Revista de Investigación Multidisciplinaria

CTSCAFE PARA CIUDADANOS.....

http://www.ctscafe.pe

ISSN 2521-8093

Volumen VI- Nº 17 Julio 2022

http://www.ctscafe.pe

Lima - Perú

REVISTA DE INVESTIGACIÓN MULTIDISCIPLINARIA

CTS CAFE Para ciudadanos…

http://www.ctscafe.pe

Volumen VI- N° 17 Julio 2022

ISSN 2521-8093

Técnicas de la ingeniería social más usadas que amenazan tu privacidad digital

Srta. Geraldine Adela Roncal Sánchez
Universidad Nacional de Trujillo
Correo Electrónico: groncal@unitru.edu.pe

Srta. Ericka Paola Salvador Llaro
Universidad Nacional de Trujillo
Correo Electrónico: esalvador@unitru.edu.pe

Dr. Alberto Carlos Mendoza De Los Santos
Universidad Nacional de Trujillo
Correo Electrónico: amendozad@unitru.edu.pe

Resumen: La tecnología ha crecido de manera exponencial, sin embargo, junto con ella, también se ha incrementado los ciberataques y lamentablemente, según estudios, muchas personas han sido afectadas por ello. Por ende, es de suma importancia realizar una investigación sistemática sobre las técnicas de la ingeniería social que amenazan la privacidad de las personas tanto en ambientes personales como laborales. En este contexto, es importante responder a la siguiente pregunta investigativa: ¿Cuáles son las técnicas más usadas de la ingeniería social que amenazan la privacidad digital de las personas? Teniendo en cuenta como objetivo de esta investigación el identificar las técnicas más usadas de la ingeniería social que amenazan la privacidad digital de las personas, tomando como base a la metodología PRISMA a partir de la revisión de publicaciones académicas en diferentes bases de datos de los últimos cinco años para poder mostrar como resultado dichas técnicas, y poder mitigar los riesgos de un ciberataque. Obtuvimos como resultados, que la técnica más usada en la ingeniería social en los artículos académicos encontrados es el phishing (61.5%), seguido del baiting (15.4%), vishing y smishing (15.4%). Todas estas técnicas atentan contra nuestra privacidad digital, es por ello, que se debe tener conocimiento y contar con información verídica y confiable sobre estos tipos de ataques, para evitar que nos genere problemas.

Palabras clave: Ingeniería social/ Phishing/ Baiting/ Vishing/ Smishing.

Abstract: Technology has grown exponentially, however, along with it, cyberattacks have also increased and unfortunately, according to studies, many people have been affected by it. Therefore, it is of utmost importance to carry out systematic research on social engineering techniques that threaten people's privacy in both personal and work environments. In this context, it is important to answer the following research question: What are the most used techniques of Social Engineering that threaten people's digital privacy? Taking into account the objective of this research to identify the most used techniques of social engineering that threaten the digital privacy of people, based on the PRISMA methodology from the review of academic publications in different databases of the last five years to be able to show such techniques as a result, and to be able to mitigate the risks of a cyber-attack. We obtained as results that the most used technique in social engineering in the academic articles found is phishing (61.5%), followed by

baiting (15.4%), vishing and smishing (15.4%). All these techniques threaten our digital privacy, which is why we must have knowledge and have truthful and reliable information about these types of attacks, to avoid generating problems for us.

Keywords: Social engineering/ phishing/ baiting/ Vishing/ Smishing.

Résumé : La technologie a connu une croissance exponentielle, cependant, avec elle, les cyberattaques ont également augmenté et, malheureusement, selon des études, de nombreuses personnes en ont été affectées. Par conséquent, il est de la plus haute importance de mener des recherches systématiques sur les techniques d'ingénierie sociale qui menacent la vie privée des personnes dans les environnements personnels et professionnels. Dans ce contexte, il est important de répondre à la question de recherche suivante : Quelles sont les techniques d'ingénierie sociale les plus utilisées qui menacent la vie privée numérique des personnes ? Tenant compte de l'objectif de cette recherche d'identifier les techniques d'ingénierie sociale les plus utilisées qui menacent la vie privée numérique des personnes, basée sur la méthodologie PRISMA à partir de l'examen des publications académiques dans différentes bases de données des cinq dernières années pour pouvoir montrer ces techniques en conséquence, et être en mesure d'atténuer les risques d'une cyberattaque. Nous avons obtenu comme résultats que la technique la plus utilisée en ingénierie sociale dans les articles académiques trouvés est le phishing (61,5%), suivi du baiting (15,4%), du vishing et du smishing (15,4%). Toutes ces techniques menacent notre vie privée numérique, c'est pourquoi nous devons être conscients et disposer d'informations véridiques et fiables sur ces types d'attaques, pour éviter qu'elles ne nous causent des problèmes.

