

DOI: https://doi.org/10.37811/cl_rcm.v7i2.5696

Análisis del uso de las técnicas de ingeniería social caso de estudio: Instituto Superior Tecnológico Huaquillas - Ecuador

Cristian Stalin Sancho López

cssancho@isthuaquillas.edu.ec

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

Instituto Superior Tecnológico Huaquillas, Huaquillas, Ecuador

Jessica Pilar Alejandro Becerra

jpalejandro@isthuaquillas.edu.ec

<https://orcid.org/0000-0003-1612-2988>

Instituto Superior Tecnológico Huaquillas, Huaquillas, Ecuador

Jorge David Herrera Sarango

jdherreira@isthuaquillas.edu.ec

<https://orcid.org/0000-0002-0407-730X>

Instituto Superior Tecnológico Huaquillas, Huaquillas, Ecuador

Sandra Jacqueline Machuca Toapanta

sjmachuca@isthuaquillas.edu.ec

<https://orcid.org/0000-0001-7255-2240>

Instituto Superior Tecnológico Huaquillas, Huaquillas, Ecuador

Paquita Alejandra Cuadros García

pacuadros@isthuaquillas.edu.ec

<https://orcid.org/0000-0002-0734-6114>

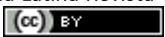
Instituto Superior Tecnológico Huaquillas, Huaquillas, Ecuador

Correspondencia: jpalejandro@isthuaquillas.edu.ec

Artículo recibido: 25 enero 2023. Aceptado para publicación: 25 febrero 2023

Conflictos de Interés: Ninguna que declarar

Todo el contenido de **Ciencia Latina Revista Científica Multidisciplinar**, publicados en este sitio están disponibles bajo

Licencia [Creative Commons](https://creativecommons.org/licenses/by/4.0/) 

Cómo citar: Sancho López, C. S., Alejandro Becerra, J. P., Herrera Sarango, J. D., Machuca Toapanta, S. J., & Cuadros García, P. A. (2023). Análisis del uso de las técnicas de ingeniería social caso de estudio: Instituto Superior Tecnológico Huaquillas - Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, 7(1), 11471-11479.

https://doi.org/10.37811/cl_rcm.v7i2.5696

RESUMEN

La ingeniería social es uno de los mayores enemigos para los internautas con desconocimiento en seguridad informática, es por ello que en este trabajo se analizó la incidencia del uso de las técnicas de ingeniería social a través de una investigación bibliográfica y se la aplicó en un escenario práctico a la población académica del Instituto Superior Tecnológico Huaquillas (ISTH) y de esta manera determinar el porcentaje de personas que son víctimas de este problema, para el desarrollo de este trabajo se aplicó un método de investigación exploratoria y método deductivo, por ello se somete a la población académica del ISTH a un escenario práctico con una de las técnicas de ingeniería social denominada “suplantación de identidad”. Logrando obtener que el 14,46% de una población de 83 estudiantes de la carrera de Redes y Telecomunicaciones fueron quienes proporcionaron información real, adicionalmente se realizó un nuevo ataque de vulneración de cámara dirigido a los estudiantes de primer periodo académico en el cual se logró la victimización del 4,36% de los estudiantes. Con estos resultados se pudo determinar que la comunidad académica institucional está preparada para no ser víctima de ataques basados en ingeniería social.

Palabras clave: ingeniería social; phishing; redes; telecomunicaciones.

Analysis of the use of social engineering techniques, case study: Instituto Superior Tecnológico Huaquillas - Ecuador.

ABSTRACT

Social engineering is one of the biggest enemies for Internet users with lack of knowledge in computer security, that is why in this work the incidence of the use of social engineering techniques was analyzed through a bibliographic research and applied in a practical scenario to the academic population of the Instituto Superior Tecnológico Huaquillas (ISTH) and thus determine the percentage of people who are victims of this problem, For the development of this work an exploratory research method and deductive method was applied, therefore the academic population of the ISTH was subjected to a practical scenario with one of the techniques of social engineering called "identity theft". It was obtained that 14.46% of a population of 83 students of the Networking and Telecommunications career were those who provided real information, additionally a new attack of camera vulnerability was carried out directed to the students of the first academic period in which 4.36% of the students were victimized. With these results it was possible to determine that the institutional academic community is prepared to avoid being a victim of attacks based on social engineering.

