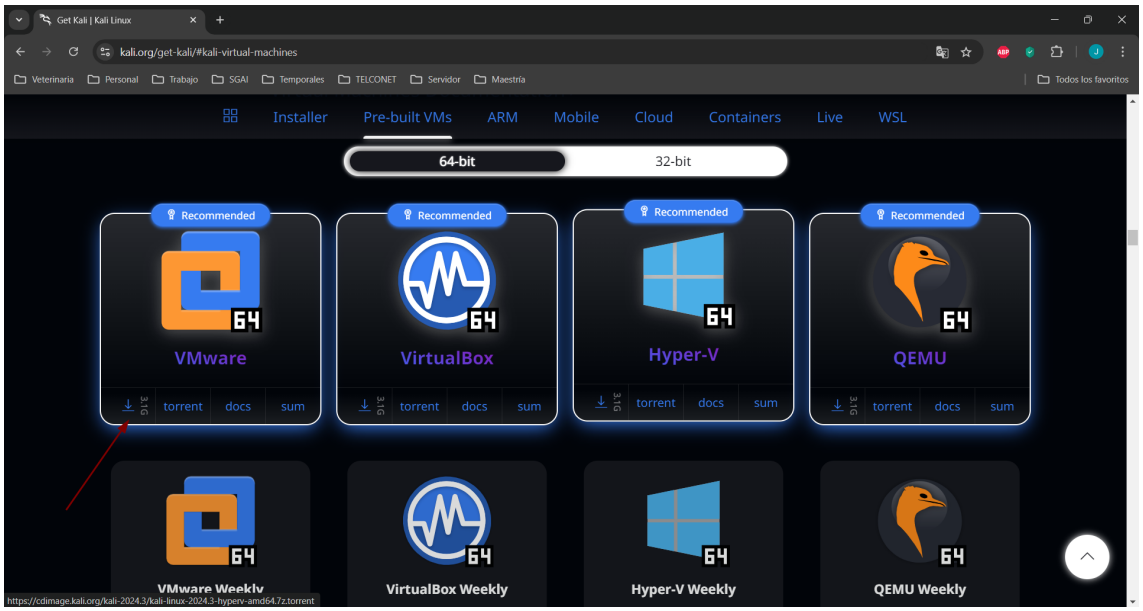

Ilustración 8: Portal web de Kali Linux

Se procedió a abrir el programa VMware Workstation, luego se dio clic en Open a Virtual Machine (Ilustración 9).

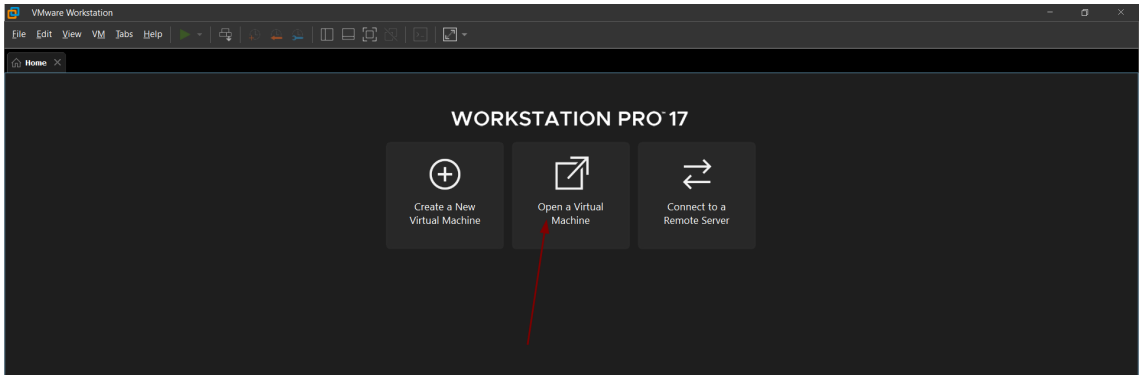

Ilustración 9: VMware Workstation

Se mostrará una ventana donde debemos seleccionar el sistema operativo descargado, posteriormente se dio clic en el botón Abrir (Ilustración 10).

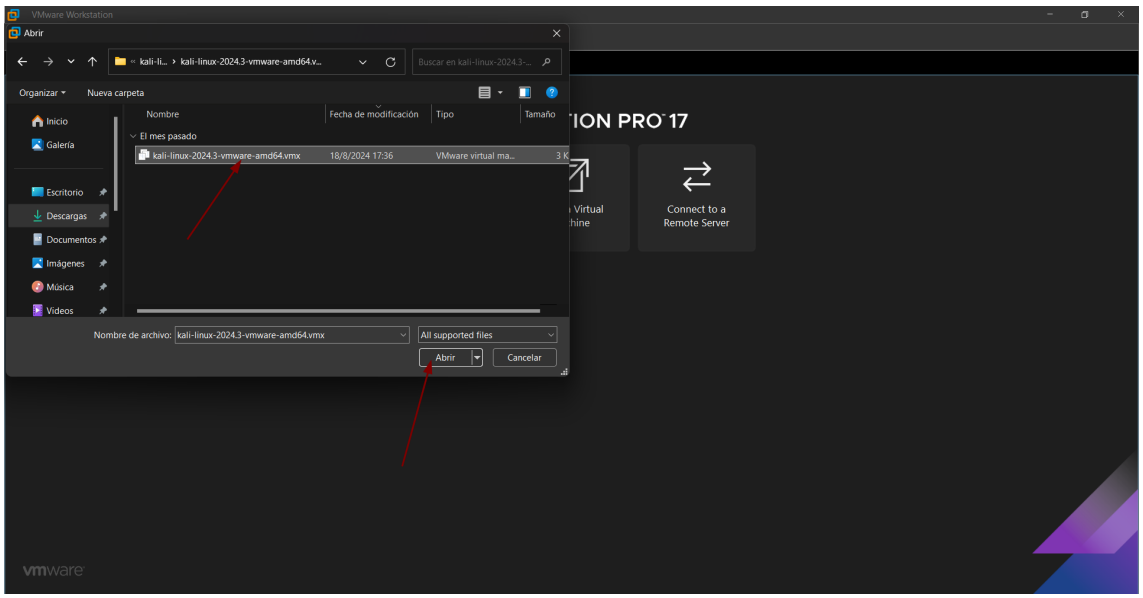

Ilustración 10: Selección de sistema operativo

Se procede a encender la máquina virtual, dando clic en la opción Power on this virtual machine (Ilustración 11).

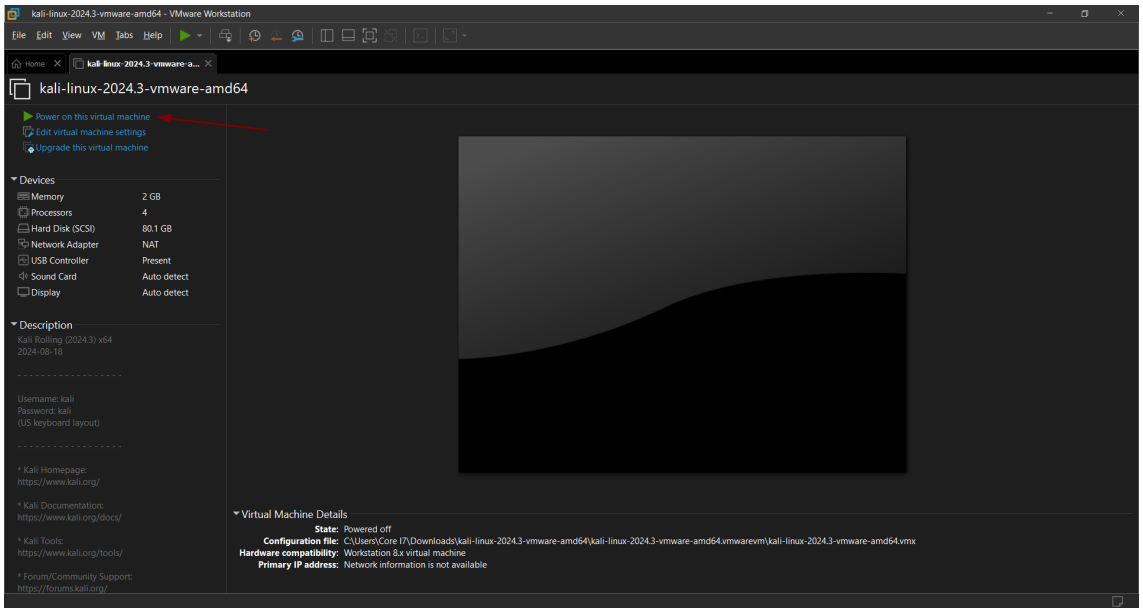

Ilustración 11: Encender máquina virtual

Una vez iniciado el sistema operativo se deja seleccionado la opción por defecto (Ilustración 12).

Ilustración 12: Sistema Operativo Kali Linux

Para iniciar sesión se usan las credenciales por defecto, *kali* en ambos (Ilustración 13).