Mots-clés: Ingénierie sociale/ Phishing/ Baiting/ Vishing/ Smishing.

1. Introducción

Las tendencias en ciberataques han sido más frecuentes en los últimos años. De acuerdo al reporte “Estado de la ciberseguridad 2020” de ISACA, los ciberataques han sido categorizados como el crimen de mayor crecimiento en Estados Unidos. Además, el 53% de los encuestados, responde que espera un ciberataque en los próximos 12 meses. Por otro lado, Perú fue el país que registró el mayor porcentaje de ataques de ingeniería social (31%), seguido por Brasil con más del 18% y México con casi el 17% de las detecciones en América Latina. (Lubeck, 2021).

En este contexto, la ingeniería social, puede ser definida como la aplicación de ciertas técnicas, utilizadas por hackers para timar a un usuario autorizado de sistemas informáticos de una empresa u organización para revelar información sensible, o lograr que realice acciones con el objetivo que la seguridad pueda ser explotada. (Mitnick, 2015).

Por otro lado, Monsalve J. (2018) define a la ingeniería social como “una técnica de fraude para la obtención de información confidencial, acceso o privilegios en sistemas de información, a través de la manipulación de usuarios legítimos”. La ingeniería social se basa en el principio ‘los usuarios son el eslabón más débil’, es por ello que aprovechan la predisposición de las personas de proporcionar detalles financieros a un supuesto empleado de un banco o un aparente compañero de trabajo.

La ingeniería social ha existido desde hace muchísimo tiempo, en la que se combina la ciencia, psicología y arte. En la actualidad, debido a nuevas tecnologías, nuevas

amenazas y la falta de concientización sobre la seguridad de información, se ha logrado que tanto personas como organizaciones sean mucho más fáciles de sufrir un ataque de ingeniería social, teniendo como consecuencia la obtención de información ilegal y/o privada. (Espitia, 2014).

El internet, y el crecimiento exponencial de las redes sociales día a día ha llevado a que sea más sencillo exhibir información de los usuarios, pues no son conscientes de las posibilidades amenazas y riesgos que pueden surgir cuando se realiza alguna publicación de información personal o de interés público. Entonces, los ciberdelincuentes se aprovechan de dichas vulnerabilidades para recolectar información confidencial y luego utilizarla en un cibercrimen. Monsalve J. (2018).

Así mismo, Hernández A. (2019), indica que la ingeniería social se encuentra presente en nuestra vida diaria, desde que somos niños al momento de manipular a cualquier adulto para obtener lo que queramos, hasta en el campo laboral; en donde personas mal intencionadas hacen uso de técnicas de manipulación, para dañar la confidencialidad que se le dio.

La ingeniería social reta la seguridad de todas las redes, dando como consecuencia el aumento de ciberataques en las redes actuales. De acuerdo a cibernética Cyence, concluyó que los Estados Unidos, era el país que recibía mayores ataques de ingeniería social, teniendo un costo de 121, 22 mil millones de dólares. Además, las empresas también se ven afectadas por estos ataques cibernéticos, en donde los delincuentes piratean información valiosa, ocasionando que tenga un impacto negativo en la economía y privacidad mundial. (Salahdine & Kaabouch, 2019).

De acuerdo a una encuesta realizada a 1000 adultos en los Estados Unidos, se concluyó que la mayoría de los entrevistados serían capaces de abrir correos electrónicos, incluso si estos contienen virus o son considerados sospechosos. Con esto se observa que a pesar de las múltiples campañas en donde indican el riesgo de abrir correos sospechosos, aún existen personas que son vulnerables a estos ataques de ingeniería social. (Conteh & Schmick, 2016).

La ingeniería social se ha convertido en una gran amenaza para las comunidades virtuales, debido a que ataca a los sistemas de información; es por esto que, en la actualidad, los servicios que usan los trabajadores han mejorado sus herramientas para combatir estos ataques de ingeniería social. (Krombholz, Hobel, Huber & Weippl, 2015).