Keywords: *social engineering; phishing; networks; telecommunications.*

INTRODUCCIÓN

La evolución de la tecnología ha permitido mejorar la calidad de vida de las personas, y así también ha abierto oportunidades para nuevas formas de estafas, entre ellas está la ingeniería social el cual es uno de los mayores enemigos para los internautas con desconocimiento en seguridad informática, es por ello que la población nacional está sujeta a ser víctima de un ataque a través de la ingeniería social, debido al mal uso de redes sociales y otros aplicativos, estos ataques se pueden producir porque en los usuarios existe desconocimiento de seguridad informática. De acuerdo con el periódico ecuatoriano Diálogo Américas (2022) se conoció sobre un ataque informático en contra del banco Pichincha, la superintendencia de bancos se pronunció sobre ello e indicó que este incidente se debió al incremento de transacciones virtuales debido a la pandemia y los responsables del ataque fueron expertos reconocidos internacionalmente. Por otro lado las personas exponen datos delicados a través de las redes sociales esto con la intención de ser populares, apoyándose de las facilidades que brindan las redes sociales, sumando a esto, las posibilidades de ser victimizado, aumentan al aceptar solicitudes de amistad de personas desconocidas que pueden estar buscando explotar los datos expuestos para obtener algún beneficio fraudulento de ellos.

El Panorama de Amenazas en América Latina 2021, realizado por el gigante ruso de la ciberseguridad Kaspersky indica que el crecimiento de los ciberataques se refleja en todos los países de la región, con la excepción de Costa Rica, que registró un leve aumento del 2 %. El repunte, que se da en medio de un auge del teletrabajo a causa de la pandemia, lo lidera Ecuador, con un alza del 75 %, seguido por Perú con un 71 %, Panamá con un 60 %, Guatemala con el 43 % y Venezuela con 29 %, de acuerdo con el reporte basado en datos obtenidos por las soluciones de Kaspersky instaladas en usuarios de la región. Así mismo, Gonzalo García, jefe de la Unidad Nacional de Ciberdelitos de la Policía, entregó cifras de los ciberdelitos que se investigan en el país, en lo que va del año. En ese sentido, García aseguró que, en 2020 se registraron 682 indagaciones de este tipo; en 2021 se presentaron 1.852 y, en lo que va del 2022, ya hay 393 casos. Para García esto está directamente relacionado con la falta de cultura digital que existe en el país pues, aunque el 75.6% de la población ecuatoriana usa las nuevas tecnologías de la información como el internet, solo el 10% tiene un conocimiento digital. Entre los delitos cibernéticos más comunes que se cometen en el Ecuador están la apropiación fraudulenta por medios

tecnológicos y la suplantación de identidad, los cuales, según Gonzalo García, están tipificados en el Código Integral Penal (COIP). (Notimundo, 2022). Considerando el nivel de incidencia de ciberdelitos en Ecuador, es importante el estudio de este tema para conocer el impacto que tiene en la comunidad educativa del ISTH.

Por todo lo expuesto se plantea analizar la incidencia del uso de las técnicas de ingeniería social a nivel nacional a través de una investigación bibliográfica y aplicar un escenario práctico a la población académica del Instituto Superior Tecnológico Huaquillas para conocer si la comunidad es victimizada por este problema.

METODOLOGÍA

Durante el desarrollo de esta investigación se ha utilizado el método de la investigación cuantitativo y de carácter exploratorio, así mismo se realizó una investigación bibliográfica, documental sobre las técnicas de ingeniería social a nivel global y también se la enfoca a nivel del Ecuador, así mismo se aplicó una investigación de campo sobre la población académica del Instituto Superior Tecnológico Huaquillas la cual es de 83 estudiantes, donde a través de un formulario de Google se aplicó la técnica de ingeniería social denominada “suplantación de identidad” lo que permitió la recolección de los datos correspondientes de los estudiantes y cuantificar las víctimas de este ataque. Adicionalmente, se resalta la aplicación del método deductivo debido a que la investigación empieza en la población nacional del Ecuador para luego centrarse en la población estudiantil del ISTH.