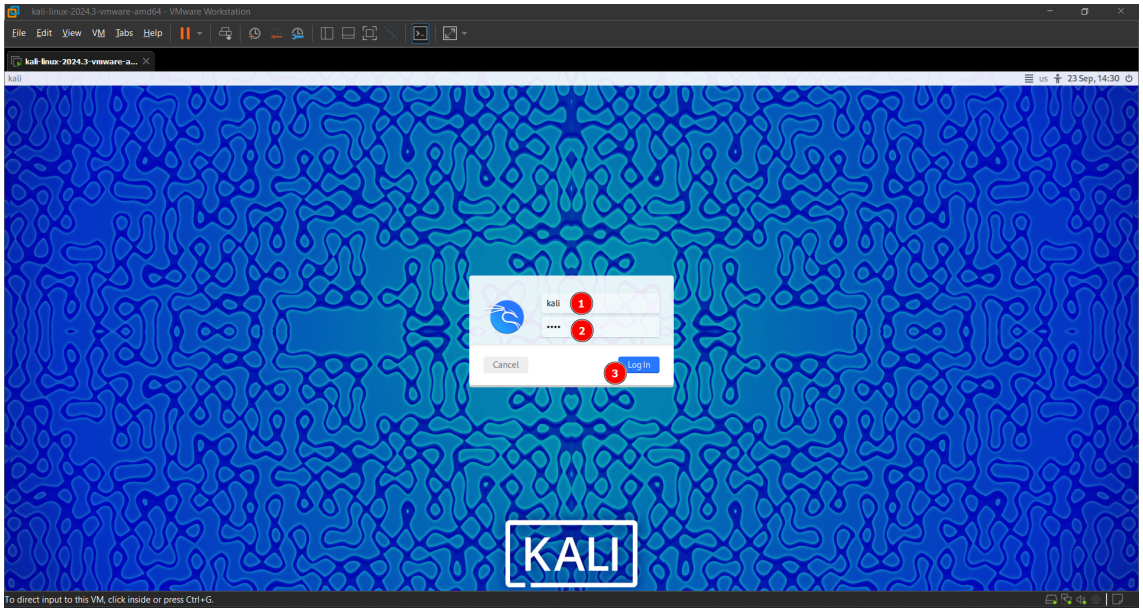

Ilustración 13: Inicio de sesión Kali Linux

En el sistema operativo, se procede a abrir un terminal (Ilustración 14).

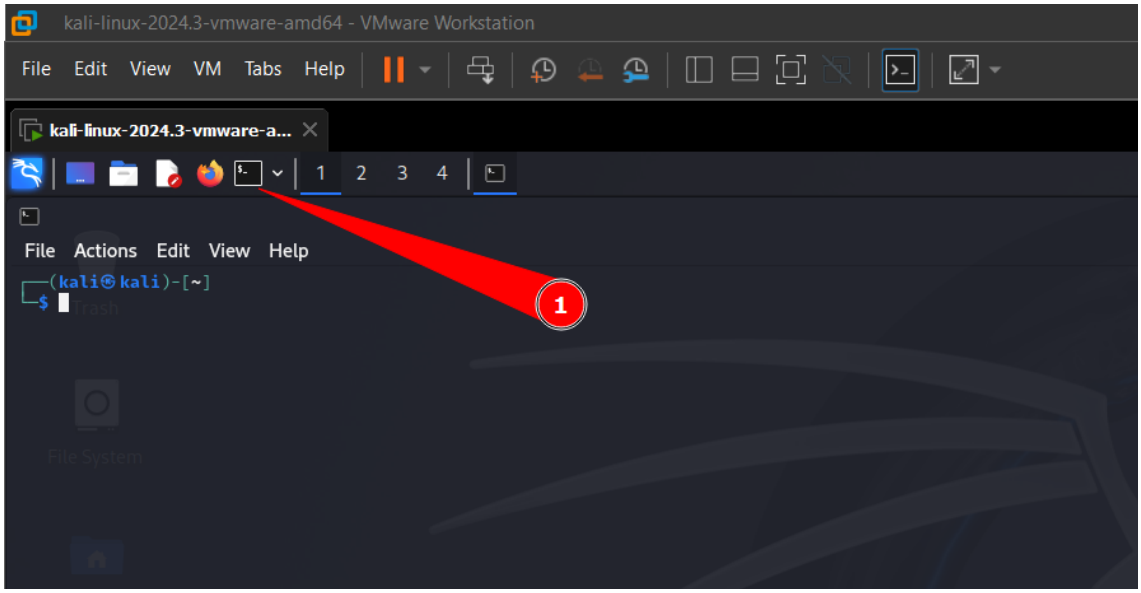

Ilustración 14: Terminal de Kali Linux

Se procede a poner rol de super usuario, con el comando *sudo su*, se debe colocar la misma contraseña con la que se inició sesión *kali*, finalmente se inicia el SET con el comando *setoolkit* (Ilustración 15).

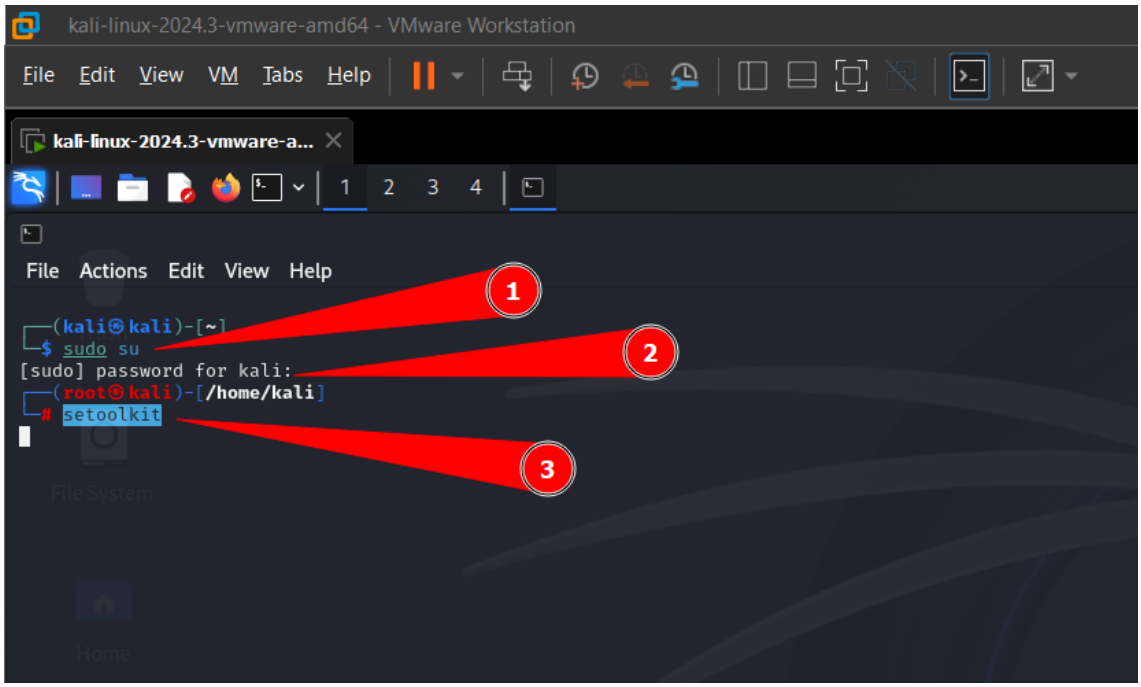

Ilustración 15: Iniciar SET

Se aceptan los términos de uso del servicio (Ilustración 16).

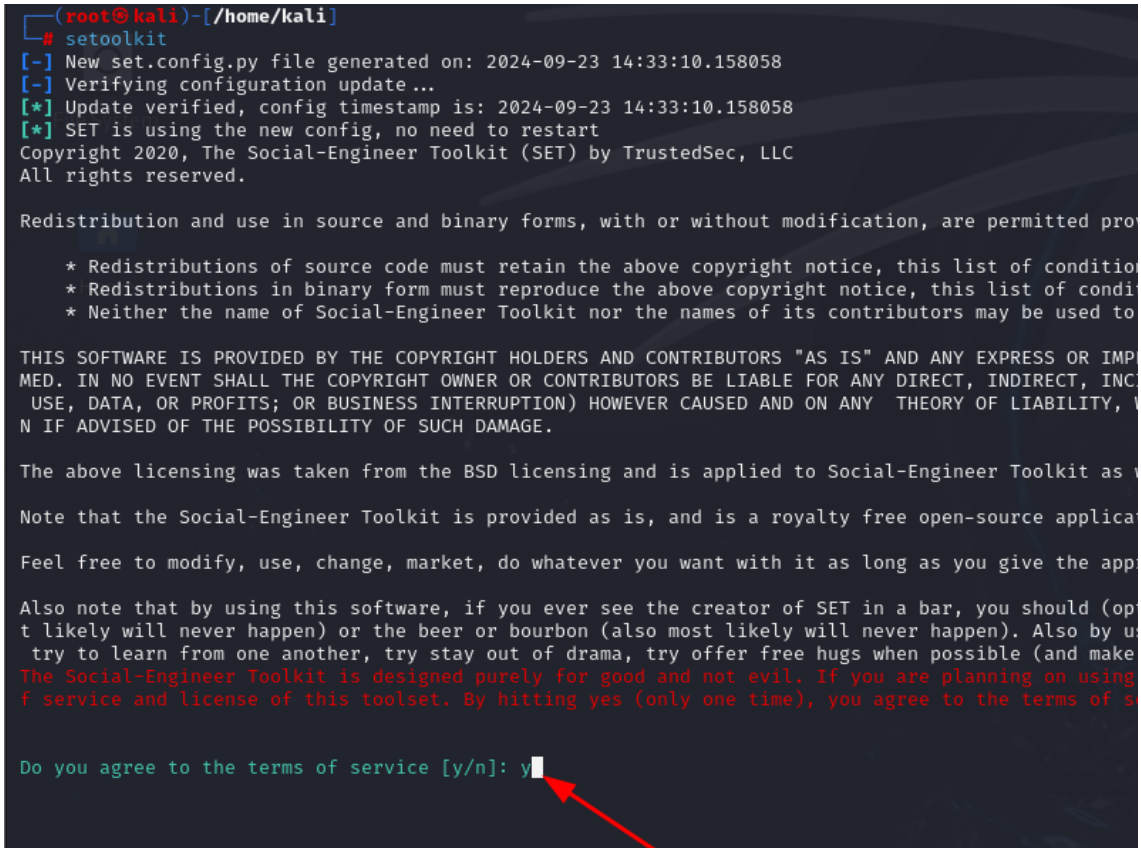

Ilustración 16: Términos de uso del servicio SET

Ahora se pueden ver las diferentes opciones (Ilustración 17) que ofrece la herramienta, pero la que se ocupará es: Ataques de ingeniería social. Para aquello se digita la opción 1.

