Vol.7 No.4 (2023): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.7.4.2023.610-633

Social engineering and its consequences in the technological academic population of El Oro Province.

Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro.

Autores:

Sancho-López, Cristian Stalin
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica
Cuenca – Ecuador

cristian.sancho.17@est.ucacue.edu.ec

https://orcid.org/0000-0002-2974-5896

Cuenca-Tapia, Juan Pablo
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica
Cuenca – Ecuador

jcuenca@ucacue.edu.ec

https://orcid.org/0000-0001-5982-634X

Ortega-Castro, Juan Carlos
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica
Cuenca – Ecuador

jcortegac@ucacue.edu.ec

https://orcid.org/0000-0001-6496-4325

Fechas de recepción: 03-SEP-2023 aceptación: 03-OCT-2023 publicación: 15-DIC-2023

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Problema: La Ingeniería social puede tener un alcance significativo en los estudiantes de tecnología debido a su alta exposición a los medios tecnológicos, convirtiéndolos en blancos fáciles para delincuentes en el cibersepacio. Objetivo: Analizar el efecto de la Ingeniería social en la población académica tecnológica de la provincia de El Oro, con el fin de identificar las vulnerabilidades existentes en la seguridad informática. Metodología: Se basó el desarrollo de la investigación en la metodología OWASP, en virtud de que permite realizar un proceso que abarca recolección de información análisis de vulnerabilidades y resultados. Resultados: Dentro los resultados del primer escenario, se logró identificar que el 25% de la población que accedieron al link malicioso, otorgaron sus credenciales, mientras que en un segundo escenario esto disminuyó en gran medida, porque solo el 7% volvió a caer, lo que permitió concluir que la comunidad académica conlleva a un nivel de riesgo medio, sin embargo, con una advertencia este disminuye.

Palabras clave: Seguridad de la información, ingeniería social, ataque, mitigación, tecnología.

Abstract

Problem: Social engineering can have a significant impact on technology students due to their high exposure to technological media, making them easy targets for criminals in cyberspace. Objective: To analyze the effect of social engineering in the technological academic population of the province of El Oro, in order to identify existing vulnerabilities in computer security. Methodology: The development of the research was based on the OWASP methodology, since it allows to carry out a process that includes information gathering, vulnerability analysis and results. Results: Within the results of the first scenario, it was possible to identify that 25% of the population that accessed the malicious link, gave their credentials, while in a second scenario this decreased to a great extent, because only 7% fell again, which allowed concluding that the academic community carries a medium risk level, however, with a warning this decreases.

Keywords: Information security, social engineering, stroke, mitigation, technology.

Introducción

La Ingeniería social se ha convertido en una amenaza latente en la era digital, afectando a todas las personas que interactúan en línea, independientemente de su nivel de conocimiento en seguridad informática. Esta técnica de manipulación psicológica utiliza la persuasión y el engaño para obtener información confidencial o realizar actividades malintencionadas en la red. (Redaccion Digital, 2022)

En el ámbito académico tecnológico, la Ingeniería social puede tener consecuencias graves en la seguridad de la información, la privacidad y la reputación de las instituciones educativas. La población académica, en particular, está expuesta a este tipo de amenaza debido a su alta exposición a la tecnología y a la gran cantidad de información confidencial que manejan.

A pesar de que existen medidas de seguridad para prevenir los ataques de Ingeniería social, como la capacitación y la concientización sobre la importancia de proteger la información, muchos usuarios continúan siendo víctimas de estas tácticas. Esto puede deberse a la falta de conocimiento o a la falta de implementación de políticas de seguridad efectivas.

Además, las consecuencias de un ataque de Ingeniería social pueden ser significativas para la población académica tecnológica. Los ataques pueden poner en peligro la información confidencial, incluyendo datos de investigación, contraseñas y correos electrónicos, lo que puede resultar en la pérdida de la propiedad intelectual y la reputación de la institución educativa. También puede haber consecuencias financieras, como multas o costos de reparación. (Montenegro, 2017)

Material y métodos

Metodología

La metodología del presente proyecto de investigación fue de carácter exploratorio debido a que se basó en la investigación y estudio de campo de la Ingeniería social y las consecuencias en la población académica objeto de estudio. Además, se aplicaron métodos deductivos, porque el desarrollo del proyecto estudió elementos generales hasta llegar a los particulares.

"La metodología de OWASP es aquella que se enfoca en la seguridad de aplicaciones, que pretende alentar a las personas a evaluar y tomar una medida de la seguridad a través de todo el proceso de desarrollo" (Misava, 2013, pág. 25), por lo que es indispensable identificar cada una de las etapas para el desarrollo de la investigación, siendo estas las siguientes:

Recolección de información: para ello fue necesario conocer y mantener un escenario planteado, por lo general, en esta etapa se identificaron las posibles vulnerabilidades de los participantes en sus dispositivos. Esto se realizó en dos tipos de prueba: pruebas a ciegas y pruebas con información, dentro de esta prueba se realizó la prueba con información, con el objetivo principal de obtener datos de la víctima.

Análisis de vulnerabilidades: es fundamental para el proceso de ataque debido a que identifica si con los datos recogidos con anterioridad, existe la manera de lograr vulnerar a los usuarios, de acuerdo a sus debilidades.

Explotación de Vulnerabilidades: en esta etapa se ejecuta en sí el ataque con el fin de confirmar y a su vez de conocer sobre las vulnerabilidades a las que están expuestos los usuarios, es de gran importancia realizar este proceso sin ningún fin malicioso.

Análisis de Resultados: dentro de esta fase, se documentó la información obtenida a través de todo el proceso del ataque con los resultados respectivos.

