Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas

TEMA:

Diseño de una campaña de ataques de ingeniería social

AUTOR:

Sofía Daniela Villacís Miranda

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE TECNOLOGÍAS DE LA INFORMACIÓN

QUITO, JULIO – 2023

DEDICATORIA

Para mi abuelita Bolita, que para mí ha sido un ejemplo de fortaleza y perseverancia desde que tengo memoria. En todo este camino me supo mostrar que el esfuerzo y la constancia son fundamentales para alcanzar mis metas. Quiero honrarle por su amor incondicional, por su sabiduría y por su dedicación hacia mí.

Es un pilar fundamental en mi vida, y este logro no sería posible sin usted. Me siento afortunada de tener una abuela tan especial como usted, alguien a quien puedo admirar y amar con todo mi corazón. Espero que esta dedicatoria sea un humilde reconocimiento a la gran mujer que es y una muestra de mi cariño y agradecimiento.

AGRADECIMIENTO

Agradezco principalmente a mis padres que a lo largo de este caminando siempre me han apoyado para poder cumplir todo lo que he deseado. Gracias por haberme guiado por el mejor camino y siempre estar pendientes de mí. Estoy realmente agradecida por cada sacrificio que hicieron para que mis hermanos y yo siempre podamos tener lo mejor. Se que sin su apoyo no sería la mujer que soy hoy en día.

También quiero agradecer a mis hermanos, que siempre me han ayudado en cada paso que he dado y aunque a veces tengamos algunos desacuerdos, yo siempre estaré para ustedes.

RESUMEN

El proyecto se centra en la ingeniería social y como esta afecta a las personas en cuanto al tema de su información confidencial y los riesgos que puede traer si es víctima de uno de estos ataques. Para evaluar esta situación se implementó un pequeño ataque de phishing controlado el cual tiene la finalidad de crear una campaña de ingeniería social. Esto es de gran utilidad ya que se identificó que la mayor causa por la cual las personas caen en este tipo de ataque es debido a la falta de conocimiento sobre el tema. En este proyecto la metodología utilizada fue descriptiva, se identificó los factores que hacen que las personas sean vulnerables a un ataque de ingeniería social y se demostró las fases que se usa para realizar este tipo de ataque. Los resultados obtenidos arrojaron que la primera fase que es la de investigación es de suma importancia para poder tener éxito en el publico deseado. Se identifico que al no poner ninguna restricción en el campo contraseña las personas que ingresaron sus datos utilizan contraseñas débiles relacionas con su información persona o con temas sociales. Gracias a la concientización que se mandó a cada correo electrónico registrado se ha logrado cumplir con la campaña de ingeniería social en este proyecto. Para futuras investigaciones se propone realizar no solo ataques de phishing, si no probar otros ataques de ingeniería social para evaluar cual es el que más caen las personas.

ÍNDICE

ÍNDICE DE FIGURAS

CAPÍTULO I: INTRODUCCIÓN

1. Marco de Referencia

1.1. Justificación

El presente proyecto propone la campaña de ingeniería social como solución para que los usuarios dejen de ser víctimas de estos ataques por falta de conocimiento sobre el tema. Al aplicar las campañas se lograría reducir el riesgo que los empleados o personas que pertenezcan a una organización caigan en engaños, que su información sea robada o que ejecuten cualquier tipo de virus que afecte no solo personalmente si no a la organización a la que pertenecen. Además de proporcionar conocimiento a las personas, se puede cerrar una brecha de seguridad en las organizaciones que son los mismos usuarios. Por las razones expuestas anteriormente, es que se identificó que las campañas de ingeniería social son una solución para mostrar el riesgo a que se pueden enfrentar los usuarios y proporcionar información de cómo evitar ser víctimas de este ataque.

1.2. Planteamiento del problema

A lo largo del tiempo se ha desarrollado una dependencia a la tecnología y está creció mucho más en la pandemia por la covid-19 en el año 2019. Debido a este crecimiento en, en el año 2020 se observa un aumento de ataques de ingeniería social (Lubeck, 2021).Por consecuencia, muchos usuarios se vuelven vulnerables a que sus datos sean robados debido a que no existen campañas de ingeniería social que los eduque y muestre como identificar un ataque de este tipo. Los ataques de ingeniería social se han vuelto una seria amenaza porque es más fácil sacar información de una persona que de un sistema (Koyun & Al Janabi, 2017).Logrando que la propia persona de sus datos sin que se dé cuenta. Con esta

simple información es más que suficiente para un cracker vulnerar una contraseña que hacer un ataque de fuerza bruta. Es importante mencionar que la información obtenida puede ser usada con malas intenciones, vendida en el mercado negro o en la Deep web (Salahdine y Kaabouch, 2019).

1.3. Objetivo General

Implementar una campaña de ingeniería social que instruya a los usuarios sobre los riesgos asociados con las técnicas utilizadas en este arte, mediante la demostración de un ataque de ingeniería social

1.4. Objetivos Específicos

- Fundamentar las características principales y etapas de la ingeniería social mediante revisión bibliográfica
- Implementar un ataque real utilizando ingeniería social a diferentes usuarios.
- Analizar los factores determinantes para que el usuario sea víctima del robo de información mediante ataques informáticos.
- Concientizar las vulnerabilidades de los usuarios mediante una campaña de ingeniería social

1.5. Alcance

Implementar un ataque de ingeniería social controlado en el cual se pueda instruir a los usuarios a tener precaución con este tipo de ataques. Esto se logrará al enviar un correo de concientización a todas las personas que hayan ingresado sus datos. El presente proyectó se limitará a exponer que es la ingeniería social, los riesgos que trae, una campaña de concientización y un análisis de los resultados obtenidos.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1.Antecedentes

2.1.1. Historia

El término "ingeniería social" apareció por primera vez en el contexto de la informática en 1990, introducido por los llamados "crackers", quienes a diferencia de los "hackers", utilizan su conocimiento técnico con fines malintencionados. Los crackers comenzaron a emplear técnicas psicológicas como la persuasión y la manipulación para violar sistemas. Es importante destacar que estos métodos psicológicos resultaron más efectivos que tratar de vulnerar directamente los sistemas informáticos. En lugar de intentar forzar la entrada a un sistema, los crackers se dieron cuenta de que era más fácil obtener información confidencial a través de la manipulación de las personas que lo utilizan.

Uno de los pioneros en utilizar la ingeniería social es Kevin Mitnick, quien fue capturado por el FBI el 15 de febrero de 1995 y condenado a 5 años de prisión por realizar actos considerados ilegales utilizando esta técnica. Pero ¿cómo lograba Mitnick obtener la información que necesitaba? Su estrategia consistía en no preguntar directamente lo que necesitaba, sino en aparentar que ya tenía esa información, pero equivocada, para que las personas corrigieran sus errores con la información correcta. De este modo, Mitnick demostró que las personas son el eslabón más débil en la seguridad informática. Al aplicar estas técnicas psicológicas junto con sus habilidades técnicas, podía acceder a los sistemas y obtener una gran cantidad de información. (Pastor, 2018)

Desde este antecedente la suplantación de identidad, manipulaciones psicológicas, correos engañosos, entre otros. Se volvieron algo común para los crackers. Esto evolucionó y hoy en día

el Phishing, que se explicará más a detalle más adelante, se convirtió en el año 2020 el ataque de ingeniería social más popular. (¿Qué es la ingeniería social?, s.f.)

