Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos

Naturales No Renovables

Maestría en Telecomunicaciones

Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish.

Trabajo de Investigación previa a la obtención del título de Magíster en Telecomunicaciones.

AUTOR:

Ing. Cristian Leonardo Calderón Ordoñez

DIRECTOR:

Ing. John Tucker Yépez, Mg. Sc.

Loja – Ecuador

2023

Certificación

Loja, 19 de abril del 2023

Ing. John Jossimar Tucker Yépez, Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish,** previo a la obtención del título **de Magíster en Telecomunicaciones,** de la autoría del estudiante **Cristian Leonardo Calderón Ordoñez** , con **cédula de identidad N° 1104617053 ,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
JOHN JOSSIMAR
TUCKER YEPEZ

Ing. John Jossimar Tucker Yépez, Mg. Sc.
DIRECTOR DE TRABAJO DE INVESTIGACIÓN

Autoría

Yo, Cristian Leonardo Caderón Ordoñez, declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Cédula de Identidad: 1104617053

Fecha: 04/05/2023

Correo electrónico: clcalderono@unl.edu.ec

Teléfono: 0989150745

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.

Yo, **Cristian Leonardo Calderón Ordoñez**, declaro ser autor del Trabajo de Titulación denominado: **Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los cuatro días del mes de mayo de dos mil veintitrés.

Firma:

Cédula de identidad: 1104617053

Dirección: Carigan

Correo Electrónico: **clcalderono@unl.edu.ec**

Teléfono: 0989150745

DATOS COMPLEMENTARIOS:

Director de trabajo de investigación: Ing. John Tucker Yépez, Mg. Sc.

Dedicatoria

Le dedico el presente trabajo a Dios, a mis padres, esposa e hijas, por ser el principal motor de mi vida, siendo el pequeño universo que me impulsa a seguir adelante y a todas las personas que fueron parte de esta gran aventura

Cristian Leonardo Calderón Ordoñez

Agradecimiento

Primero agradezco a Dios y a mis padres por ser los promotores de mis sueños y apoyo durante mi carrera académica, gracias por inculcarme valores como el esfuerzo, la perseverancia y la dedicación, que me han permitido llegar hasta aquí.

A mi esposa e hijas que me brindaron su apoyo e infinita paciencia y cedieron su tiempo para que "Papá estudie" y recordarme lo lindo de una travesía caóticamente hermosa de la vida.

Al Ing. Juan Carlos Riofrío y de demás compañeros de la (DTI), por estar siempre presente, con sus orientaciones y palabras de aliento para culminar dicha investigación.

A mi tutor el Ing. John Tucker Yépez, Mg. Sc, por sus consejos, su paciencia y su motivación constante, sin los cuales este trabajo no habría sido posible y demás docentes de la Universidad, que han sido personas de gran sabiduría quienes se han esforzado por ayudarme a llegar al punto en el que me encuentro hoy.

¡¡¡Gracias totales!!!

Cristian Leonardo Calderón Ordoñez

Índice de Contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Título

Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish.

2. Resumen

El Internet a través de los años ha evolucionado, siendo esta la red más grande del mundo donde se encuentra la mayor cantidad de información, al mismo tiempo los ciberataques a sistemas informáticos también van evolucionando, valiéndose de un sinnúmero de técnicas siendo una de ellas la ingeniería social que se basa en la suplantación de identidad y engaño (Phishing), el cual pone en riesgo la información de instituciones públicas y privadas, atentando contra la confidencialidad, integridad y disponibilidad de la información. La presente investigación tiene como objetivo contribuir al mejoramiento de la seguridad informática en la Universidad Nacional de Loja, específicamente en lo que se refiere a la prevención de ataques de ingeniería social conocido como Phishing para ello será necesario implementar una campaña de simulación de un ataque de ingeniería social denominado Phishing con fines éticos, misma que está dirigida hacia el personal administrativo de la institución, se la realizará por medio de los correos institucionales de los funcionarios administrativos, haciendo uso de la herramienta GoPhish, dicha herramienta permite recrear un ambiente de simulación de ataques de ingeniería social cómo Phishing, con el objetivo de conocer su nivel de conocimiento, en cuanto a los ataques Phishing se refiere, recopilando y almacenando los resultados de la simulación pudiendo identificar la cantidad de personas que fueron víctimas de la simulación del ataque informático, cuyo resultados se darán a conocer al personal de la Dirección de Tecnología de Información (DTI), con el objetivo de que se implementen posteriores campañas sobre la prevención de ataques informáticos bajo esta modalidad, finalmente se procederá a capacitar al personal administrativo de Universidad Nacional de Loja, que fueron víctimas de la simulación del ataque Phishing, dando a conocer las causas y consecuencias a las que se exponen al ser víctimas efectivas de esta modalidad de ataque, y de esta forma se lo mantiene prevenido y alerta al funcionario para evitar el robo de información que es confidencial tanto del funcionario, como para la institución en la que se encuentra laborando.

***Palabras claves**: Phishing, Seguridad Informática, Ingeniería Social, GoPhish, Simulación, Ataque Informático.*

2.1.Abstract

Over the years, the Internet has evolved, becoming the largest network in the world, where the largest amount of information can be found. Simultaneously, cyber-attacks on computer systems are also evolving, using countless techniques, including social engineering, which is based on identity theft and deception (Phishing), which puts the information of public and private institutions at risk, threatening the confidentiality, integrity and availability of information. The objective of this research is to contribute to the improvement of information security at the Universidad Nacional de Loja, specifically regarding the prevention of social engineering attacks known as Phishing. To achieve this, it will be necessary to implement an ethical simulation campaign of a social engineering attack called Phishing, directed towards the administrative staff of the institution. This will be carried out through the institutional emails of the administrative staff, using the GoPhish tool, which allows recreating a simulation environment of social engineering attacks such as Phishing, with the aim of assessing the level of knowledge of the administrative staff regarding Phishing attacks. Results of the simulation will be collected and stored, identifying the number of people who were victims of the cyberattack simulation, which will be shared with the Technology Department (DTI) personnel. This will enable them to implement subsequent campaigns on the prevention of cyber-attacks under this modality. Finally, administrative staff at Universidad Nacional de Loja who were victims of the Phishing attack simulation will be trained, explaining the causes and consequences of being victims of this type of attack, and how to remain vigilant and prevent the theft of confidential information belonging to both the staff and the institution they work for.

Keywords: Phishing, Information Security, Social Engineering, GoPhish, Simulation, Cyber-Attack.

3. Introducción

Hoy en día el Phishing es una de las herramientas más utilizadas por los ciberdelincuentes a nivel global para el hurto de información, los ciberdelincuentes se han percatado de que es más fácil manipular a las personas que romper vulnerabilidades informáticas, las instituciones invierten en asegurar su infraestructura informática adquiriendo firmwares, sistemas de prevención de intrusos, licencias anti-malware, anti-spam etc, pero lamentablemente no le podemos poner un parche a la ingenuidad humana por tal motivo las personas seguimos siendo el eslabón más débil en la cadena de seguridad informática; a razón de ello el cibercrimen a nivel mundial ha crecido de manera astronómica, ascendiendo a los dos trillones de dólares en pérdidas económicas según Juniper Research (2019), en Latinoamérica el costo del cibercrimen ascendió a los 90,000 millones de dólares anuales, generando alrededor de 677 millones de ataques informáticos en año 2020 según ANEPE (Chile 2019), en Latinoamérica los países más atacados por Phishing son Brasil con 28,28%, Guatemala con 20,34%, Chile con 20,1%, Venezuela y en quinto lugar Ecuador con 19.55%. Según la revista Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina (Pág. 21-23), así mismo el sector educativo ha sido el segundo más afectado por el Phishing en 2020, sólo después del sector financiero, según Kumar, V., & Tripathi, N. (2020).

Por tales motivos es necesario realizar campañas continuas de ingeniería social, capacitando al personal para que identifique los fraudes electrónicos a los que se ven expuestos, evitando ser víctimas de los ciberdelincuentes y exponiendo la información personal o de la organización. Para ello existen herramientas informáticas como es GoPhish, que ayudan a tales objetivos ya que permiten simular ataques de ingeniería social, y posteriormente realizar una capacitación al personal de la institución, haciéndoles saber que se simularon ataques de ingeniería social, y explicándoles en qué consiste la ingeniería social, los distintos tipos de fraudes informáticos (Phishing) y cómo identificar ataques y evitar ser víctima de a los ciberdelincuentes y de esta forma se reduce la brecha de conocimiento y se promueve la conciencia y la educación en torno a la seguridad cibernética.

Objetivos

Objetivo general

Concientizar en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish.

Objetivos específicos

- Analizar el funcionamiento de la herramienta GoPhish, para ingeniería social.

- Implementar y simular ataques de ingeniería social Phishing, con la herramienta GoPhish, para el personal administrativo de la Universidad Nacional de Loja.

- Presentar los resultados obtenidos del ataque de ingeniería social Phishing, para determinar la brecha de conocimiento sobre ataques informáticos Phishing y su posterior retroalimentación.

4. Marco teórico

En el presente apartado se realizará la revisión bibliográfica afines a la seguridad informática que se debe tener en cuenta para poder analizar la presente investigación.

4.1.Antecedentes

Las amenazas cibernéticas empezaron a suscitar el interés de la comunidad internacional a mediados de los años 90, cuando la importancia de los sistemas informáticos empezaba a incrementarse. Sin embargo, la idea parecía algo futurista y lejano, pero tras los atentados en Estados Unidos del 11 de septiembre de 2001, y en los años siguientes mientras se desarrollaban conflictos bélicos entres las naciones de Rusia y Georgia, surgieron los denominados ataques cibernéticos y que con el pasar de los años fueron modificándose y multiplicándose, cada vez se muestran nuevas formas de realizar ataques informáticos como es el caso de ingeniería social. De igual manera se han desarrollado herramientas y técnicas para prevenir este tipo de ataques denominados Phishing, pero se debe realizar énfasis en el último eslabón de la cadena como es el usuario ya que es allí donde la seguridad puede ser vulnerada por la falta de conocimiento.

4.2.Seguridad informática

La seguridad informática es un proceso continuo que requiere la evaluación y la gestión constante de los riesgos y amenazas a la seguridad de los sistemas y la información. Esto implica implementación de políticas y procedimientos de seguridad, así como el uso de tecnologías y herramientas de seguridad para prevenir, detectar y responder a las posibles violaciones de seguridad como son: (M. E. Whitman y H. J. Mattord 2021).

4.2.1. Vulnerabilidad

Una vulnerabilidad es una debilidad o fallo en un sistema informático o en una aplicación que puede ser explotada por un atacante para comprometer la seguridad del sistema o acceder a la información protegida. (M. E. Whitman y H. J. Mattord 2021).

4.2.2. Riesgo

Un riesgo se refiere a la probabilidad de que una amenaza específica explote una vulnerabilidad y cause un daño o pérdida en un sistema informático o en la información que contiene. (Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos 2020).

4.2.3. Amenaza

Una amenaza puede ser intencional (producida por un atacante con motivaciones maliciosas) o no intencional "por ejemplo, el fallo de un equipo". (Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos 2020).

4.3.Seguridad de la información

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un enfoque de gestión de riesgos y la implementación de controles de seguridad apropiados. (ISO/IEC 27001:2022).

4.3.1. Confidencialidad

La confidencialidad implica que la información sólo es accesible por aquellos usuarios o sistemas autorizados para hacerlo, y que está protegida contra posibles amenazas y vulnerabilidades que puedan comprometer su privacidad. (ISO/IEC 27001:2022).

4.3.2. Integridad

La integridad se refiere a la propiedad de la información que asegura que ésta es precisa, completa y fiable a lo largo de su ciclo de vida. La integridad garantiza que la información no ha sido manipulada de manera malintencionada o accidental, y que su contenido es auténtico y no ha sido alterado sin autorización. (ISO/IEC 27001:2022).

4.3.3. Disponibilidad

La disponibilidad implica que la información está disponible para su uso legítimo y autorizado, en el momento en que se requiere, y que no está bloqueada o no está disponible debido a posibles amenazas o vulnerabilidades. (ISO/IEC 27001:2022).

4.4.Ataques informáticos

Un ataque informático es un acto intencional por el cual una entidad intenta evadir servicios de seguridad y violar la política de seguridad de un sistema (RFC 4949 y X.800), mismos que se los clasifica de la siguiente manera:

4.4.1. Según la intención:

Ataque Informático Intencional. Se refiere a un ataque que es llevado a cabo con la intención de causar daño a un sistema o recurso de una organización, los ataques intencionales pueden ser perpetrados por personas externas o internas a la organización y que tienen acceso legítimo a los sistemas y recursos. (RFC 4949 y X.800).

Ataque Informático No Intencional. Se refiere a un ataque que no es llevado a cabo de manera intencional, sino que es causado por una acción inadvertida o accidental. Los ataques no intencionales pueden ser causados por errores humanos, fallas de hardware o software, o problemas de configuración. Estos tipos de ataques pueden tener consecuencias graves, incluso si no fueron intencionales. (RFC 4949 y X.800).

Pasivo. El atacante intenta aprender o usar información del sistema pero no afecta a los recursos del sistema, por medio de escuchas (eavesdropping) o monitorización de transmisiones para obtener información que está siendo transmitida como por ejemplos: Captura de paquetes (sniffing) Obtención del contenido de los paquetes, análisis de tráfico, adivinar los detalles de la comunicación basándose en patrones de mensajes.

Activo. El atacante intenta alterar los recursos del sistema o afectar su funcionamiento, modificando o creando un flujo de datos falso como por ejemplo:
Suplantación (masquerade): Una entidad se hace pasar por otra.

Repetición (replay): Se capturan datos de forma pasiva y se transmiten posteriormente para producir un efecto no autorizado.

Modificación (modification): Se altera una porción de un mensaje legítimo, o se retardan o reordenan los mensajes para producir un efecto no autorizado.

Denegación de servicio (denial of service): Impide el uso o gestión normal de redes o sistemas.

4.4.2. Según el punto de iniciación:

Interno: se refiere a un ataque realizado por alguien que tiene acceso legítimo a los recursos y sistemas de una organización, como un empleado o contratista. Los ataques internos pueden ser intencionales o accidentales, y pueden incluir divulgación de información confidencial, alteración de datos o destrucción de sistemas. (RFC 4949 y X.800).

Externo: se refiere a un ataque realizado por alguien que no tiene acceso legítimo a los recursos y sistemas de una organización, como un hacker o un atacante externo. Los ataques externos pueden incluir explotación de vulnerabilidades en el software, ingeniería social y suplantación de identidad. (RFC 4949 y X.800). La recomendación (X.800) establece que las organizaciones deben implementar una variedad de medidas de seguridad para proteger sus recursos y sistemas, incluyendo políticas y procedimientos de seguridad, controles de acceso, criptografía y monitoreo de la red. La recomendación (X.805) proporciona un marco de trabajo para la gestión de la seguridad de la información, y establece que las organizaciones deben tener en cuenta tanto los riesgos intencionales como no intencionales al desarrollar su estrategia de seguridad de la información. También establece la importancia de la concienciación y formación de los empleados y contratistas para minimizar el riesgo de errores no intencionales.

4.5.Tipos de ataques informáticos más comunes

4.5.1. Malware

El malware es un software malicioso que se utiliza para dañar, controlar o robar información de los sistemas informáticos. Los tipos comunes de malware incluye virus, troyanos, ransomware y spyware (Proofpoint Security 2022).

4.5.2. Ataques de fuerza bruta

Un ataque de fuerza bruta es un intento de descifrar una contraseña mediante el uso de un programa que prueba sistemáticamente todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta. (Proofpoint Security 2022).

4.5.3. Ataques de denegación de servicio (DoS)

Un ataque de denegación de servicio es un intento de interrumpir o desactivar un sitio web o servicio en línea mediante la sobrecarga de tráfico o la saturación del sistema (Proofpoint Security 2022).

4.5.4. Inyección de SQL

La inyección de SQL es una técnica utilizada para explotar vulnerabilidades en las aplicaciones web que utilizan bases de datos. Los atacantes insertan código malicioso en las consultas de bases de datos, lo que les permite acceder a información confidencial o tomar el control del sistema. (Proofpoint Security 2022).

4.5.5. Ataques de ransomware

Un ataque de ransomware es un tipo de ataque de malware en el que los atacantes cifran los datos de la víctima y exigen un rescate a cambio de la clave de descifrado. (Proofpoint Security 2022).

4.5.6. Ingeniería social

La ingeniería social es una técnica utilizada por los atacantes para engañar a las personas y obtener información confidencial. Los atacantes pueden utilizar técnicas como la suplantación de identidad, la persuasión o la manipulación emocional para obtener información confidencial o acceder a sistemas. (Proofpoint Security 2022).

Ingeniería social por teléfono. Se trata de una forma de ataque donde el atacante llama por teléfono a la víctima, haciéndose pasar por alguien que necesita ayuda o información, con el fin de obtener información confidencial o instalar malware (3 Ciencias 2019).

Ingeniería social por correo postal. Este tipo de ataque implica enviar por correo físico cartas o paquetes falsificados con el objetivo de obtener información confidencial o instalar malware. (Proofpoint Security 2022).

Engaño o baiting. Este tipo de ataque implica ofrecer una recompensa o beneficio para que la víctima revele información personal o confidencial, como contraseñas o información bancaria. (Proofpoint Security 2022).

Ataque de ingeniería social física. Este tipo de ataque se enfoca en engañar a las personas en situaciones cara a cara, como hacerse pasar por un empleado de mantenimiento para obtener acceso a instalaciones confidenciales (3 Ciencias 2019).

Phishing. Un ataque de Phishing es un intento de engañar a una víctima para que revele información confidencial, como nombres de usuario, contraseñas o información financiera. Los atacantes suelen enviar correos electrónicos, mensajes de texto o sitios web falsificados o fraudulentos que parecen ser legítimos, imitando a instituciones confiables, engañando a la víctima para que haga clic en un enlace o descargue un archivo malicioso (3 Ciencias 2019).

Spear Phishing. Esta variante del Phishing es más específica y personalizada, y busca engañar a una persona o grupo específico de individuos, generalmente con información que se ha obtenido previamente a través de redes sociales o investigaciones previas (3 Ciencias 2019).

4.6.Fases de un ataque

4.6.1. Reconocimiento

La primera fase de un ataque, se conoce como "Reconocimiento" o "Footprinting", los atacantes recopilan información sobre el objetivo de su ataque. Esta información puede incluir detalles sobre la red, los sistemas, y sitios web públicos, escaneo de puertos la recolección de información de DNS, aplicaciones, infraestructura de la organización, redes sociales de personas que utilizan los sistemas, entre otras identificar posibles vulnerabilidades que les permite planificar su ataque y seleccionar las técnicas y herramientas adecuadas para comprometer la seguridad de los sistemas y la información (José Luis Calle Condori 2019).

4.6.2. Escaneo

Una vez que el atacante ha recopilado información suficiente sobre el objetivo, procede a explorar su infraestructura de red y sistemas en busca de vulnerabilidades y posibles puntos de entrada (José Luis Calle Condori 2019).

4.6.3. Intrusión

Si el atacante ha encontrado una vulnerabilidad o punto de entrada, intentará explotarlo para obtener acceso a los sistemas y/o información, una vez dentro el atacante intentará mantener su acceso y controlar el sistema de forma continua (José Luis Calle Condori 2019).

4.6.4. Robo de información

Una vez que el atacante ha obtenido acceso y control sobre los sistemas objetivo, intentará extraer información valiosa de la organización. Esto puede incluir información financiera, propiedad intelectual o datos personales (José Luis Calle Condori 2019).

4.6.5. Ocultamiento del ataque

El atacante intentará borrar toda evidencia de sus actividades realizadas durante la intrusión para evitar ser detectado por el profesional de seguridad, para poder seguir accediendo al sistema

atacado. Por lo general se eliminan los archivos de registro (log) o alarmas del sistema de detección de intrusos (IDS) (José Luis Calle Condori 2019).