De acuerdo a la investigación hecha por el Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19, los resultados fueron que en el 49% de las empresas peruanas hubo aumento de los ciberataques, siendo la más afectada la industria bancaria, con un 52% de incremento percibido. La encuesta también revela que el 21% considera que la ingeniería social (phishing) es el ciberataque que más se ha incrementado, mientras que el 20% sostiene que ha sido el malware.

Monsalve J. (2018) en su artículo de investigación define al fishing como el envío masivo de correos electrónicos a una organización que, a pesar de aparentar ser fiable, intentan obtener datos confidenciales, para luego utilizarlos para algún tipo de fraude. Su método de ataque es por medio de un enlace que dirige a páginas web falsas. De esta manera, el usuario cree estar en un sitio seguro, por lo que introduce alguna información solicitada que, en realidad, va directamente hacia las manos de los ciber atacantes. Es uno de los métodos más comunes de ingeniería social que se usan para estafar y lograr la obtención de información sensible como contraseñas, tarjetas de crédito, entre otros.

En este contexto es importante responder a la siguiente pregunta: ¿Cuáles son las técnicas más usadas de la ingeniería social que amenazan la privacidad digital de las

personas? Por ello, el objetivo de esta investigación es identificar las técnicas más usadas de la ingeniería social que amenazan la privacidad digital de las personas a partir de la revisión de publicaciones académicas en bases de datos de los últimos cinco años para poder mostrar como resultado dichas técnicas, para poder mitigar los riesgos de un ciberataque.

2. Material y métodos

Se llevó a cabo una revisión sistemática científica con el apoyo de la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). La interrogante de investigación establecida para guiar el proceso metodológico fue la siguiente: ¿Cuáles son las técnicas más usadas de la Ingeniería social que amenazan la privacidad digital de las personas?

La revisión sistemática se conoce por tener y describir el desarrollo para recoger, seleccionar, evaluar de forma crítica la evidencia útil con respecto a un tema de estudio. (Moreno, Muñoz & Cuellar, 2018). Tomando en cuenta la definición, se demuestra la importancia del método de estudio, debido a que es explícito, repetible y considera la evaluación del riesgo de sesgos.

Es una herramienta importante para simplificar información científica útil, aumenta la validez de las conclusiones de estudios que fueron hechos de forma individual, además reconoce áreas en donde es necesario hacer una investigación. (González, Urrútia & Coell, 2011). Así mismo, Aguilera R. (2014), lo define como una manera de estudio en donde se recoge y suministra un resumen de un tema en particular, que está dirigido a resolver la interrogante de la investigación.

Para poder comenzar con la búsqueda de información se usaron los siguientes términos a partir de la interrogante de estudio: “social engineering”, “skills”, “ingeniería social”, “técnicas”. Para tener una búsqueda mucho más clara y concisa, se diseñó un protocolo en donde se combinó los términos con operadores booleanos: [("social engineering") and (“skills”)], [("ingeniería social") and (“técnicas”)]. Además, se definió como base datos para la investigación, a EBSCO, MDPI, SCIENCEDIRECT, CJES, IGI GLOBAL y diferentes repositorios de universidades. Las consultas de búsqueda específicas se describen a continuación: EBSCO (“Ingeniería social” and “técnicas”), MDPI (“Ingeniería social”), SCIENCEDIRECT (“Ingeniería social”) y CJES (“Ingeniería social”).

En el presente estudio, se incluyeron artículos académicos originales publicados durante los años 2016 al 2021, tanto en inglés como en español. Cada uno de dichos artículos comprende diferentes técnicas de ingeniería social que logran amenazar constantemente nuestra privacidad digital. Se estableció, además, como criterio de exclusión a aquellos artículos académicos con información obsoleta, de acuerdo a su año de publicación. Las búsquedas de información fueron realizadas en diferentes bases de datos bibliográficas, y revisores de forma independiente.