2.1.2. Caso Real

Un caso famoso sobre ingeniería social es asociado con la empresa “Uber”. Este ocurrió en el año 2022, el atacante aplico la ingeniería social y logró tener acceso a procedimientos internos y a un medio de comunicación interno de la organización. Este ataque conllevo a que la organización obtenga mala fama y afecciones económicas.

La persona que realizó el ataque en vez de intentar un ataque de fuerza bruta que le tomaría mucho tiempo, optó por aplicar la técnica de ingeniería social haciéndose pasar por un técnico oficial de la organización y pidiendo al trabajador que ingrese sus credenciales en un sitio no oficial. De esta forma es que el atacante logró tener acceso en unos cuantos minutos.

Tuvo acceso a un sistema de comunicación interno de la organización “Slack” en el cual pudo mandar algunos mensajes sobre los accesos que tuvo como el código fuente de Uber, email y diferentes sistemas internos. El atacante tenía 18 años y tuvo acceso a toda la información de la empresa y demostró que “Uber” tiene una brecha de seguridad de información. (Conger y Roose, 2022)

En este caso se evidencia la falta de capacitación a los trabajadores sobre temas comunes como el phishing. La ingeniería social a punta al eslabón más débil que sería las personas.

2.1.3. Tipos de ataques comunes en la actualidad.

En la era digital que se vive actualmente los atacantes buscan cualquier vulnerabilidad para explotarla y poder ingresar al sistema. Según el sitio web Crowdstrike, los ataques que se muestran a continuación son los más comunes. (Baker, 2023)

- **Malware:** implica el tener un software malicioso, el cual al ser ejecutado este puede robar información. Dentro de este ataque se encuentra el ransomware, troyanos, spyware, virus, gusanos, keyloggers, bots, cryptojacking.
- **Denegación de Servicio (DoS):** Está dirigido a un objetivo en específico y lo que hace es que envía muchas peticiones al servidor para que este se sobrecargue y muchas veces al no tener bien configurado este servidor puede liberar información. Lo que provoca este ataque es que los trabajadores de la organización no tengan acceso a los servicios que normalmente usan, causando a la organización una paralización de procesos y esto conlleva pérdidas económicas.
- **Inyección de código:** Este tipo de ataque se centra en ingresar cierto código malicioso en una vulnerabilidad. Al lograr inyectar este código el adversario puede realizar cualquier cosa para llegar a su objetivo final. En este ataque entra el sql injection el cual es ingresar sentencias en una base de datos que le permita ya sea borrar, obtener o alterar la información. También esta cross-site Scripting el cual es muy común en blogs y sitios web que permiten a los usuarios publicar información. Este ejecuta un script infectado y permite ver información sensible de las personas. Finalmente, en este tipo de ataque se encuentra el Malveritising, este está en sitios web que contienen anuncios y una vez la persona hace clic en un anuncio este puede instalar malware o un adware.
- **DNS Tunneling:** En este ataque el adversario tiene un servidor al cual llegará la información. El Tunneling de DNS lo que hace es enrutar las solicitudes del DNS hacia el servidor del atacante. Lo que proporciona un canal de comando y control. Este tipo de ataque es muy lento ya que la data enviada por DNS no puede ser muy

extensa. Además, este ataque es difícil de detectar debido a que el servidor DNS siempre está intercambiando información.

- **Ataques de IoT:** Al vivir en una era tecnología se ve la tendencia de hacer una casa inteligente. Estos dispositivos pueden ser vulnerables ya que todos necesitan una conexión a internet. El atacante tiene dos opciones, la primera es ingresar a la red y de esta forma tener control de los dispositivos o tener acceso a cualquier dispositivo e ingresar a la red para obtener información. Este ataque es muy peligroso ya que por ejemplo si un atacante tiene acceso al seguro de la puerta, tranquilamente este puede abrir o cerrarlo y puede ocasionar pérdidas económicas al poder entrar y robar la casa.
- **Ingeniería social:** El ataque más usado actualmente. Este ataque requiere de ingenio por parte del adversario. Ya que trata de una investigación previa para que la víctima caiga. En este ataque entra el phishing o el spoofing. También otros tipos de ataques que se verá a detalle más adelante.

2.2.Ingeniería Social

2.2.1. Introducción

Según la página de Kaspersky, se puede definir a la Ingeniería Social como una técnica de manipulación que se aprovecha de las vulnerabilidades de las personas para conseguir información confidencial. Esto también es conocido como hacker a la persona. (Kaspersky, s.f.)

El principal objetivo para este tipo de ataque es aprovecharse de la falta de conocimiento sobre este tema. Y ¿Cómo y por qué lo hace? Se lo hace ya que una persona puede dar su información sin que se dé cuenta y con esto ya se puede acceder. Lo que, contrastado con hacer un ataque de fuerza bruta, aplicar la ingeniería social es mejor ya que no lleva mucho tiempo. Ahora

bien, existe una serie de etapas para llevar a cabo este tipo de ataque. Estas serán detalladas más adelante, pero lo principal es ganarse la confianza de la víctima y sacar su información.

En general se puede decir que la ingeniería social es un ataque que mediante el uso de técnicas psicológicas se saca información para poder tener acceso a algún sistema, datos bancarios, causar fraude, suplantar identidades, entre otros para poder obtener muchas de las veces una ganancia económica.

2.2.2. Tipos de Ingeniería Social

A continuación, se describirá en que consiste cada tipo de ingeniería social. Estos fueron tomados de la fuente Kaspersky. (Kaspersky, s.f.)

- ***Phishing:*** es un tipo de ataque en el que los delincuentes envían correos electrónicos que hacen que la víctima crea que necesita proporcionar sus credenciales para poder seguir utilizando un servicio en línea. Sin embargo, no solo buscan obtener credenciales, sino que también pueden usar el phishing para infectar la computadora de la víctima con malware y así obtener acceso a mucha más información.

  Dentro de este tipo de ataque, existe el spear phishing, en el que el delincuente se hace pasar por un alto mando de una organización o una persona conocida por la víctima, lo que genera más confianza y hace que la víctima caiga más fácilmente en la trampa. El segundo tipo dentro de esta categoría es el spam phishing, en el que el delincuente envía el correo varias veces hasta que la persona dude de su veracidad y caiga en el engaño. Es importante mencionar que estos correos suelen venir con una historia detrás, por ejemplo, que la persona tiene un juicio pendiente o una deuda por pagar.

- ***Baiting:*** El principal objetivo es infectar de malware la computadora. Para esto, es común que cuando una persona descargue música o algún programa gratis, estos vengan con malware el cual pueda sacar información. Por otro lado, el hecho de dejar un flash infectado y que alguien más la tome y la conecte también es una forma de baiting.
- ***Tailgating:*** Se trata de seguir a una persona que tiene los permisos que se necesita. Parar lograrlo puede ser de manera física. Por ejemplo, que la persona que tiene acceso al datacenter antes de que se cierre la puerta ingrese alguien más. También puede ser mediante la computadora que usa si la deja desbloqueada alguien podría aprovecharse de esto.
- ***Pretexting:*** El delincuente realiza una situación que sabe que la víctima está pasando y ofrece ayudarle. Para esto le solicita cierta información. Un ejemplo muy común que usan los ladrones de Ecuador es que, una vez robado un iPhone mandan un mensaje a un familiar de la víctima haciéndose pasar por Apple para que este pueda bloquear el celular y solicitan las credenciales.
- ***Quid Pro quo:*** Esta es una estafa ya que se ofrece lo que la víctima desee a cambio de información o simplemente dinero. Por ejemplo, si se quiere obtener las respuestas a algún examen o simplemente un anuncio que diga que te has ganado un iPhone 14.
- ***Scareware:*** Se trata de falsas alarmas que crean los delincuentes para hacer creer que necesitan bajar cierto programa para que se libere el malware de su dispositivo que realmente no existe. Pero al momento de bajarlo, este software lo infecta.