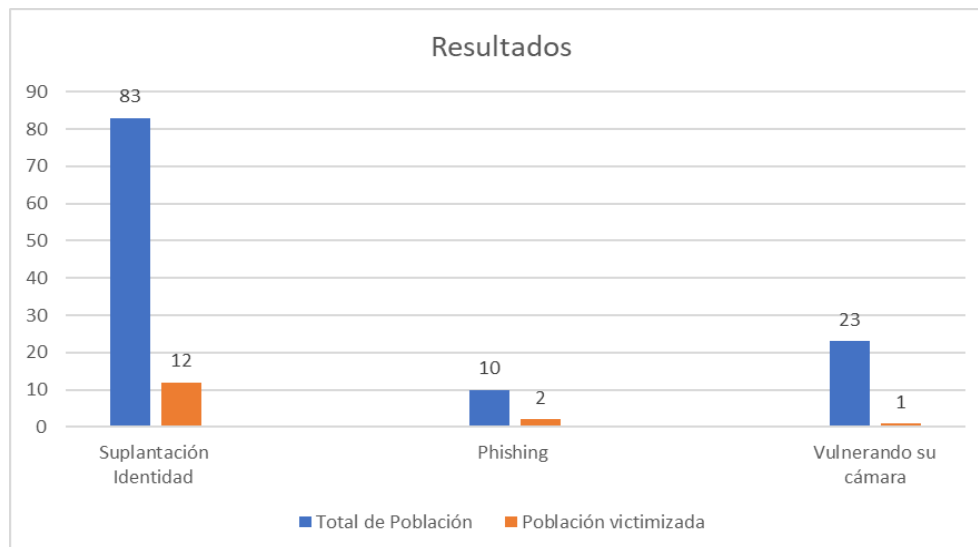
RESULTADOS

La técnica del Phishing inicialmente fue aplicada a 83 estudiantes de la comunidad del ISTH mediante un correo electrónico suplantando la identidad de un Centro de Idiomas de un instituto conocido por la comunidad académica, con asunto “Certificaciones A1-A2 en Inglés”, el correo solicitaba llenar un formulario de Google, de ellos solo 12 es decir el 14.45% fueron víctimas de la técnica, de estos solo 10 proporcionaron el número de teléfono, lo cual permitió enviar un mensaje de whatsapp con un link malicioso, en este nuevo levantamiento de datos se logró obtener las credenciales de 2 estudiantes, de los cuales solo el 10% de ellos compartió información válida, logrando ingresar al correo del alumno. En un tercer intento por vulnerar la seguridad se envía un correo electrónico a 23 estudiantes de primer semestre de la carrera Tecnología en Redes y Telecomunicaciones con el asunto: “FaceApp” que es una aplicación comúnmente usada

para editar fotografías y conocer nuevas personas de distintas partes del mundo, al abrir el link que contenía el correo electrónico, las víctimas deberían dar permiso a las cámaras del dispositivo, para automáticamente tener acceso a su cámara mientras ellos estén dentro del link, finalmente el 4.35% de las víctimas accedió y permitió el acceso a su cámara de la cual capturó dos fotografías y los datos del sistema de su teléfono celular.

Figura 1

Resultados de los tipos de ataques realizados.



Nota: en la figura se presenta los ataques que se realizó a la comunidad académica del ISTH y los resultados obtenidos con cada uno de ellos.

DISCUSIÓN

Los integrantes de las instituciones de educación superior no son excluyentes de ser victimizados por las técnicas de ingeniería social, ya que en Ecuador se han realizado muchos estudios sobre la incidencia de estas, es así que en la investigación de Espinosa (2012), se aplicó la técnica del phishing a través de correos falsos, a 20 estudiantes de la Universidad Técnica Particular de Loja obteniendo que el 40% de las personas fueron victimizadas. Peñafiel (2022) muestra en los resultados de su investigación que el 54% de estudiantes de la Universidad estatal de la Península de Santa Elena brindaron información sensible a través de un correo electrónico enviado por una página clonada. Así mismo Camino y Puente (2020) muestran que el 29.6% de los empleados de la Universidad Politécnica Salesiana de Quito brindaron datos sensibles, que a través de un seguimiento de estos datos permitió ubicar su dirección de domicilio, títulos

universitarios, firma y nombres de familiares los cuáles pueden ser usados para amenazas y estafas. Todo lo expuesto por los investigadores citados revelan que los integrantes de las comunidades académicas pueden ser víctimas de diversas técnicas de ingeniería social, en dos de los casos citados se ve un bajo nivel de incidencia lo cual concuerda con el nivel de victimización obtenida en la institución de educación superior de estudio, sin embargo, se debería difundir estrategias preventivas para evitar caer en técnicas de ingeniería social.

Estrategias preventivas en base al caso práctico.

Tabla 1

Estrategias para evitar vulnerar la información

<i>Caso práctico.</i>	<i>Estrategia</i>
<i>Ingresar información en un formulario.</i>	No entregar información delicada en formularios o redes sociales, sin antes verificar que se trata de una empresa real.
<i>Acceder a un link desconocido recibido por Gmail y z WhatsApp.</i>	No aceptar ofertas, regalos o dar clic sobre links desconocidos sin corroborar que es real.
<i>Otorgar permisos de cámara</i>	Nunca otorgar permisos de cámara y micrófono, en ninguna página no segura.
<i>Entregar credenciales</i>	No entregar credenciales de acceso de ningún tipo.

Nota: Se muestra las estrategias que se deben considerar para evitar caer en estos ataques.