Caso Práctico: Técnica Suplantación de identidad (PHISHING)

En el primer escenario, se realizó la creación de una dirección de correo electrónico falsa bajo el nombre del Centro de Idiomas del Instituto Superior Tecnológico Ismael Pérez Pazmiño, utilizando el correo instIPpeducacioncontinua.cursos@gmail.com, a través de esta dirección se envió un mensaje a los estudiantes de la comunidad académica tecnológica objeto de estudio de la investigación, con el objetivo de difundir un formulario de Google

titulado "Certificaciones A1-A2 en inglés", mismo que contenía preguntas para recolectar información personal de los participantes.

En el segundo escenario, entre los datos que se recogieron se incluyó el número de teléfono móvil, el cual sería el principal medio para difundir el enlace malicioso por medio de la aplicación de mensajería más conocida como WhatsApp.

Para la creación del enlace se usó un software instalado en el sistema operativo Kali Linux, este es denominado Zphisher, más conocido como una herramienta para hacer phishing, pues este permite clonar páginas de las redes sociales más usadas y levantarlas en el localhost, para luego direccionarlas a la web con una IP pública con el fin de redirigir a los usuarios a sitios web falsos sin su conocimiento o consentimiento.

Para ocultar el enlace malicioso se usó Maskphisk (Software Kali Linux), una vez ya con los usuarios en el sitio web falso, se pidió que registren sus credenciales de acceso de su cuenta de Gmail, con el objetivo de vulnerar sus credenciales, al abrir el enlace las credenciales que registraron los participantes se guardaron en un archivo de texto, dentro de una carpeta del software, en la figura 1 se puede observar la definición de la población para esta investigación.

Figura 1
Definición de la población.

INSTITUCIÓN DE TERCER NIVEL	POBLACIÓN
Instituto Superior Tecnológico Huaquillas	100
Instituto Superior Tecnológico Ismael Pérez Pazmiño	500
Instituto Superior Tecnológico El Oro	800
Instituto Superior Tecnológico Ochoa León	500
TOTAL	1900

Fuente: Fuente propia

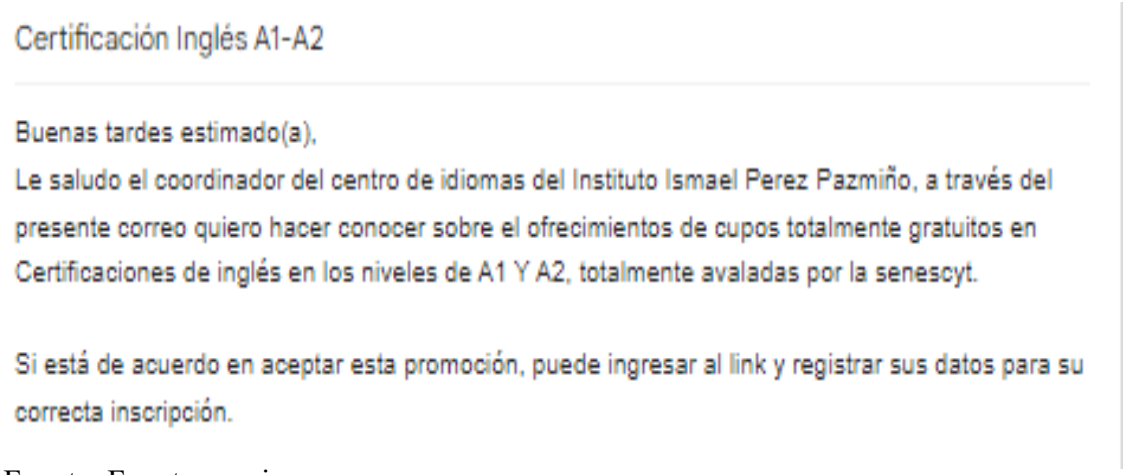
Se toma en cuenta a los siguientes institutos de la provincia, debido a que mantienen carreras tecnológicas, por lo general, son más propensos a ser vulnerados. Tomado del autor.

Medio Ataque: WhatsApp

Para el desarrollo de la investigación se tomó una muestra de la población objeto de estudio con fin de determinar sin son victimizados de alguna u otra manera, el medio de ataque es la app denominada WhatsApp, esta última se prevé que sea más eficaz debido a que es

mensajería instantánea, en lo que respecta al contenido del mensaje: es una oferta especial de parte del centro de idiomas del Instituto Ismael Pérez Pazmiño con una matrícula gratuita para los niveles y subniveles de las certificaciones A2 en inglés.

Figura 2.
Mensaje emitido por WhatsApp.



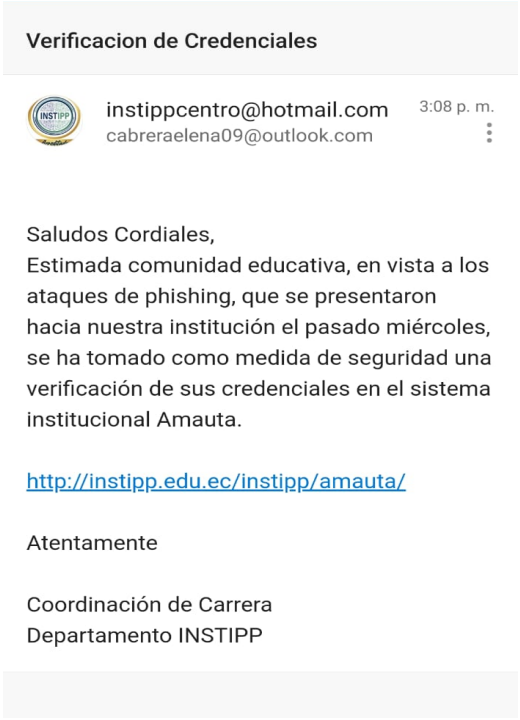
Fuente: Fuente propia

Medio de Ataque: Correo Electrónico

En el tercer y último escenario se tomó cuenta él envió de un correo electrónico, en base a la herramienta Gophish, que se encarga y comúnmente es utilizada para la realización de campañas de phishing, esta permite la clonación de cualquier sitio web, e incluso copia de correos electrónico.