2.2.3. Riesgos

La ingeniería social tiene como principal objetivo a los humanos, quienes sin saberlo proporcionan información valiosa. Sin embargo, compartir información personal con un

desconocido puede tener consecuencias graves. La respuesta a la pregunta de si compartir información personal conlleva riesgos tiene dos perspectivas. Por un lado, si la persona con la que se comparte información no tiene malas intenciones, es poco probable que haya repercusiones graves. Por otro lado, los crackers pueden utilizar esta información con intenciones maliciosas, desde robar dinero hasta infectar dispositivos con ransomware.

Es importante tener en cuenta algunos de los riesgos que la ingeniería social trae consigo. Estos riesgos pueden incluir la exposición de información personal y confidencial, la suplantación de identidad, el acceso no autorizado a cuentas bancarias o de redes sociales y la propagación de virus informáticos. A continuación, se detalla algunos de los riesgos que existen.

- **Exposición de información personal:** la ingeniería social puede llevar a la revelación de información personal confidencial, como contraseñas, números de seguridad social, direcciones de correo electrónico, direcciones físicas, números de teléfono y otros datos personales. Esta información puede ser utilizada por los crackers para cometer fraudes o delitos de otro tipo.
- **Suplantación de identidad:** los crackers pueden utilizar la información obtenida a través de la ingeniería social para suplantar la identidad de una persona y acceder a sus cuentas financieras o de redes sociales. Esto puede llevar a la pérdida de recursos financieros, la propagación de virus informáticos y la exposición de información personal.
- **Pérdida de recursos financieros:** los crackers pueden utilizar la información obtenida a través de la ingeniería social para acceder a cuentas bancarias y robar dinero. También pueden utilizar la información para cometer fraudes o solicitar créditos a nombre de otra persona. (Easydmarc, 2022)

- **Daño a la reputación:** la ingeniería social puede llevar a la publicación de información personal o confidencial en línea, lo que puede dañar la reputación de una persona o empresa. (Easydmarc, 2022)

2.2.4. Medios de ataque de Ingeniería Social

Los atacantes utilizan diferentes medios para diferentes ocasiones en las que se quiere aplicar la ingeniería social. Junto con los principios de la ingeniería social que se explicará más adelante es más probable que el ataque sea más exitoso. A continuación, se muestra los 4 distintos medios según el artículo "Social Engineering Attacks". (Koyun & Al Janabi, 2017)

Por Teléfono

Por este medio se inició la ingeniería social como se mencionó anteriormente las personas se hacen pasar por una persona importante o que tenga los permisos necesarios para que el atacante pueda tener acceso. Este es un medio que hasta en la actualidad se sigue ocupando y muchas veces ha resultado como por ejemplo el caso de "Uber" que se mencionó anteriormente.

Por Internet

Este medio ahora es el más común y el más utilizado hoy en día. El phishing es uno de los ataques de ingeniería social que más usa este medio para robo de información o para infectar de malware por medio de un link. Otra técnica poco común que se utiliza en este medio es poner una ventana emergente en la que la persona cree que esta en la página correcta e ingresa sus datos.

Por Dumpter Diving

Este medio es poco utilizado, pero se trata en buscar entre la basura para sacar información normalmente de empresas. Con esa información que el atacante encuentre, puede usarlo a su favor y obtener buenos resultados al aplicar el ataque de ingeniería social.

Manipulación Psicológica

Este medio es el que se puede combinar con los otros medios. Principalmente se centra en manipular a las personas para que sin que se den cuenta den su información.

CAPÍTULO III: METODOLOGÍA

3.1.Proceso para aplicar la ingeniería social

3.1.1. Definición de método

Para el presente trabajo se utilizará el método descriptivo ya que se pretende obtener de los resultados los factores determinantes que hacen que las personas caigan en ataques de ingeniería social. Los datos serán obtenidos una vez que se realicé el ataque. A continuación, se describirá como será el proceso que se llevará a cabo desde el inicio hasta culminar el ataque.

3.1.2. Principios de la ingeniería social

Los siguientes principios son mencionados por Christopher Hadnagy en su libro "Social Engineering The Science of Human Hacking". En este libro se describe como es que la ingeniería social funciona y como los siguientes principios son fundamentales para aplicarla. (Hadnagy, 2018)

- Principio 1: Reciprocidad

El principio de reciprocidad se puede describir en una sola palabra: altruismo. Cuando se ofrece algo que la otra persona quiere escuchar o necesita, es posible que esta persona sienta una especie de deuda emocional, lo que puede generar un deseo de ser recíproco. Esto genera la oportunidad de mencionar lo que se desea. Dando como resultado obtener lo que se quiere.

- Principio 2: Obligación

El principio de obligación se basa en hacer que las personas se comporten de acuerdo con lo que se considera socialmente correcto. En el contexto de la ingeniería social, este principio se puede utilizar para establecer una relación de confianza con una víctima, para que permita acciones sin la necesidad de contar con los permisos necesarios. Hadnagy, en su libro, explica que, para

entrar en un lugar sin credencial, basta con crear una situación en la que la otra persona sienta la necesidad de hacer lo correcto. Por ejemplo, entrar a un lugar con muchas cajas pesadas y hacer que la otra persona abra la puerta. Si bien la persona puede solicitar la credencial, el manipulador puede solicitar ayuda para sacarla del bolsillo, lo que crea una situación incómoda y lleva a la otra persona a ceder.

- Principio 3: Concesión

El principio de concesión se basa en hacer que la otra persona ceda a lo que se necesita de manera indirecta. Es decir, se ofrece algo exagerado en primer lugar, y después, cuando se niega, se ofrece algo que se sabe que la persona está dispuesta a dar. Al analizar las dos opciones, la persona probablemente cederá a la segunda opción, que es lo que el atacante quería desde el principio. Este mismo principio se puede aplicar para obtener información. Simplemente se proporciona información errónea para que la víctima entregue la información correcta.

- Principio 4: Escasez

El principio de escasez se refiere a convertir una situación que puede no ser muy importante en una situación que necesita atención inmediata. Para lograr esto, se intenta hacer parecer que, si no se actúa de inmediato, se enfrentarán consecuencias graves. Esto lleva a la otra persona a ceder y tomar medidas inmediatas para resolver el problema y evitar cualquier posible problema. Sin embargo, esto también puede permitir que el atacante tenga pleno acceso a información sensible o tomar control de una situación.

- Principio 5: Autoridad

El principio de autoridad se basa en investigar quién tiene el mayor rango o autoridad en la organización o situación a la que se quiere acceder. Una vez que se ha identificado a esta persona, se puede utilizar su nombre o cargo para influir en otras personas y conseguir lo que se

necesita. Esto funciona debido a que la figura de autoridad genera temor en las personas a cometer errores o a actuar en contra de lo que se ha ordenado, por lo que a menudo cederán ante el nombre o cargo de la figura de autoridad.

- Principio 6: Constancia y Compromiso

El Principio de constancia y el compromiso muestra que para lograr obtener la información deseada. Para ello, el atacante debe tener una estrategia clara que le permita establecer una relación de confianza o amabilidad con la víctima. Es fundamental que el atacante sea capaz de anticiparse a las posibles situaciones y adaptar su estrategia según sea necesario para lograr su objetivo.