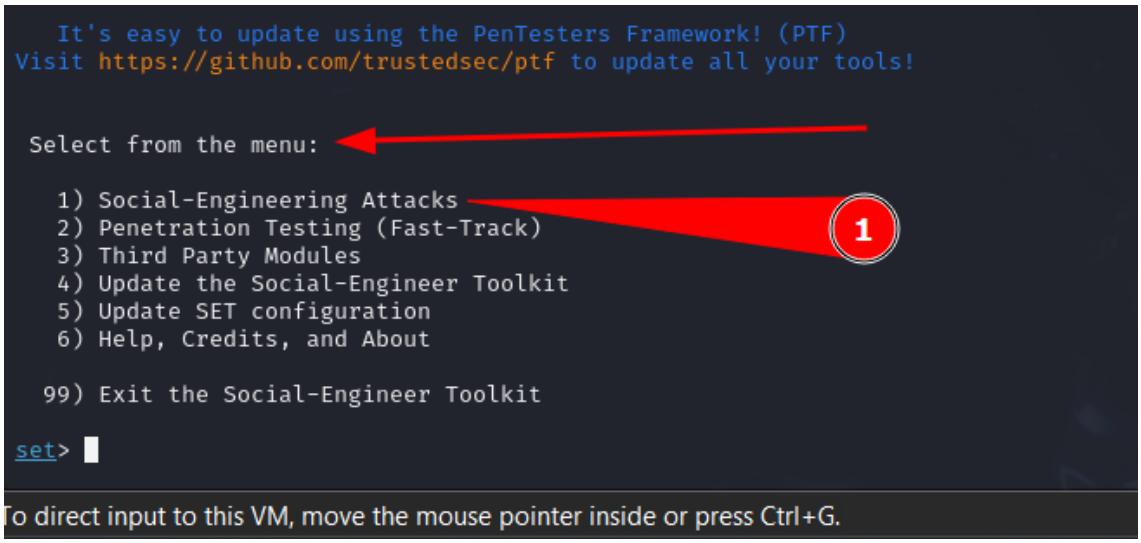

Ilustración 17: Opciones del menú SET

Una vez accedido se pueden visualizar las demás opciones (Ilustración 18), en este caso se seleccionará: Vector de ataque a sitios web. Para aquello se digitará la opción 2.

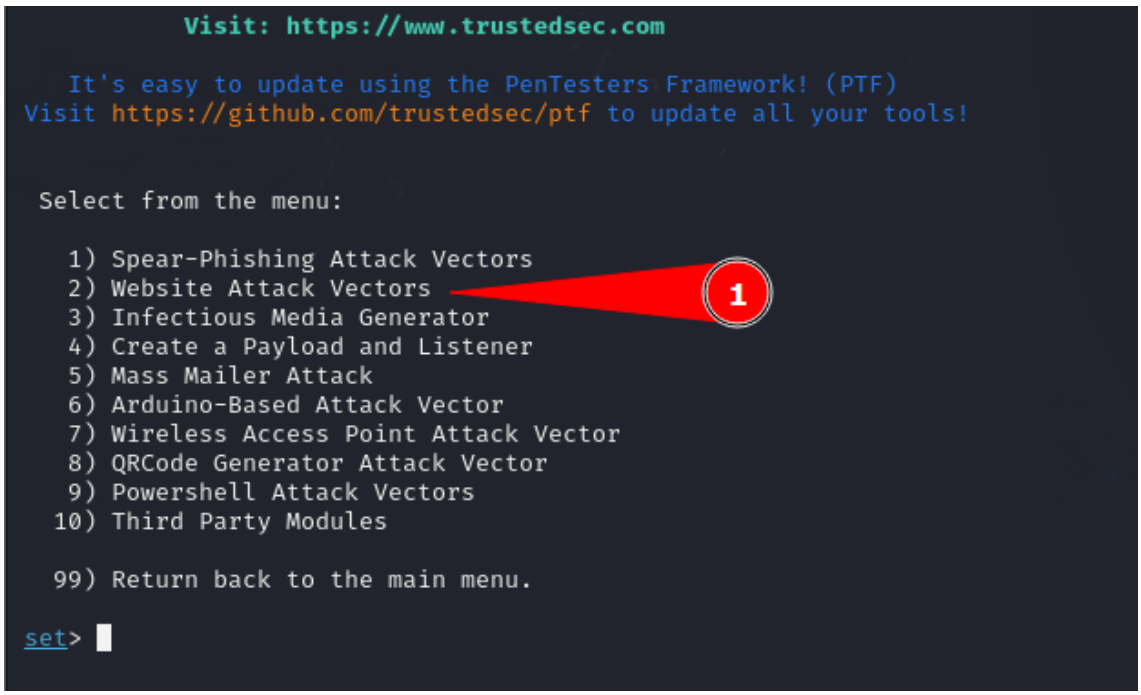

Ilustración 18: Opciones de menú de ataques de ingeniería social

De igual manera se muestran más opciones (Ilustración 19), el que nos interesa es: Método de ataque de recolección de credenciales. Para aquello se digita la opción 3.

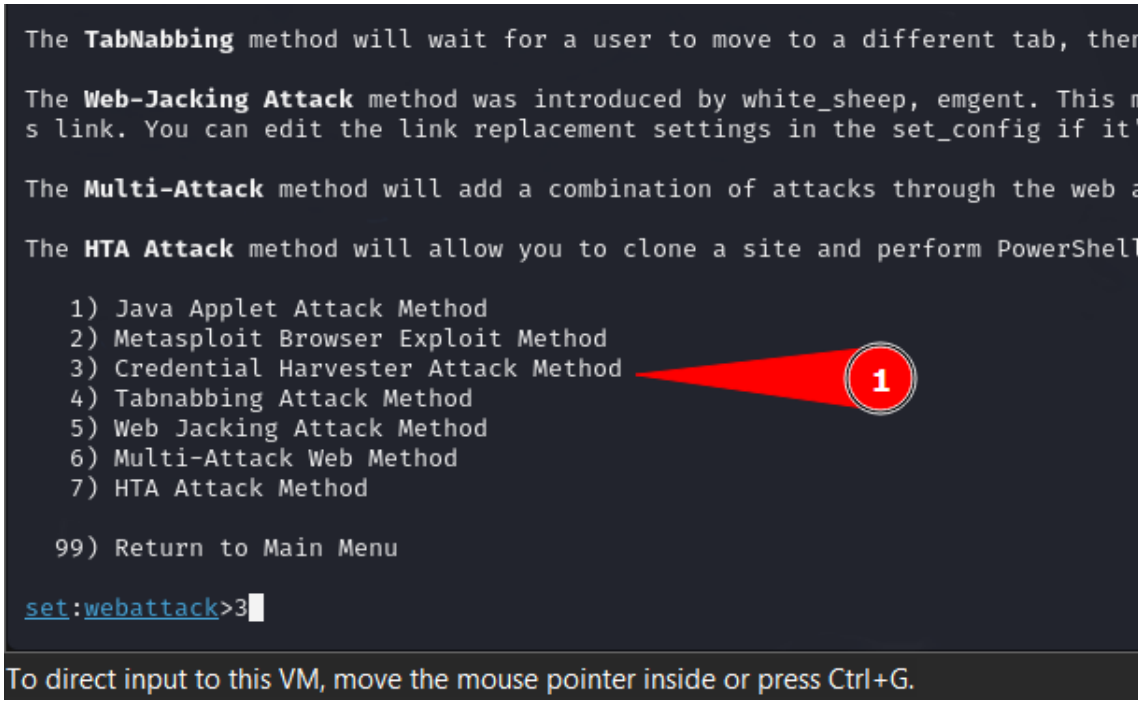

Ilustración 19: Opciones de menú de vector de ataque a sitios web

Ahora se selecciona la opción de clonador de sitios (Ilustración 20). Para aquello se digita la opción 2.

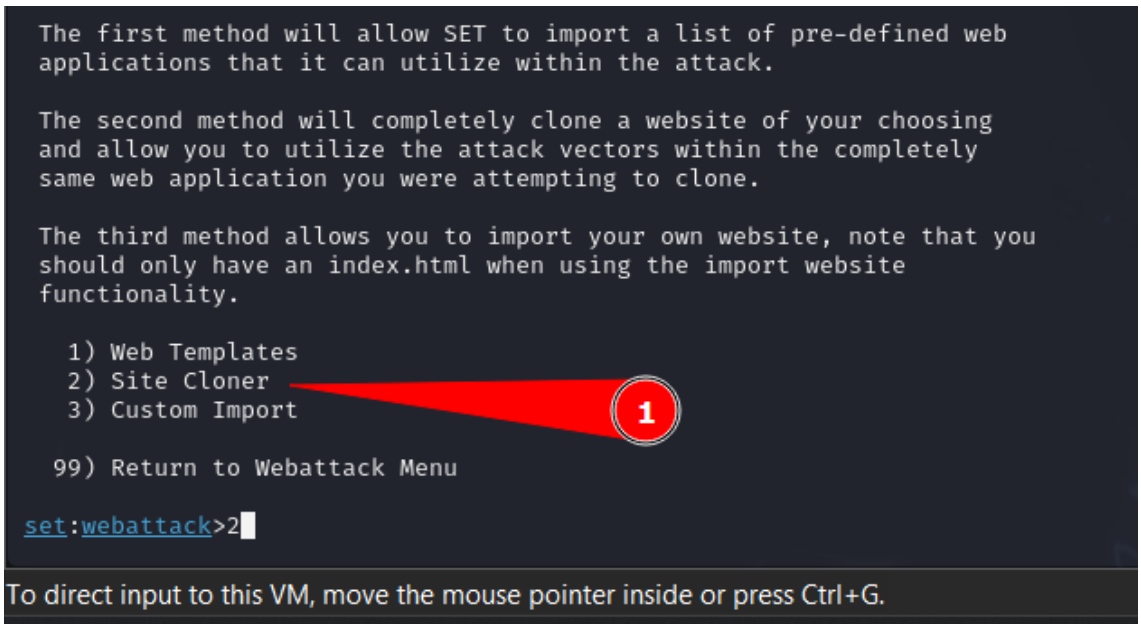

Ilustración 20: Opciones de menú de método de ataque de recolección de credenciales

Primero se dejará la opción por defecto, luego se debe ingresar la dirección del sitio web, para este caso se usará Facebook[1], pero el atacante podría colocar páginas como entidades bancarias, redes sociales, lugares del trabajo, páginas del gobierno, sitios de interés del atacante, finalmente se observa que se clona la dirección de donde se receptan las credenciales (Ilustración 21).