4.7.Herramientas para campañas anti phishing

Como se puede observar en la descripción de los apartados anteriores, los ataques de ingeniería social bajo la modalidad de Phishing es una técnica utilizada por los ciberdelincuentes para obtener información personal y financiera de los usuarios a través de la suplantación de identidad. Sin embargo, existen medidas preventivas que se pueden aplicar dentro de una organización u empresa con el objetivo de mantener a los usuarios prevenidos o alertados para detectar y evitar ataques informáticos de Ingeniería Social tipo Phishing, para ello existen herramientas que se pueden utilizar para crear campañas anti phishing para educar al usuario sobre los riesgos y consecuencias que se exponen al ser víctimas efectivas de este tipo de ataques, entre las más comunes tenemos:

4.7.1. Herramientas de entrenamiento de Phishing

Se utilizan para proporcionar a los usuarios información sobre cómo detectar y evitar los ataques de Phishing. Pueden incluir videos de entrenamiento, pruebas de Phishing simuladas y juegos interactivos, Ejemplo: PhishLine, Wombat Security y SecurityIQ.

4.7.2. Servicios de detección de Phishing

Se utilizan para detectar y alertar sobre ataques de Phishing en tiempo real. Los servicios de detección de Phishing pueden monitorear correos electrónicos, sitios web y redes sociales en busca de actividad sospechosa. Ejemplos: Agari, Barracuda y Proofpoint.

4.7.3. Herramientas de autenticación de correo electrónico

Se utilizan para verificar la autenticidad de los correos electrónicos entrantes y salientes. Las herramientas de autenticación de correo electrónico pueden ayudar a prevenir el spoofing de correo electrónico y otros ataques de Phishing. Ejemplos DMARC, SPF y DKIM

4.7.4. Simuladores de Phishing

Estas herramientas se utilizan para crear correos electrónicos y sitios web falsos que imitan a una empresa o entidad legítima. Los simuladores de Phishing pueden ser utilizados para enviar correos electrónicos de prueba a los empleados de una empresa y evaluar su capacidad para detectar y evitar los ataques de Phishing. Ejemplos de simuladores de Phishing incluyen KnowBe4, PhishMe, y GoPhish.

Tabla 1

Análisis Comparativo de las herramientas anti phishing

HERRAMIENTA	VENTAJAS	DESVENTAJAS	USABILIDAD	COMPATIBILIDAD
KnowBe4	_Interfaz de usuario intuitiva y fácil de usar. _Ofrece una amplia variedad de plantillas de correo electrónico y páginas de Phishing personalizables. _Proporciona informes detallados de las pruebas de Phishing.	_Los precios pueden ser elevados para pequeñas y medianas empresas. _Algunas características avanzadas pueden requerir experiencia técnica adicional	_Fácil de usar para usuarios de todos los niveles.	_Compatible con Windows, MacOS, iOS y Android.
PhishMe	_Ofrece simulaciones de Phishing altamente personalizables. _Proporciona una amplia variedad de opciones de informes y análisis. _Se integra con otras herramientas de seguridad para mejorar la protección contra el Phishing.	_El costo puede ser elevado en comparación con otras herramientas de simulación de Phishing. _Algunas características pueden requerir conocimientos técnicos avanzados.	_Fácil de usar para usuarios de todos los niveles.	_Compatible con Windows y MacOS.
GoPhish	_Herramienta de código abierto y gratuito. _Proporciona plantillas de correo electrónico y páginas de Phishing personalizables. _Ofrece integraciones con otras herramientas de seguridad.	_Requiere conocimientos técnicos avanzados para su instalación y configuración. _La interfaz de usuario puede ser menos intuitiva en comparación con otras herramientas de simulación de Phishing	_Requiere experiencia técnica para su uso efectivo.	_Compatible con Windows, MacOS y Linux.

Fuente: Elaborada por el autor

Después de haber realizado un análisis comparativo de las herramientas que existen para realizar campañas de anti phishing se determina que GoPhish es la herramienta adecuada para poder llevar a cabo la presente investigación por las características técnicas que ofrece esta herramienta.

5. Metodología

Para el desarrollo de la presente investigación se hizo uso la metodología de enfoque experimental ya que se evaluarán los resultados de la simulación de un ataque Phishing haciendo uso de la herramienta GoPhish, sobre un grupo de participantes (Personal Administrativos de la Universidad Nacional de Loja), la metodología experimental consta de las siguientes fases.

Etapa I: Selección y muestreo de la población. La campaña de simulación de ataques Phishing, se realizará al Personal Docente y Administrativo de la Universidad Nacional de Loja.

Etapa II: Diseño del experimento. Se diseña el correo electrónico simulado y personalizado que será enviado al personal Docente y Administrativo de la Universidad, utilizando la herramienta GoPhish, dicho correo electrónico debe ser idéntico a los correos electrónicos que suelen recibir en las actividades laborales diarias.

Etapa III: Intervención. Configurar la herramienta GoPhish, definir el tipo de ataque Phishing que va a ser simulado en la campaña, y enviar los correos electrónicos simulados, rastreando el comportamiento de los participantes (víctimas) que dieron clics en los enlaces, cabe mencionar que dicha simulación es con fines netamente académico e investigativos, razón por la cual se respetará la privacidad y confidencialidad de la información personal.

Etapa IV: Análisis de resultados. Analizar los resultados obtenidos durante la campaña de la simulación del ataque Phishing para poder diseñar una retroalimentación con recomendaciones y técnicas de concientización anti phishing para evitar que el personal docente y administrativo pueda ser víctimas de los ataques Phishing

Etapa V: Conclusiones: Conclusiones generales sobre la efectividad de la campaña y posibles mejoras que se pueden realizar en el futuro. También se deben mencionar las limitaciones del estudio y las implicaciones prácticas.

Así mismo se hizo uso de la técnica de **búsqueda bibliográfica** en bases de datos especializadas en tecnología y ciberseguridad, como por ejemplo IEEE Xplore, ACM Digital Library, ScienceDirect, entre otras, utilizando palabras clave como "phishing", "ciberseguridad", "concientización" y "GoPhish, adquiriendo los argumentos teóricos para la instalación, configuración y creación de campañas de simulación de ataques phishing en la herramienta GoPhish.

5.1.Etapa I: Población de estudio

En los objetivos de la presente investigación se plantea realizar una simulación de un ataque de Ingeniería Social denominado Phishing utilizando los correos electrónicos asignados al Personal Administrativo de la institución con la excepción de las autoridades de la institución, sin embargo, por pedido de la *Dirección de Tecnologías de Información (DTI)* se incluyó los correos electrónicos asignados al Personal Docente de la istitucion. En la siguiente tabla se muestra la población total que será utilizada para en la presente investigación:

Tabla 2
Población Universitaria.

REGIMEN LABORAL	DESIGNACIÓN	CANTIDAD
Ley Orgánica de Educación Superior (LOES)	Personal Docente	780
Ley Orgánica de Servicio Público (LOSEP)	Personal Administrativo	440
Total Población Universitaria		1220

Fuente: Sistema SIAAF, Módulo Talento Humano

5.2.Etapa II: Diseño del experimento

5.2.1. Servidor de correos

En el menú ***"Sending Profiles"*** de GoPhish se requieren configurar entre otras cosas lo siguiente:

- Usuario = (correo electrónico).
- Contraseña = (password).
- Host = (servidor de correos.com:puerto)

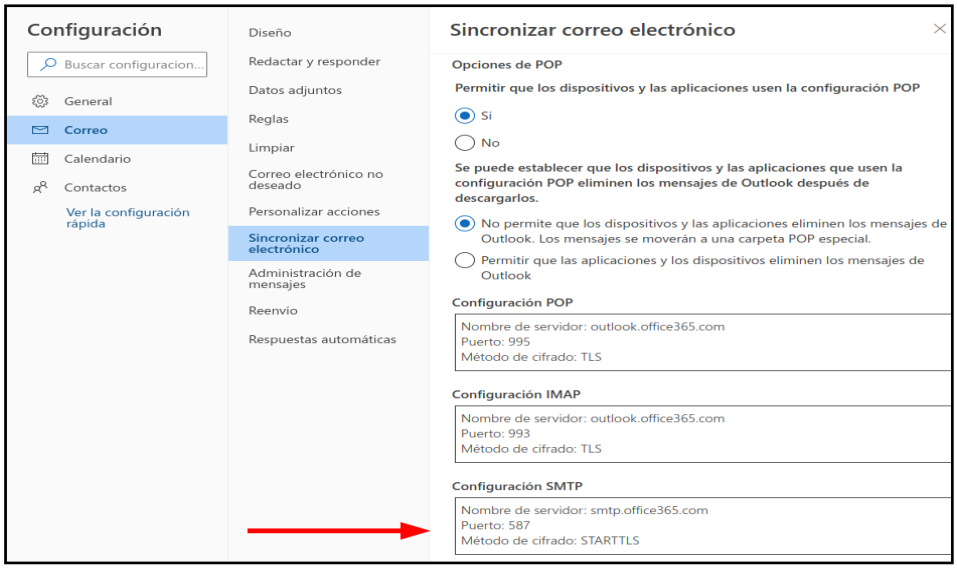
A razón de ello, se debe establecer con qué servidor de correos se va a trabajar dentro de la herramienta GoPhish para la configuración de las campañas, ya sea con ***@gmail.com*** o con ***@outlook.es***.

5.2.1.1.Outlook

En caso de que se decida trabajar con ***"@outlook.es",*** no es necesario realizar ninguna configuración adicional en la cuenta de correo electrónico, simplemente hay que navegar por el menú ***"Configuración, Ver toda la configuración de Outlook, Correo, Sincronizar correo electrónico"***, una vez dentro, identificar el servidor de correo y el puerto que utiliza tal como se muestra en la siguiente imagen:

Figura 1

Configuración del servidor SMTP de Outlook.



Fuente: El autor

Para este caso puntual en la herramienta GoPhish se debe llenar los campos requeridos de la siguiente manera:

- Usuario = (usuario@outlook.es).
- Contraseña = (clave de inicio de sesión).
- Host = (smtp.office365.com:587).

5.2.1.2.Gmail

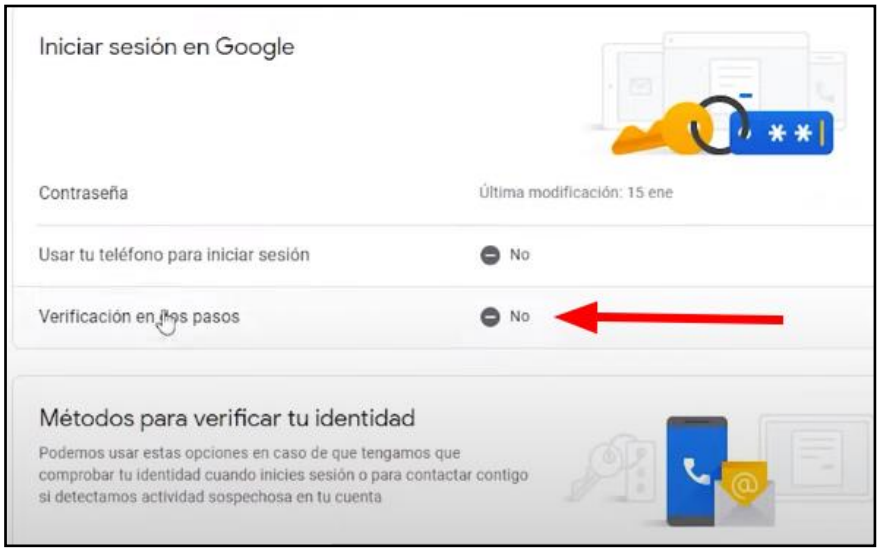
Para trabajar con ***@gmail.com*** es necesario realizar configuraciones adicionales como:

- Verificación de dos pasos.
- Contraseñas de aplicaciones.

Para configurar y activar ***verificación de dos pasos***, dentro de la cuenta de Gmail, navegar por el menú: ***"Seguridad, Acceso a Google, Verificación en dos pasos"***, tal como se muestra en la siguiente imagen:

Figura 2

Verificación en dos pasos de la cuenta Gmail.

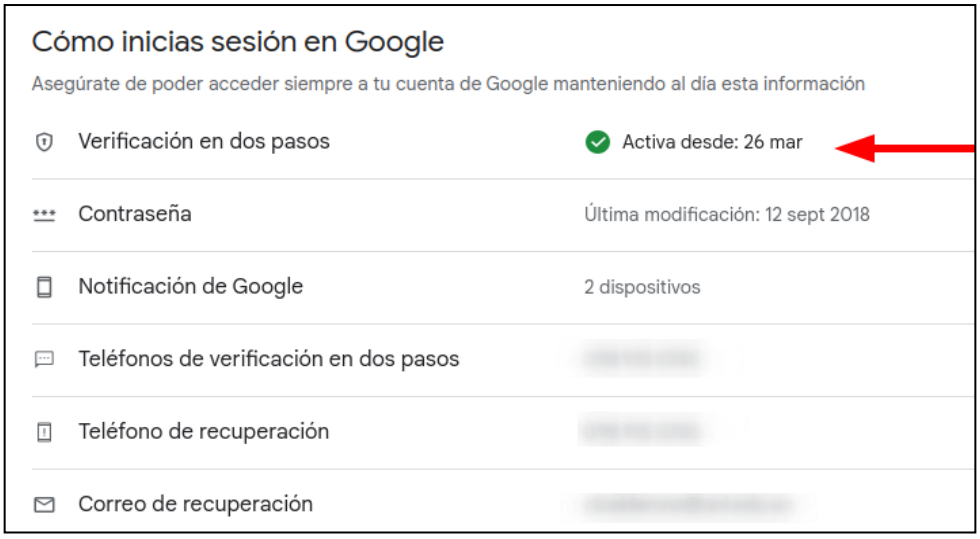


Fuente: El autor

Una vez dentro de este menú, ingresar "contraseña de inicio de sesión, número de teléfono, código de verificación (SMS enviado número de teléfono registrado)", y se activa esta opción.

Figura 3

Verificación de dos pasos activada en Gmail.



Fuente: El autor

Una vez activada la ***verificación de dos pasos***, se mostrará en el menú la opción ***contraseñas de aplicaciones***, hacer clic e ingresar la contraseña de la cuenta, en la parte inferior existe un menú desplegable, seleccionar ***Otra (nombre personalizado)*** ponemos un nombre y clic en ***GENERAR*** se mostrará un código o contraseña el cual deberá ser utilizado en el campo password de la ***Sending Profiles:***

Figura 4

Activación de contraseñas de aplicaciones en Gmail**.**

Fuente: El autor

Nota: Si usas una cuenta de trabajo, institución educativa o algún otro grupo, deberás, comunícate con tu administrador para obtener ayuda. Entonces en la herramienta GoPhish se debe llenar los campos requeridos de la siguiente manera:

- Usuario = (usuario@gmail.com)
- Contraseña = (código generado con la opción contraseñas de aplicaciones)
- Host = (smtp.gmail.com:587)

5.2.2. Creación del correo electrónico

Dentro de la Universidad Nacional de Loja, existe el departamento de la Dirección de Comunicación e Imagen Institucional que se encarga de realizar notificaciones y avisos masivos a toda la comunidad universitaria a través del siguiente correo electrónico:

Tabla 3
Correo electrónico institucional

LOGO	NOMBRE	CORREO
	Información Institucional - Unl	<masinfo@unl.edu.ec>

Fuente: Elaborada por el autor

Conocido la estructura del correo electrónico institucional se elige Gmail, para utilizarlo en los envíos de correos y se procede a crear tres (3) correos electrónicos, parecidos al descrito en la tabla 2, mismos que serán utilizados para la campaña de GoPhish.

Tabla 4
Correos electrónicos ficticios.

LOGO	NOMBRE	CORREO
	Información Institucional - Unl	<masinfor.unl.edu.ec@gmail.com>
	Información Institucional - Unl	<massinfo.unl.edu.ec@gmail.com>

Fuente: Elaborada por el autor

En cada uno de los correos electrónicos se debe configurar y habilitar obligatoriamente las opciones de: *verificación de dos pasos y contraseñas de aplicaciones*, cabe mencionar que, si no se configura estas dos opciones no se podrá realizar la campaña GoPhish con este servidor de correos *(Gmail),* ya que es aquí donde se genera una clave o password, misma que será utilizada cuando se configuren los parámetros de la herramienta GoPhish, específicamente en el menú ***"Sending Profiles"***, así mismo con la habilitación de estas dos opciones se evita que los correos sean bloqueados o se envíen a la bandeja de correos no deseados. La razón del porqué se crearon tal cantidad de correos electrónicos, es para garantizar la entrega de todos los correos anexados en la campaña de Phishing que se a ejecutar a través de herramienta GoPhish, tomando en cuenta las siguientes limitantes:

- **Gmail** permite enviar un máximo de (500) correos electrónicos dentro de las 24 horas, esta cantidad puede ser limitada o reducida por algunos factores como:

  - Antigüedad de la cuenta.
  - Historial de uso de la cuenta.
  - Contenido de los correos electrónicos.
  - Cumplimiento de las políticas de uso de Google.
  - Cantidad y calidad de los correos enviados y recibidos.

- **GoPhish** puede enviar campañas sin limitación de correos electrónicos sin embargo se corre el riesgo que los proveedores de correo electrónico los identifiquen como spam o intentos de Phishing, lo que puede provocar que los correos electrónicos sean bloqueados o enviados a la carpeta de correo no deseado por ende se recomienda enviar un número razonable de correos electrónicos desde una dirección IP (Protocolo de Internet) en particular o en su defecto desde distintas cuentas de correos electrónico, estas campañas, también pueden verse afectada por las siguientes razones:

- Hardware del servidor
- Capacidad de transmisión de la red.
- Configuración de la campaña (página clonada, contenido del correo, cantidad de correos, etc.

Así mismo, las campañas de GoPhish es recomendable que se ejecuten con intervalos de tiempos prudenciales como mínimo después de que haya transcurrido una hora desde que se lanzó la última campaña con el fin de evitar que los servidores de correos bloquean las entregas o en su defectos, los envíen a la bandeja de correos no deseados (SPAM).

5.2.3. Personalización del correo electrónico

Una vez creado y configurado el correo electrónico se procede con la personalización del mismo, ideando y diseñando el mensaje que será enviado durante la campaña de Phishing, el cual debe ser llamativo y lo más real posible, con el fin de engañar al funcionario de la Universidad Nacional de Loja. Como es de conocimiento público la comunidad universitaria registra el ingreso y salida de las actividades laborales a través del sistema institucional denominado: *"Sistema de Información Académico Administrativo Financiero" (SIAAF)*, dicho registro se puede realizar desde cualquier dispositivo móvil conectado a la red de datos del campus universitario, al tener este servicio se generan retrasos, olvidos o marcaciones erróneas por parte del funcionario, el cual al final del mes de sus actividades laborales requiere saber cuál es su historial de ingreso y egreso, a razón de ello se han generado múltiples requerimientos hacia la *Dirección de Tecnologías de Información (DTI)*, para que se cree y se habilite un módulo informático donde se pueda consultar el historial de registros, evitando así los pedidos formales al *Departamento de Talento Humano*. Por los antecedentes descritos, se procedió a diseñar el correo electrónico con imágenes y/o texto que contengan mensajes persuasivos y propagandísticos orientados hacia la creación y disponibilidad de un módulo de consulta y reportes de asistencia.

Figura 5

Mensaje Propagandístico Gmail.

Fuente: El autor

Así mismo se agregó una imagen donde el funcionario tendrá la opción de poder ingresar a revisar el supuesto Módulo de Consulta de Atrasos, es precisamente allí donde se encuentra el fraude o engaño ya que en esta imagen se ingresará el link que dirige hacia una página clonada o falsa.

Figura 6

Botón de redirección hacia la página de alerta.