Una vez con las configuraciones correspondientes, se realizó el ataque, para ello se clonó el sistema institucional del Instituto Ismael Pérez Pazmiño, y se realizó la difusión de un mensaje de correo electrónico con el mensaje que muestra la figura 3, este mismo contiene el link original de la página institucional, pero con la diferencia que esta redirigido al sitio clonado.

Figura 3.
Email recibido por los participantes.



Fuente: Fuente propia

Plan de mitigación para problemas y ataques de Ingeniería social.

Para evitar y minimizar los riesgos que consigo traen la perdida y vulneración de información, se debe de tomar en cuenta las siguientes normas:

- Revisión de fuentes originales: es de manera indispensable asesorarse y verificar la fuente de cualquier mensaje que se reciba, esto se puede hacer revisando mensajes con el mismo destinatario, o en caso de ser algún tipo de promoción, buscar la empresa real y acercarse para preguntar.
- Al recibir correos electrónicos: es necesario identificar el correo remitente para conocer si es un correo real o se trata de un falso, generalmente los correos con información educativa, mantienen correos institucionales.
- No abrir link: muchas veces la emoción es la peor enemiga, por lo que somos muy susceptibles a caer en algún tipo de ataque, para evitar esto es mejor no ingresar al link ni por curiosidad.

- Al recibir correos con formularios que manifiesten que se registren datos personales, como dirección, numero celular y entre otras cosas, es mejor no entregar este tipo de información, debido a que puede ser manipulada para otros fines.
- Una de las más importantes, es no entregar credenciales de acceso por ningún mensaje, aplicativo o en formularios, recuerden que las credenciales son de uso personal, y si llegan a ser vulneradas pueden ser usadas para fines delictivos.
- No otorgar permisos de cámara, micrófono e incluso de almacenamiento, al momento de ingresar a un sitio nuevo.
- Mantener activado un antivirus en sus dispositivos electrónicos, con el fin de evitar ataques de todo tipo.
- Capacitarse de manera continua, debido a que el avance de la tecnología está en su auge, y consigo avanza la criminalidad informática.
- Realizar cada cierto tiempo, análisis de vulnerabilidades.

Resultados

Con respecto al desarrollo del proyecto, el primer escenario que fue la suplantación del centro de idiomas de INSTIPP, ofertando cupos totalmente gratis, para ello se realizó la creación de un formulario con el fin de obtener datos personales como el número de contacto, con este último dato se puede proceder a la realización del segundo escenario, la población identificada se presenta en la tabla 1.

Tabla 1.

Población del primer escenario.

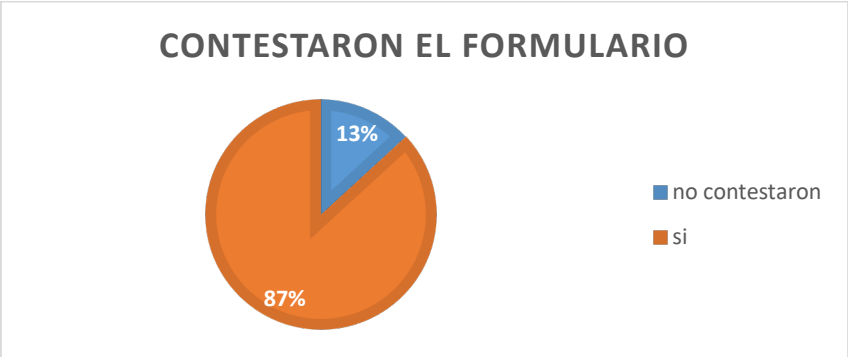
POBLACIÓN	CANTIDAD
PERSONAS QUE CONTESTARON	250
QUE NO CONTESTARON	1650
TOTAL	1900

Fuente: Fuente propia

Con la población académica tecnológica, se envió un formulario para adquirir números telefónicos. Tomado del autor.

Figura 4.

Resultado del formulario.

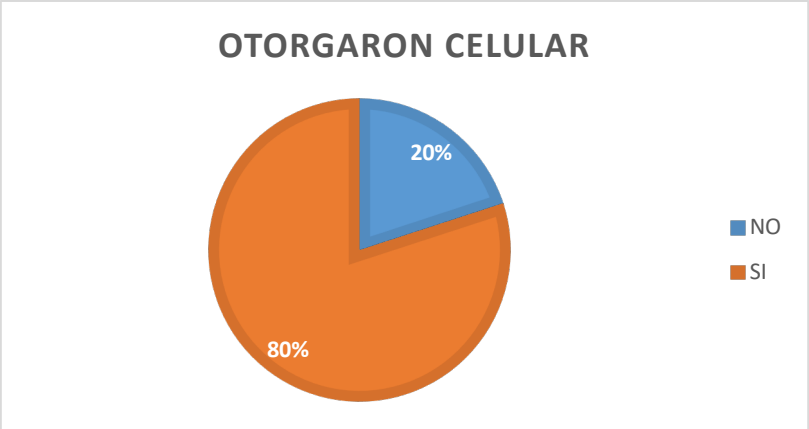


Fuente: Fuente propia

El 87% de la población no contesto al formulario enviado a través de correo electrónico, y un 13% que equivale a 250 personas, si lo hicieron.

En una de las preguntas esenciales estaba recolectar el número celular de quienes serán las víctimas, del cual solo un 78% de los encuestados, otorgaron sus números celulares, ver figuras 5 y 6.