Además, es importante tener en cuenta que el proceso de obtener información debe ser gradual y no debe empezarse de manera directa. De esta manera, el atacante puede ir construyendo la confianza con la víctima de forma progresiva, lo que aumentará las posibilidades de éxito en la manipulación. En definitiva, la perseverancia y la paciencia son claves para lograr los objetivos de la ingeniería social.

3.1.3. Diseño de investigación

La investigación es la primera fase para un ataque de ingeniería social. Aquí se define que escenario es el más adecuado para realizar el ataque. Para que una persona se convierta en víctima se tiene que establecer una relación de confianza. Por lo que se debe tomar en cuenta los distintos tipos de ingeniería social que se mencionó anteriormente. En el presente proyecto se lo realizará por medio de una propaganda donde se oferte algo atractivo para que las personas tengan el sentimiento de revisar de que se trata. Esto hace referencia a Quid Pro quo.

3.1.4. Ejecución de ataque

Se realiza el desarrollo de una página web utilizando PHP y mysql. Para poder cargar la página a internet, se hizo uso de un hosting y un dominio. Además, se pegó propagandas con el

código QR en ciertos lugares específicos. Finalmente se esperan los resultados obtenidos para esto poder ser analizados.

3.1.5. Procedimientos éticos

El presente trabajo no tiene como objetivo realizar actividades maliciosas con los datos obtenidos. Estos serán usados únicamente para hacer un análisis y realizar una campaña de concientización sobre ingeniería social. Posteriormente los datos serán eliminados, la página web dada de baja, y los usuarios que hayan sido víctimas recibirán un correo sobre los cuidados que se debe tener al momento de ingresar información personal.

3.1.6. Proceso para denunciar páginas de Phishing

Existen diferentes páginas web que se encargan de categorizar una página web si se detecta como Phishing o sospechosa. Es primordial denunciar el hosting en donde está la página web ya que es en el hosting donde está almacenada la página, al denunciarla las personas encargadas la pueden dar de baja definidamente. Para saber a qué hosting pertenece se puede poner la url en la página https://www.whois.com/whois/ esta página detecta el dominio y muestra la información. así como contactos para denunciar un abuso y el hosting al que pertenece. En la Figura 1 a se muestra el proceso.

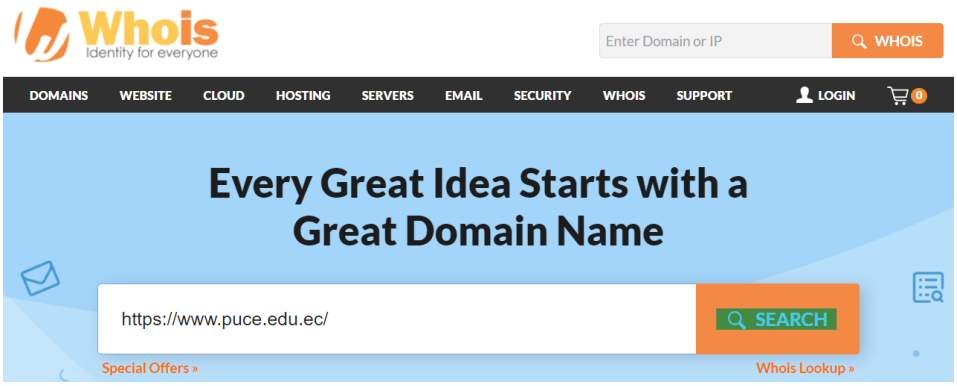

Figura 1*Primer paso para búsqueda de información del dominio*

Nota. Poner la url del sitio que se quiere buscar y dar clic en el botón de “search”

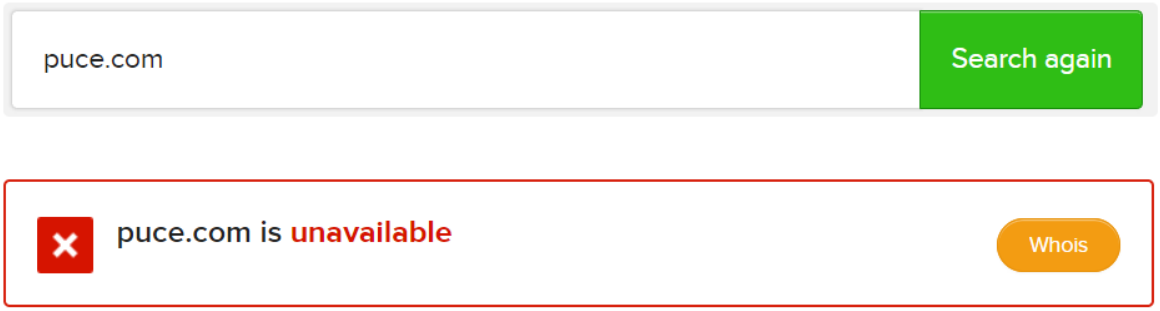

Figura 2 *segundo paso para búsqueda de información del dominio*

Nota. Dar clic en el botón “Whois” para que muestre la información

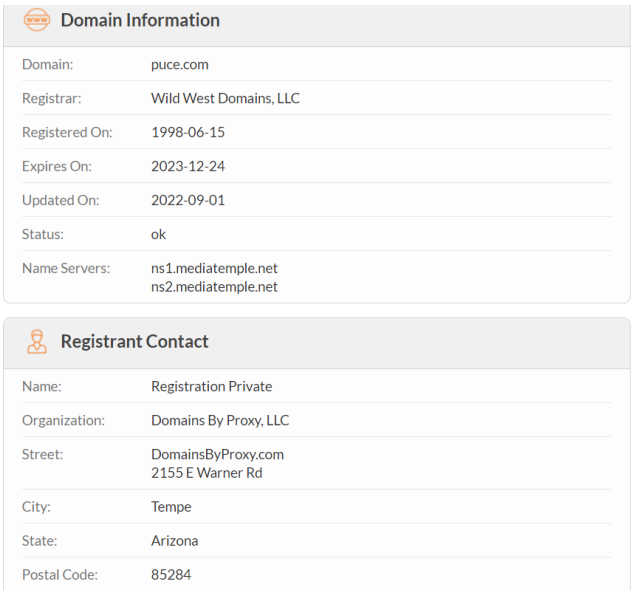

Figura 3 *Tercer paso para búsqueda de información del dominio*

Nota. Se muestra toda la información encontrada sobre el dominio consultado.

En cuanto a las páginas web que califican a una página como maliciosa o phishing(Indicadores de compromiso) en las figuras de la 4 a la 7 se muestran cada página. En cada una de ellas se debe poner la página web a denunciar y llenar los campos requeridos. Después de realizar las denuncias dependiendo el análisis que hagan se lo calificará como malicioso y si se consulta la url en la herramienta de VirusTotal está ya contará con indicadores de compromiso. Con esto se logrará que las personas no caigan en ataques como Phishing.