Fuente: El autor

Una vez que el funcionario de clic en la imagen, está deberá dirigir hacia un página donde tendrá que ingresar sus credenciales para el ingreso al sistema, es allí donde se debería capturar la

información confidencial del funcionario, es decir su usuario y contraseña. Sin embargo por cuestiones de seguridad y evitar caos y pánico en el funcionario administrativo, la *Dirección de Tecnologías de Información (DTI)* no autorizo que se clonara ninguna página o peor aún se capturará información confidencial, autorizando únicamente que el link de redirección lleve a hacia una página que muestre un mensaje de alerta, para que el funcionario sepa que fue una víctima de una estafa o engaño, este link estará dentro de página web principal de la Universidad Nacional de Loja. Finalmente se agregaron detalles adicionales en el cuerpo del correo electrónico, como imágenes y firmas similares a los que se utilizan por parte del departamento de *Dirección de Comunicación e Imagen Institucional.*

Figura 7

Cuerpo del correo electrónico

Fuente: El autor

5.2.4. Contenido para mostrarse en la página web de la UNL

Como se mencionó en el apartado anterior, la *Dirección de Tecnologías de Información (DTI)* recomendó que se realizará un contenido donde se indique al funcionario que ha sido víctima de un engaño por un ciberataque, a razón de ello, en el presente apartado se elabora el contenido que posteriormente se mostrará en un micrositio web alojado en la página principal de la Universidad Nacional de Loja.

¡¡¡ Usted ha caído en el engaño!!!

Usted pudo ser víctima de un ciberataque

Tabla 5

Mensaje de alerta a Comunidad Universitaria

La Universidad Nacional de Loja a través de la Dirección de Tecnologías e Información (DTI), desarrolla y aplica simulación de un ciberataque bajo la modalidad de Ingeniería Social "Phishing", con el fin de concientizar y resguardar la confidencialidad, integridad y disponibilidad de la información de la comunidad universitaria.

Fuente: Elaborada por el autor

CIBERATAQUES BAJO LA MODALIDAD DE INGENIERÍA SOCIAL

¿Qué es la ingeniería social?

La ingeniería social es una técnica utilizada por los ciberdelincuentes para manipular a las personas con el objetivo de obtener información confidencial como contraseñas, números de tarjeta de crédito, entre otros datos personales, valiéndose del eslabón más débil de una organización (Usuario final, empleados y trabajadores), razón por la cual la Ingeniería Social es definida como "la manipulación de la psicología humana para obtener acceso no autorizado a información, sistemas o recursos". Los ataques de Ingeniería Social se realizan a través de correo electrónico, mensajes de texto, redes sociales, entre otros medios, por ende es importante que todos estemos alerta ante los ataques de Phishing y que tomemos medidas de seguridad para proteger la información personal o de la institución en la que se está elaborando, en la siguiente imagen se grafica el modus operandi de este tipo de ataque informático (Phishing).

Tabla 6

Técnicas de Ingeniería Social

TÉCNICAS MÁS COMUNES DE UN ATAQUE DE INGENIERÍA SOCIAL			
			
Phishing	Vishing	Baiting	Redes Sociales
Consiste en engañar al usuario mediante la suplantación de identidad, correos electrónicos y sitios web ficticios con el fin de extraer información confidencial como por ejemplo contraseñas de cuentas bancarias.	Consiste en estafar al usuario a través de llamadas telefónicas o mensajes de voz, logrando extraer información sensible y confidencial como números de tarjetas de crédito.	Consiste en manipular a los usuarios para que acceda a conectar un dispositivo de almacenamiento como memorias USB infectadas y preparadas para recopilar todo tipo de datos una vez se conecte a un equipo.	Consiste en engañar al usuario creando perfiles falsos en las redes sociales.

Fuente: Elaborada por el autor

5.3.Etapa III: Intervención.

5.3.1. Instalación de GoPhish

GoPhish es una herramienta ***open-source*** con una interfaz amigable y multiplataforma (Linux, Mac OS y Windows), la cual permite recrear un ambiente de simulación para realizar campañas de ataques de ingeniería Phishing de forma ética a través de los correos electrónicos. Gracias a este tipo de campañas se puede llegar a comprobar el grado de conocimiento que tienen los usuarios en cuanto a los ataques de ingeniería social denominados Phishing y sobre estos resultados se puede realizar una retroalimentación con medidas preventivas y técnicas de anti phishing para mantener prevenido y alertado al personal administrativo de la institución. La implementación de GoPhish se realizó en un ***Servidor Privado Virtual (VPS)*** de la Universidad Nacional de Loja, accesible mediante el intérprete de órdenes seguro, ***Secure SHell (SSH)*** con dirección ***IP 192.168.1.1 (IP Ficticia por seguridad)*** Cuyas características técnicas principales son las siguientes:

- Memoria RAM: 1 GB
- Capacidad de almacenamiento: 25 GB SSD.
- Sistema Operativo: Debian

Una vez que se habilitó y se permitió el acceso al servidor por parte del personal de la Dirección de Tecnologías de Información de la Universidad Nacional de Loja, se procedió a instalar GoPhish, cabe mencionar que toda la configuración se lo debe realizar en modo *root* tal como se detalla a continuación: Se habilitó el servicio ***ssh*** en el servidor para poder acceder mediante sesión *ssh* con el siguiente comando:

<<sudo apt install openssh-server>>

GoPhish al ser un software Open Source se encuentra alojado en un repositorio de GitHub en el siguiente enlace: *https://github.com/GoPhish/GoPhish/*.

Dentro del servidor se crea el directorio denominado ***"GoPhish"*** en la carpeta ***"opt"***, del sistema operativo, y se ingresa a dicho directorio con los siguientes comandos:

<<mkdir GoPhish>>
<<cd GoPhish>>

Dentro del directorio se procede a descargar GoPhish que actualmente se encuentra en la versión ***"v0.12.1"*** y es accesible desde la siguiente URL *https://github.com/GoPhish/GoPhish/releases/download/v0.12.1/GoPhish-v0.12.1-linux-64bit.zip*, con el siguiente comando:

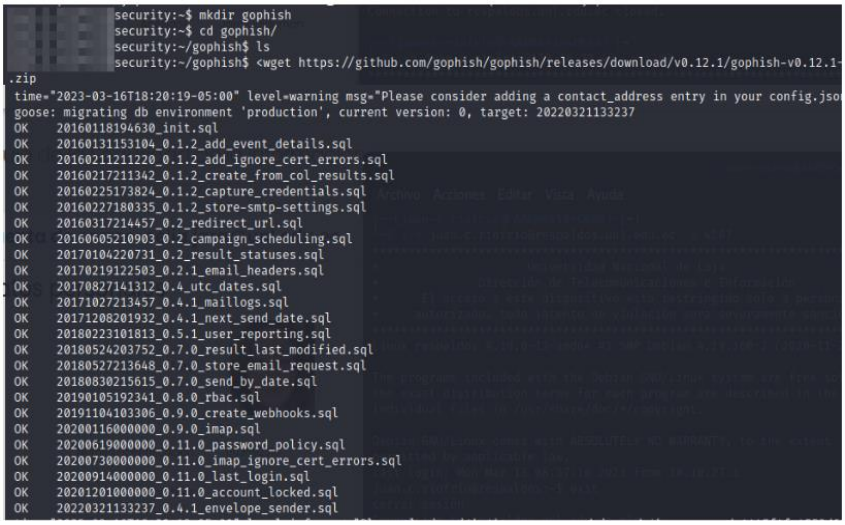
<<wget https://github.com/GoPhish/GoPhish/releases/download/v0.12.1/GoPhish-v0.12.1-linux-64bit.zip>>

Finalmente se descomprime el fichero **.zip** que fue descargado con el siguiente comando:

<<unzip GoPhish-v0.12.1-linux-64bit.zip>>

Figura 8

Comandos para la instalación de GoPhish.



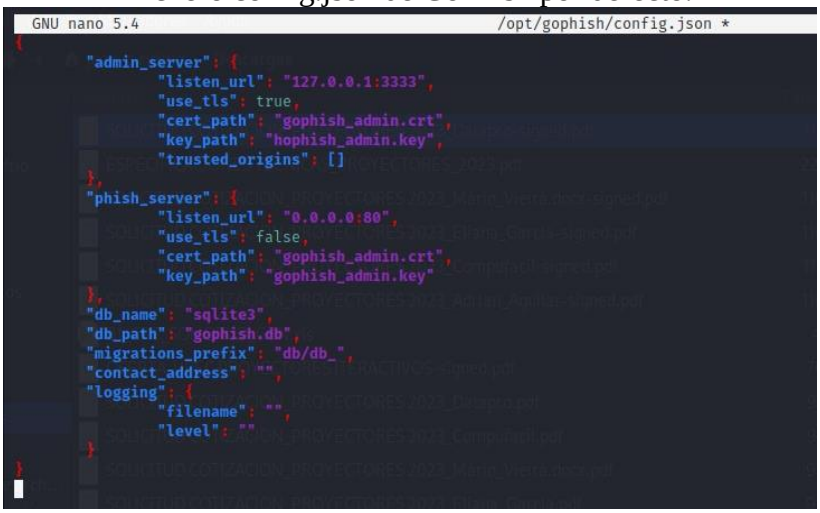
Fuente: El autor

Una vez descomprimido la herramienta, es necesario realizar algunos cambios en los archivos de configuración específicamente en el fichero "config.json", para ello es necesario ejecutar el siguiente comando: <<***nano config.json***>>

En la siguiente figura se muestra el fichero de configuración ***"config.json",*** con los parámetros de configuración por defecto de GoPhish.

Figura 9

Fichero config.json de GoPhish por defecto.



Fuente: El autor

Dentro de la configuración ***"config.json",*** podemos destacar los siguientes apartados:

La primera parte contiene las configuraciones del ***admin_server*** de administración. Tenemos la URL de escucha del servidor de administración ***127.0.0.1:3333*** y los certificados ***.crt*** y la clave ***.key***.

La segunda parte de la configuración contiene las configuraciones del ***server_phish***. La URL de escucha para el servidor de Phishing ***"0.0.0.0:80"*** y los certificados ***.crt*** y la clave ***.key*** para el servidor de Phishing. La última sección contiene la configuración de la base de datos. El marco está configurado para usar la base de datos **"*SQLite*"**, sin embargo, esta puede ser cambiada o modificada de acuerdo a la necesidad del usuario.

Los parámetros que se reemplazaron en el del archivo **"*config.json*"** son:

admin_server

listen_url: ***127.0.0.1:3333*** por ***192.168.1.1:3380***

crt_path: ***gophish_ admin.crt*** por ***unl_edu_ec_2022_2023.crt***

key_path: ***gophish_admin.key*** por ***server.key***

phish_server

listen_url: ***0.0.0.0:80*** por ***192.168.1.1:443***

use_tls***: false*** por ***true***

crt_path: ***gophish_ admin.crt*** por ***unl_edu_ec_2022_2023.crt***

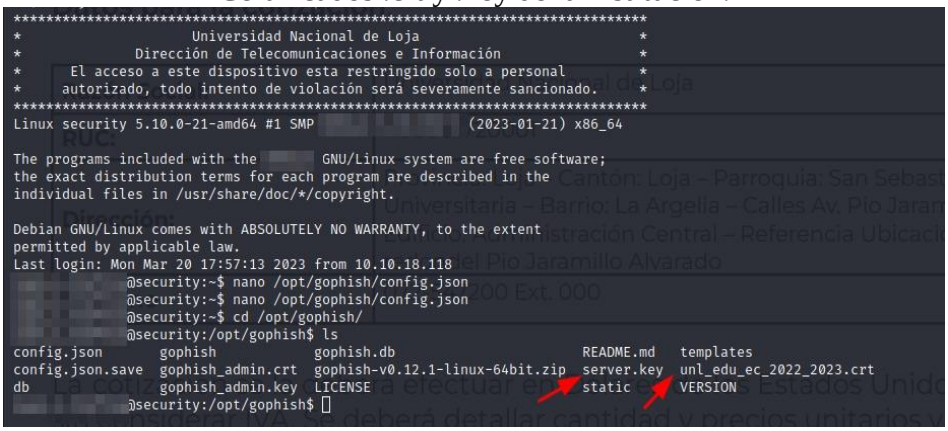
key_path: ***gophish_admin.key*** por ***server.key***

5.3.2. Configuración de certificados SSL en GoPhish

La Universidad Nacional de Loja cuenta con certificados, **".crt y .key"**, mismos que fueron adquiridos para la implementación de medidas de seguridad en los sistemas informáticos y cifrar las comunicaciones entre cliente servidor, razón por la cual se hizo uso de los certificados antes mencionados en la implementación de GoPhish. Para hacer uso de dichos certificados es necesario replicarlos en el directorio que contiene a GoPhish ***/opt/GoPhish***, tal como se muestra en la siguiente imagen.

Figura 10

Certificados .crt y .key de la institución.

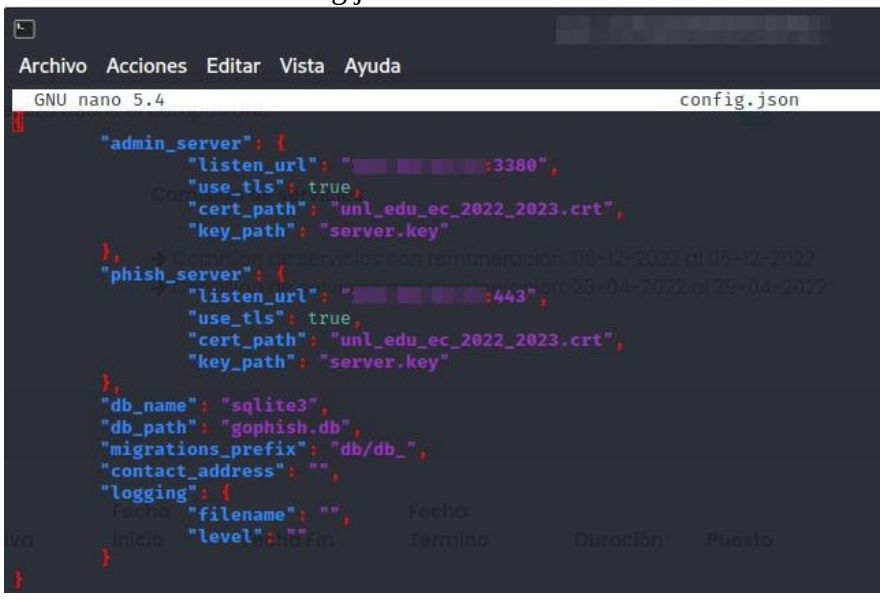


Fuente: El autor

Es necesario implementar todas estas medidas por políticas de seguridad que mantiene la institución, esto permitirá ser más creíble y real la simulación del ataque Phishing debido a que se hará uso de la navegación segura ***https*** y no ***http***. Una vez modificados todos estos parámetros se guardan los cambios, quedando modificado el archivo ***"config.json"*** tal como se muestra en la siguiente imagen:

Figura 11

Fichero config.json de GoPhish modificado.



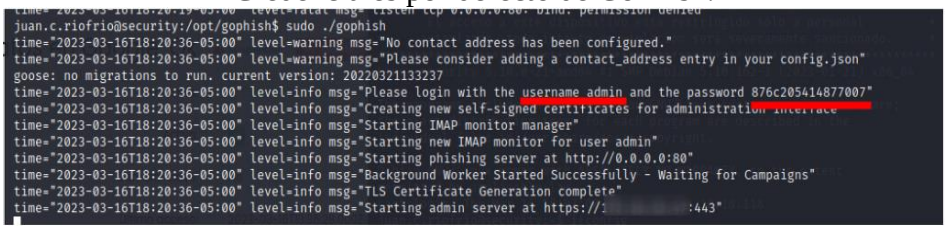
Fuente: El autor

Finalmente le damos los permisos necesarios y ejecutamos GoPhish, usando los siguientes comandos. << ***chmod +x Gophish***>> << ***./gophish*** >>

Cuando se ejecuta GoPhish por primera vez, las credenciales por defecto se muestran en la consola de administración, tal como se observa en la siguiente figura:

Figura 12

Credenciales por defecto de GoPhish.



Fuente: El autor

La Universidad Nacional de Loja cuenta con un certificado ***SSL WildCard (Secure Sockets Layer capa de sockets seguros)***, mismo que permite certificar todos los subdominios asociados a un mismo dominio ***"*.unl.edu.ec***," por ende a GoPhish se le asignó el siguiente dominio https://security.unl.edu.ec:3380/ el cual se debe ingresar. Para iniciar sesión en GoPhish abrimos el navegador e ingresamos el dominio antes mencionado, colocando las credenciales por defecto, acto seguido se debe cambiar la contraseña de forma obligatoria bajo el criterio del usuario.

Figura 13

Inicio de sesión y cambio de credenciales en GoPhish.

Fuente: El autor

5.3.3. Ejecución automática de gophish

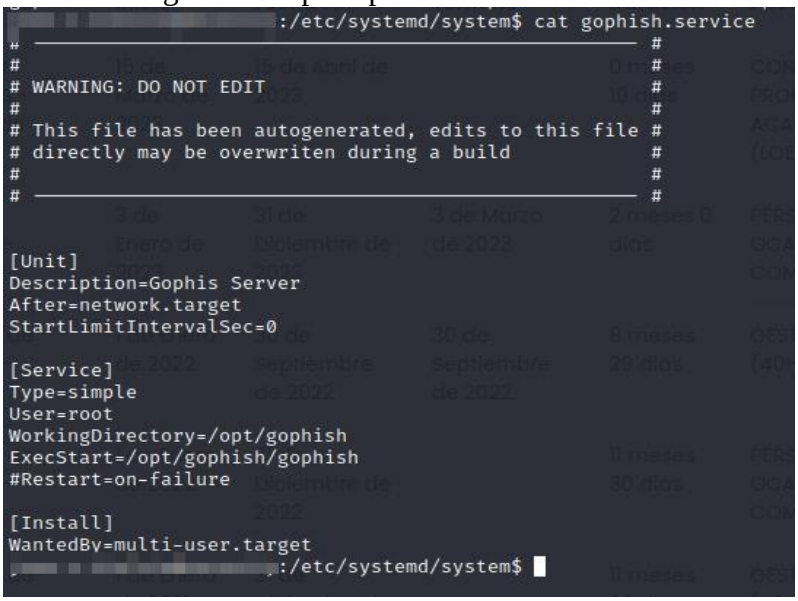
La herramienta GoPhish no se ejecuta automáticamente al arrancar el servidor, razón por la cual, es necesario configurar un Script para que se ejecute cada vez que arranque el servidor. Se crea el script en el directorio ***/etc/systemd/system*** con el siguiente comando:

<<sudo nano /etc/systemd/system/GoPhish.service>>

Dentro del archivo se agrega el siguiente código:

<<[Unit]
Description=Gophis Server
After=network.target
StartLimitIntervalSec=0
[Service]
Type=simple
User=root
WorkingDirectory=/opt/GoPhish
ExecStart=opt/GoPhish/GoPhish
#Restart=on-faiture
[install]
WantedBy-multi-user.target>>

Figura 14
Código del Script implementado en el servidor



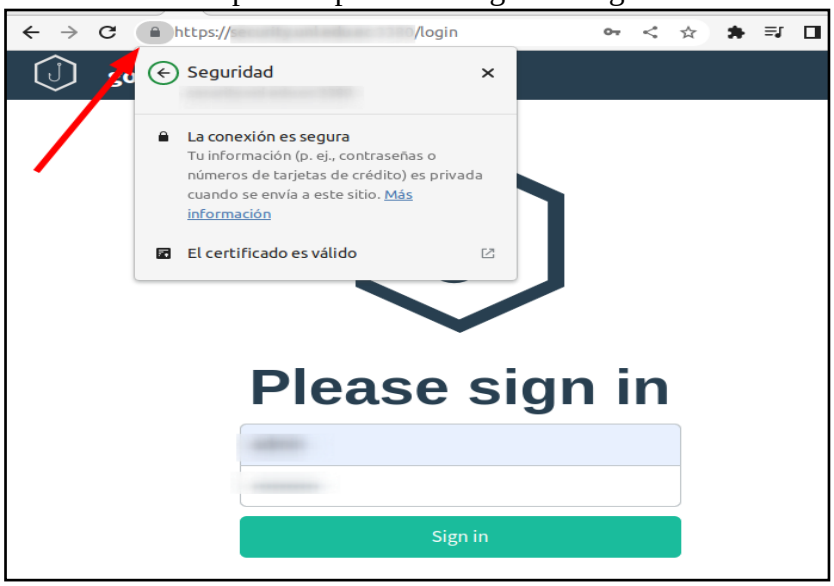
Fuente: El autor

5.3.4. Panel de control de GoPhish

Luego de haber instalado y configurado tanto el servidor así como la herramienta GoPhish, con todas las medidas y políticas de seguridad que exige la Universidad Nacional de Loja, se procedió con la creación, personalización y diseño del correo electrónico que será enviado, al funcionario administrativo, así mismo se elaboró y se agregó el contenido teórico que se muestra en la página web principal de Universidad Nacional de Loja, finalmente se procede a configurar los parámetros para lanzar la campaña de simulación del ataque de Ingeniería Social denominado Phishing dentro de la herramienta GoPhish tal como se muestra en los siguientes apartados. Recordemos que GoPhish ya se encuentra operativo y en producción por ende únicamente hay que abrir el navegador e ingresar el dominio o la dirección *IP* del servidor *192.168.0.1*, ingresamos las credenciales de acceso tal como se muestra en la *Figura 13*, así mismo se puede apreciar que los *certificados SSL*, que fueron configurados se están ejecutando para la navegación segura.