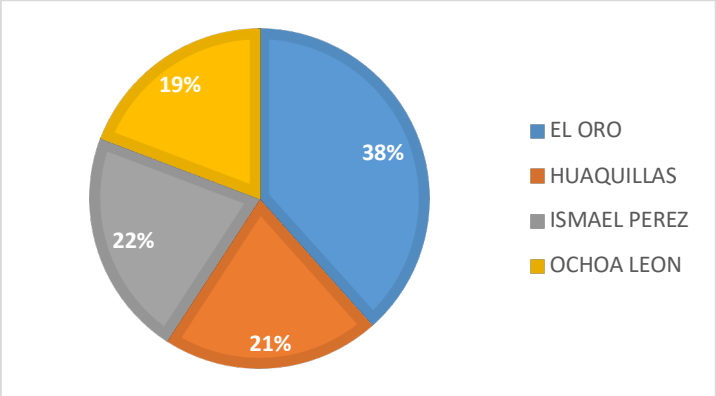
Figura 5.
Resultados de entregar número celular.



Fuente: Fuente propia

Como se menciona con anterioridad un 80% de las 250 personas que contestaron al formulario, entregaron sus números celulares, mientras que un 20% no lo entregó.

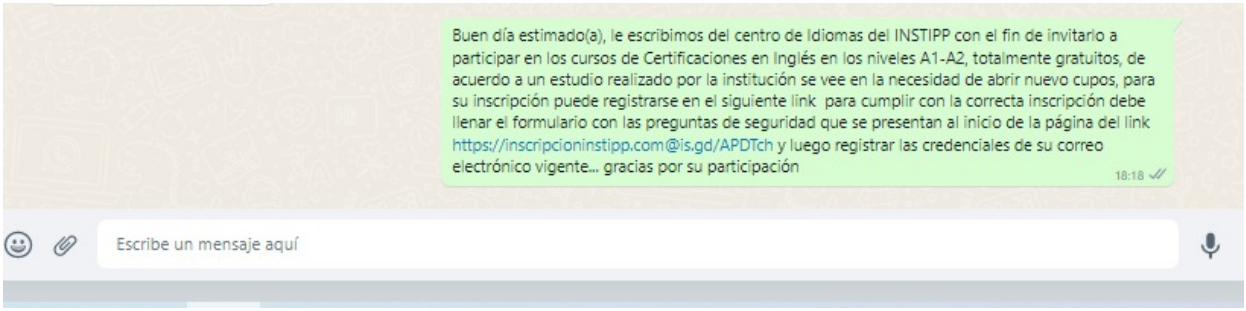
Figura 6.
Población que contesto el formulario según institutos.



Fuente: Fuente propia

Instituto El Oro va puntero con un 38%, mientras le sigue el Ismael, seguido del ISTH, y El Ochoa león sería el porcentaje más bajo en entregar información a través de formularios. De acuerdo a los resultados en el segundo escenario, se logró enviar el mensaje con el link malicioso a través de la plataforma de WhatsApp, como se observa en la figura 7.

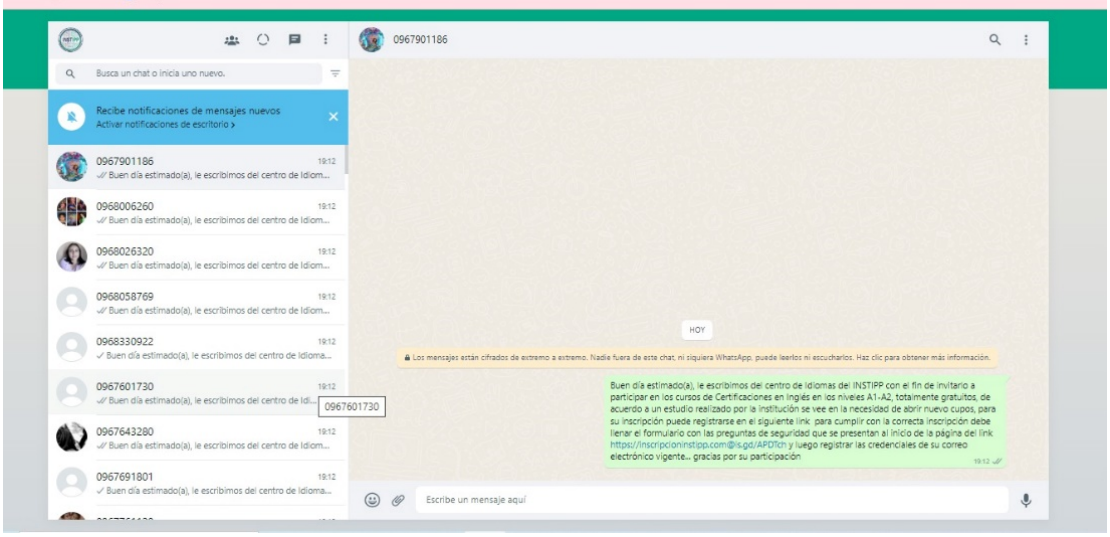
Figura 7.
Mensaje enviado a través de WhatsApp.



Fuente: Fuente propia

Dentro del mensaje llevaba en su contenido el link malicioso.