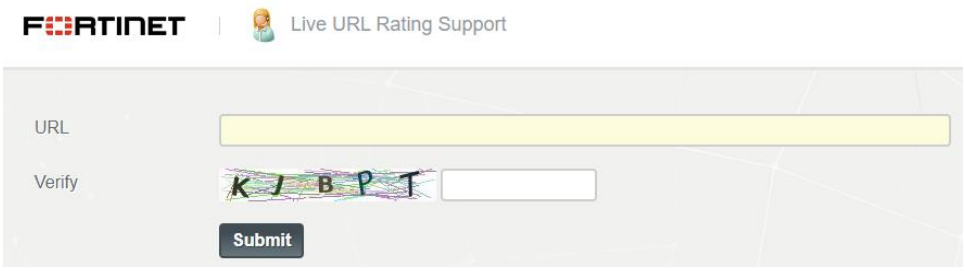

Figura 4 *Denuncia Fortinet*

Nota. https://url.fortinet.net/rate/submit.php

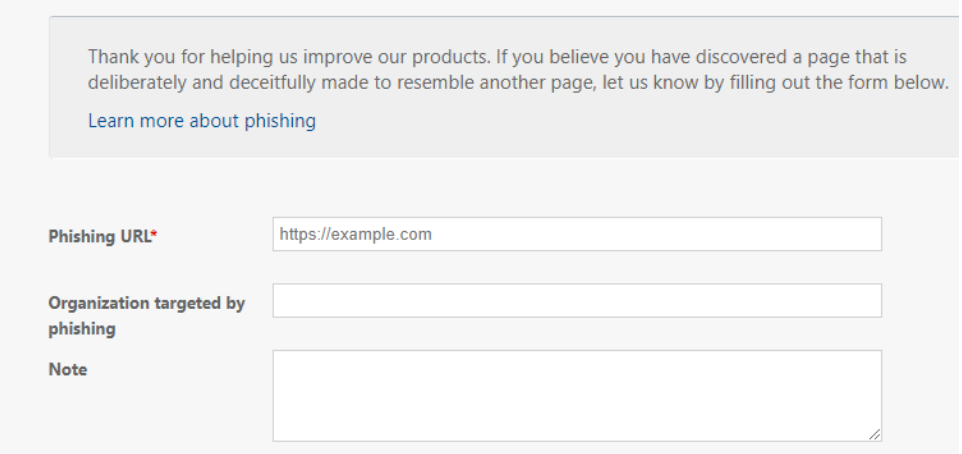

Figura 5 *Denuncia ESET*

Nota. https://phishing.eset.com/report

Figura 6 *Denuncia Palo Alto*

Nota. https://urlfiltering.paloaltonetworks.com

Figura 7 *Denuncia Safebrowsing.google*

Nota. https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en

En cuanto a la denuncia del hosting dependerá del que se esté usando. Una vez identificado a que hosting pertenece solo se debe buscar la opción de reportar y se sigue el mismo procedimiento anterior de llenar los datos solicitados. Personal del hosting hará el respectivo análisis y tomaran las acciones necesarias.

CAPÍTULO IV: ANÀLISIS DE HERRAMIENTAS DE INGENIERÍA SOCIAL

6.1. Herramientas de ataque

Existen herramientas open source que permiten a las personas realizar ataques de ingeniería social con ciertas limitaciones. Para hacer uso de estas se debe contar con el sistema operativo Kali Linux. En este sistema operativo algunas herramientas vienen instaladas y otras hay que clonar un repositorio que se encuentra en internet.

6.1.1. Social Engineering Toolkit

Esta herramienta está entre las más populares, fue creada por TrustedSec LLC, y permite hacer un ataque en unos pocos minutos. Ofrece vectores como social-Enginineering Attacks, Penetration Testing y Third Party Modules, en especial se hablará del primer vector que trata sobre ingeniería social. En la figura 8 se visualiza las opciones que ofrece para ingeniería social.

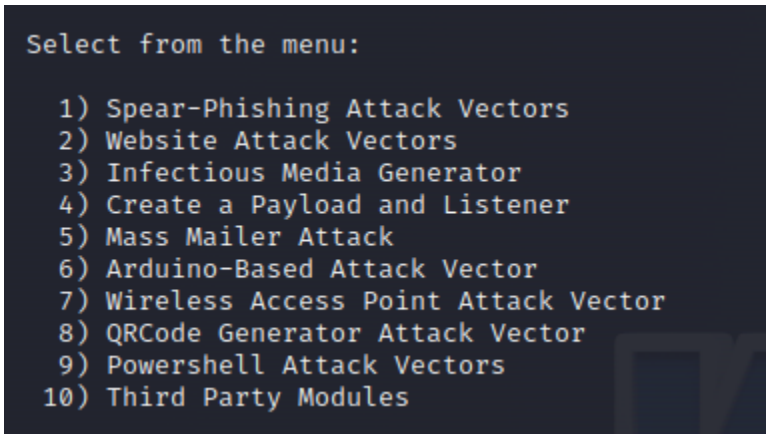

Figura 8 *Menú de opciones Set Toolkit*

- Spear Phishing Attack Vectors: permite crear un correo electrónico con un archivo malicioso para que se envié a un determinado grupo.

- Website Attack Vector: hace es la clonación de un sitio web para el robo de información también conocido en el ámbito de la ciberseguridad como credential hardvesting. Al finalizar la recolección de datos este lo guarda en un archivo txt.
- Infectious Media Generator: permite la creación de un malware para ponerlo ya sea en un cd, usb o DVD. Una vez este se inserte en la computadora ejecutará el archivo infectado que se creó.
- Create a Payload and Listener: Usa Metasploit para crear un archivo ejecutable que pueda dañar la PC de una víctima. El ejecutable se usa para monitorear o ver las acciones que realiza. Sin embargo, para ejecutar este ejecutable, un atacante debe instalarlo físicamente en la computadora del objetivo.
- Mass Mailer Attack: Permite el envío de correos de phishing de forma masiva a una o más direcciones. También puede usar este módulo para agregar enlaces o archivos dañinos a los correos electrónicos que ya se han enviado.
- Arduin-o-Based Attack Vector: El dispositivo está programado usando un dispositivo basado en Arduino. Puede programar de forma remota. Los dispositivos se registran como teclados USB y se desactiva cualquier ejecución automática o protección de punto final en el sistema.
- Wireless Access Point Attack Vector: Crea un punto de acceso falso que redirige a las víctimas al servidor web SET obteniendo información para ingresar a la red.
- QRCode Generator Attack Vector: Generador de códigos QR esta opción está disponible para que sea usado combinado con los otros vectores.

- Powershell Attack Vectors: Los exploits específicos de PowerShell, como los inyectores de shellcode, los shells inversos y los shells de enlace, son posibles cuando se usa este vector. (Kennedy, 2022)

6.1.2. Maxphiser.py

Esta herramienta se centra en phishing y ofrece las opciones que se observan en la figura 9

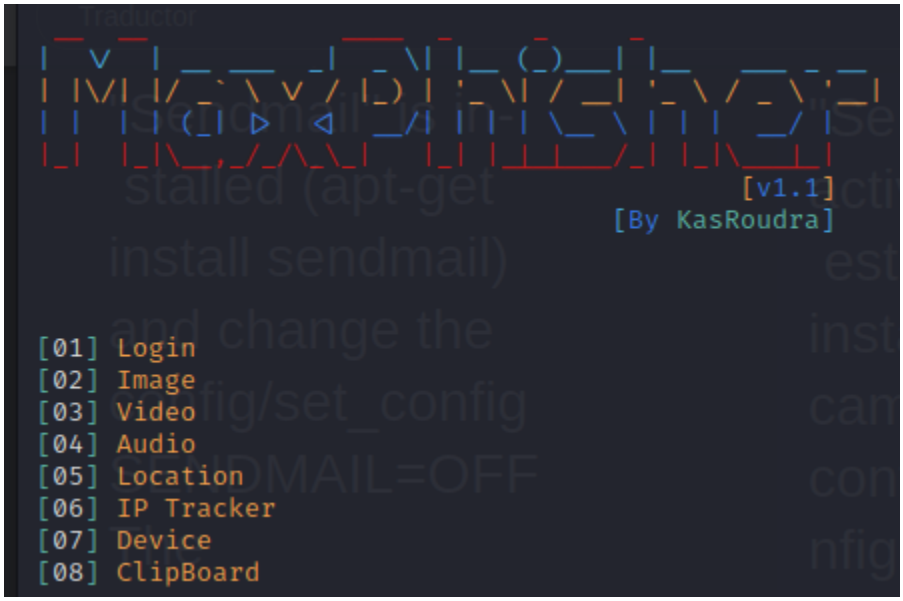

Figura 9 *Herramienta MaxPhisher*

Maxphiser ofrece el servicio de tunneling lo que genera una redirección de la página clonada. También ofrece esconder la url. Lo que significa que se puede poner palabras personalizadas en el link que recibirá la víctima. Esta herramienta cuenta con 75 plantillas lo que hace que sea más rápido realizar un ataque al igual que la anterior herramienta los resultados obtenidos se guardan en un txt. (KasRoudra, 2023)