Figura 15

Certificado SSL aplicado para la navegación segura en GoPhish.

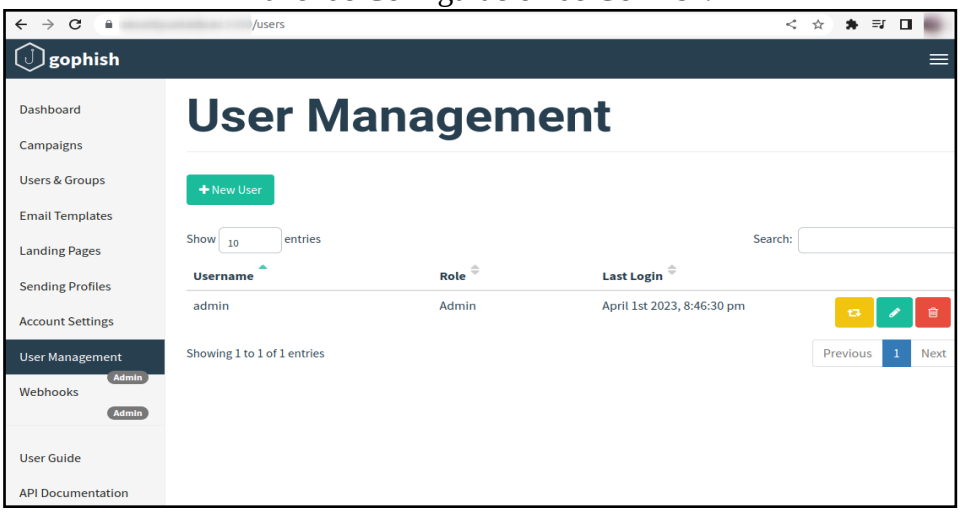


Fuente: El autor

Dentro de la interfaz web de GoPhish se visualiza el menú de configuración el cual incluye varias opciones, que permiten a los usuarios administrar campañas de Phishing.

Figura 16

Panel de Configuración de GoPhish.



Fuente: El autor

A continuación, se presenta un resumen de todas las opciones del menú de GoPhish:

- **Dashboard:** proporciona una visión general de las campañas en ejecución, incluidos los recuentos de correos electrónicos enviados, los clics y las entregas.
- **Campaigns:** permite a los usuarios crear, administrar y ver informes de las campañas
- **Users:** permite a los usuarios agregar y administrar usuarios de GoPhish.
- **Groups:** permite a los usuarios crear y administrar grupos de usuarios para enviar campañas de Phishing específicas a grupos de destinatarios.
- **Email Templates:** permite a los usuarios crear y administrar plantillas de correo electrónico para las campañas de Phishing.
- **Landing Pages:** permite a los usuarios crear y administrar páginas de destino personalizadas para las campañas de Phishing.
- **Sending Profiles:** permite a los usuarios configurar las cuentas de correo electrónico desde las que se enviarán los correos electrónicos de la campaña.
- **Account Settings**: permite a los usuarios configurar opciones de sistema, como la configuración de la cuenta, el registro de auditoría y el intervalo de actualización.
- **User Management:** permite a los administradores agregar y administrar usuarios en la plataforma, estableciendo diferentes niveles de acceso y permisos para cada usuario.

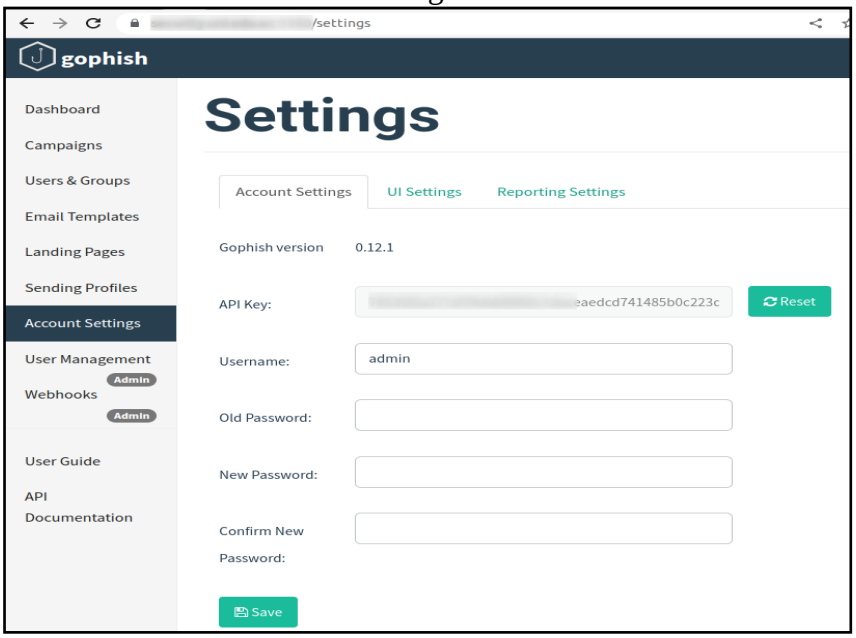
- **Webhooks:** permite a los usuarios configurar una URL de destino para recibir datos en tiempo real sobre las interacciones de los usuarios con las campañas de Phishing.
- **API Documentation & User Guide:** contienen información del uso y manejo de la herramienta GoPhish.

5.3.5. Configuración de la campaña en Gophish

5.3.5.1.Account Settings

Para la creación de la campaña es recomendable realizar la configuración desde abajo hacia arriba, por ende primeramente se configura el apartado **Account Settings**, en esta sección podemos cambiar las credenciales, también disponemos de la ***API Key*** que nos permitirá interactuar con la herramienta desde cualquier lenguaje de programación o scripting, por si preferimos usar otro método que no sea su interfaz web. Como recomendación, en la pestaña ***UI Settings*** podemos habilitar la opción **Show campaign results map** para mostrar los resultados de cada campaña en un mapa, por si las víctimas accedieron a la campaña desde distintos países, cuyo resultado se aprecia en el apartado **Dashboard.**

Figura 17
Panel de Settings de GoPhish.

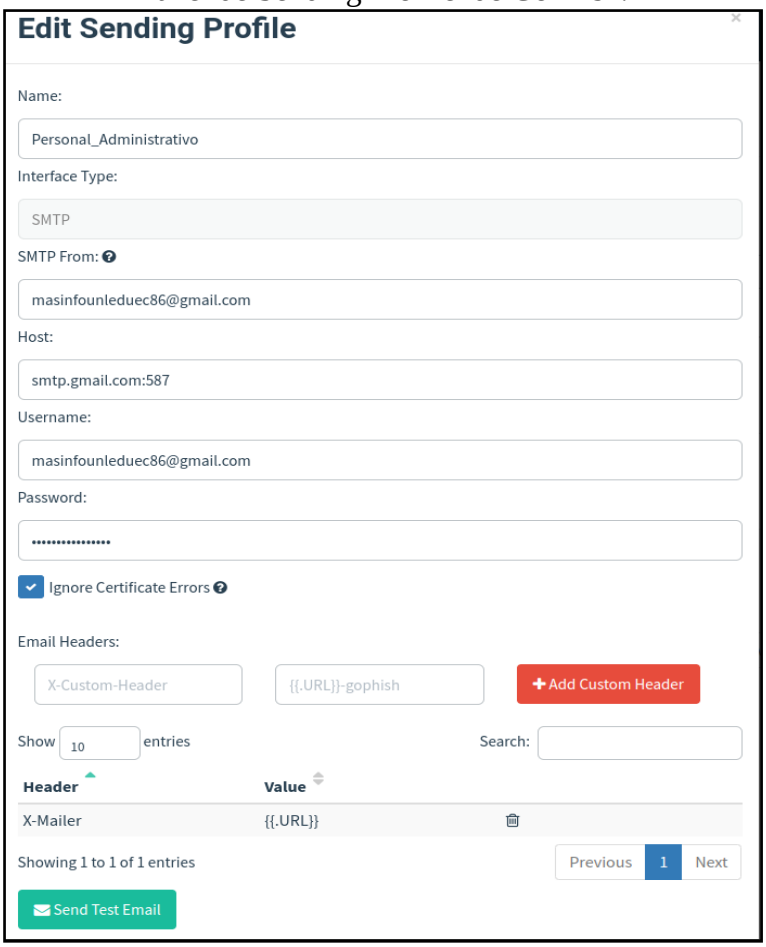


Fuente: El autor

5.3.5.2.Sending Profiles

En este apartado se deben configurar los perfiles de la cuenta de correo que procederá a enviar a los distintos objetivos de la campaña.

Figura 18
Panel de Sending Profile de GoPhish.



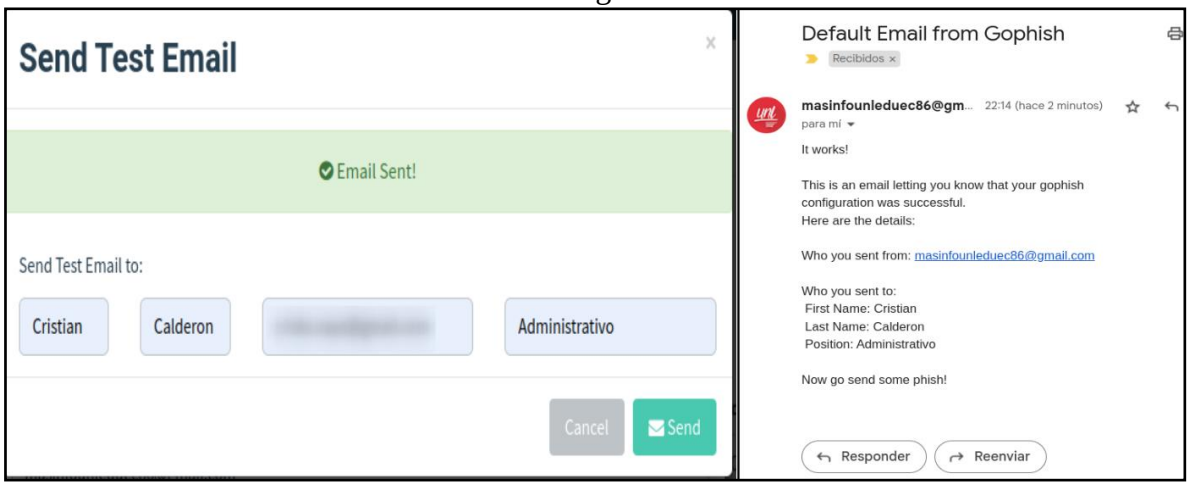
Fuente: El autor

- **Name**: Nombre con el que se va a identificar al perfil
- **Interface Type:** Actualmente GoPhish únicamente permite el uso de SMTP, por lo que esta será la configuración por defecto y la única que se admite.
- **SMTP From:** Este dato es muy importante ya que esto es lo que aparece en la cabecera From de los mensajes *SMTP* que se enviaran con este perfil.

- **Host**: Servidor correo a el que GoPhish enviará los mensajes de Phishing para que, a su vez, este lo envíe a los destinatarios. Aquí podemos usar servidores de correos gratuitos que usamos usualmente como *Outlook* o *Gmail*, o podemos usar nuestro propio servidor de correo.
- **Username**: cuenta de correo electrónico desde la que se enviarán los correos**.**
- **Password**: contraseña que fue habilitada con la opción ***"contraseña de aplicaciones"*** en el caso de *Gmail*, si se estuviera usando *Outlook* se ingresa la contraseña de inicio de sesión a cuenta.
- **Email Headers:** este campo es muy interesante debido a que podemos rellenar las cabeceras del protocolo *SMTP* con la información que se quiera.

Configurado todo se puede enviar un email de prueba ya sea a la misma cuenta registrada o a una cuenta diferente con el botón ***"Send Test Email"***, en cual se solicita el Nombre, Apellidos, Correo Electrónico y la posición dentro de la empresa, si el correo se entregó con éxito se mostrará el siguiente mensaje ***"email sent",*** mientras que en la bandeja de entrada de la cuenta que se ha elegido de prueba debe llegar un email parecido al siguiente:

Figura 19
Afirmación de la entrega del Perfil de Envío.

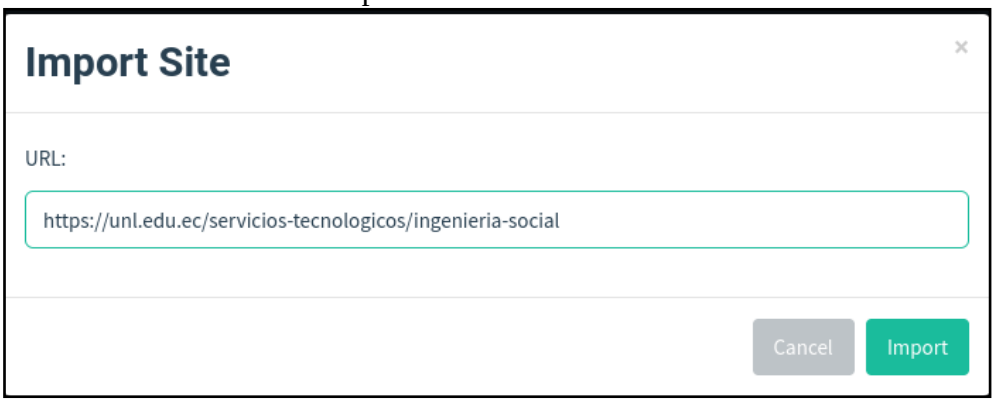


Fuente: El autor

5.3.5.3.Landing Pages

En esta sección se crean las páginas web que suplantan a una original para realizar un ataque de Phishing, para ello se hace uso de la facilidad que da GoPhish para suplantar páginas webs únicamente teniendo su URL, tal como se muestra en la siguiente imagen.

Figura 20
Importación del sitio Web.



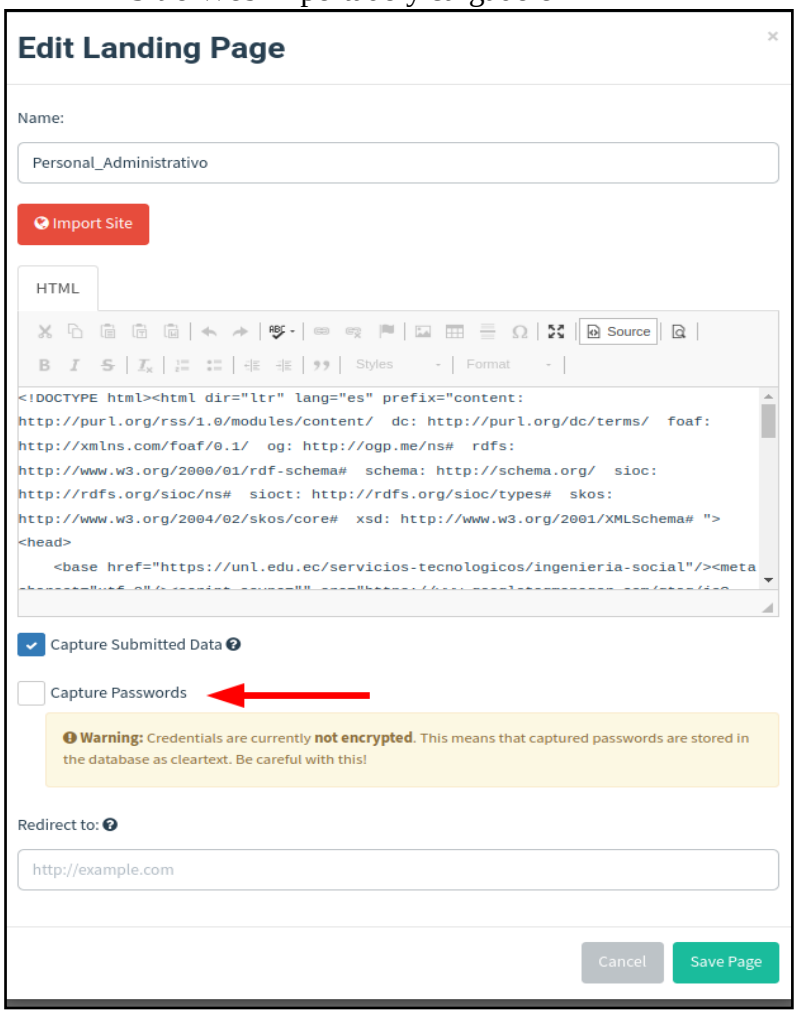
Fuente: El autor

Los campos que deben llenarse son los siguientes:

- **Name:** Un nombre descriptivo para identificar la página.
- **Import Site:** Se puede importar el diseño de una web que se vaya a suplantar, dando clic en Import site, copiar la URL del sitio web a suplantar, que en este caso es el sitio web, https://unl.edu.ec/servicios-tecnologicos/ingenieria-social, mismo que fue incorporado en la página web principal de la Universidad Nacional de Loja, con el contenido teórico con el mensaje de alerta al funcionario administrativo de la institución.
- **HTML:** Aquí se visualiza o se implementa el código HTML de la página web a suplantar, ya sea la que fue importada o en su defecto desarrollada por el atacante.
- **Capture Submitted Data:** Esta opción debe activarse únicamente si se requiere capturar los datos, marcar esta opción no significa que capturemos las contraseñas de los objetivos.
- **Capture Password:** Al marcar la opción anterior también se habilitarán dos opciones adicionales, una de ellas es para capturar las contraseñas de los usuarios ***"Capture Password".***

Figura 21

Sitio Web importado y cargado en HTML



Fuente: El autor

Habrá que tener cuidado con esta opción y estar seguros de que se tiene el GoPhish alojado de forma segura ya que las contraseñas se almacenarán en claro, mientras que la segunda opción es para redirigir a la víctima al sitio web verdadero ***"Redirect to".***

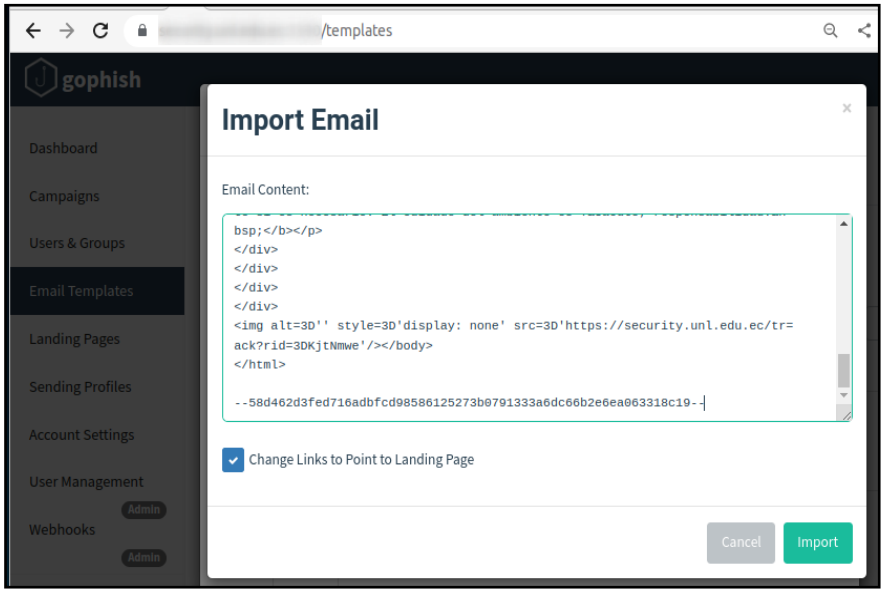
Cabe mencionar que la presente investigación es únicamente con fines investigativos por lo que se respetará estrictamente la ética y confidencialidad de la información, razón por la cual, no se ha marcado la opción de ***"capture password"*** ya que el objetivo no es capturar información confidencial.