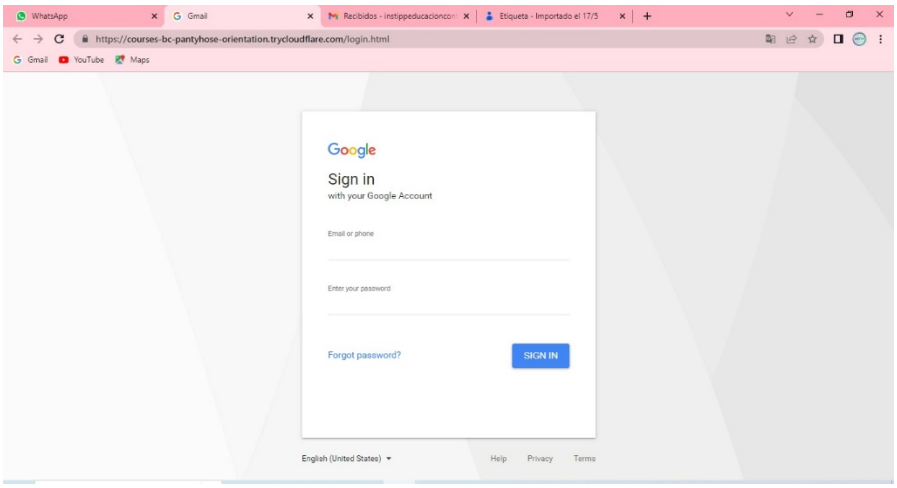
Figura 8.
Momento en el que se envió el mensaje a través de WhatsApp.



Fuente: Fuente propia

Este mensaje fue enviado a través de WhatsApp, a una cantidad de 200 personas que fueron las que otorgaron sus números celulares a través del formulario. Una vez enviado el mensaje a los participantes, al hacer clic en el link se levantaba la página clonada de Gmail, con el fin que registren sus credenciales de acceso, figura 9.

Figura 9.
Página de Gmail clonada.

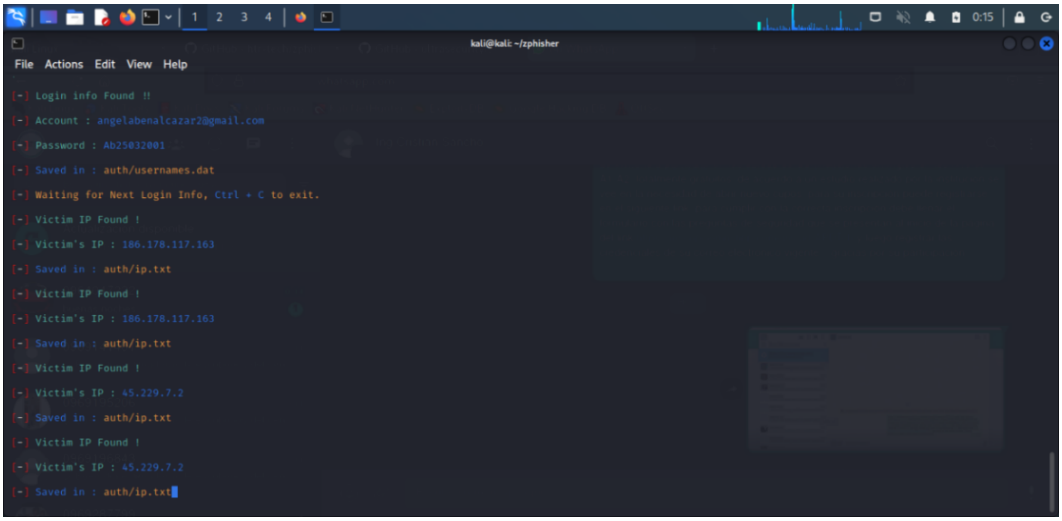


Fuente: Fuente propia

Al hacer clic en el enlace, a través del programa Zphisher, se lograba identificar las direcciones IP que accedían, sin embargo, no todos se atrevían a registrar sus credenciales como se observa en las figuras 10 y 11.

Figura 10.

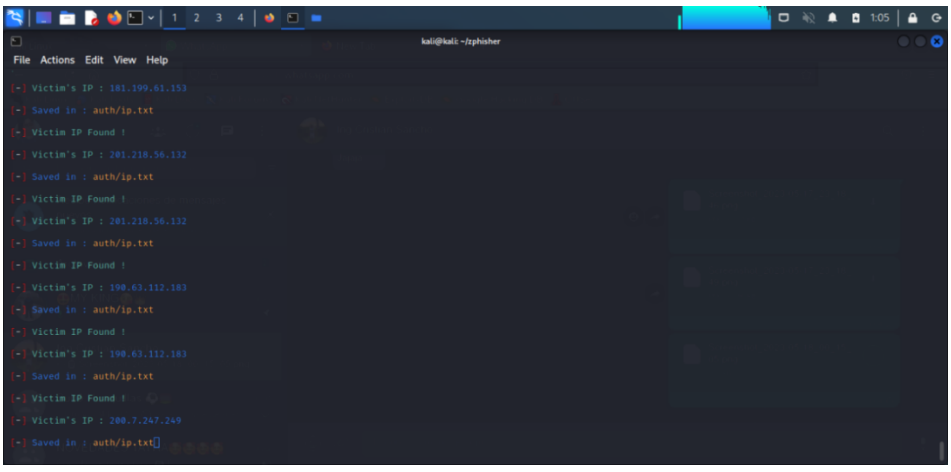
Direcciones IP y credenciales de registro.



Fuente: Fuente propia

Figura 11.

Direcciones IP registradas.