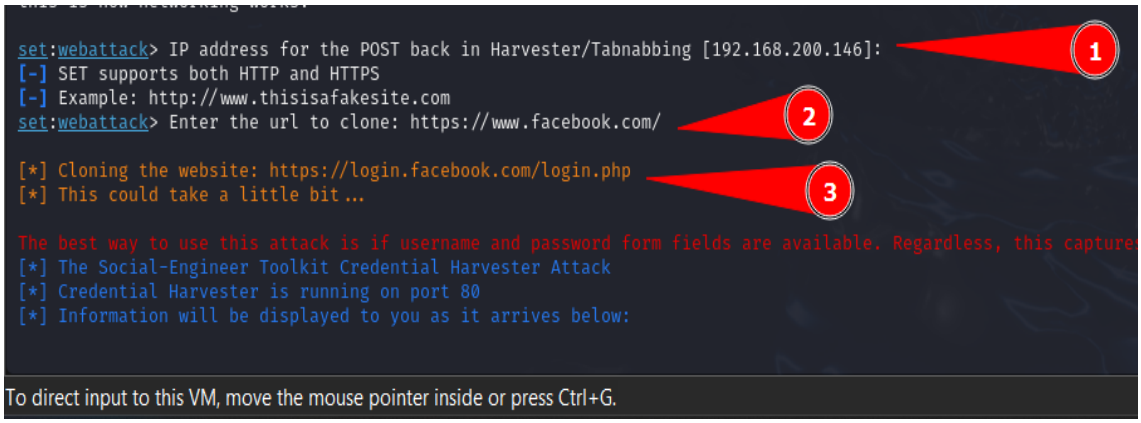

Ilustración 21: Clonación de página

[1] https://www.facebook.com/

En este punto el atacante puede contar con una dirección pública y mediante algún servidor de DNS puede intentar replicar la dirección del sitio web original. También, se puede ocultar el nombre o dirección del sitio clonado mediante acortadores de direcciones web para intentar despistar al usuario (Ilustración 22).

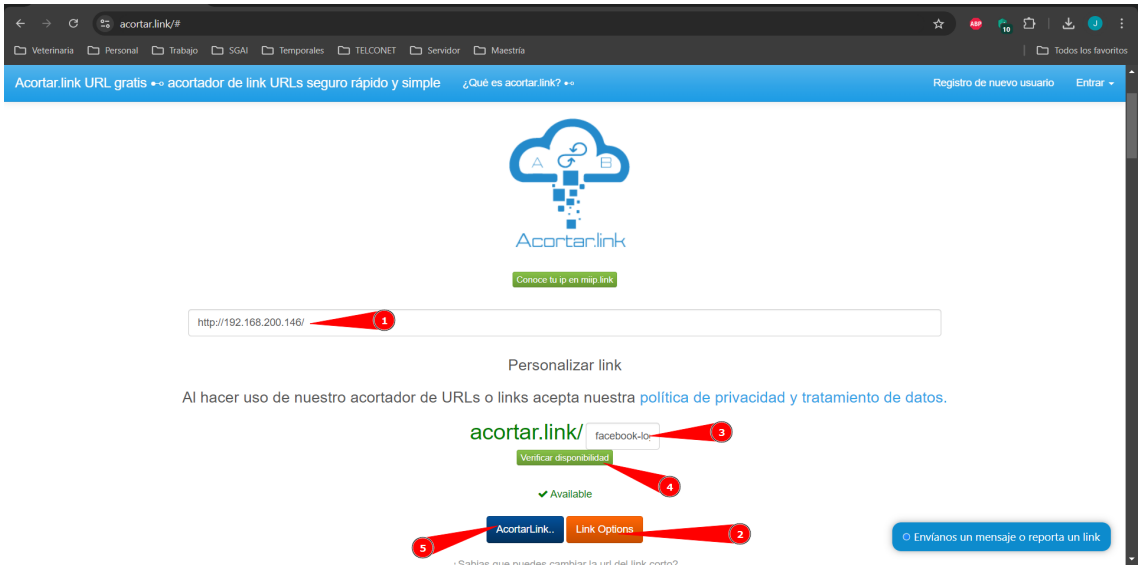

Ilustración 22: Acortador de enlaces

Una vez generado la dirección[2] mediante el acortador que intente despistar a la víctima del atacante, entra la parte de la ingeniería psicológica que es contactar por cualquier medio a la víctima y que acceda a la dirección web (Ilustración 23).

Ilustración 23: Enlace generado

[2] https://acortar.link/facebook-log-real

En la siguiente ilustración, se puede observar un ejemplo en un ambiente controlado de intento de Phishing mediante la aplicación de WhatsApp, por el desconocimiento de la mayoría de las personas y por el temor a perder la cuenta, puede acceder al enlace para verificar que ocurre (Ilustración 24).

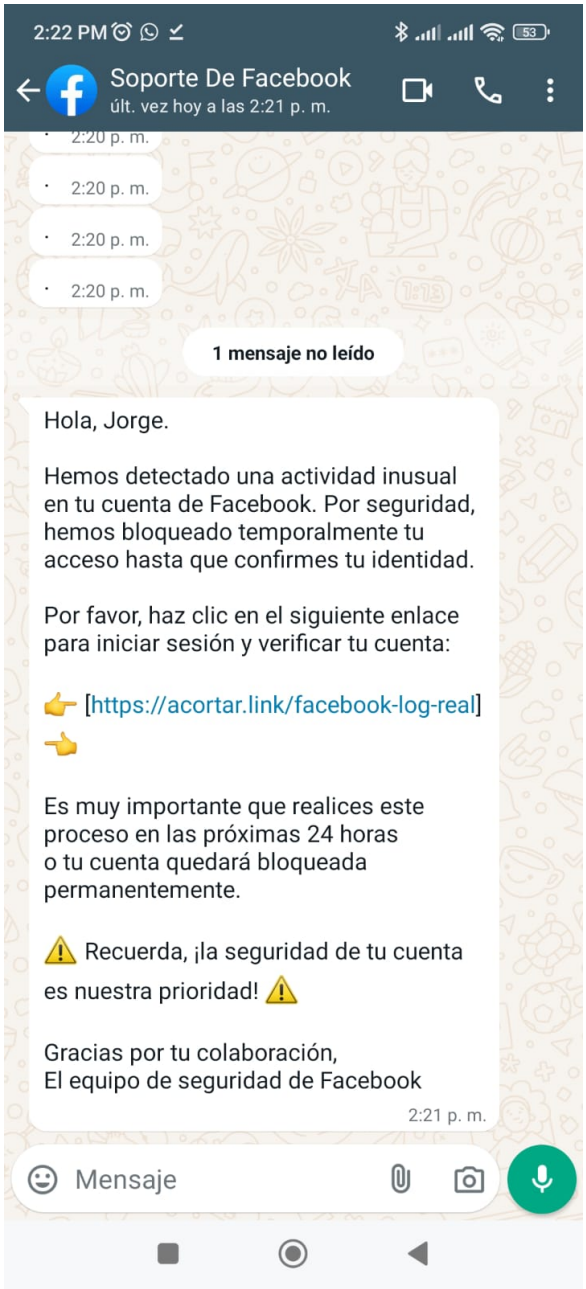

Ilustración 24: Ejemplo de ingeniería social con Phishing

El usuario por falta de conocimiento de temas de ciberseguridad accedería al enlace, la mayoría de los usuarios no se percata de la dirección original de la página (Ilustración 25), cómo se mencionó anteriormente si se cuenta con un dominio o un DNS dinámico.

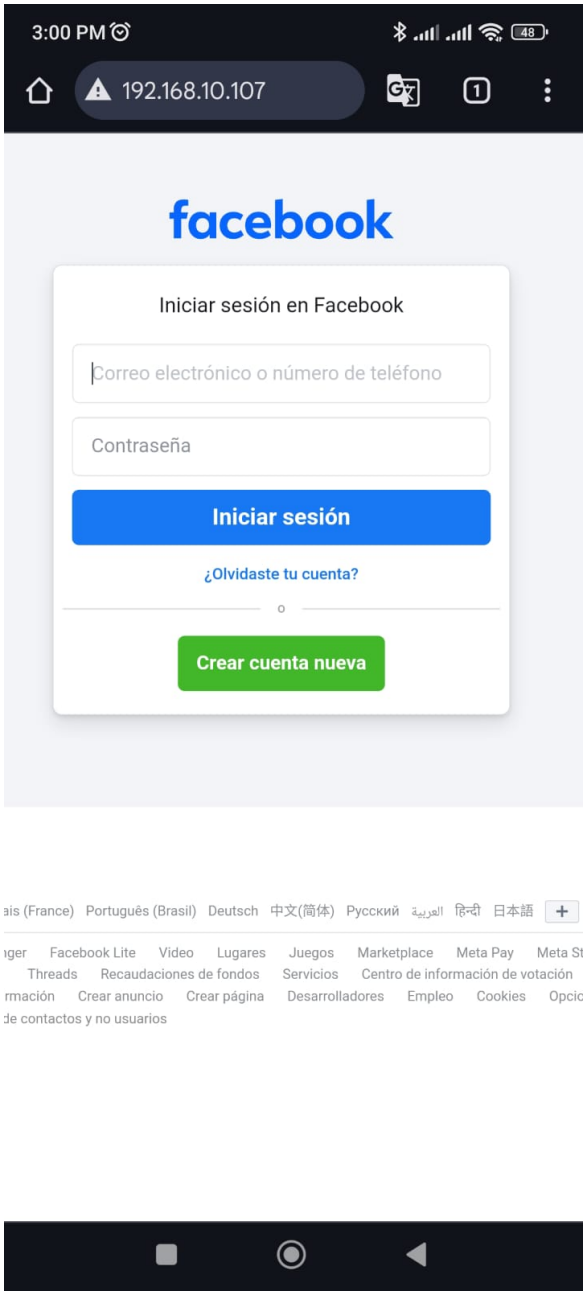

Ilustración 25: Sitio web clonado

El usuario digitará sus credenciales (Ilustración 26).