5.3.5.4.Email Template

En este apartado se crean la o las plantillas de los correos electrónicos falsos que se enviarán a los objetivos de la campaña, para este caso se enviará el correo electrónico que fue creado el cual contiene mensajes persuasivos y propagandísticos, y que redirige hacia el sitio web que se aloja en la página web principal de la Universidad Nacional de Loja, tal como se describe en los apartado anteriores.

Figura 22

Importación del correo electrónico.



Fuente: El autor

Así mismo dentro de la plantilla hay una serie de opciones que deben configurar como son:

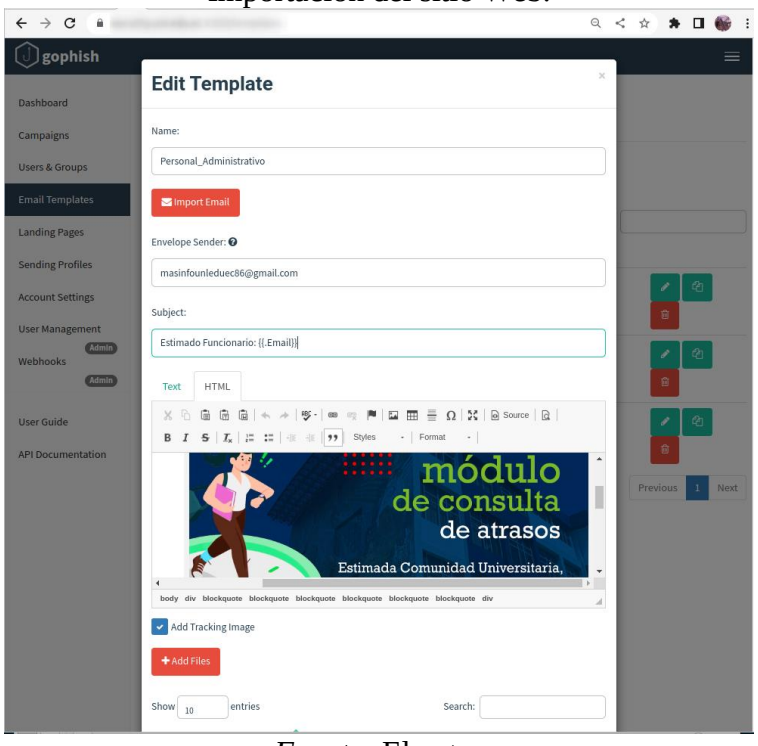
- **Name**: Nombre de la plantilla creada.
- **Import Email:** Se puede importar un email si se tiene su contenido.
- **Subject:** asunto que aparecerá en el correo electrónico que se mandará a los usuarios.
- **Text/HTML:** En caso de que no se importe el correo electrónico en este apartado se escribirá el email que será enviado a los objetivos de la campaña. Para que los correos sean individuales y personalizados para cada usuario, tomando en cuenta el siguiente formato {{.Nombre Variable}}, entre las más relevantes tenemos:

Tabla 7
Variables de GoPhish.

VARIABLE	DESCRIPCION
{{.RId}}	Identificador del usuario.
{{.FirstName}}	Nombre del usuario, definido en el apartado de Users & Groups.
{{.LastN ame}}	Apellidos del usuario, definido en el apartado de Users & Groups
{{.Position}}	Posición del usuario, definido en el apartado de Users & Groups.
{{.Email}}	Correo electrónico del usuario, definido en el apartado de Users & Groups.
{{.From}}	Persona que queremos suplantar en la campaña de Phishing.
{{.TrackingURL}}	URL utilizada para el tracking al usuario.
{{.Tracker}}	Imagen utilizada en el correo para conocer si el usuario abrió o no.
{{.URL}}	URL desde la que se realiza el Phishing.
{{.BaseURL}}	URL del servidor de Phishing pero sin el identificador (rid) de la URL

Fuente: El autor

Figura 23
Importación del sitio Web.



Fuente: El autor

- **Add Files:** Aquí se puede añadir un adjunto a la plantilla de correo electrónico, viéndolo desde el del hacking ético se podría añadir un documento informativo sobre lo peligroso que hubiese sido abrir un fichero infectado en un correo electrónico de un ataque real.

5.3.5.5.Users & Groups

La plantilla de "Usuarios y Grupos" de la plataforma GoPhish se utiliza para crear y gestionar usuarios y/o grupos de usuarios, es decir aquí se ingresa la población que recibirán los correos electrónicos con la simulación del Ataque Phishing, antes de explicar los detalles de la configuración de este apartado es necesario definir los grupos que serán que serán ingresados.

Como se mencionó en el apartado **(Población de Estudio),** se tiene un universo de 1220 funcionarios dentro de la institución, por lo que es necesario segmentarlos en grupos más pequeños para evitar que el servidor de correos los bloque o sean enviados a bandeja de SPAM, o en el peor de los casos sea bloqueada la cuenta desde donde se está enviando la campaña Phishing.

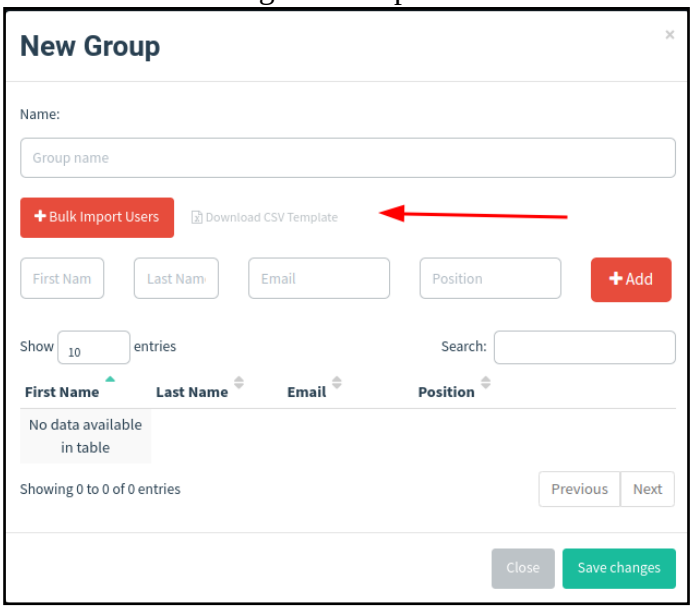
Tabla 8
Distribución de Grupos.

PERFIL	CANTIDAD	CORREO ELECTRÓNICO ASOCIADO	GRUPOS	CANTIDAD POR GRUPO
Personal Docente	780	masinfor.unl.edu.ec@gmail.com massinfo.unl.edu.ec@gmail.com	Personal Docente G1	130
			Personal Docente G2	130
			Personal Docente G3	130
			Personal Docente G4	130
			Personal Docente G5	130
			Personal Docente G6	130
Personal Administrativo	440	masinfounleduec86@gmail.com	Personal Administrativo G1	110
			Personal Administrativo G2	110
			Personal Administrativo G3	110
			Personal Administrativo G4	110
Muestra Total	1220	Total correos electrónicos 3	Total Grupos 10	Total correos a enviar 1220

Fuente: El autor

GoPhish da la opción a descargar un fichero ***.csv*** de ejemplo para saber cómo se debe rellenar la información, con la opción ***"Download csv Template"*** que aparece a la derecha de ***"Bulk Import Users".***

Figura 24
Descarga de Templete .csv.



Fuente: El autor

El fichero ***.csv***, tiene definida la estructura donde se debe rellenar los datos como: Nombres, Apellidos, Correo Electrónico y posición en la empresa, tal como se muestra en la siguiente figura:

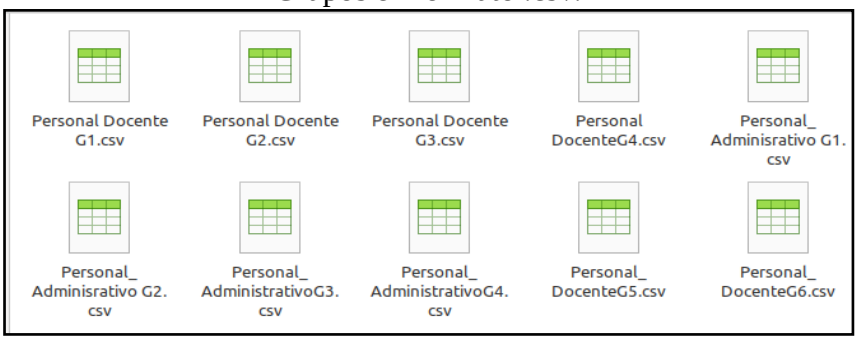
Figura 25
Fichero .csv de GoPhish

Fuente: El autor

Se debe mencionar que poder enviar toda esta cantidad de correos y evitar que se bloquean o se envíen a SPAM los correo electrónicos, se dividió en grupos más pequeños con un formato .csv siguiendo los lineamientos que requiere GoPhish, estos grupos se asignaron a cada uno de los correos creados, En la siguiente figura, se muestran los grupos creados en el formato .csv, que requiere GoPhish mismo que posteriormente fueron cargados al sistema.

Figura 26

Grupos en formato .csv.



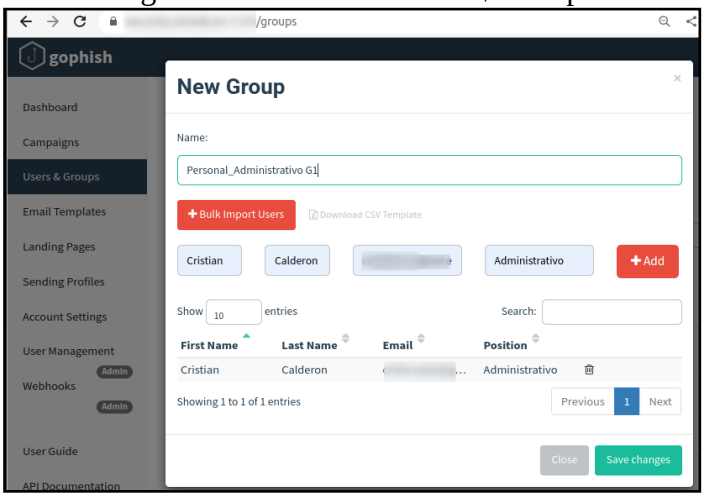
Fuente: El autor

Para cargar cada uno de los grupos a la plataforma GoPhish existen dos formas de hacerlo:

- **Primera:** Este método es más sencillo si no se tiene una lista previa en un fichero ***.csv*** aunque es más lento ya que los datos que se ingresan como: Nombre, Apellidos, email y posición, se ingresan uno a uno con el botón ***Add.***

Figura 27

Página de creación de Users $ Groups

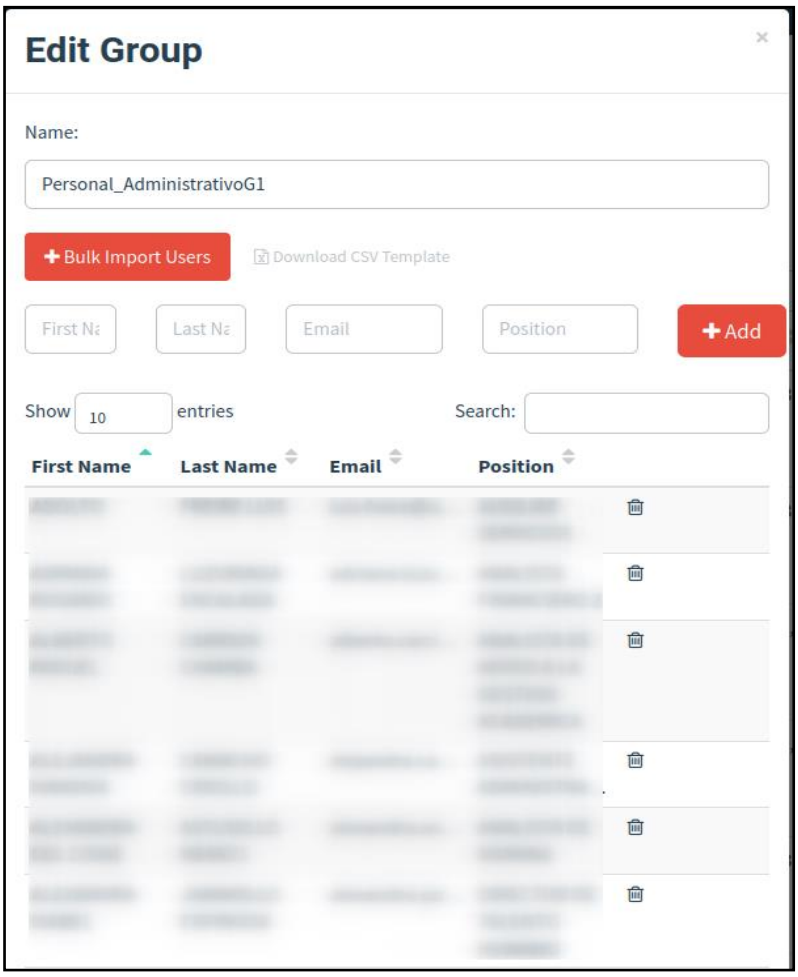


Fuente: El autor

- **Segunda:** Con el botón ***"Bulk Import User"*** se importa desde el directorio local los ficheros ***.csv***, que contienen los grupos, se agrega un nombre y se guardan los cambios.

Figura 28

Grupo 1 (Personal Administrativo G1)



Fuente: El autor

El total de grupos creados para la presente campaña fueron 10, tal como se muestra en la siguiente imagen:

Figura 29
Total de Grupos Creados

Fuente: El autor

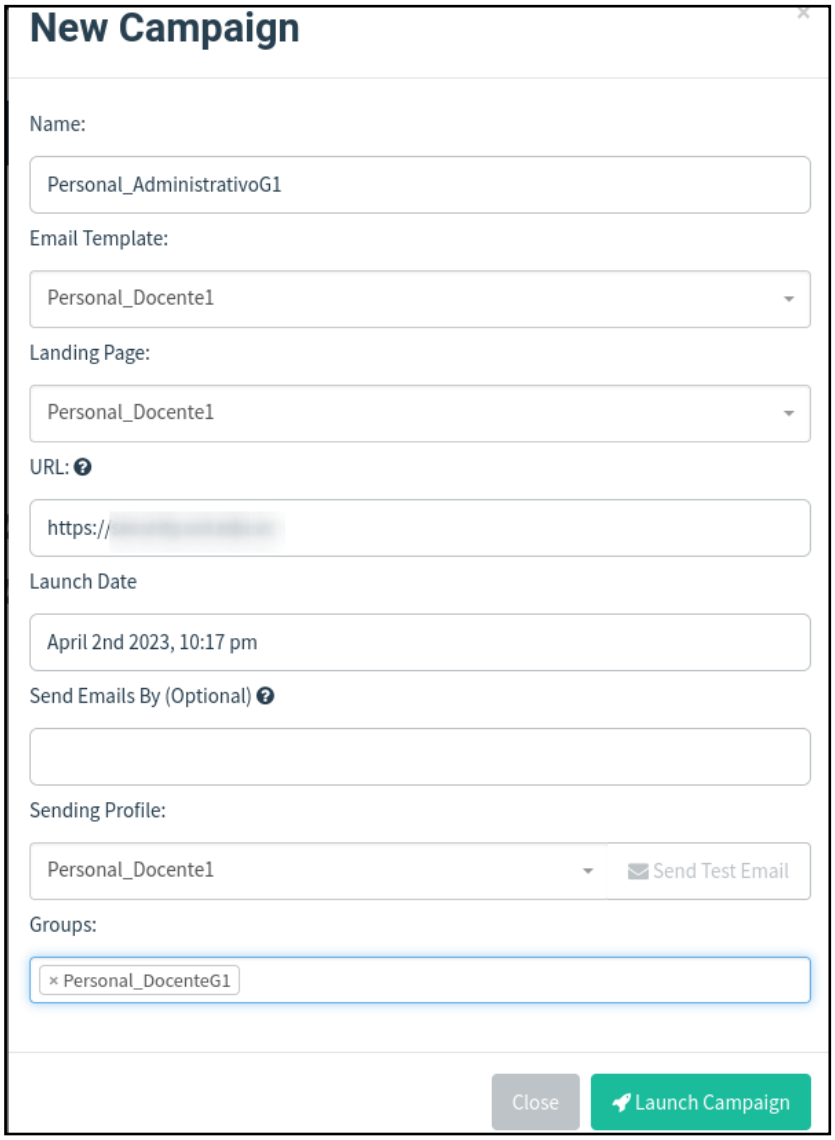
5.3.5.6.Campaing:

En este apartado se crea y se lanza la campaña hacia la población de estudio para ello es necesario configurar los siguientes parámetros:

- **Name:** Nombre con el que identificará la campaña.
- **Email template:** Correo electrónico que será enviado a los objetivos de la campaña.
- **Landing Page:** página web a la que apuntarán los diferentes enlaces (no necesariamente todos) del correo.
- **URL:** Se agrega la dirección IP, o Dominio del Servidor donde se aloja GoPhish.
- **Launch Date:** Fecha y hora en la que se programar y/o lanzar la campaña.
- **Send Emails By:** Es un parámetro opcional que ofrece GoPhish en donde se pueden enviar los correos de manera distribuida en el tiempo antes de lanzar la campaña.

- **Sending Profile:** Configuración de la cuenta que enviará los correos de Phishing en la campaña. Nuevamente desde aquí se podrá enviar un correo de prueba con la opción **"Send Test Email".**
- **Groups:** Grupos de objetivos para la campaña creada, se pueden seleccionar varios. Una vez creada se añadirá a la lista de campañas, y desde ahí podremos ver los resultados en tiempo real.

Figura 30
Página de creación de nueva campaña



Fuente: El autor

El número de campañas creadas es igual al número de grupos creados, las mismas que fueron enviadas en distintos horarios con el fin de que no se bloqueen los correos electrónicos enviados, cuya explicación se la realizó en el apartado ***Creación de Correo Electrónico,*** estas campañas se mantuvieron activas en un lapso de 20 horas aproximadamente quedando registradas las campañas tal como se evidencia en la siguiente imagen.

Figura 31
Total Campañas Creadas

Fuente: El autor

5.3.5.7.Dashboard

Una vez ejecutada la campaña se podrá ver los resultados en tiempo real dentro de la Dashboard, dentro de las principales estadísticas que se muestran podemos rescatar lo siguiente:

- **Email Sent.** Correo enviado.
- **Email Opened.** Correo enviado, esto se sabrá gracias al Tracker.
- **Clicked Link.** Si el usuario ha abierto alguno de los enlaces que apuntan a la URL de Phishing.

- **Submitted Data.** En caso de que se haya marcado la opción en la plantilla del correo, si se han capturado datos de formularios.
- **Email Reported.** Si se le ha configurado a nuestro usuario un monitor IMAP, podremos saber si los usuarios han reportado el Phishing enviado o no.