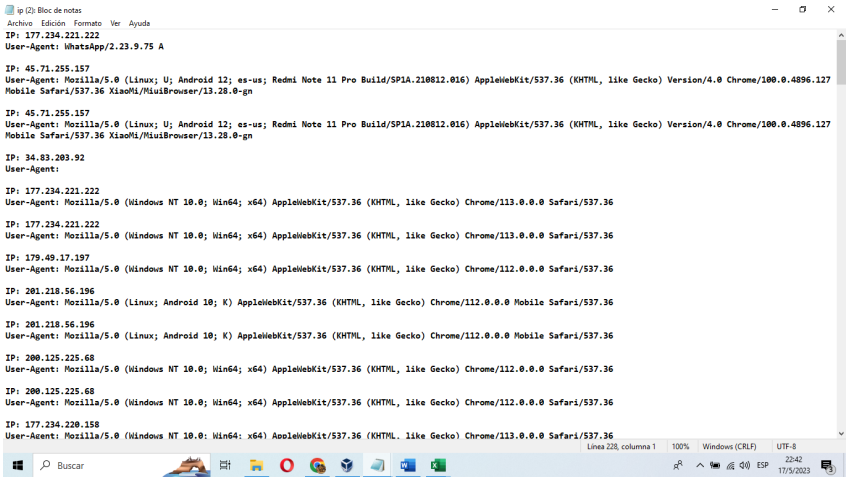


Fuente: Fuente propia

A partir de los archivos de texto que se guardaban de manera automática en la ruta del programa, se logró identificar la cantidad exacta de direcciones IP que hicieron clic en el link, al menos se logró identificar que unas 100 personas de las 200 que recibieron el mensaje, accedieron al link mas no se registraron, figura 12.

Figura 112.

Archivo de texto generado por el programa.

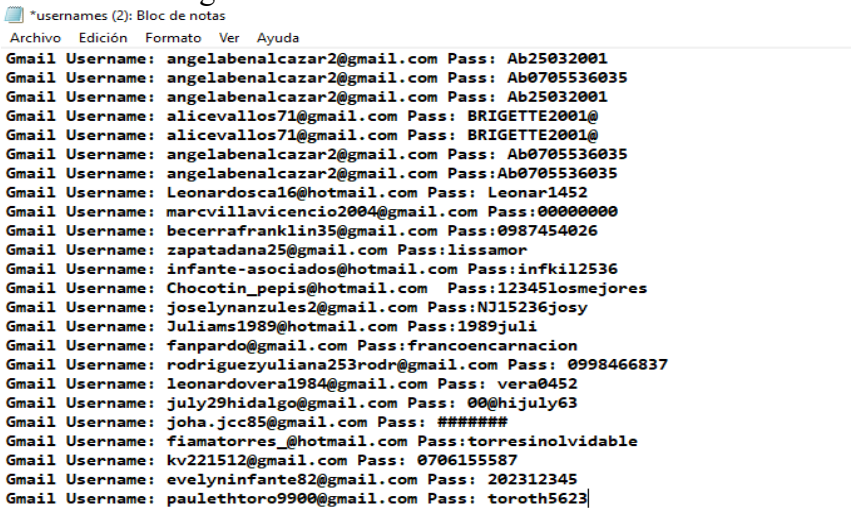


Fuente: Fuente propia

Por lo tanto, en la figura 13 se observa que, de las 100 personas que accedieron al link solo unas 25 ingresaron sus credenciales de acceso, es así como lo demuestra el archivo de texto generado por el aplicativo.

Figura 123.

Credenciales registradas.



Fuente: Fuente propia

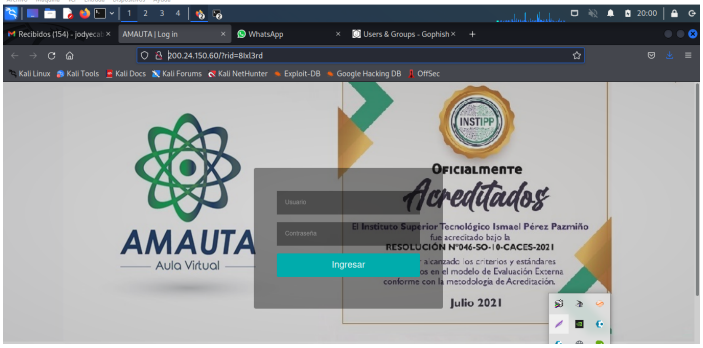
De acuerdo con la ejecución del ataque del segundo escenario, el centro de idiomas INSTIPP informo a la comunidad tecnológica sobre un ataque de phishing, donde emitió un comunicado (figura 14), a través de sus canales oficiales que informa lo siguiente **"A la comunidad educativa del INSTIPP, hemos detectado que desde cuentas de correo y números que no pertenecen a nuestra institución, se ha remitido información referente a supuestos Cursos del Centro de Idiomas del INSTIPP, información que es FALSA. Evite registrar su información en esos enlaces, evite el robo de información personal. La información del Centro de Idiomas la indicaremos a través de los coordinadores de carrera"**

Figura 13.
Comunicado emitido por redes sociales.

Fuente: Fuente propia

Por lo que fue conveniente la realización del ataque del tercer escenario, con el fin de conocer si la población, a pesar de advertencias por la misma institución, es capaz de creer nuevamente y caer en una de las técnicas de Ingeniería social más famosas, que es el phishing. En la figura 15 se muestra como quedo la clonación de la página web institucional del INSTIPP, el link original de la página incluido en el correo electrónico redireccionaba a esta que se presenta.