CONCLUSIONES

De acuerdo a lo investigado se pudo concluir que en Ecuador también se aplican técnicas de ingeniería social siendo una de las más aplicadas el phishing que se basa en la suplantación de identidad con el fin de obtener datos sensibles que permitan ser victimizados. En base a lo expuesto se aplicó la técnica suplantación de identidad, como caso práctico de ingeniería social a la comunidad educativa del ISTH, observando que existe un nivel de incidencia bajo para caer en ataques de este tipo, esto aclara que en la población académica existen bases fundamentales que permiten identificar a los posibles ataques que están expuestos. Del 100% de la población total solo un 14.45% contestaron al formulario de suplantación de identidad, y donde solo el 12% entregó sus números celulares, quienes fueron víctimas del método phishing y pharming de esa

proporción de jóvenes solo un 2.40% de la población accedieron al link, y proporcionaron sus credenciales de su cuenta Gmail.

LISTA DE REFERENCIAS

Alcázar, J. P. (2021). Ecuador Estado Digital Enero 2021.

Cervantes, R. (2020). JÓVENES: UNA BREVE MIRADA A SU INCLUSIÓN SOCIAL. Ministerio de Igualdad.

Camino Ruiz, E. S., & Puente Pacheco, E. D. (2020). Análisis y Evaluación de la seguridad en la red de la unidad educativa salesiana cardenal spellman, utilizando herramientas de ingeniería social, y recomendar medidas preventivas. Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/19001/1/UPS%20-%20TTS061.pdf>

Castellanos, E. S. (2011). Ingenieria Social, corrompiendo la mente humana. Seguridad. Cultura de prevención para TI.

CEPAL. (2020). Gestión de datos de investigación. Obtenido de <https://biblioguias.cepal.org/c.php?g=495473&p=4398118>

Comercio, E. (25 de Julio de 2022). 3183 casos de delitos informaticos. EL COMERCIO. Dussan, C. (2006). Políticas de seguridad informática. Redalyc, 91.

Espinosa Armijos, A. S. (2020). Ingenieria Social y sus niveles de incidencia en la UTPL. Obtenido de <https://dspace.utpl.edu.ec/bitstream/123456789/4247/3/Espinosa%20Armijos%20Andrea%20Susana.pdf>

El Universo. (04 de Agosto de 2021). Delitos con pena de prision en Ecuador. El Universo.

El Universo. (31 de Agosto de 2021). Ecuador en la lista: ciberataques en Latinoamérica han aumentado un 24 % este año. El Universo.

Garcia, G. (05 de Mayo de 2022). Delitos Informaticos en Ecuador. (NotiMundo, Entrevistador)

Global Cybersecurity Index (GCI). (2018). Global Cybersecurity Index (GCI). Obtenido de <https://drive.google.com/file/d/1roXfVn3K-DiMSlWuTvyEkIfNCK7gyb15/view>

Hadnagy, C. (2010). Ingeniería social. El arte del hacking personal. Anaya Multimedia.

ISOTools . (11 de Marzo de 2021). ISOTools. Obtenido de Qué es la seguridad de la información y cuantos tipos hay: <https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/>

Ministerio de Telecomunicaciones. (2020). Política pública sobre internet seguro para niñas, niños y adolescentes.

MINTEL. (2018). Ecuador trabaja en medidas preventivas de ciberdelitos. Quito.

- MINTEL. (2021). La Unión Europea asesora a Ecuador en temas de Ciberseguridad. Quito.
- Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis. Bogotá: Ediciones de la U.
- Onofa, M. (Junio de 2022). Ataques cibernéticos amenazan seguridad en Ecuador. Dialogo Americas.
- PandaSecurity. (19 de Septiembre de 2022). PandaSecurity. Obtenido de <https://www.pandasecurity.com/es/mediacenter/seguridad/pharming/>
- Rosero, A. (11 de Enero de 2022). Ciberdelincuentes en el Ecuador. El Comercio.
- Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina. Revista de Derecho.
- Pacheco, M. (2015). Metodología mixta: su aplicación en México en el campo de la demografía. Estudios Demográficos y Urbanos.
- Peñafiel Suárez, M. R. (2022). Ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales. Obtenido de <https://repositorio.upse.edu.ec/bitstream/46000/8683/1/UPSE-TTI-2022-0040.pdf>
- Tamayo, L. (Agosto de 2020). <https://repository.unad.edu.co>. Obtenido de Tecnicas de Ingeniería Social aplicadas a los estudiantes: <https://repository.unad.edu.co/bitstream/handle/10596/37622/ldtamayoar.pdf?sequence=1&isAllowed=y>