Así mismo recordemos que en el apartado Account Settings se habilitó la opción Show campaign results map para mostrar los resultados de cada campaña en un mapa, por si las víctimas accedieron a la campaña desde distintos países, y efectivamente se puede visualizar que se responden correos desde otros países como Estados unidos y México, tal como se muestra en la siguiente imagen:

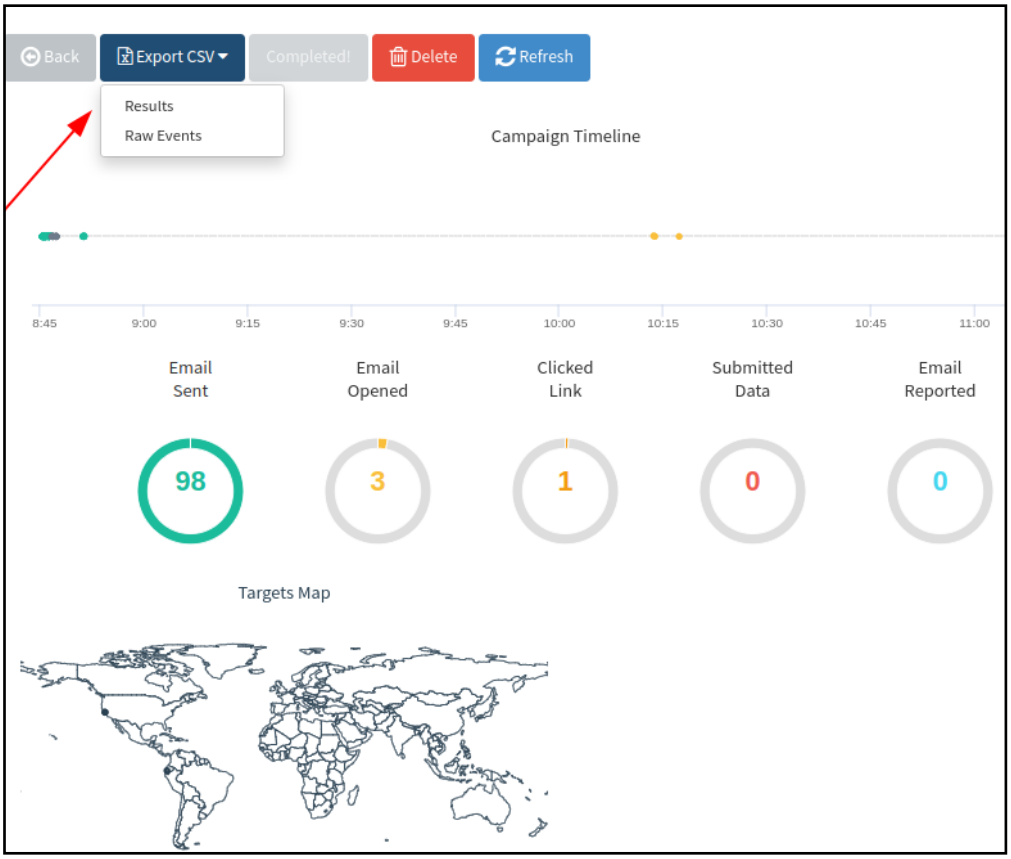
Figura 32
Resultados de un grupo de campaña y con usuarios de otros países.

Fuente: El autor

5.3.5.8.Interpretando campañas

GoPhish tiene la facultad de mostrar datos estadísticos con más detalles, y poder realizar un análisis minucioso o de la víctima, estos son muy útiles para el personal encargado de la seguridad, para ello podemos descargar un archivo ***.scv***, se elige la campaña que se desea analizar entre sus principales botones está ***export csv***, el cual tiene dos opciones ***Result*** y ***Raw Events*** pudiendo descargar cualquiera de ellos para su posterior análisis.

Figura 33
Reportes de correo Fraudulentos a la DTI

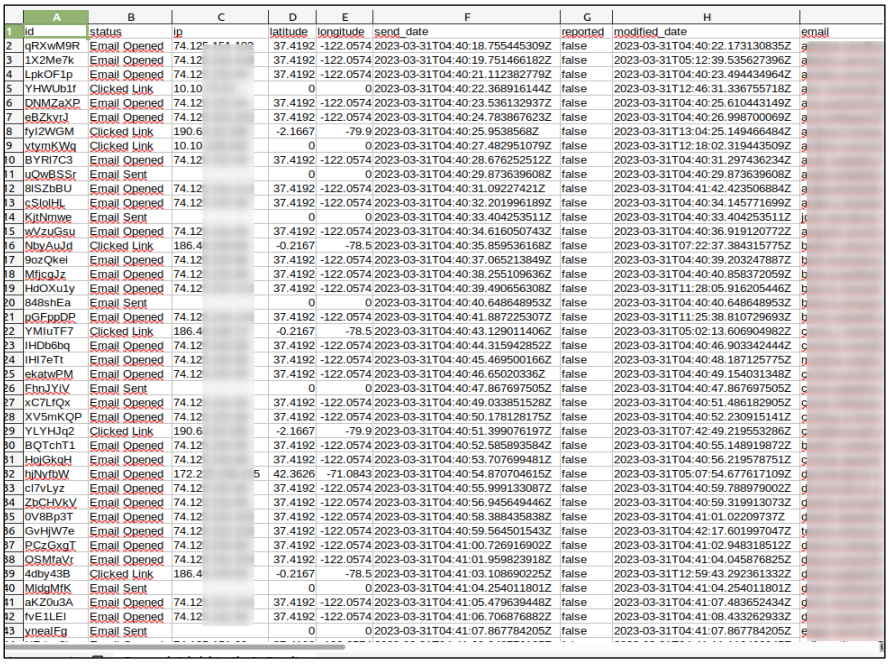


Fuente: El autor

Una vez descargados estos ficheros se puede analizar su contenido como por ejemplo desde qué IP y ubicación geográfica fue respondido el correo electrónico, entre otras cosas tal como se muestra en la siguiente imagen.

Figura 34

Detalle de Resultado de la campaña



	A	B	C	D	E	F	G	H	
1	id	status	ip	latitude	longitude	send_date	reported	modified_date	email
2	qRXwM9R	Email Opened	74.125.151.109	37.4192	-122.0574	2023-03-31T04:40:18.7554453097	false	2023-03-31T04:40:22.1731308357	a
3	1X2Me7k	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:19.7514661822	false	2023-03-31T05:12:39.5356273967	a
4	LpkOF1p	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:21.1123827792	false	2023-03-31T04:40:23.4944349647	a
5	YHWUb1f	Clicked Link	10.10	0	0	2023-03-31T04:40:22.3689161447	false	2023-03-31T12:46:31.3367557187	a
6	DNMZaXP	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:23.5361329377	false	2023-03-31T04:40:25.6104431497	a
7	eBZkvrJ	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:24.7838676237	false	2023-03-31T04:40:26.9987000697	a
8	fyI2WGM	Clicked Link	190.6	-2.1667	-79.9	2023-03-31T04:40:25.9538568Z	false	2023-03-31T13:04:25.1494664847	a
9	vtymKWq	Clicked Link	10.10	0	0	2023-03-31T04:40:27.4829510797	false	2023-03-31T12:18:02.3194435097	a
10	BYRI7C3	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:28.6762525127	false	2023-03-31T04:40:31.2974362347	a
11	uQwBSSr	Email Sent		0	0	2023-03-31T04:40:29.8736396087	false	2023-03-31T04:40:29.8736396087	a
12	8ISZbBU	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:31.09227421Z	false	2023-03-31T04:41:42.4235068847	a
13	cSlolHL	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:32.2019961897	false	2023-03-31T04:40:34.1457716997	a
14	KjtNmwe	Email Sent		0	0	2023-03-31T04:40:33.4042535117	false	2023-03-31T04:40:33.4042535117	j
15	wVzuGsu	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:34.6160507437	false	2023-03-31T04:40:36.9191207727	a
16	NbyAuJd	Clicked Link	186.4	-0.2167	-78.5	2023-03-31T04:40:35.8595361687	false	2023-03-31T07:22:37.3843157757	b
17	9ozQkei	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:37.0652138497	false	2023-03-31T04:40:39.2032478877	b
18	MfjcgJz	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:38.2551096367	false	2023-03-31T04:40:40.8583720597	b
19	HdOXu1y	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:39.4906563087	false	2023-03-31T11:28:05.9162054467	b
20	848shEa	Email Sent		0	0	2023-03-31T04:40:40.6486489537	false	2023-03-31T04:40:40.6486489537	b
21	pGFppDP	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:41.8872253077	false	2023-03-31T11:25:38.8107296937	b
22	YMluTF7	Clicked Link	186.4	-0.2167	-78.5	2023-03-31T04:40:43.1290114067	false	2023-03-31T05:02:13.6069049827	c
23	IHDb6bq	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:44.3159428527	false	2023-03-31T04:40:46.9033424447	c
24	IHI7eTt	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:45.4695001667	false	2023-03-31T04:40:48.187125775Z	n
25	ekatwPM	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:46.65020336Z	false	2023-03-31T04:40:49.1540313487	c
26	FbnJYiV	Email Sent		0	0	2023-03-31T04:40:47.8676975057	false	2023-03-31T04:40:47.8676975057	c
27	xC7LfQx	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:49.0338515287	false	2023-03-31T04:40:51.4861829057	c
28	XV5mKQP	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:50.1781281757	false	2023-03-31T04:40:52.2309151417	c
29	YLYHJq2	Clicked Link	190.6	-2.1667	-79.9	2023-03-31T04:40:51.3990761977	false	2023-03-31T07:42:49.2195532867	c
30	BQTchT1	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:52.5858935847	false	2023-03-31T04:40:55.1489198727	b
31	HojGkqH	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:53.7076994817	false	2023-03-31T04:40:56.2195787517	c
32	hjNyfbW	Email Opened	172.2	42.3626	-71.0843	2023-03-31T04:40:54.8707046157	false	2023-03-31T05:07:54.6776171097	d
33	cl7vLyz	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:55.9991330877	false	2023-03-31T04:40:59.7889790027	d
34	ZbCHVkV	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:56.9456494467	false	2023-03-31T04:40:59.3199130737	d
35	0V8Bp3T	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:58.3884358387	false	2023-03-31T04:41:01.02209737Z	d
36	GvHjW7e	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:40:59.5645015437	false	2023-03-31T04:42:17.6019970477	te
37	PCzGxgT	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:41:00.7269169027	false	2023-03-31T04:41:02.9483185127	d
38	QSMfaVr	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:41:01.9598239187	false	2023-03-31T04:41:04.0458768257	d
39	4dby43B	Clicked Link	186.4	-0.2167	-78.5	2023-03-31T04:41:03.1086902257	false	2023-03-31T12:59:43.2923613327	d
40	MldgMfK	Email Sent		0	0	2023-03-31T04:41:04.2540118017	false	2023-03-31T04:41:04.2540118017	d
41	aKZ0u3A	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:41:05.4796394487	false	2023-03-31T04:41:07.4836524347	d
42	fvE1LEl	Email Opened	74.12	37.4192	-122.0574	2023-03-31T04:41:06.7068768827	false	2023-03-31T04:41:08.4332629337	d
43	ynealEg	Email Sent		0	0	2023-03-31T04:41:07.8677842057	false	2023-03-31T04:41:07.8677842057	e

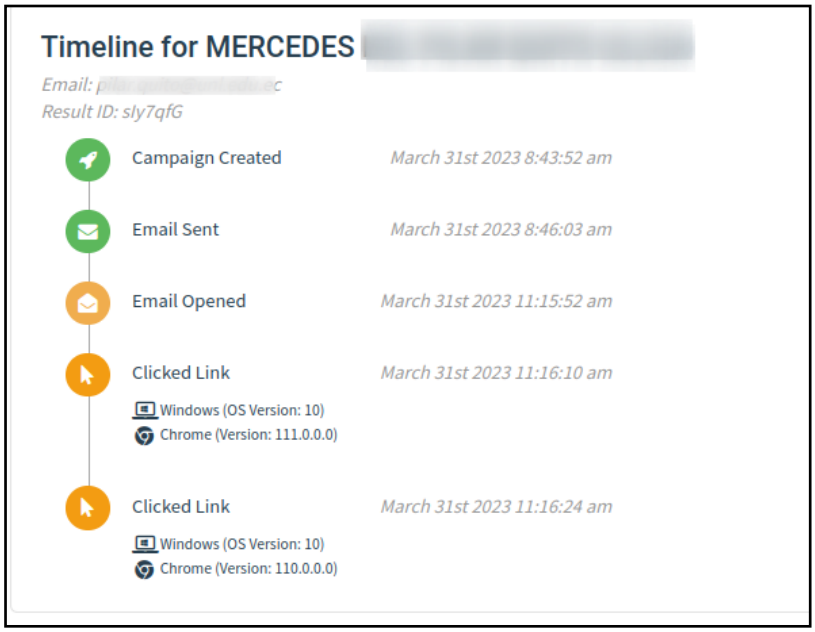
Fuente: El autor

Finalmente, GoPhish ofrece un historial de seguimiento de la campaña de manera individual, es decir, se puede visualizar información confidencial de la víctima de forma puntualizada:

- Creación de la campaña.
- Correo de envío.
- Correo abierto.
- Correo cliqueado.

En esta última opción se puede monitorizar si el correo fue cliqueado una o varias veces, incluyendo desde qué dispositivo móvil fue cliqueado, qué sistema operativo tiene el dispositivo, que versión del navegador posee, así mismo, si la campaña tuviese el objetivo de capturar información confidencial también se mostrará dicha información en este apartado, todas las opciones descritas anteriormente con su respectiva fecha y hora de las acciones realizadas tal como se muestra en la siguiente imagen:

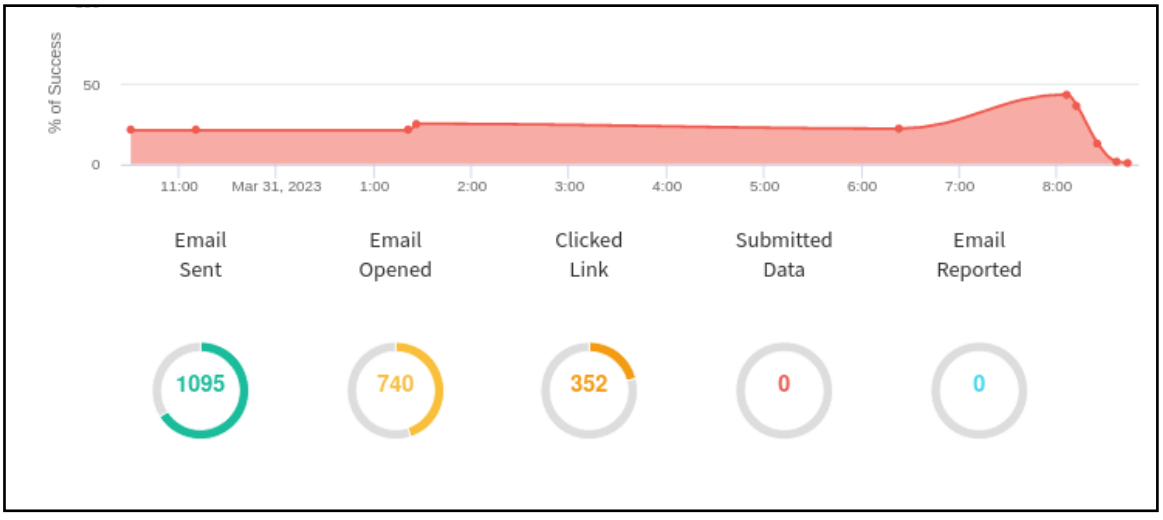
Figura 35
Detalle de monitoreo de la campaña



Fuente: El autor

Finalmente en el panel principal del Dashboard se muestran los resultados obtenidos de todo el consolidado de las campañas que fueron enviadas en los diferentes grupos (Personal Administrativo, Personal Docente) tal como se muestra en la siguiente imagen.

Figura 36
Resultados de la campaña.



Fuente: El autor

6. Resultados

Una vez obtenidos los resultados de la campaña se procede con el análisis de los datos que fueron capturados por la herramienta GoPhish, tal como se describe en las siguientes tablas:

Tabla 9

Resultados de la campaña al Personal Docente

POBLACIÓN TOTAL	GRUPO	CAMPAÑA	FECHA INICIO	FECHA FIN	CORREO ENVIADOS	CORREOS ABIERTOS	LINK CLIQUEADO	CAPTURA DE DATOS	EMAIL REPORTADOS
780	Personal_DocenteG1	Personal_DocenteG1	March 31st 2023, 1:21:14 am	March 31st 2023, 18:00:52 pm	105	101	48	0	0
	Personal_DocenteG2	Personal_DocenteG2	March 31st 2023, 1:26:19 am	March 31st 2023, 18:00:52 pm	121	116	57	0	0
	Personal_DocenteG3	Personal_DocenteG3	March 31st 2023, 6:22:48 am	March 31st 2023, 18:00:52 pm	117	99	49	0	0
	Personal_DocenteG4	Personal_DocenteG4	March 31st 2023, 8:24:51 am	March 31st 2023, 18:00:52 pm	123	28	16	0	0
	Personal_DocenteG5	Personal_DocenteG5	March 31st 2023, 8:36:27 am	March 31st 2023, 18:00:52 pm	107	5	3	0	0
	Personal_DocenteG6	Personal_DocenteG6	March 31st 2023, 8:43:52 am	March 31st 2023, 18:00:52 pm	98	3	1	0	0
Total 1220	**Total Grupos: 10**	**Total Campañas: 10**	**Total horas 20**		**671**	**352**	**174**	**0**	**0**
				Porcentajes	**86,03%**	**52,46**	**25,93**	**0,00%**	**0,00%**

Fuente: El autor

Tabla 10

Resultados de la campaña al Personal Administrativo

POBLACIÓN TOTAL	GRUPO	CAMPAÑA	FECHA INICIO	FECHA FIN	CORREO ENVIADOS	CORREOS ABIERTOS	LINK CLIQUEADO	CAPTURA DE DATOS	EMAIL REPORTADOS
440	Personal_AdministrativoG1	Personal_AdministrativoG1	March 30th 2023, 10:30:18 pm	March 31st 2023, 18:00:52 pm	103	101	46	0	0
	Personal_AdministrativoG2	Personal_AdministrativoG2	March 30th 2023, 11:10:29 pm	March 31st 2023, 18:00:52 pm	104	96	46	0	0
	Personal_AdministrativoG3	Personal_AdministrativoG3	March 31st 2023, 8:05:44 am	March 31st 2023, 18:00:52 pm	108	102	40	0	0
	Personal_AdministrativoG4	Personal_AdministrativoG4	March 31st 2023, 8:12:05 am	March 31st 2023, 18:00:52 pm	109	89	40	0	0
Total 1220	**Total Grupos: 4**	**Total Campañas: 4**	**Total horas 20**		**424**	**388**	**172**	**0**	**0**
				Porcentajes	**96,36%**	**91,51**	**40,57**	**0,00%**	**0,00%**

Fuente: El autor

Tabla 11

Resultados de la campaña de toda la población de estudio

POBLACIÓN TOTAL	GRUPO	CAMPAÑA	FECHA INICIO	FECHA FIN	CORREO ENVIADOS	CORREOS ABIERTOS	LINK CLIQUEADO	CAPTURA DE DATOS	EMAIL REPORTADOS
440	Personal_AdministrativoG1	Personal_AdministrativoG1	March 30th 2023, 10:30:18 pm	March 31st 2023, 18:00:52 pm	103	101	45	0	0
	Personal_AdministrativoG2	Personal_AdministrativoG2	March 30th 2023, 11:10:29 pm	March 31st 2023, 18:00:52 pm	104	96	46	0	0
	Personal_AdministrativoG3	Personal_AdministrativoG3	March 31st 2023, 8:05:44 am	March 31st 2023, 18:00:52 pm	108	102	40	0	0

POBLACIÓN TOTAL	GRUPO	CAMPAÑA	FECHA INICIO	FECHA FIN	CORREOS ENVIADOS	CORREOS ABIERTOS	LINK CLIQUEADO	CAPTURA DE DATOS	EMAIL REPORTADOS
780	Personal_AdministrativoG4	Personal_AdministrativoG4	March 31st 2023, 8:12:05 am	March 31st 2023, 18:00:52 pm	109	89	47	0	0
	Personal_DocenteG1	Personal_DocenteG1	March 31st 2023, 1:21:14 am	March 31st 2023, 18:00:52 pm	105	101	48	0	0
	Personal_DocenteG2	Personal_DocenteG2	March 31st 2023, 1:26:19 am	March 31st 2023, 18:00:52 pm	121	116	57	0	0
	Personal_DocenteG3	Personal_DocenteG3	March 31st 2023, 6:22:48 am	March 31st 2023, 18:00:52 pm	117	99	49	0	0
	Personal_DocenteG4	Personal_DocenteG4	March 31st 2023, 8:24:51 am	March 31st 2023, 18:00:52 pm	123	28	16	0	0
	Personal_DocenteG5	Personal_DocenteG5	March 31st 2023, 8:36:27 am	March 31st 2023, 18:00:52 pm	107	5	3	0	0
	Personal_DocenteG6	Personal_DocenteG6	March 31st 2023, 8:43:52 am	March 31st 2023, 18:00:52 pm	98	3	1	0	0
Total 1220	**Total Grupos: 10**	**Total Campañas: 10**	**Duración de la campaña 20 horas**		**Total: 1095**	**Total: 740**	**Total: 352**	**Total: 0**	**Total: 0**
		Porcentajes			**89,75**	**67,58**	**32,15**	**0,00**	**0,00**