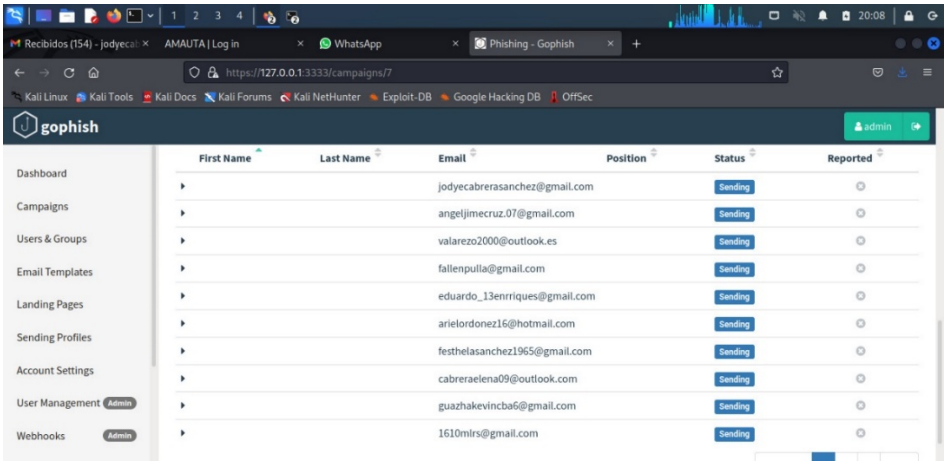
Figura 14.
Página Web Institucional clonada.



Fuente: Fuente propia

Esta es la página que se clono del sitio web institucional. Tomado del autor.

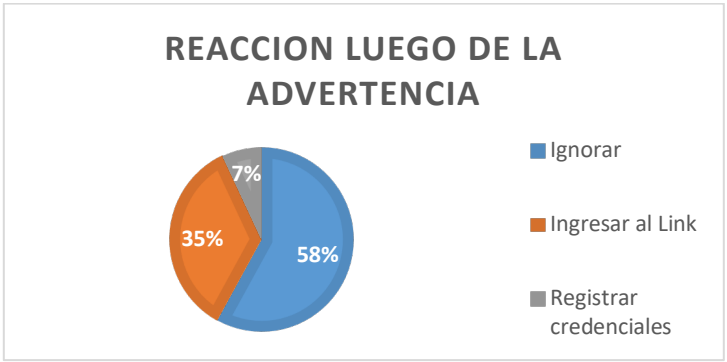
Figura 15.
Momento del envió de la campaña.



Fuente: Fuente propia

De acuerdo a los resultados se aplica a la misma cantidad de participantes (200), de los cuales solo accedieron al link de la página clonada de su sitio web institucional ***http://instIPp.edu.ec/instIPp/amauta/***, un 35% de la población, sin embargo, en este ataque se registró que un 7% nuevamente otorgaron sus credenciales de acceso, como se aprecia en la figura 17.

Figura 16.
Resultados luego de la advertencia.



Fuente: Fuente propia

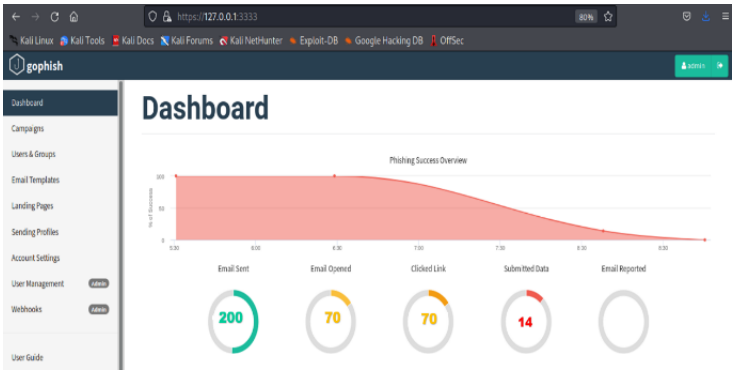
De acuerdo al 100% de los 84 participantes, en un 80% no ingresaron credenciales, pero, sin embargo, dieron clic en el link, mientras que el 20% emitió sus credenciales en el sitio clonado (figura 18).

Figura 17.
Resultados de emitir credenciales.

Fuente: Fuente propia

La herramienta de Gophish permitió identificar a través de un dashboard los resultados que emite cada participante (ver figuras 19 y 20), adicionalmente registra las veces que los participantes ingresan al link, cuando abren el correo electrónico emitido, y en caso de llegar a llenar sus credenciales, también las recopila.

Figura 19.
Dashboard de Gophish

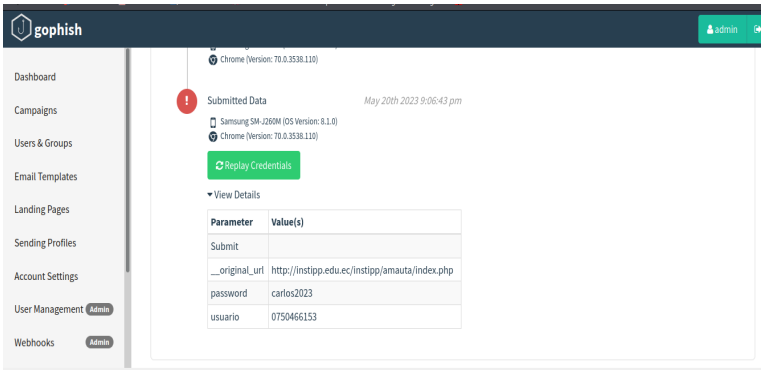


Fuente: Fuente propia

La aplicación Gophish permite la visualización de un dashboard con las estadísticas de los resultados. Tomado del autor.

Figura 18.

Registro de Credenciales.



Fuente: Fuente propia

De esta manera se representan los datos en la herramienta Gophish. Tomado del autor.

Discusión

A nivel mundial los usuarios de la tecnología se han visto inmersos en casos de vulneración de información, chantajes o estafas, y si esto ha sido posible es gracias a que han sido víctimas de alguna de las famosas técnicas de ingeniera social.

En lo que respecta del país se han escuchado casos de vulneración de información delicada muchas veces es debido a la Ingeniería social, pero ¿será solo este tipo de consecuencia?, pues no, las técnicas que emplean la Ingeniería social pueden desencadenar más problemas e incluso llegar a delitos informáticos penados por la ley.