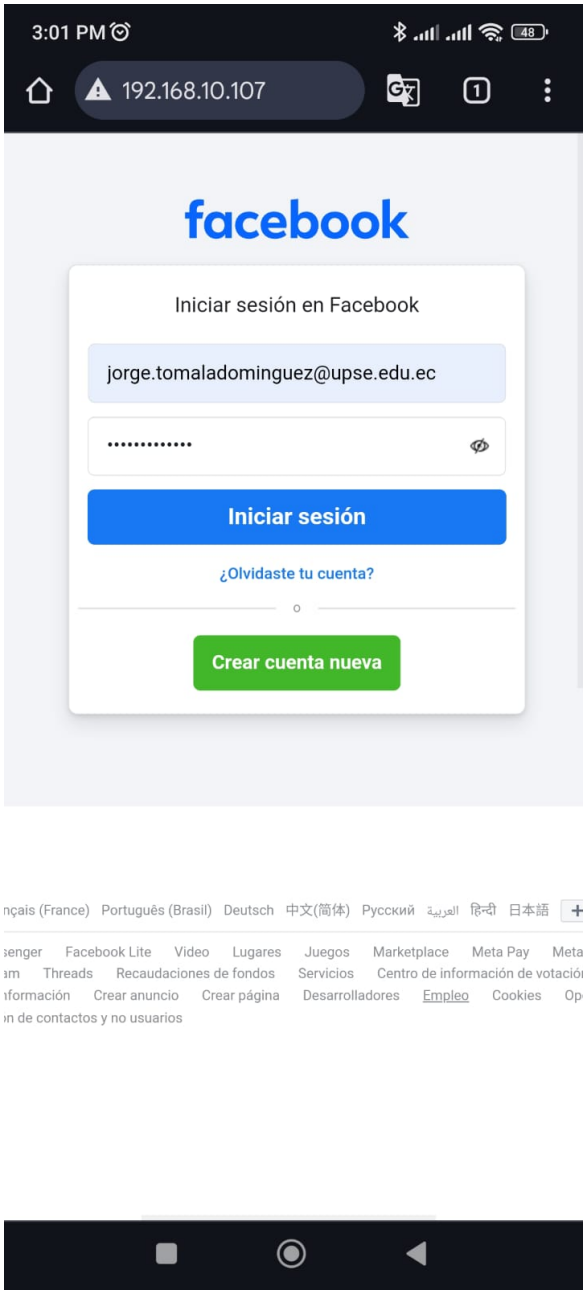

Ilustración 26: Recepción de credenciales en sitio web clonado

Una vez capturado las credenciales automáticamente se redirige el usuario al sitio oficial de la página clonada (Ilustración 27), de esa forma el usuario asumirá que se confundió en sus credenciales.

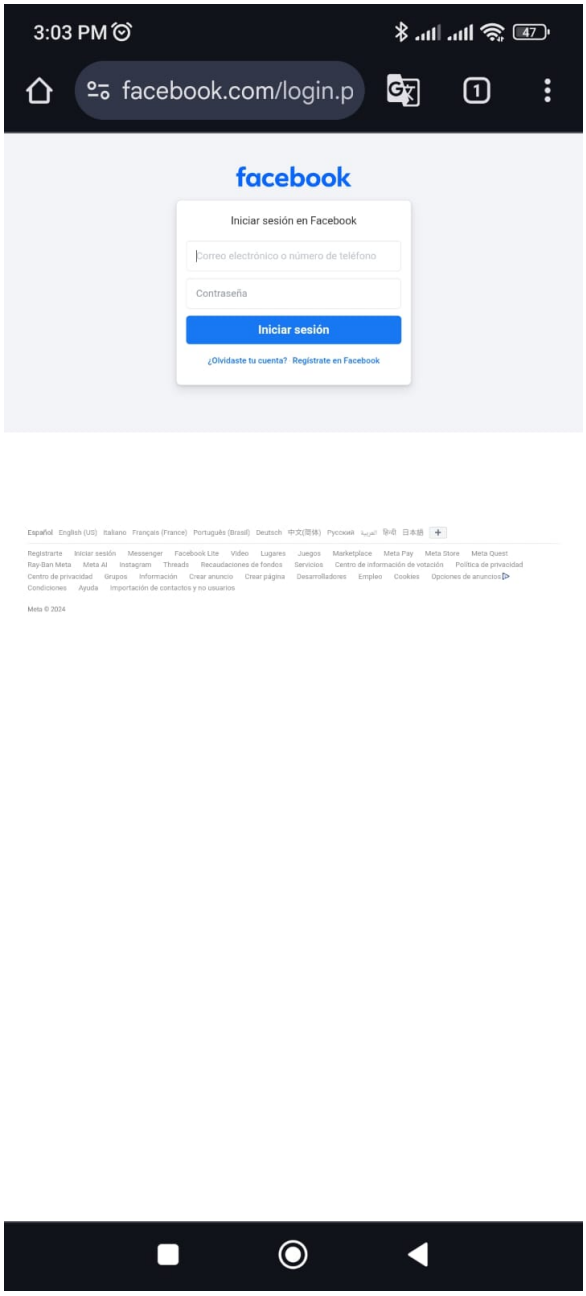

Ilustración 27: Redirección al sitio oficial

Mediante la herramienta de SET el atacante podrá capturar las credenciales, en este caso podemos visualizar que capturó el correo y la contraseña ingresada en el ambiente controlado (Ilustración 28).

Ilustración 28: SET, captura de credenciales

3.1.5 DESARROLLO DE LA PÁGINA INFORMATIVA

Para la parte de la página informativa se dividirá en tres secciones:

- Información: Contiene datos de concepto sobre el Phishing (Ilustración 29, Ilustración 30)
- Ejemplos o Guías: Contiene ejemplos prácticos de como detectar Phishing.
- Recomendaciones: Contiene consejos para mantenerse seguros y de cómo manipular el Phishing en caso de detectarlo (Ilustración 31).

Ilustración 29: Página informativa

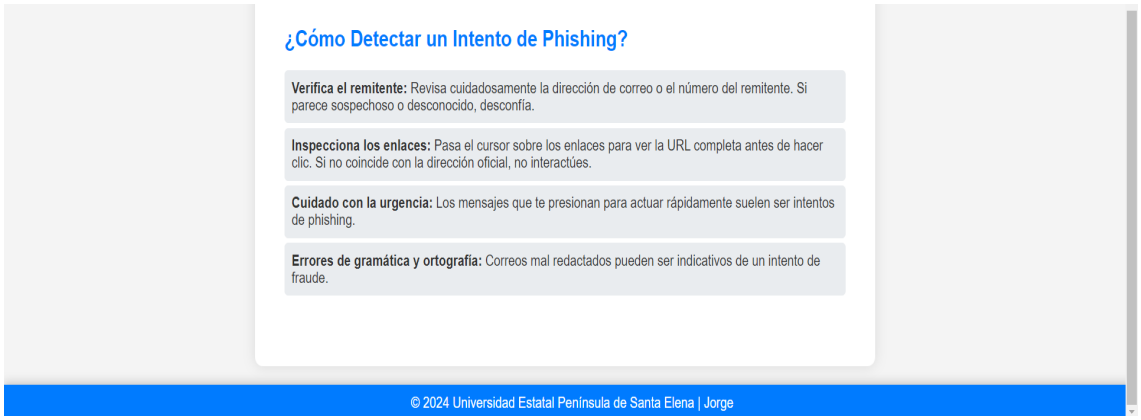

Ilustración 30: Página informativa

Ilustración 31: Página informativa, sección recomendaciones

A continuación, se muestra un ejemplo de Smishing (Ilustración 32). Consejo: Al tener un mensaje debemos fijarnos en el remitente, generalmente los primeros dígitos nos indican el país del número telefónico, de igual manera debemos fijarnos en el texto generalmente los Phishing nos piden información y tratar de hacer presión mediante acciones que no serían positivas para el usuario, tales como: bloquear la cuenta, perder un paquete, etc.