Fuente: El autor

Tabla 12

Correo entregados & Correos no entregados

POBLACIÓN		CORREOS ENVIADOS	PORCENTAJE DE ENVÍO	COREOS NO ENVIADOS	PORCENTAJE DE PÉRDIDA
Personal Administrativo	440	424	96,36%	16	3,64%
Personal Docente	780	671	86,03%	109	13,97%
Total	**1220**	**1095**	**89,75%**	**125**	**10,24%**

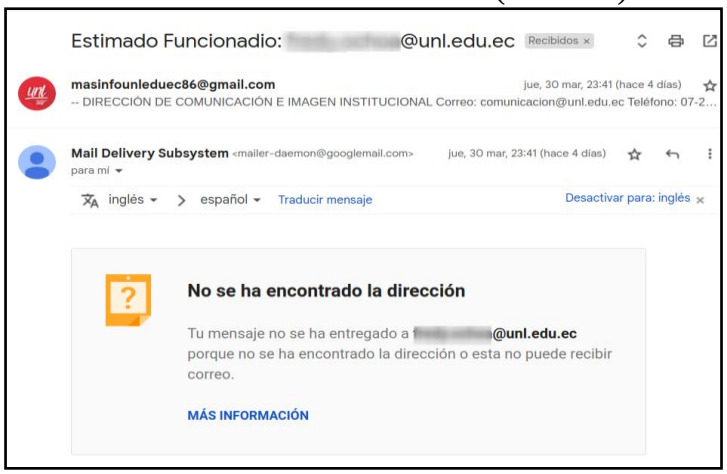
Fuente: El autor

La campaña se realizó durante 20 horas y se dividieron a la población en 10 grupos (4 de Personal Administrativo y 6 de Personal Docente) a los que se les enviaron correos electrónicos simulando un ataque de Phishing. Los resultados indican que se enviaron un total de 1095 correos electrónicos en la campaña de simulación de phishing. De estos, 740 fueron abiertos y 352 tuvieron clics en los enlaces (ver figura 35). Es importante destacar que esta campaña se llevó a cabo únicamente con fines éticos y educativos, por lo que no se capturaron datos ni se reportaron correos electrónicos sospechosos. En general, la campaña obtuvo una buena tasa de participación y atención por parte de la población universitaria. Se registró una tasa de apertura de correo del 67,58% y una tasa de clics en los enlaces del 32,15%. Esto significa que aproximadamente un tercio de los destinatarios cayeron en la trampa del phishing e hicieron clic en el enlace malicioso incluido en el correo. Estos resultados son útiles para evaluar la efectividad del simulacro y detectar áreas de mejora en la concienciación y formación en seguridad cibernética de los funcionarios de la institución. Es importante proporcionar retroalimentación y orientación a los funcionarios que han caído en la trampa del phishing para ayudarles a evitar futuras amenazas. Así mismo es necesario mencionar las razones por que no todos los correos fueron entregados ya que existe una pérdida de un total de 125 correos equivalente al 10,24% del total de la población, esto se produjo las siguientes razones:

No se encontró la dirección de algunos de estos correos electrónicos (rebotaron)

Figura 37

Correo electrónico no enviado (rebotado)

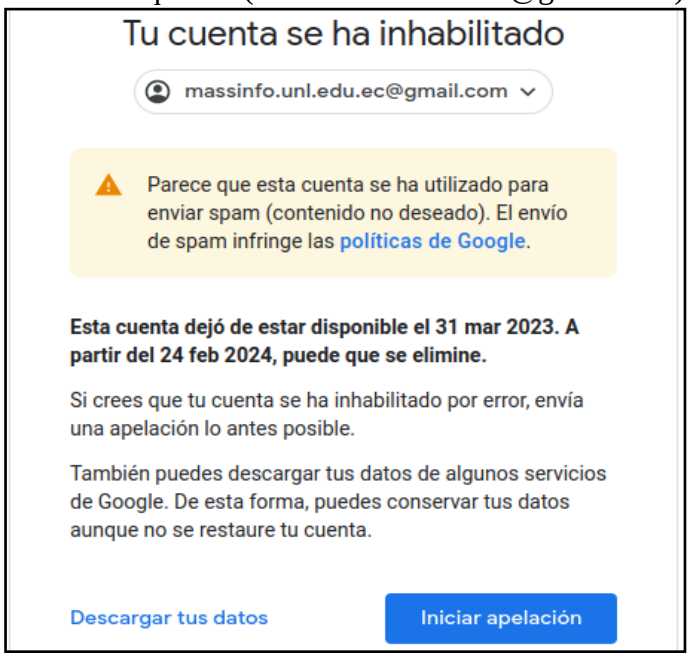


Fuente: El autor

Una de las cuentas creadas fue bloqueada, después de haber realizado algunas entregas.

Figura 38

Cuenta bloqueada (massinfo.unl.edu.ec@gmail.com)

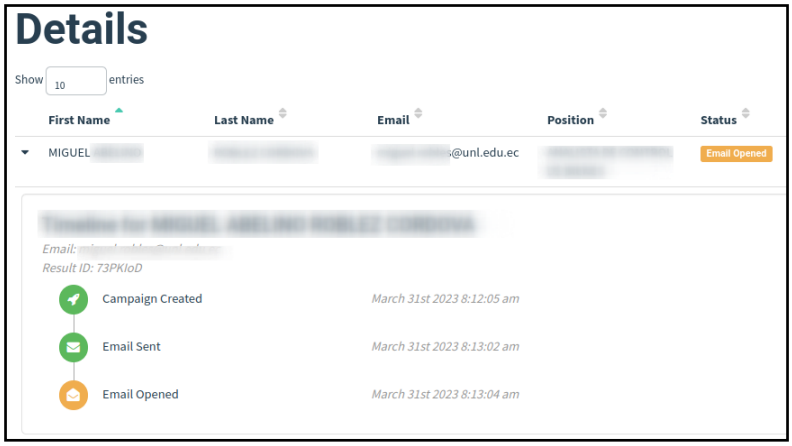


Fuente: El autor

Por otra parte se hace notar que existen funcionarios que tienen configurados sus correos electrónicos con la opción **"Activar respuesta automática"** por lo que la herramienta GoPhish lo considera como un correo abierto tal como se muestra en la siguiente imagen:

Figura 39

GoPhish detectando un correo abierto

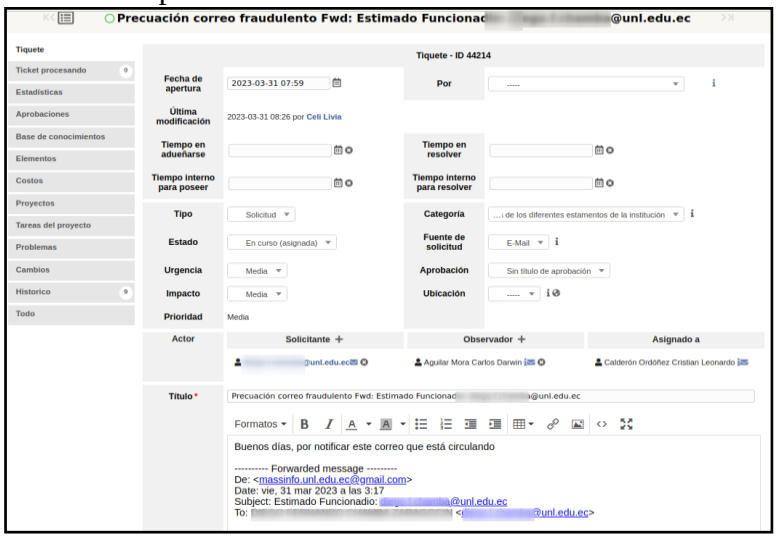


Fuente: El autor

De igual manera algunos funcionarios se dieron cuenta de que era un correo falso o engañoso, por lo que procedieron a reportarlo a la mesa de servicio a través del correo electrónico soporte.uti@unl.edu.ec o por otros medios no oficiales como (llamadas telefónicas)

Figura 40

Reportes de correo Fraudulentos a la DTI



Fuente: El autor

6.1.Campaña de concientización a la Comunidad Universitaria

Una vez obtenidos los resultados y haber identificado que existen un número considerable de la población que ha caído en el engaño del ataque Phishing 31,60%, se realiza una retroalimentación con algunas recomendaciones para alertar a la comunidad universitaria que se mantenga atenta y preparada evitando que sea víctima de esta modalidad de ataques informáticos, siendo su objetivo principal apoderarse de los datos confidenciales y/o personales de los funcionarios. Dicha capacitación se lo realizará a través de un correo electrónico institucional masinfo@unl.edu.ec por medio del departamento de la *Dirección de Comunicación e Imagen Institucional*, hacia toda la comunidad universitaria cuyo se detalla en los siguientes párrafos:

6.2.Elaboración de correo electrónico de concientización.

Asunto: ***Campaña de concientización sobre Phishing***

Estimada Comunidad Universitaria:

La Dirección de Tecnologías de Información en colaboración con el Ing. Cristian Leonardo Calderón Ordoñez, maestrante de Telecomunicaciones de la UNL, realizaron una simulación de un ataque de Ingeniería Social bajo la modalidad Phishing, que consistió en simular un ataque perpetrado por un ciberdelincuente para apropiarse de sus datos.

Es importante estar alerta y tomar medidas preventivas para protegerse contra este tipo de fraudes.

Revise las siguientes recomendaciones:

Figura 41

Recomendaciones de técnicas anti phishing

Fuente: El autor

Te invitamos a difundir esta información a la comunidad universitaria, tus amigos y familiares, para que todos estén informados y protegidos contra los ataques de phishing.

Tabla 13

Botón de Dirección a un micro sitio web

Conozca más sobre mas sobre la prevención de ataques cibernéticos

Fuente: El autor

Para reportar cualquier incidente de ciberseguridad escribir a soporte.dti@unl.edu.ec

Figura 42

Correo enviado en la campaña de concientización

Fuente: El autor

Recordemos que durante la campaña de simulación de ataques phishing, se creó un micrositio web en la página principal de la Universidad Nacional de Loja para alentar a la comunidad universitaria a tomar medidas de prevención y concienciar sobre las técnicas de prevención de ataques phishing. En dicho sitio se agregó contenido informativo sobre los ataques phishing en el sitio y se incluyó un botón de dirección dentro del correo electrónico para que el personal pudiera acceder fácilmente al sitio y mejorar su capacidad para detectar y prevenir este tipo de amenazas.

6.3.Contenido del micrositio web para la concientización.

Evite ser víctimas de ataques de Ingeniería social

6.3.1. Conoce más sobre el Phishing

El Phishing es una combinación de técnicas de engaño y manipulación para obtener datos confidenciales como contraseñas, información bancaria, etc. Su objetivo es lucrar a través del robo de dinero de cuentas bancarias, tarjetas de crédito, chantajes, entre otros comportamientos delictivos.

Figura 43
Robo de Credenciales

Fuente: El autor

Los ataques de Phishing se llevan a cabo principalmente mediante correos electrónicos falsos que imitan a entidades confiables, como bancos o empresas comerciales. Estos correos electrónicos contienen enlaces que conducen a sitios web falsos donde se solicita información personal o confidencial. En la siguiente imagen se describe la información que los ciberdelincuentes buscan obtener y los medios de comunicación que utilizan para propagar sus ataques.

Figura 44

Robo de Información y medios de Propagación del Phishing.

Fuente: El autor

6.3.2. Fases de un ataque Phishing.

- Investigación y selección del objetivo: El atacante investiga y elige a su objetivo.
- Creación del mensaje: El atacante crea un mensaje de correo electrónico o de texto convincente que parece legítimo para engañar al objetivo.

- Envío del mensaje: El atacante envía el mensaje a la lista de contactos del objetivo.
- Engaño: El objetivo recibe el mensaje y es engañado para que haga clic en un enlace malicioso o para que revele información confidencial.
- Explotación: El atacante utiliza la información obtenida para acceder a sistemas o realizar fraudes.

Figura 45

Fases de un ataque Phishing.

Fuente: El autor

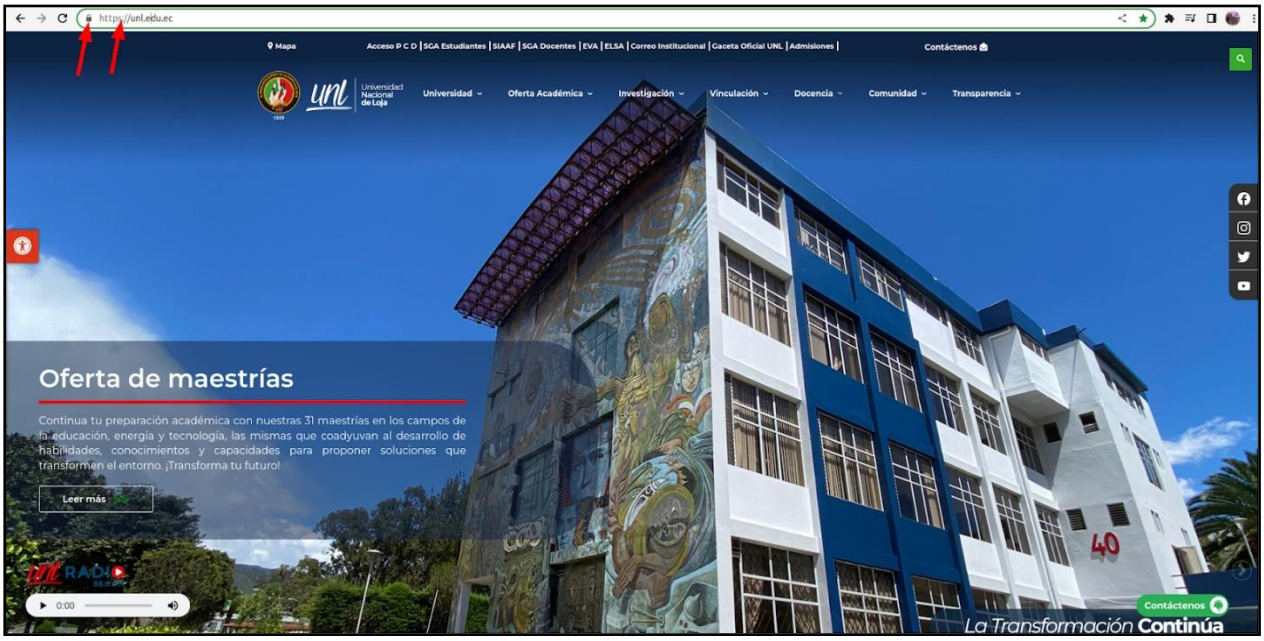
6.3.3. Cómo prevenir un ciberataque Phishing

- No hagas clic en enlaces sospechosos, si recibes un correo electrónico o mensaje de texto que parece sospechoso o no conoces al remitente, no hagas clic en ningún enlace ni descargues ningún archivo adjunto.
- Verifica la autenticidad del remitente antes de hacer clic en cualquier enlace o proporcionar información personal, asegúrate de verificar que el remitente sea legítimo.

- No compartas información personal como contraseñas o números de tarjeta de crédito, a menos que estés seguro de que el sitio web o servicio es legítimo y confiable.
- Revise que el sitio web sea seguro verificando que éste muestre un ícono de candado a la izquierda del URL y las siglas *"**https**"*. Por ningún motivo abra páginas inseguras que muestren únicamente las siglas *"**http**"* y peor aún ingreses datos personales en estos sitios.

Figura 46

Estructura de un sitio web seguro.



Fuente: El autor

Es importante que todos estemos al tanto de los peligros del Phishing y que tomemos medidas para proteger nuestra información personal e institucional. Si tienes alguna duda o sospecha de un posible ataque de Phishing, comunícate con la Dirección de Tecnologías de Información de la Universidad. soporte.dti@unl.edu.ec

6.4.Cómo Identificar un Correo Fraudulento

El correo electrónico es un medio de comunicación oficial dentro de una institución, razón por la cual los ciberdelincuentes utilizan este medio de comunicación para realizar estafas y robo de información. A continuación se presentan las características más comunes de correos electrónicos de Phishing, así como una guía que te ayudará a identificar un correo falso.

Tabla 14

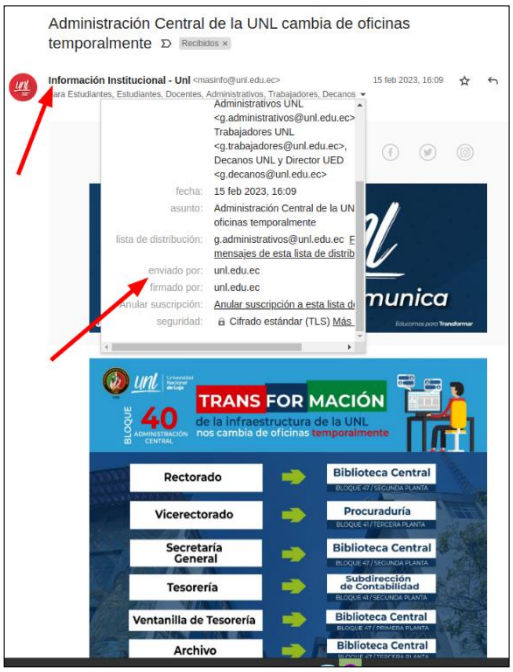
Comparativa de correos electrónicos.

En la siguiente imagen, a la izquierda se muestra un correo oficial de la institución y a la derecha una falsificación que busca robar sus datos, instalar un virus, comprometer los sistemas institucionales, etc.	
CORREO ENVIADO POR LA INSTITUCIÓN	**CORREO ENVIADO POR UN CIBER DELINCUENTE**
	

Es muy importante antes de abrir un correo electrónico verificar siempre el remitente, cuando se trata de un correo institucional, están bajo el dominio "@unl.edu.ec" si encuentra este dominio alterado elimínelo de inmediato o márquelo como SPAM, y si el correo es de un tercero,

verifique bien el remitente y acepte los correos únicamente si conoce la fuente o el origen, caso contrario eliminarlos y evite abrir su contenido (adjuntos, enlaces, etc.)

CORREO ENVIADO POR LA INSTITUCIÓN

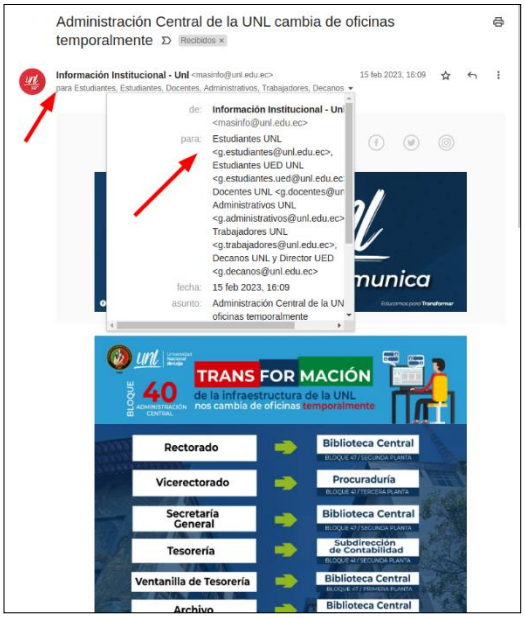


CORREO ENVIADO POR UN CIBER DELINCUENTE

Los correos de carácter informativo siempre son enviados a un grupo determinado de personas, si detecta que un correo informativo está dirigido exclusivamente para usted, dude y revise bien el remitente.