Según el Diario El Universo (2021) indicó que el mayor banco privado del Ecuador no ha revelado públicamente la naturaleza del ataque que sufrió el y que provocó la caída de la mayoría de sus servicios en línea y cajeros automáticos, el mismo que se trataría de un ataque de ransomware con actores de amenazas que instalan una baliza Cobalt Strike en la red.

Uno de los casos relacionados a la Ingeniería social, es el caso de la suplantación de identidad de Plaza Nova, que es una institución dedicada a la venta de distintos artículos de la línea de ropa, belleza, hogar. Las victimas recibían este mensaje: "¡Felicidades! Estás seleccionado para formar parte de un giveaway. Después de participar, este es su paso final para ganar mi premio. Gana 3 Paykards de $500. Para recibir su regalo, registre su nombre en mi sitio web", y es así como obtenía información de estas personas, así lo menciona (El Diario Expreso, 2022).

Generalmente las instituciones más afectadas por estas técnicas son las entidades bancarias, pero claro que no se quedan atrás los usuarios comunes quienes se ven perjudicados por la propagación de phishing a través de redes sociales, los atacantes ven al usuario como el eslabón más débil, los estudian y de esta manera, identifican la manera más hábil de atacar.

En el Ecuador se ha logrado identificar casos prácticos de técnicas de Ingeniería social en ámbitos empresariales, con el fin de tomar medidas para precautelar la seguridad de la información de alguna institución en especial, uno de estos casos es la aplicación de phishing en la empresa denominada Omnidata, clonaron su sitio web para lograr obtener las credenciales de acceso de los funcionarios de la misma, y los resultados del grado de riesgo son de un nivel medio, así lo indica el autor (Diaz, 2021).

Otro de los ejemplos de aplicación de escenarios prácticos fue realizado por (Edison Camino, 2020) con el objetivo de clonar una de las página de Esemtia quien es una de las más usadas en la Unidad Educativa Salesiana Cardenal Spellman, con el fin de robar sus

credenciales y de esta manera vulnerar la in formación de cada una de sus víctimas, en los resultados se comprobó con los cálculos realizados, que se obtuvo un 29.6% de éxito al utilizar el correo electrónico, en comparación al 8% de éxito que se obtuvo a través de WhatsApp.

Los principales objetivos para este tipo de atacantes son las entidades bancarias, sin embargo, es importante recalcar que a través de esta recopilación de información se ha logrado comprobar que los escenarios prácticos que han estudiado otros autores, han tenido resultados de nivel medio en lo que es seguridad de la información, ya que su población ha caído en estos escenarios, y muchas veces esto se debe al desconocimiento de estas técnicas de Ingeniería social.

Conclusiones

Las consecuencias de la Ingeniería social a nivel educativo tecnológico, conllevan a un nivel de riesgo medio, debido a que, si existe una información delicada vulnerada, la misma puede servir para fines delictivos como extorsión, además que, al obtener las credenciales de sus correos electrónicos, pueden mantener acceso a todas las otras redes sociales, que se vinculan al mismo.

De acuerdo con los resultados, de la población inicial que se pretendía engañar, solo fue un porcentaje pequeño quien vulnero su información que fueron los 200 participantes, que tiene un equivalente a 25 personas, sin embargo, el 13% de esta población logro registrar sus credenciales y vulnerar su información, y el 87% no lo registro porque los participantes tienen bases fundamentales sobre este tipo de ataques en su sociedad académica.

A pesar que la institución que estaba siendo suplantada, emitió un comunicado acerca de los ataques de los primeros escenarios, existió un porcentaje de víctimas en el tercer escenario, claro que aún más bajo que el primero, por lo que se puede concluir que aún falta conocimiento para mitigar estas técnicas de Ingeniería social.

Finalmente, es importante conocer sobre las consecuencias que conllevan la Ingeniería social, para de esta manera mantener una seguridad de la información impecable y manejar con mayor responsabilidad el uso de nuestras credenciales de acceso a cualquier aplicativo.

Referencias bibliográficas

Diario El universo. (4 de Agosto de 2021). El Universo. Obtenido de https://www.eluniverso.com/noticias/seguridad/los-delitos-informaticos-con-pena-de-prision-en-ecuador-nota/

Diaz, J. P. (2021). Ingenieria Social, un ejemplo practico. REVISTA UISRAEL, 54.

Edison Camino, E. P. (Agosto de 2020). https://dspace.ups.edu.ec. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/19001/1/UPS%20-%20TTS061.pdf

El Diario Expreso. (05 de Mayo de 2022). https://www.expreso.ec/. Obtenido de https://www.expreso.ec/ciencia-y-tecnologia/ataque-ingenieria-social-utiliza-plaza-navona-103948.html

El Universo. (Octubre de 2021). Ataque Ransonware. El Universo, pág. 25.

IBM. (25 de Octubre de 2019). IBM. Obtenido de https://www.ibm.com/es-es/topics/social-engineering

Misava. (Febrero de 2013). https://seguridadinformaticahoy.blogspot.com/. Obtenido de https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

Montenegro, L. (2017). https://dspace.ucuenca.edu.ec. Obtenido de https://dspace.ucuenca.edu.ec/bitstream/123456789/28604/1/Tesis.pdf

Panda Security. (18 de Julio de 2020). Panda Security. Obtenido de https://www.pandasecurity.com/es/security-info/phishing/

Redaccion Digital. (Mayo de 2022). https://revistaempresarial.com. Obtenido de https://revistaempresarial.com/author/redaccion-digital/

Tecon. (12 de Mayo de 2019). Obtenido de https://www.tecon.es/la-seguridad-de-la-informacion/

UNIR. (2019). UNIR. Obtenido de https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.