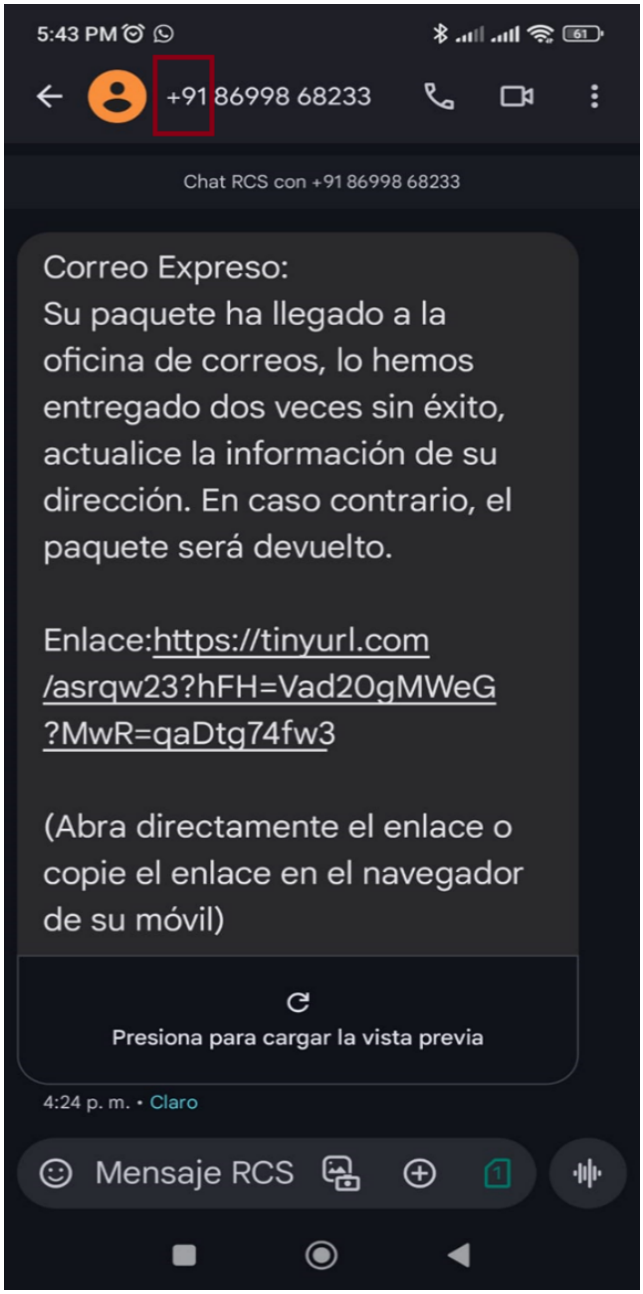

Ilustración 32: Ejemplo de Smishing

Se puede utilizar la siguiente herramienta de la página web de Truecaller[3] para colocar el número del remitente y saber de qué país proviene (Ilustración 33). Está herramienta es útil ya que permite reportar cómo spam el número telefónico.

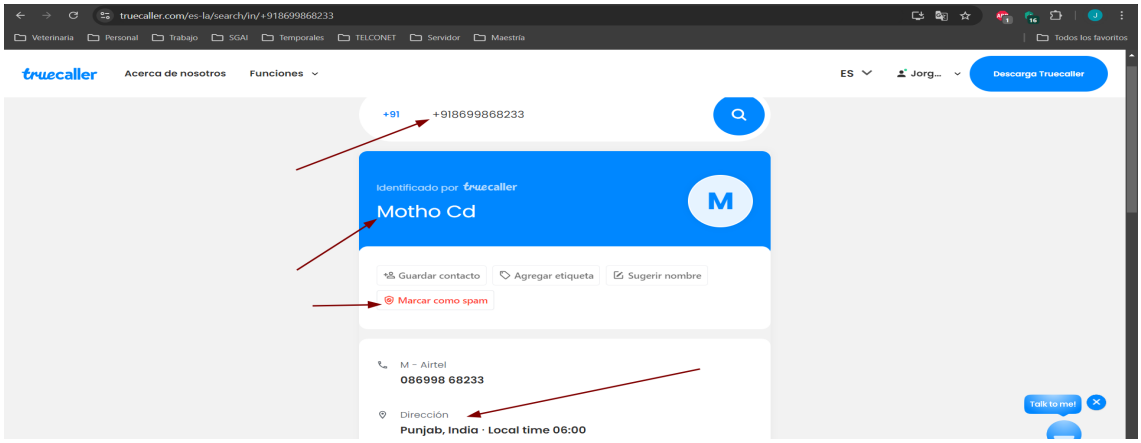

Ilustración 33: Ejemplo de uso Truecaller

Cómo se observa, el mensaje también contiene un enlace, se debe evitar abrir el enlace, o en caso se haya abierto por error, cerrarlo y no ingresar ningún tipo de información. Se puede copiar el enlace y usar otra herramienta web para analizar direcciones web de Phishing, en esta ocasión será la de VirusTotal[4], se coloca el enlace y se espera que termine el análisis (Ilustración 34).

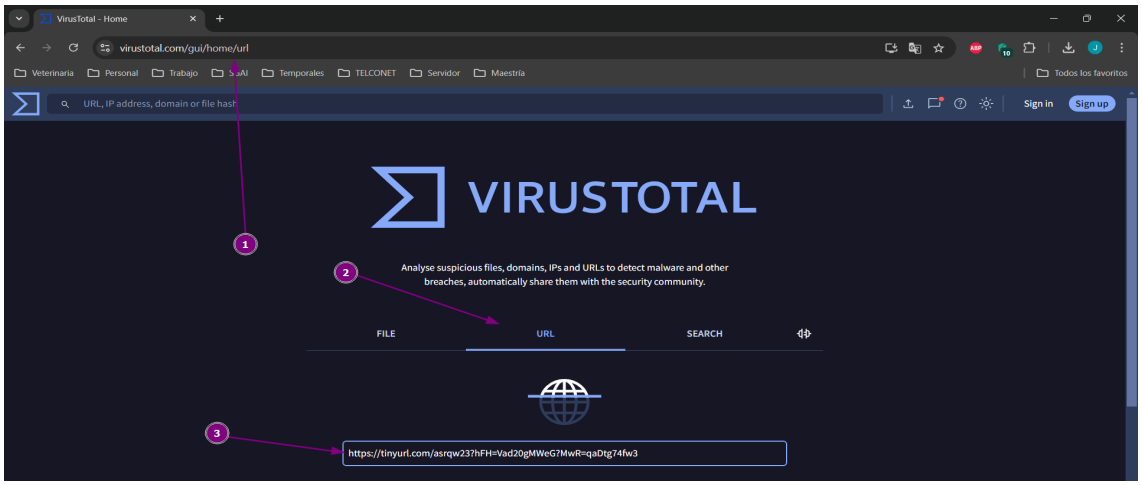

Ilustración 34: Ejemplo de uso VirusTotal

[3] https://www.truecaller.com/es-la

[4] https://www.virustotal.com/gui/home/url

Una vez finalizado el análisis saldrá el reporte, el cual se observa que se encuentra de color rojo y muestra que es una dirección que contiene Phishing (Ilustración 35).

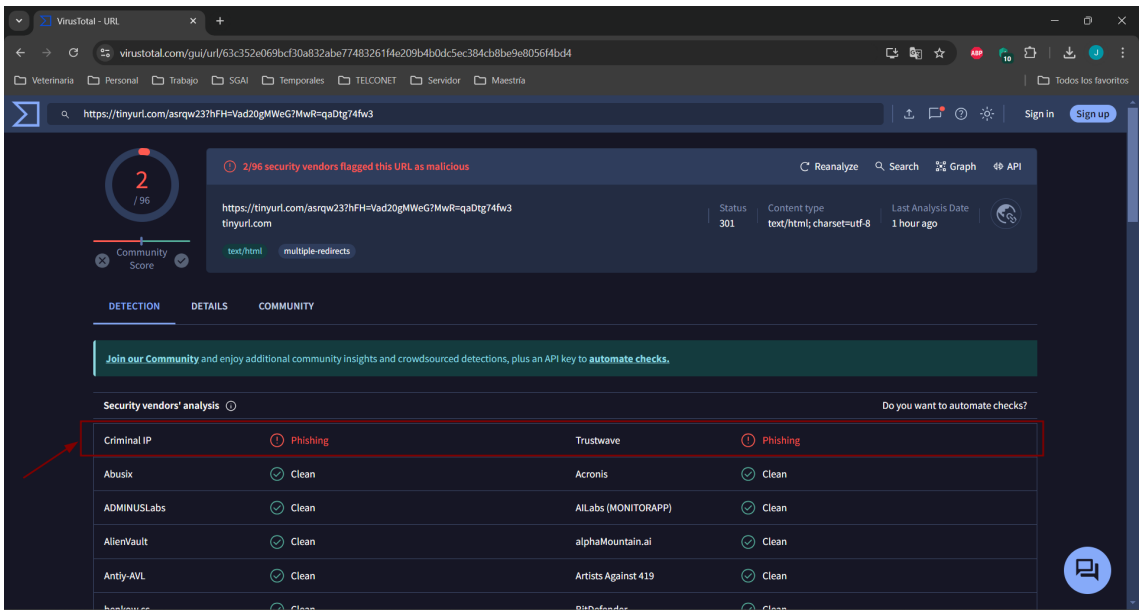

Ilustración 35: Resultado del análisis en VirusTotal

3.1.6 ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Durante las simulaciones realizadas utilizando herramientas como el Social Engineering Toolkit (SET) en un entorno controlado, se observaron los siguientes patrones:

Porcentaje inicial de usuarios vulnerables: En la primera fase de las simulaciones, el 84% de los usuarios no identificó los intentos de Phishing, principalmente debido a la falta de atención a los enlaces acortados y la apariencia convincente de los sitios clonados.

Cambios tras la capacitación: Después de implementar las estrategias educativas, este porcentaje disminuyó significativamente al 4%. Esto evidencia un aumento en la capacidad de los usuarios para identificar amenazas, validando la efectividad de las estrategias propuestas.

Los resultados obtenidos respaldan lo señalado por Buckley et al. (2023), quienes destacan que la capacitación y la conciencia sobre los signos de Phishing son determinantes para reducir la vulnerabilidad.

Se realizaron encuestas a los usuarios antes y después de la capacitación para medir su percepción y habilidades frente al Phishing. Los datos incluyen:

Capacidad de identificación inicial:

Solo el 30% de los encuestados indicó sentirse seguro al identificar mensajes de Phishing antes de recibir capacitación.

Un 50% expresó incertidumbre respecto a su capacidad para evaluar mensajes sospechosos.

Resultados tras la capacitación:

El 76% de los usuarios afirmó poder identificar con confianza los intentos de Phishing tras la intervención educativa.

Además, el 90% manifestó interés en participar regularmente en programas de concientización.