3. Resultados

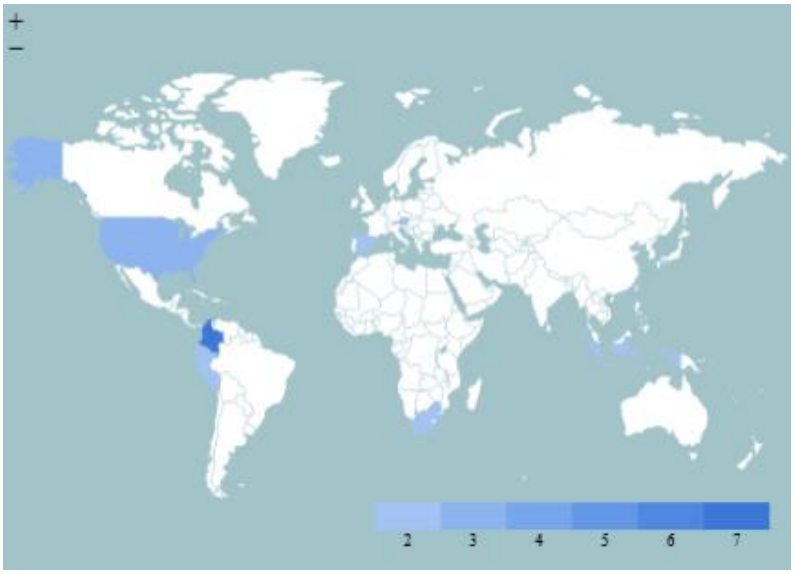
La búsqueda de artículos en las bases de datos y motores de búsqueda arrojó un total de 13 artículos en el periodo de tiempo de 2016 a 2021, distribuidos así: EBSCO 6 artículos, MDPI 1 artículo, SCIENCEDIRECT 2 artículos, CJES 1 artículo, y 3 de repositorios de diferentes universidades. Entonces, con respecto a lo anteriormente mencionado, no se eliminó ninguno por duplicidad de datos, tampoco hubo artículos excluidos que estuvieran fuera del rango de la fecha establecida propuesta anteriormente, ya que en la búsqueda se indicó explícitamente los años requeridos. De esta forma, se obtuvo un valor final de 13 artículos originales para la presentación de resultados. En los 13 artículos seleccionados, se procedió a identificar las técnicas más usadas de la ingeniería social que amenazan la privacidad digital de las personas en los diferentes países del mundo. En la siguiente tabla se muestran dichos artículos encontrados, listándolos por autor, título, año y país.

Tabla N°1: Base de datos de los 13 artículos seleccionados el periodo de tiempo de 2016 a 2021.

N°	Autor(es)	Título	Año	País
1	Benavides Eduardo, Fuertes Walter, Sánchez Sandra	Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura	2020	Ecuador
2	Michelle Nugraha, Nadhia Prili Banglali, Juneman Abraham, Moondore Ali, Esther Widhi	Insights on media literacy and social engineering vulnerability predictors: Lifelong learning gravity	2020	Indonesia
3	Nina Klimburg - Witjes, Alexander Wentland	¿Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses	2021	Austria
4	Francois Mouton, Louise Leenen, H.S. Venter	Social Engineering Attack Examples, Templates and Scenarios	2016	Sudáfrica
5	Fatima Salahdine, Naima Kaabouch	Social Engineering Attacks: A Survey	2019	Estados Unidos
6	Marianne Junger, Lorena Montoya, Floris-JanOverink	Priming and warnings are not effective to prevent social engineering	2017	Estados Unidos
7	Espitia Angélica María	Ingeniería social, amenaza latente para la seguridad informática	2018	Colombia
8	Mendoza Dennis Fabian	Ingeniería social en práctica empresarial	2018	España
9	Cortés Hernández Andrés Mauricio	Ingeniería Social: Phishing y Baiting	2016	Colombia
10	Camacho Nieto Nelson Andrés	Una breve mirada a la ingeniería social	2016	Colombia
11	Silvia Quiroz Zambrano, David Macías Valencia	Seguridad en informática: consideraciones	2016	Ecuador
12	Alejandro Méndez Carvajal	Estudio de metodologías de ingeniería social	2018	España
13	Romero Diego	El arte de la ingeniería social	2018	Colombia

Fuente: Elaboración propia

Figura Nº1: Número de artículos por país representado en un mapa coroplético.