6.1.3. Maltego

Esta herramienta reconocida a nivel mundial tiene dos perspectivas en el ámbito de la ciberseguridad. La primera es el uso de ella con fines maliciosos. Hablando desde la perspectiva

de la ingeniería social, el uso de Maltego sirve para la primera fase que es investigación. Gracias a esta herramienta se puede investigar a una persona en minutos lo que facilitaría al atacante poder vulnerar a cierto objetivo. Por otro lado, está el uso de Maltego para investigaciones de SOC (Security Operation Center) en el cual se lo usa para combatir ataques haciendo diagramas de flujos sobre alertas o al implementarlo con el SIEM se puede hacer la investigación de un ataque mucho más rápido. (Maltego Technologies, s.f.)

6.1.4. Ettercap

Ettercap admite la disección de protocolos activos y pasivos (incluidos los protocolos cifrados) y proporciona numerosas funciones para el análisis de redes y hosts.

La inyección de datos en una conexión existente también es concebible, al igual que el filtrado sobre la marcha (sustituir o descartar un paquete) para mantener la conexión sincronizada. Orientado a Ingeniería social esta herramienta permite redireccionar para que la página web falsa se abra sin que se vea un link malicioso y la víctima caiga. (Kali, 2023)

6.2.Herramientas empresariales para protección contra la ingeniería social

6.2.1. SIEM

En cuanto a ingeniería social, se sabe que el phishing es uno de los ataques más en auge hoy en día. Gracias al SIEM (Security Information and Event Management) que recolecta información sobre todo lo que sucede en la empresa y junto con ciertas directivas puede enviar alertamientos sobre posibles ataques (Trellix, 2023). Por ejemplo, si un empleado ha sido víctima de phishing y este ha descargado malware. El SIEM enviará una alerta y el equipo de SOC se encargará de avisar a la empresa lo sucedido. De esta forma se evita que una vulnerabilidad se

convierta en un riesgo. Algunos de los SIEM pueden ser AlienVault, Trellix, Darktrace, entre otros.

6.2.2. Directivas de correo

Se puede configurar protocolos de correo que otorgarán un poco más de seguridad en cuanto a recibir correos electrónicos dentro de una organización.

DKIM: Por sus siglas en inglés (Domain Keys Identified Mail) Permite agregar una firma digital a los correos, con el fin de que puedan ser validados y que se tenga la certeza de que el emisor es legítimo. Para validar esta firma se necesita de una llave pública que se encuentra en el servidor DNS de la organización. El funcionamiento de DKIM es el siguiente:

Cuando se recibe un correo entrante el servidor de correo revisa dkim en el servidor DNS. Compara la llave del correo con la llave del servidor y si las dos coinciden, entonces se valida que el correo es legítimo y que no ha sido alterado. (ProofPoint, s.f.)

SPF: Sus siglas en ingles son (Sender Policy Framework). Este es un protocolo de autenticación de correo electrónico. Permite identificar que un correo haya sido enviado desde un servidor de correo autorizado. Para usar este protocolo se necesita primero crear el SPF record. En este se enlista las direcciones ip autorizadas para enviar correos desde el dominio. Con esto listo al enviar un correo se verifica si este está dentro del SPF record, si es así el correo es aceptado, caso contrario el correo falla debido al SPF. (Bone, 2023)

DMARC: Este protocolo es una combinación de SPF y DKIM. Este fue creado por paypal, Google, Microsoft y Yahoo. Ayuda a protegerse de ataques como spoofing, spam y phishing. Dmarc permite a las organizaciones publicar una política en el servidor DNS que permite dar instrucciones a los correos entrantes, es decir si el correo es aceptado o rechazado. (Fortinet, s.f.)

6.3.Herramientas personales para protección contra la ingeniería social

6.3.1. VirusTotal

Esta herramienta que es accesible para todos proporciona información sobre si tiene o no indicadores de compromiso ya sea una dirección ip, un hash o una url. Con esta herramienta cualquier persona podrá consultar el dominio o la url que le haya llegado por correo y la persona podrá tener información si está catalogado como malicioso o no. Virustotal ofrece una extensión en el navegador lo que facilita a los usuarios a dar clic derecho y que Virutotal investigue el link deseado. Los resultados en esta herramienta son actualizados en tiempo real y es de gran ayuda para la comunidad. (How it works, 2021)

6.3.2. MxToolbox

Con esta herramienta se puede consultar si el dominio se encuentra en listas negras. Si lo está ya es un indicador de que esté siendo víctima de phishing. Es una buena herramienta para verificar la veracidad del correo.

6.4.Unshorten

Una página web la cual permite verificar si un link tiene algo oculto. Es un sitio muy simple de usar que muestra qué hay detrás de un enlace acortado mostrando el enlace original y una imagen de vista previa para que se pueda comprender que hay dentro del contenido. Además, informa si la página se encuentra en una lista negra y si es segura. Es una muy buena herramienta para evitar ejecutar algún malware. (BIURRUN, 2022)

CAPÍTULO V: DESARROLLO DE ATAQUE DIRIGIDO

Como ya se mencionó anteriormente para aplicar un ataque de ingeniería social se deben seguir ciertas fases. A continuación, se detalla lo que se realizó en cada fase para el ataque de phishing controlado.

5.1. Investigación

En esta fase se definió cual sería el motivo por el cual la víctima sienta curiosidad de entrar al QR he ingresas su información. Para este ataque se propuso temas sociales que son populares en la actualidad. Lo que se quiere es obtener los datos personales y la contraseña que la víctima pondría, para esto se pensó en un servicio que requiera de un registro.

En esta misma fase se investigó a la organización a ser clonada. Se buscó publicaciones e información para poder utilizarla en la página web y que esta sea lo más semejante. Una vez definido el tema en este caso un formulario de registro, el siguiente paso es identificar cual sería el lugar idóneo para pegar la publicidad.

Finalmente, se debe tomar en cuenta que se debe establecer una relación de confianza con la víctima por lo que se hizo que la página web se vea verídica para que las personas que ingresen sientan que están en el sitio oficial. El medio por el cual se desplegará será pegar la publicidad con el código QR en paradas de buses en la Ciudad de Quito en la parroquia Iñaquito por un tiempo de una semana.

5.2. Diseño

Para el diseño de la propaganda publicitaría hay que tener en cuenta que para que sea convincente, debe ser lo más parecido a una publicidad que la organización publica en sus redes sociales. Además, está debe ser de alta calidad y con la mayor producción. Para lograr este resultado se investigó en la red social Instagram el estilo de publicaciones que hace la organización.