Estos datos corroboran los hallazgos de Prümmer et al. (2024), quienes señalan que las simulaciones prácticas y la capacitación continua son herramientas efectivas para reforzar la conciencia y la seguridad cibernética en los usuarios.

A partir de los resultados obtenidos, se pueden identificar los siguientes aspectos clave:

Fortalezas de las estrategias implementadas:

- La combinación de simulaciones prácticas con materiales educativos logró un impacto positivo y tangible en la reducción de la vulnerabilidad de los usuarios frente al Phishing.
- La alta participación en los programas de capacitación sugiere una aceptación y compromiso de los usuarios para mejorar su seguridad cibernética.

Áreas de mejora:

- Es necesario abordar la falta de familiaridad de algunos usuarios con las herramientas de análisis de enlaces y dominios sospechosos.
- Ampliar el alcance del programa para incluir a usuarios con menor experiencia tecnológica, quienes mostraron mayor vulnerabilidad en los resultados iniciales.

CONCLUSIONES

Este estudio abarca una exploración detallada de las tácticas de Phishing y las técnicas de ingeniería social, subrayando la creciente sofisticación y prevalencia de estos ataques en el ámbito digital.

A lo largo del estudio, se demuestra que la educación y la capacitación continua son fundamentales. Los usuarios equipados con el conocimiento adecuado y las herramientas necesarias, como se propone en la campaña de concientización y los talleres de formación, muestran una capacidad significativamente mayor para identificar y manejar mensajes de Phishing y otros engaños.

Se encuentra que los participantes que se involucran regularmente en programas de concientización no solo mejoran su capacidad para detectar intentos fraudulentos, sino que también desarrollan mejores prácticas de seguridad digital, como verificar la autenticidad de los mensajes y utilizar software de seguridad actualizado.

Las estrategias implementadas y evaluadas en este estudio ilustran claramente la efectividad de la educación y capacitación proactiva en la reducción de la susceptibilidad al Phishing. Esta relación causal no solo respalda la idea de que el conocimiento es poder en el contexto de la ciberseguridad, sino que también proporciona un marco replicable para otras organizaciones y comunidades que buscan mitigar los riesgos asociados con los ataques cibernéticos.

Se recomienda la continuidad de los esfuerzos de concientización y la adaptación de los programas de capacitación para incluir las últimas tendencias y técnicas de Phishing, asegurando que las defensas de los usuarios evolucionen a la par de las tácticas empleadas por los ciberdelincuentes. Asimismo, es crucial fomentar una cultura de seguridad que priorice la vigilancia y la educación continua como pilares de la ciberseguridad en todas las esferas de interacción digital.

RECOMENDACIONES

- Establecer sesiones regulares de capacitación en seguridad informática, enfocándose en las tácticas de Phishing más comunes y las herramientas para identificarlas, se sugiere utilizar simulaciones prácticas y dinámicas interactivas para reforzar los conocimientos adquiridos.
- Crear y distribuir materiales educativos, como trípticos informativos, videos tutoriales y guías prácticas, que expliquen de manera clara y concisa cómo reconocer y prevenir ataques de Phishing.
- Actualizar y reforzar las políticas de seguridad en instituciones públicas y privadas, incluyendo procedimientos específicos para la gestión de mensajes sospechosos y la implementación de protocolos de respuesta rápida.
- Promover el uso de software especializado para analizar enlaces sospechosos y herramientas de seguridad que permitan identificar posibles ataques en tiempo real.
- Establecer campañas de concientización a nivel comunitario y organizacional para sensibilizar sobre la importancia de la seguridad cibernética y las amenazas emergentes.
- Implementar un sistema de monitoreo periódico para evaluar la efectividad de las estrategias de prevención y adaptar las medidas a las tácticas emergentes de los atacantes. Realizar encuestas y simulaciones para medir el impacto de las iniciativas y determinar áreas de mejora.

REFERENCIAS

Broadcom. (2024). *VMware Workstation*. https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware%20Workstation%20Pro.

Buckley, J., Lottridge, D., Murphy, J. G., & Corballis, P. M. (2023). Indicators of employee Phishing email behaviours: Intuition, elaboration, attention, and email typology. *International Journal of Human-Computer Studies*, *172*, 102996. https://doi.org/10.1016/J.IJHCS.2023.102996

Center for Internet Security. (2024). *The 18 CIS Critical Security Controls*. https://www.cisecurity.org/controls/cis-controls-list.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of Phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/J.ESWA.2018.03.050

ENISA. (2023). *ENISA THREAT LANDSCAPE 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in Phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671. https://doi.org/10.1016/J.COSE.2023.103671

ISO/IEC. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. https://www.iso.org/es/contents/data/standard/08/28/82875.html.

Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. *Technology in Society*, *76*, 102470. https://doi.org/10.1016/J.TECHSOC.2024.102470

Liew, S. W., Sani, N. F. M., Abdullah, M. T., Yaakob, R., & Sharum, M. Y. (2019). An effective security alert mechanism for real-time Phishing tweet detection on Twitter. *Computers & Security*, *83*, 201–207. https://doi.org/10.1016/J.COSE.2019.02.004

OffSec Services Limited. (2024). *Kali Linux*. https://www.kali.org/features/.

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/J.COSE.2023.103585

Singer, P. W. (Peter W. (2014). *Cybersecurity and cyberwar : what everyone needs to know* (A. Friedman, Ed.) [Book]. Oxford University Press.

TrustedSec. (2020). *The Social-Engineer Toolkit (SET)*. https://github.com/trustedsec/social-engineer-toolkit.

ANEXOS

Anexo 1: Encuesta a los usuarios finales

¿Ha recibido alguna vez un mensaje sospechoso que podría ser un intento de Phishing?

a) Sí, con frecuencia
b) Sí, ocasionalmente
c) No estoy seguro
d) No, nunca

¿Sabe cómo identificar un mensaje de Phishing?

a) Sí, siempre puedo identificarlo
b) A veces, depende del contenido del mensaje
c) No estoy seguro
d) No, no sé cómo identificarlos

¿Ha participado en algún programa de concientización sobre seguridad informática que incluya información sobre Phishing y técnicas de ingeniería social?

a) Sí, regularmente
b) Sí, pero solo una vez
c) No, nunca he participado
d) No estoy seguro

¿Qué medidas de seguridad toma al recibir un mensaje sospechoso?

a) Lo marco como spam y bloqueo el remitente
b) Lo elimino de inmediato
c) Lo abro, pero no hago clic en ningún enlace

Lo investigo más antes de tomar alguna acción

Anexo 2: Codificación de la encuesta

Experiencia con mensajes sospechosos:

a) Sí, con frecuencia: Código 4
b) Sí, ocasionalmente: Código 3
c) No estoy seguro: Código 2
d) No, nunca: Código 1

Capacidad para identificar mensajes de Phishing:

a) Siempre puedo identificarlos: Código 4
b) A veces, depende del contenido: Código 3
c) No estoy seguro: Código 2
d) No sé cómo identificarlos: Código 1

Participación en programas de concientización sobre seguridad informática:

a) Regularmente: Código 4
b) Solo una vez: Código 3
c) Nunca he participado: Código 2
d) No estoy seguro: Código 1

Medidas de seguridad al recibir un mensaje sospechoso:

a) Marco como spam y bloqueo el remitente: Código 4
b) Elimino de inmediato: Código 3
c) Abro, pero no hago clic en enlaces: Código 2
d) Investigar más antes de tomar acción: Código 1

Anexo 3: Datos Pre-Capacitación

Experiencia con mensajes sospechosos:

a) Sí, con frecuencia: (3 personas)
b) Sí, ocasionalmente: (5 personas)
c) No estoy seguro: (25 personas)
d) No, nunca: (17 personas)

Capacidad para identificar mensajes de Phishing:

a) Sí, siempre puedo identificarlo: (3 personas)
b) A veces, depende del contenido: (5 personas)
c) No estoy seguro: (10 personas)
d) No, no sé cómo identificarlos: (32 personas)

Participación en programas de concientización sobre seguridad informática:

a) Sí, regularmente: (3 personas)
b) Sí, pero solo una vez: (1 personas)
c) No, nunca he participado: (42 personas)
d) No estoy seguro: (4 personas)

Medidas de seguridad al recibir un mensaje sospechoso:

a) Lo marco como spam y bloqueo el remitente: (3 personas)
b) Lo elimino de inmediato: (2 personas)
c) Lo abro, pero no hago clic en ningún enlace: (45 personas)
d) Lo investigo más antes de tomar alguna acción: (0 personas)

Anexo 4: Datos Post-Capacitación

Experiencia con mensajes sospechosos:

e) Sí, con frecuencia: (10 personas)
f) Sí, ocasionalmente: (35 personas)
g) No estoy seguro: (2 personas)
h) No, nunca: (3 personas)

Capacidad para identificar mensajes de Phishing:

e) Sí, siempre puedo identificarlo: (38 personas)
f) A veces, depende del contenido: (10 personas)
g) No estoy seguro: (2 personas)
h) No, no sé cómo identificarlos: (0 personas)

Participación en programas de concientización sobre seguridad informática:

e) Sí, regularmente: (45 personas)
f) Sí, pero solo una vez: (5 personas)
g) No, nunca he participado: (0 personas)
h) No estoy seguro: (0 personas)

Medidas de seguridad al recibir un mensaje sospechoso:

e) Lo marco como spam y bloqueo el remitente: (38 personas)
f) Lo elimino de inmediato: (2 personas)
g) Lo abro, pero no hago clic en ningún enlace: (0 personas)
h) Lo investigo más antes de tomar alguna acción: (10 personas)

Anexo 5: Entrevista a los usuarios finales.

- ¿Has presenciado algún incidente de Phishing o ingeniería social en tu entorno laboral o personal? ¿Cómo se manejó la situación?
- ¿Qué medidas de seguridad o precauciones tomas para protegerte contra ataques de Phishing en tu vida diaria?
- ¿Has participado en algún programa de concientización sobre seguridad informática en tu lugar de trabajo o educación?
- ¿Cómo crees que podrían mejorar las organizaciones la concientización sobre Phishing entre sus empleados o miembros?