Fuente: Elaboración propia

En los artículos revisados se halló la comparación de la ingeniería social del pasado con la de hoy, en donde nos indica que su existencia empieza desde la creación del ser humano; se puede nombrar como primer ejemplo de ingeniería social, a lo que sucedió en la ciudad de Troya cuando se dio su conquista en el año 1300 a.C. El plan de los griegos fue obsequiarles a los troyanos un caballo gigante construido en madera, conocido como el "Caballo de Troya", pero dentro de este se encontraban soldados que atacarían a la ciudad entera; lo que parecía ser un regalo, resultó siendo una trampa y la perdición para dicha ciudad.

En esa época, se demostró el uso de la ingeniería social para realizar el engaño, y comparándola con la de hoy, "el engaño" a las víctimas depende mucho de la interacción humana, debido a que se busca ganar la confianza de la persona para que se rompa cualquier procedimiento normal de seguridad, logrando así que las mismas víctimas compartan información privada por su propia voluntad. (Romero, 2019).

En el análisis de los documentos se muestra que 8 artículos consideran que la técnica más usada por las personas para realizar ingeniería social, es la de del Phishing, en donde los medios más comunes que son utilizados para los ataques son los correos electrónicos y las páginas web, buscando así estafar a sus víctimas de una manera mucho más fácil.

Tabla Nº2: Técnica phishing

N°	Autor(es)	Título	Año	País	Técnica
1	Benavides Eduardo, Fuertes Walter, Sánchez Sandra,	Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura	2020	Ecuador	Phishing Emails y por Phishing Websites
2	Francois Mouton, Louise Leenen, H.S. Venter	Social Engineering Attack Examples, Templates and Scenarios	2016	Sudáfrica	Phishing Emails, Phishing Websites y Phishing Letter
3	Fatima Salahdine, Naima Kaabouch	Social Engineering Attacks: A Survey	2019	Estados Unidos	Spear Phishing, Whaling Phishing, Business Email Compromise Phishing
4	Marianne Junger, Lorena Montoya, Floris-JanOverink	Priming and warnings are not effective to prevent social engineering	2017	Estados Unidos	Phishing Emails, Phishing Websites, Spear-Phishing Mails
5	Espitia Angélica María	Ingeniería social, amenaza latente para la seguridad informática	2018	Colombia	Ataque más usado es el Phishing
6	Mendoza Dennis Fabian	Ingeniería social en práctica empresarial	2018	España	El Phishing se da por correos
7	Camacho Nieto Nelson Andrés	Una breve mirada a la ingeniería social	2016	Colombia	Phishing es la técnica más usada
8	Silvia Quiroz, David Macías	Seguridad en informática: consideraciones	2016	Colombia	Phishing es la técnica más usada

Fuente: Elaboración propia

Por consiguiente, se muestra que 2 artículos en donde indica que otra técnica que es usada con frecuencia es el Baiting. Según Hernández A., 2016, el Baiting se define en dejar dispositivos como USB, CD, DVD infectados con algún software infectado, de esta manera esperando a que cualquier persona recoja el dispositivo y lo use, para poder obtener los datos personales de la persona. Teniendo la misma cantidad de artículos, otras de las técnicas que se usan son el Vishing y Smishing. La técnica Vishing se usa cuando el ingeniero social busca sacar información sensible por medio de llamadas telefónicas, en el caso de Smishing, los delincuentes buscan obtener información por medio de mensajes SMS en donde se indica que la persona ganó premios o fue considerado para participar en una rifa.

Tabla Nº3: Técnica baiting

N°	Autor(es)	Título	Año	País	Técnica
1	Michelle Nugraha, Nadhia Prili, Juneman Abraham, Moondore Ali, Esther Widhi	Insights on media literacy and social engineering vulnerability predictors: Lifelong learning gravity	2020	Indonesia	Una de las técnicas más comunes es el Baiting
2	Cortés Hernández Andrés Mauricio	Ingeniería Social: Phishing y Baiting	2016	Colombia	Se hace uso de USB, CD, DVD, para lograr Baiting