Una vez determinado el estilo a usar, a continuación, en la figura 10. Se detalla un modelo de como fue el anuncio publicitario.

Figura 10 *Modelo de Anuncio Publicitario*

5.2.1. Estructura del diseño de la publicidad

Las personas cuando reconocen algo conocido tienden a confiar un poco más. Por esta razón que se puso el logo de la institución. Junto al logo se encuentra un refrán, este se lo puso ya que en las publicaciones originales de la organización siempre lo ponen. Para poder facilitar el acceso a la página web se hizo uso de un código QR. Estos códigos generan curiosidad y muchas de las veces las personas solo lo escanean para ver que tiene. Junto al código QR se encuentran los pasos a seguir, en donde se indica que es lo que se debe hacer para poder registrarse. El título es

el más importante en la publicidad por eso se puso una frase atractiva para las personas y para que este flyer sea como carnada se puso que por el registro la persona podrá obtener un beneficio.

5.2.2. Estructura del diseño de la página web

Para el diseño de la página se utilizó CSS. El diseño es de una página simple la cual tiene un header, un body en el cual se encuentra un foarm con el registro y un footer. Los campos que se pusieron en el registro son: nombre, apellido, fecha de nacimiento, cédula, dirección, número de teléfono, correo electrónico, una contraseña y confirmación de contraseña. En este último campo no se puso ningún tipo de control para evaluar que ingresa la persona. En la figura 11 se muestra el diseño de la página web.

Figura 11 *Diseño de página web*

5.3. Ejecución

En este proyecto de investigación sobre ingeniería social se pondrá los anuncios publicitarios en ubicaciones específicas. El código QR envía a la página clonada estará funcionando durante una semana. La página web diseñada cuenta con un base de datos la cual permite hacer la recolección de datos, que posteriormente se pasará a un Excel para poder hacer un análisis de la información recolectada.

El funcionamiento del ataque sería el siguiente:

1. Distribución de la publicidad

2. La persona escanea el código QR que lo redirigirá a la página de registro.

3. Se espera que se ingrese los datos que se solicitan

4. Al dar clic en registrarse los datos se almacenan en la base de datos.

6. Una vez se tenga la data, se procede a analizar la información obtenida.

7. Se enviará un correo de concientización informando que han sido víctimas de un ataque de ingeniería social en un ambiente controlado y se enviará información sobre cómo evitar este tipo de ataques.

5.4. Salida

Al tratarse de una investigación en esta fase se aplicará la concientización a las personas que ingresaron su información. Como ya se mencionó antes la información obtenida solo será analizada por lo que en la fase de salida se enviará un correo a las personas para concientizar sobre este tipo de ataque cibernético. En el caso de un ataque real los atacantes en esta etapa usan los datos obtenidos con fines maliciosos ya sea intentado entrar a otras cuentas. Muchas veces también la información obtenida es vendida en la Deep web.

Como parte de la campaña de concientización a las personas que ingresaron sus datos, se envió un correo electrónico en el cual se indica que fue víctima de un ataque en un ambiente controlado y además se incluye una plantilla de concientización sobre la ingeniería social como se observa en la Figura 12

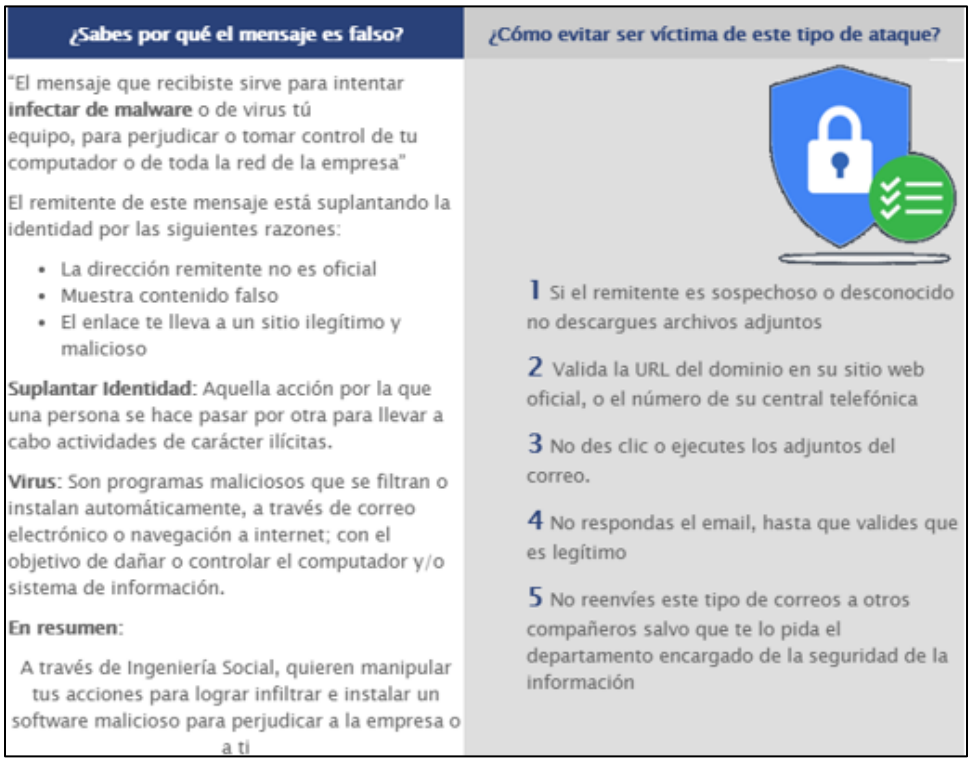

Figura 12 *Imagen de concientización sobre ingeniería Social*

CAPÍTULO VI: IMPLEMENTACIÓN

En esta capitulo se explica a detalla cada pasó que se siguió hasta finalizar el ataque controlado.

6.1. Desarrollo de página web

Se utilizó el lenguaje PHP y como base de datos mysql. La base datos cuenta con una sola tabla titulada datos, que tiene como atributos: una primary key, nombre, apellido, cédula, fecha de nacimiento, dirección, correo electrónico, contraseña y confirmación de contraseña.

La página web cuenta con un header, un form y un footer. Para que se vea verídico, se utilizó CCS para que el diseño sea lo más parecido a la página real.

A continuación, en la figura 13, 14 y 15; se muestra la configuración de la base de datos en el hosting para que funcione la página web.