Anexo 6: Tríptico informativo, parte interior

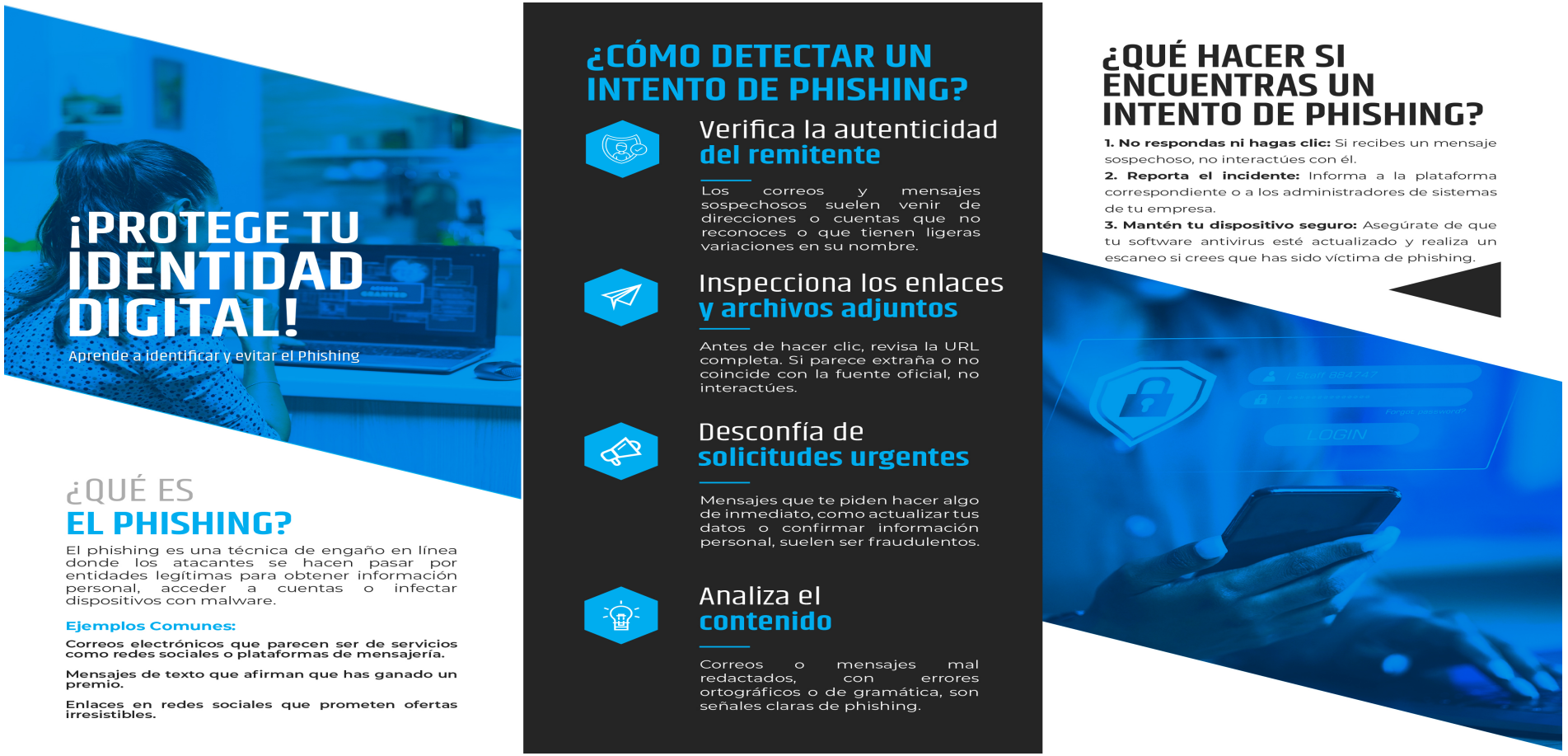

Ilustración 36: Tríptico informativo, parte interior

Anexo 7: Tríptico informativo, parte exterior.

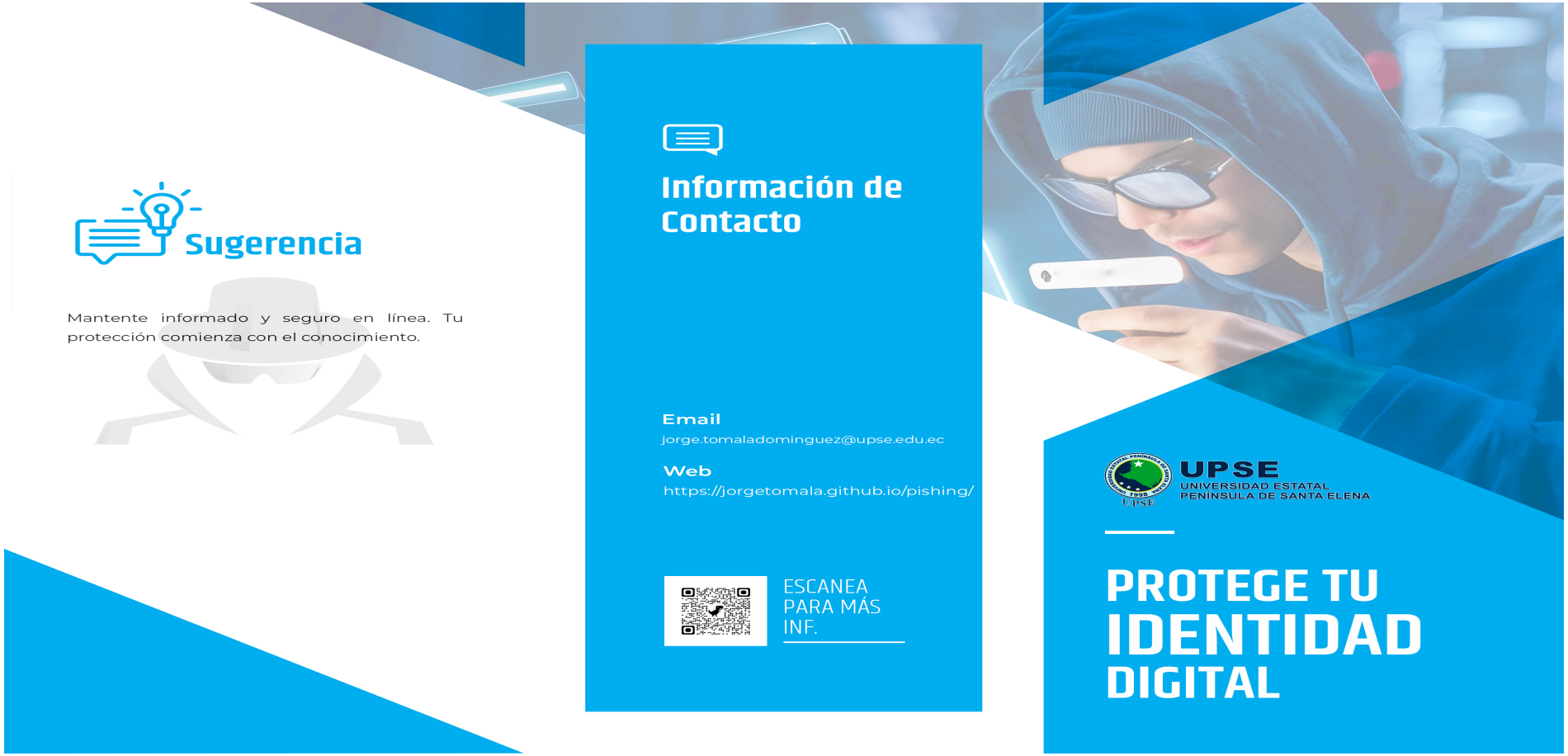

Ilustración 37: Tríptico informativo, parte exterior

Anexo 8: Código QR de la página web

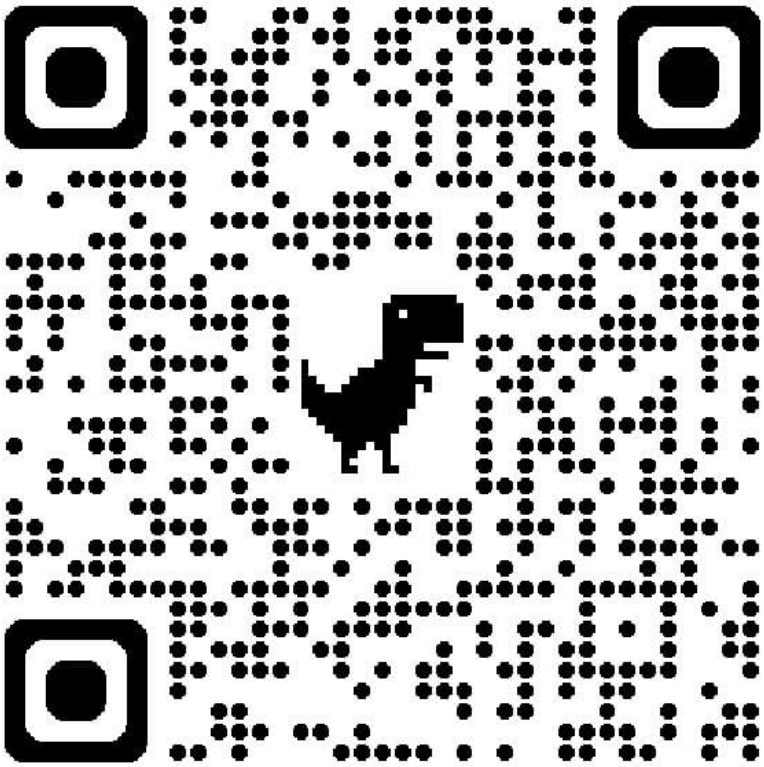

Ilustración 38: Código QR de la página informativa