Fuente: Elaboración propia

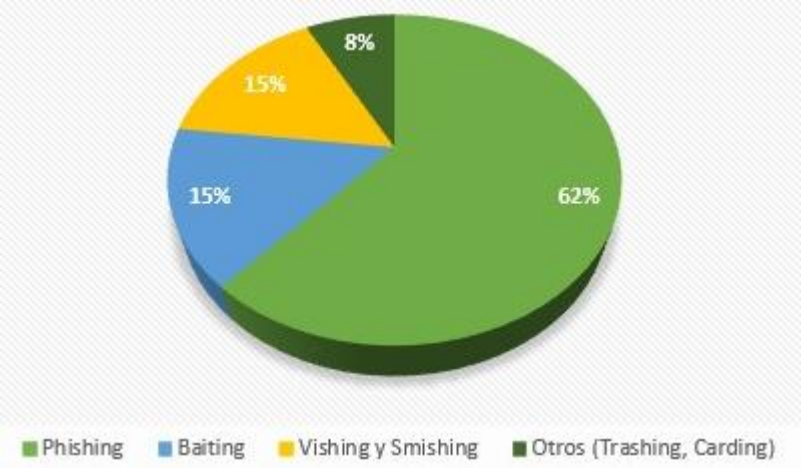
Tabla 4: Técnica vishing y smishing

N°	Autor(es)	Título	Año	País	Técnica
1	Alejandro Méndez Carvajal	Estudio de metodologías de ingeniería social	2018	Colombia	Smishing por SMS Vishing por llamadas
2	Romero Diego	El arte de la ingeniería social	2018	Colombia	Vishing por teléfono fijo Smishing con mensajes de texto

Fuente: Elaboración propia

También se detectaron otras formas poco comunes de ingeniería social, dentro de las cuales tenemos a Trashing, que consiste en que el delincuente revisa la basura en busca de documentos o aparatos electrónicos que fueron desechados, para usarlos en la obtención de información. Entre otras, se encuentra el Carding, que consiste en robar tarjetas de créditos para realizar compras ilegales hasta que sean canceladas.

Figura 2: Técnicas más usadas de la Ingeniería social.



Fuente: Elaboración propia

4. Discusión

La investigación realizada nos muestra que la ingeniería social ha existido desde tiempos antiguos, un claro ejemplo es el conocido "Caballo de Troya". Sin embargo, poco a poco este "engaño" se fue perfeccionando debido al avance de la tecnología. Una de las técnicas más usadas por las personas para realizar ingeniería social es el Phishing; lo que hace el delincuente es buscar la información sensible por medios electrónicos para beneficiarse económicamente, siendo uno de ellos los correos electrónicos y páginas web que buscan estafar a víctimas. (Benavides, Fuertes & Sánchez, 2020)

Para Cortés A. (2016), otra de las técnicas más comunes que son usadas por los ciber atacantes, es el Baiting, en donde se hace uso de dispositivos como USB o CD; lo que se busca es que la víctima tome estos dispositivos para luego usarlos en sus computadoras, de esta manera el archivo malicioso infecta la máquina y se obtiene información. Como las terceras técnicas más usadas, tenemos al Vishing y Smishing. El primero consiste en sacar información sensible por medio de llamadas telefónicas, mientras que el segundo, se basa en obtener información por medio de mensajes SMS. Ambas técnicas tienen diferentes formas de atacar, pero lo que tienen en común es el objetivo que quieren lograr, robar información privada. (Mendéz, 2018)

Por último, consideramos que otras técnicas importantes a mencionar es el Trashing, que consiste en que el delincuente revisa la basura en busca de documentos o aparatos electrónicos que fueron desechados, para usarlos en la obtención de información; y el Carding, que consiste en robar tarjetas de créditos para realizar compras ilegales hasta que sean canceladas.

La presente investigación identificó las técnicas más usadas de la ingeniería social que amenazan la privacidad digital de las personas a partir de la revisión de artículos académicos en las bases de datos EBSCO, MDP, SCIENCEDIRECT, CJES, y diferentes repositorios universitarios de los últimos cinco años.

5. Conclusiones

En la actualidad, la ingeniería social no solo debe ser tratada como una amenaza de nivel tecnológico; por su origen y necesidad de obtener información, el simple hecho de solo dar información personal por la confianza obtenida, ya nos hace vulnerables. Con el estudio realizado, podemos conocer que hay muchas técnicas en la que podemos ser víctimas de un ataque de ingeniería social, siendo las más común el Phishing (61.5%). De acuerdo a los artículos descubrimos que el Phishing está presente en nuestra vida cotidiana, ya sea por medio de un correo electrónico o SMS; otras de las técnicas que son utilizadas por los delincuentes son el Baiting (15.4%), en donde hace uso del USB o CD para obtener información sensible. Cabe mencionar las técnicas de Vishing y Smishing (15.4%), en la primera hace uso de las llamadas telefónicas, en el segundo caso, es más común el uso de SMS, engañando a la persona por medio de premios o rifas. Todas estas técnicas atentan contra nuestra privacidad digital, más aún si no se tiene conocimiento de estas, es por eso que es recomendable informarse correctamente sobre estos tipos de ataques, además de conocer la manera correcta de manejar nuestra información personal; de esta manera se evitaría perjudicarnos con estos ciberataques y generarnos problemas.