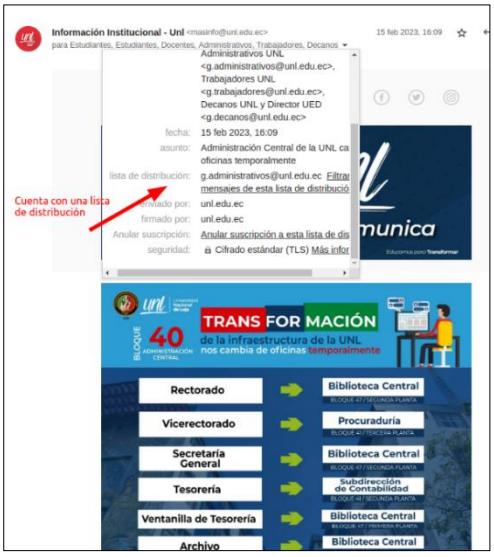
CORREO ENVIADO POR LA INSTITUCIÓN

CORREO ENVIADO POR UN CIBER DELINCUENTE

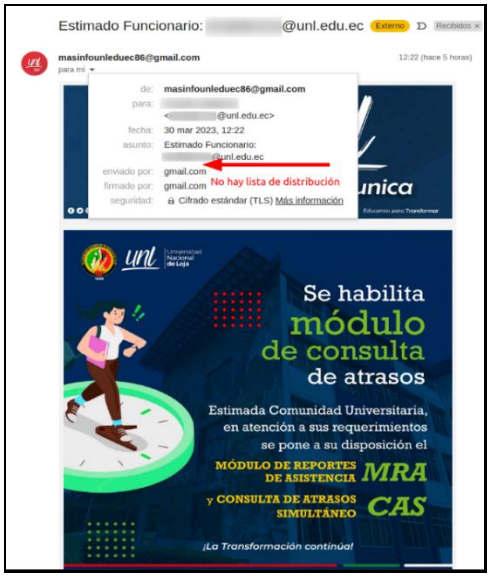


Así mismo los correos institucionales suelen tener una lista de distribución la cual debe pertenecer a un dominio "@unl.edu.ec"

CORREO ENVIADO POR LA INSTITUCIÓN



CORREO ENVIADO POR UN CIBER DELINCUENTE



Fuente: Elaborada por el autor

Estimada Comunidad Universitaria, la *Dirección de Tecnologías de Información (DTI)* pone a su conocimiento las políticas de uso de correo electrónico, las cuales son de carácter general y de cumplimiento obligatorio para todos los estudiantes, docentes, empleados y trabajadores que tienen asignada una cuenta de correo con el dominio @unl.edu.ec. La cuenta de correo identifica de manera única a cada usuario, siendo personal e intransferible, por lo que, queda estrictamente prohibido dar a otros la posibilidad de uso. Los usuarios son completamente responsables de todas las actividades realizadas con su cuenta de correo electrónico institucional; mismo que deberán ser de carácter netamente institucional. Todo inconveniente presentado con su cuenta de correo, deberá tratarlo personalmente, mediante el envío de un correo desde su cuenta institucional a nuestra mesa de servicios soporte.dti@unl.edu.ec o acudiendo directamente a la DTI.
El buen uso de su cuenta se entiende por:

Utilizar contraseñas seguras, de longitud mayor a ocho caracteres y que contenga caracteres especiales.

- No compartir la contraseña de la cuenta de correo electrónico.
- Usar su cuenta con fines académicos y/o investigación.
- Depurar su cuenta de correo no deseado.
- Respetar las cuentas de otros usuarios.
- Respetar la privacidad de los mensajes y el destinatario.
- Usar un lenguaje apropiado en sus mensajes.
- No enviar ni contestar cadenas de correo.
- No usar su cuenta para fines comerciales ni de entretenimiento.
- No enviar material obsceno o con intención de intimidar, insultar o acosar.
- La publicación o divulgación de su cuenta de correo electrónico institucional en redes sociales u otras plataformas tecnológicas externas a la institución, expone al usuario a ser víctima de ciberataques (Ingeniería social, fraudes, robo de información, suplantación de identidad, otros).
- Las entidades bancarias e instituciones públicas, nunca le solicitarán información personal por medio del correo electrónico; si llega a recibir un correo de este tipo, informe a su entidad financiera.

- Para garantizar la confidencialidad de sus datos personales nunca deberá responder a correos de destinatarios anónimos (Desconocidos) o no deseados *(SPAM)*, mucho menos descargar archivos adjuntos ni abrir enlaces presentes en estos correos.
- El incumplimiento por parte del usuario en cuanto al buen uso de su cuenta puede ocasionar la suspensión y posterior baja de su cuenta.
  Para dudas e inquietudes enviarla desde su correo institucional a nuestra mesa de servicios soporte.dti@unl.edu.ec o mediante llamada telefónica 07 2547252 ext. 179 / 129.

Cabe mencionar que el contenido teórico descrito en esta sección, mismo que va a ser mostrado en la página web de la Universidad Nacional de Loja, fue enviado en texto editable ***(.docx)*** al personal de la *Dirección de Tecnologías de Información*, para que sea convertido a código *HTML* y que posteriormente fue implementado y publicado en el micro sitió de "Ingeniería Social", mismo que se encuentra ubicado en el siguiente enlace: https://unl.edu.ec/servicios-tecnologicos/ingenieria-social.

7. Discusión

En términos generales, la campaña se la realizó con éxitos, ya que se logró una tasa de apertura de correo del 67,58% y una tasa de clics en los enlaces del 32,15%, lo que corresponde a un tercio del total de población que ha caído en la trampa del Phishing y ha hecho clic en el enlace malicioso incluido en el correo, esto se debe a la implementación de diseños similares para la falsificación del correo electrónico que utiliza la Universidad Nacional de Loja para informar de eventos masivos.

Existen proyectos de investigación con características similares al presente caso de investigación, como es el caso realizado por: **"*Francisco Javier Jiménez Olmedo de la Universidad de Sevilla Dpto. Ingeniería Telemática denominado Implantación de una herramienta que permita desarrollar campañas de phishing* en el año 2020",** donde se realiza una simulación de un ataque Phishing por medio de la herramienta GoPhish, cuyo objetivo es identificar la cantidad de funcionarios de una institución que son posibles víctimas de esta modalidad de ataque, para posteriormente hacer una campaña de concientización en técnicas de anti phishing con el fin de educarlo, y prepararlo y evitar que sea víctima de un ataque de estas características resguardando así su información confidencial ya sea personal o institucional.

Por todo lo antes mencionado, se determina que siempre va a existir un número considerable de personas dentro de una institución u organización que desconoce este tipo de ataques, ya sea por falta de capacitación del departamento encargado de la seguridad informática o simplemente no son cuidadosos a la hora de abrir un correo electrónico y poder identificar que se trate de un correo electrónico verídico o ficticio, por ende se hace necesario realizar este tipo de simulaciones y mejor manera de hacerlo de algún tipo de herramienta informáticas que respalden y automaticen los resultados para luego poder determinar y ejecutar acciones que eviten ser víctimas de un ataque informático de ingeniería social bajo la modalidad de Phishing.

Por otra y como era de esperarse surgieron algunas limitaciones sobre todo en la ejecución de la campaña principalmente en el envío de correos electrónicos debido a los siguientes factores:

GoPhish tiene un número límite (100-130) para el envío de correos masivos por cada campaña.

Gmail permite enviar hasta 500 correos dentro de las 24 horas, sin embargo esto puede variar dependiendo de la antigüedad de la cuenta, contenido y calidad de información, etc.

Dentro de los aspectos más novedosos de la actual investigación es que GoPhish permite realizar la personalización avanzada de correos electrónicos de phishing, la automatización de campañas, informes detallados y la personalización del sitio web de phishing. Estas características avanzadas ayudan a los administradores de seguridad a llevar a cabo campañas de phishing efectivas y a evaluar la preparación y conciencia de los empleados en cuanto a los ataques de phishing, las funcionalidades actuales podrían mejorarse en un futuro con la integración plataformas de gestión de riesgos y herramientas de automatización de respuesta a incidentes, mejoras en la detección de phishing, capacidades de aprendizaje automático y la integración con plataformas de formación en seguridad, es decir GoPhish seguirá evolucionando con el tiempo para ofrecer una solución de simulación de phishing más completa y efectiva.

8. Conclusiones

GoPhish es una herramienta accesible y efectiva para realizar capacitaciones al personal de cualquier institución empresa u organización en técnicas de anti phishing, con esta herramienta es posible simular ataques de Phishing y evaluar la respuesta del personal para identificar áreas de mejora en la capacitación. Esto permite mejorar la seguridad cibernética de la universidad de manera más eficiente y efectiva.

La capacitación en técnicas de anti phishing a través del uso de herramientas como GoPhish, es una estrategia efectiva para mejorar la seguridad cibernética dentro de la Universidad Nacional de Loja específicamente en los ataques de ingeniería social denominados Phishing. Al educar y/o capacitar al personal administrativo a reconocer y evitar los ataques de Phishing se crea una cultura de seguridad cibernética en la institución, dicha responsabilidad no solo debe de ser del equipo de tecnología o seguridad informática, esta debe ser responsabilidad de todos los miembros de la institución previniendo así futuros incidentes de seguridad y reduciendo significativamente el riesgo de perder o exponer la información crítica y confidencial que maneja la Universidad Nacional de Loja.

Durante la ejecución de la campaña de la simulación del ataque Phishing utilizando la herramienta GoPhish que se aplicó en esta investigación se identificó que un 67,58% de la población abrió el correo electrónico, y un 32,15%, hizo clics en el enlace, es decir fueron víctimas de las trampas del Phishing. A razón de ello se debe focalizar la concientización y la formación en seguridad cibernética sobre estos funcionarios para ayudarles a evitar futuras amenazas de phishing.

9. Recomendaciones

Sabemos que la ingenuidad humana viene siendo el eslabón más débil en la cadena de seguridad informática, por ello se recomienda al personal encargado de la seguridad informáticas dentro de la institución realizar campañas de concientización en técnicas de anti phishing, las cuales no deben ejecutarse una vez y luego olvidarse, por el contrario, estas deben ser de manera permanente y se debe aplicar a todo el personal que se encuentra laborando en la institución, considerando que las personas tienden a descuidarse y olvidarse, así mismo considerando que existen nuevas contrataciones de personal para las distintas plazas de trabajo dentro de la institución.

Para la ejecución de simulación de ataques de Ingeniería Social denominados Phishing, se recomienda utilizar la herramienta GoPhish ya que contiene una interfaz sencilla y amigable, con resultados favorables en el proceso de realizar campañas de concientización de técnicas anti phishing para instituciones educativas, empresas y organizaciones.

Se debe establecer un procedimiento formal para reportar y escalar los eventos e incidentes de seguridad. Dicho procedimiento se debe dar a conocer y aplicado a toda la comunidad universitaria.

10. Bibliografía

Ciencias (2019). Introducción a la seguridad informática y el análisis de vulnerabilidades https://www.3ciencias.com/libros/libro/introduccion-a-la-seguridad-informatica-y-el-analisis-de-vulnerabilidades/

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

José Luis Calle Condori (2019). Fases de un ataque a un Sistema Informático Universidad Mayor de San Andrés La Paz - Bolivia Fases de un ataque a un Sistema Informático - La Paz - UMSA

Juniper Research. (2019). Cybercrime & the Internet of Threats 2019: Threats, Mitigation & Detection, 2019-2024. Obtenido de https://www.juniperresearch.com/researchstore/strategy-analytics/cybercrime-the-internet-of-threats-2019.

Kumar, V., & Tripathi, N. (2020). Cyber Security in Higher Education Institutions: An Analytical Study of Cyber Attacks and Phishing Scams. International Journal of Computer Science and Mobile Computing, 9(1), 107-117.

Proofpoint Security. (2022). Programa de entrenamiento de concientización de seguridad, informe de ingeniería social. https://www.proofpoint.com/us/threat-reference/social-engineering

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.

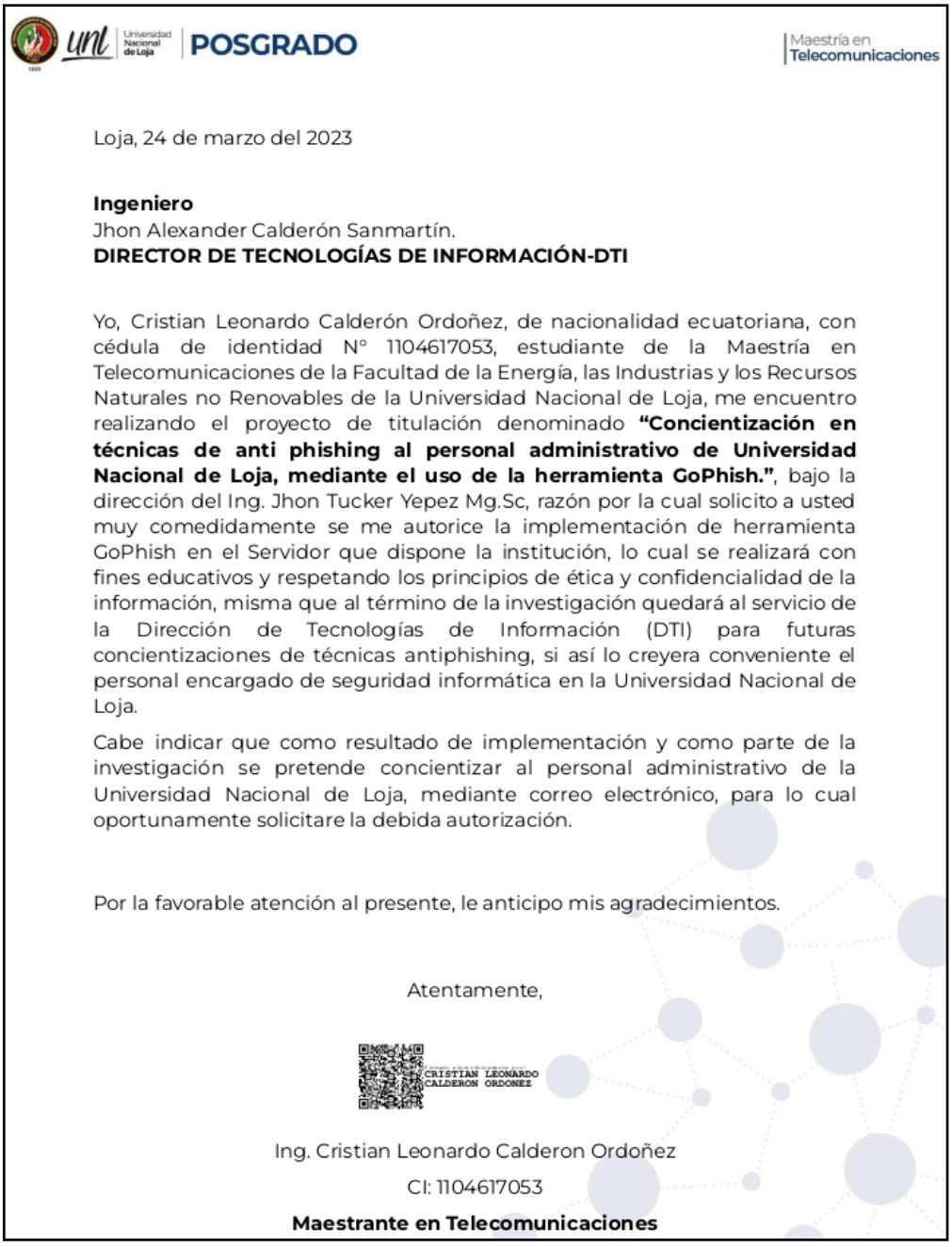
Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning. http://almuhammadi.com/sultan/sec_books/Whitman.pdf

Ross, T. J. (2009). *Fuzzy Logic with Engineering Applications* (Third). Wiley.

Zadeh, L. A. (1975). The concept of a linguistic variable and its application to approximate reasoning—I. *Information Sciences*, *8*(3), 199-249. https://doi.org/10.1016/0020-0255(75)90036-5

11. Anexos

Anexo 1. Solicitud de autorización para instalar GoPhish en el servidor.



Universidad Nacional de Loja | POSGRADO

Maestría en Telecomunicaciones

Loja, 24 de marzo del 2023

Ingeniero
Jhon Alexander Calderón Sanmartín.
DIRECTOR DE TECNOLOGÍAS DE INFORMACIÓN-DTI

Yo, Cristian Leonardo Calderón Ordoñez, de nacionalidad ecuatoriana, con cédula de identidad N° 1104617053, estudiante de la Maestría en Telecomunicaciones de la Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, me encuentro realizando el proyecto de titulación denominado **"Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish."**, bajo la dirección del Ing. Jhon Tucker Yepez Mg.Sc, razón por la cual solicito a usted muy comedidamente se me autorice la implementación de herramienta GoPhish en el Servidor que dispone la institución, lo cual se realizará con fines educativos y respetando los principios de ética y confidencialidad de la información, misma que al término de la investigación quedará al servicio de la Dirección de Tecnologías de Información (DTI) para futuras concientizaciones de técnicas antiphishing, si así lo creyera conveniente el personal encargado de seguridad informática en la Universidad Nacional de Loja.

Cabe indicar que como resultado de implementación y como parte de la investigación se pretende concientizar al personal administrativo de la Universidad Nacional de Loja, mediante correo electrónico, para lo cual oportunamente solicitare la debida autorización.

Por la favorable atención al presente, le anticipo mis agradecimientos.

Atentamente,

CRISTIAN LEONARDO CALDERON ORDOÑEZ

Ing. Cristian Leonardo Calderon Ordoñez
CI: 1104617053
Maestrante en Telecomunicaciones

Anexo 2. Aprobación de Autorización para instalar GoPhish en el servidor.

Universidad Nacional de Loja

Dirección de Tecnologías de Información

Memorando Nro.: UNL-DTI-2023-035-M
Loja, 28 de marzo de 2023

PARA: Ing. Cristian Leonardo Calderón Ordóñez
MAESTRANTE EN TELECOMUNICACIONES

ASUNTO: Autorización para la implementación de herramienta GoPhish en el Servidor que dispone la institución.

En atención al oficio de fecha 24 de marzo de 2023, suscrito por usted, en el cual manifiesta lo siguiente: *"...me encuentro realizando el proyecto de titulación denominado "Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish., bajo la dirección del Ing. Jhon Tucker Yepez Mg.Sc, razón por la cual solicito a usted muy comedidamente se me autorice la implementación de herramienta GoPhish en el Servidor que dispone la institución, lo cual se realizará con fines educativos y respetando los principios de ética y confidencialidad de la información..."*

Con lo antes expuesto, me permito informar a usted que autorizo la implementación de la herramienta GoPhish en el servidor security.unl.edu.ec que dispone la institución, sin embargo, será necesario tener en consideración los siguientes aspectos:

- Mantener estricta confidencialidad con los datos proporcionados y generados en la implementación del presente proyecto.
- En caso de requerir publicar información, esta deberá aplicar técnicas de seudonimización de datos, protegiendo datos sensibles y en especial datos personales.
- Mantener el sigilo y altruismo durante la implementación de pruebas anti-phishing con los usuarios finales.

Sin otro particular me suscribo de Usted y aprovecho la oportunidad para reiterarle el testimonio de mi más alta consideración.

Atentamente,

JHON ALEXANDER CALDERON SANMARTIN

Jhon Alexander Calderón Sanmartín
DIRECTOR DE TECNOLOGÍAS DE INFORMACIÓN

C/c:
- Archivo UTI

JC/ag/jcr

Anexo 3. Certificación de traducción del resumen

CERTIFICADO DE TRADUCCIÓN

Andrés Baldassari
MA.App.Lng

CERTIFICO:

Haber realizado la traducción de español a inglés del resumen de la tesis titulada: "Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish", de autoría CRISTIAN LEONARDO CALDERÓN ORDOÑEZ con cédula de identidad Nro. 1104617053, egresado de la facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ing. John Tucker Yépez, Mg. Sc. previo a la obtención del título de Magíster en Telecomunicaciones.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer uso del presente en lo que creyere conveniente.

ANDRES ROBERTO BALDASSARI CASQUETE

Quito, 18 de abril de 2023

Andrés Baldassari MA.App.Lng
Certified Translator – Senescyt - MDT-3104-CCL-259519
Celular: (593) 098 7030 511
Email: andresbaldassari@hotmail.com

Andres Baldassari
CERTIFIED TRANSLATOR
MDT-3104-CCL-259519