6. Literatura citada

Benavides, E., Fuertes, W., Sánchez, S., & Núñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. Ciencia y Tecnología, 13(1), 97–104. https://doi.org/10.18779/cyt.v13i1.357

Berenguer Serrato, D. (2018). Estudio de metodologías de ingeniería social. Recuperado de https://bibliotecaupn.elogim.com/auth-meta/login.php?url=https://ebsco.bibliotecaupn.elogim.com/login.aspx?direct=true&db=edsair&AN=edsair.dedup.wf.001.35f00cfebf150cab2b91cb033ddebe27&lang=es&site=eds-live

Camacho, N. (2016). Una breve mirada a la ingeniería social. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2712/Trabajo%20de%20grado3383.pdf?sequence=1&isAllowed=y

Cortés, A., (2016). Ingeniería social: phishing y baiting. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6349/Ingenieria%20social%20Phishing%20y%20Baiting.pdf?sequence=1&isAllowed=y

Espitia Garzón, A. M. (2014). Ingeniería social amenaza latente para la seguridad informática. Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2878

Espitia Garzón, A. M. (2014). Ingeniería social amenaza latente para la seguridad informática. Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2878

Hernández, C., & Mauricio, A. (2019). Ingeniería social Phishing y Baiting. Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/6349

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, 66, 75–87. https://doi.org/10.1016/j.chb.2016.09.012

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "Deficient User" in Cybersecurity Discourses. Science, Technology, & Human Values, 46(6), 1316–1339. https://doi.org/10.1177/0162243921992844

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

López Grande, C. E. (2015). Ingeniería social: el ataque silencioso. Recuperado de http://www.redicces.org.sv:80/jspui/handle/10972/2910

Lubeck, L. (2021). En 2020 se duplicaron las detecciones de ataques de ingeniería social. (2021, enero 7). Recuperado el 27 de diciembre de 2021, de WeLiveSecurity website: https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/

Mendez, M., & Yesid, J. (2018). Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos). Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/4663

Mendoza, D. (2018). INGENIERÍA SOCIAL EN PRÁCTICA EMPRESARIAL. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8584/Ingenieria%20social%20en%20pr%c3%a1ctica%20empresarial.pdf?sequence=1&isAllowed=y

Mouton, F., Leenen, L., & Venter, H. s. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Moyano Morales, S. A. (2015). La manipulación de la mente humana como arma blanca en la ingeniería social. Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2926

Nugraha, M., Banglali, N., Abraham, J., Ali, M., & Andangsari, E. (2020). Insights on media literacy and social engineering vulnerability predictors: Lifelong learning gravity. Cypriot Journal of Educational Sciences, 15, 955–975. https://doi.org/10.18844/cjes.v15i5.5124

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en informática: consideraciones. Dominio de las Ciencias, ISSN 2477-8818, Vol. 3, No. 3, 2017, pags. 676-688. Recuperado de https://bibliotecaupn.elogim.com/auth-meta/login.php?url=https://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.EF9932C&lang=es&site=eds-live

Romero, D. (2018). El arte de la ingeniería social. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingenier%C3%ADa%20social.pdf?sequence=1&isAllowed=n

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A Survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

State of Cybersecurity 2020. (s/f). Recuperado el 24 de noviembre de 2021, de ISACA website: https://www.isaca.org/go/state-of-cybersecurity-2020

REVISTA DE INVESTIGACIÓN MULTIDISCIPLINARIA

CTSCAFE Para ciudadanos…

http://www.ctscafe.pe

Volumen VI- N° 17 Julio 2022

Contáctenos en nuestro correo electrónico
revistactscafe@ctscafe.pe

Página Web:
http://ctscafe.pe

Blog:
https://ctscafeparaciudadanos.blogspot.com/

Facebook
https://www.facebook.com/Revista-CTSCafe-1822923591364746/

latindex