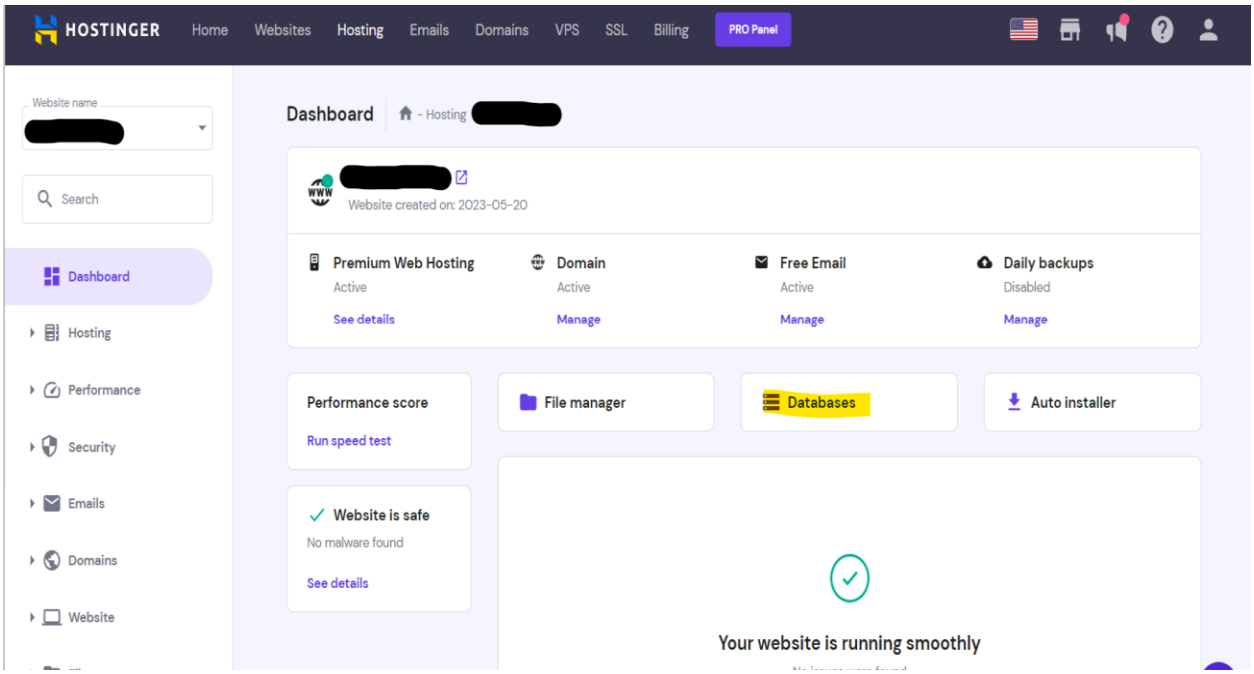

Figura 13 *Dashboard*

Nota. En la parte de Dashboard se debe seleccionar la opción de base de datos

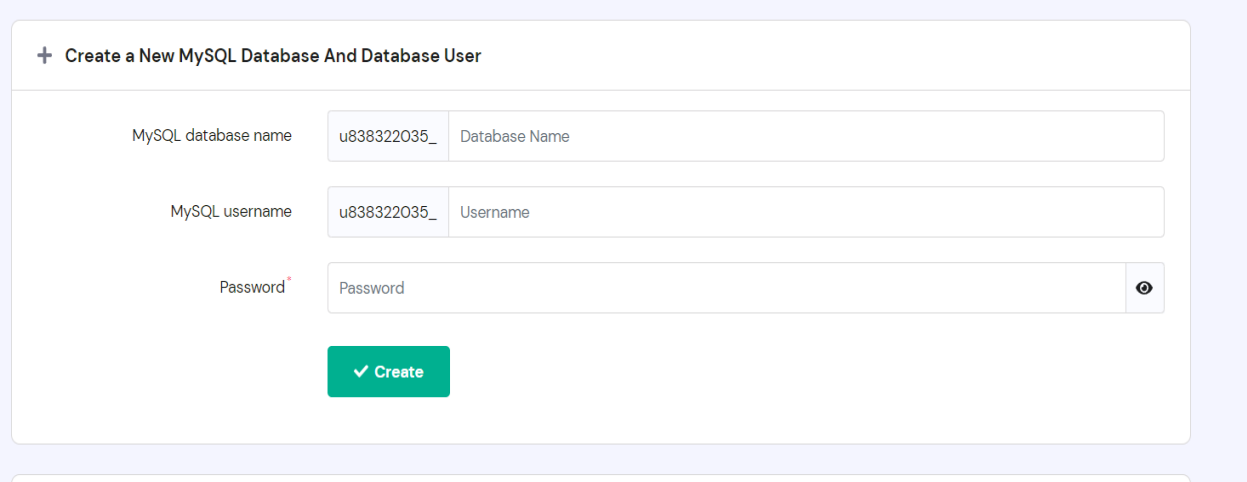

Figura 14 *Creación de Base de Datos*

Nota. Una vez dentro se abrirá la opción de crear una base de datos

Figura 15 *Configuración de conexión de Base de Datos*

Nota. Se debe poner créate y listo, estos datos ingresados que son el nombre de la base de datos, el usuario y la contraseña. Estos datos son los que se deben editar en el archivo de conexión de la página web.

6.1.1. Subida al hosting

Se utilizó el hosting “Hostinger” el cual proporciona hacer uso de un dominio o adquirir uno propio y un email con el dominio que se compró.

Una vez listo con lo anterior, los pasos a seguir para subir la página web al hosting se muestran en la figura 16, 17, 18 y 19.

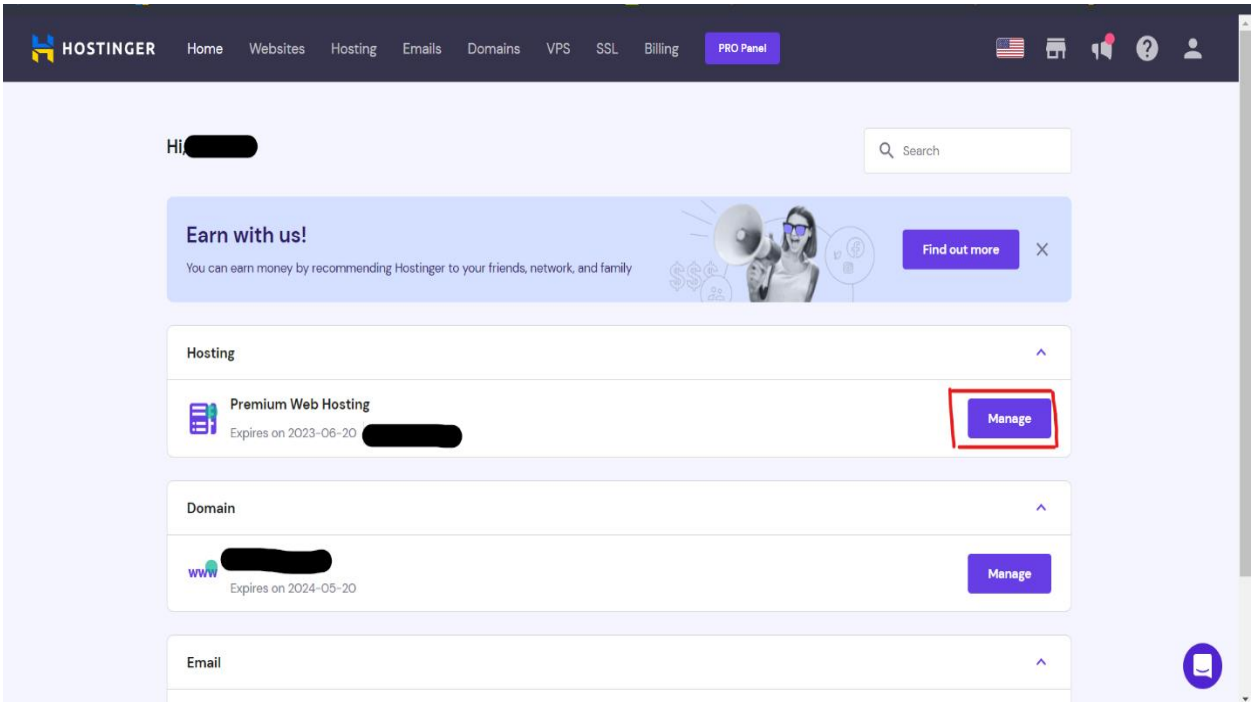

Figura 16 *Entrar a Administrar el Hosting*

Nota. En la primera pantalla seleccionar manage el hosting adquirido previamente

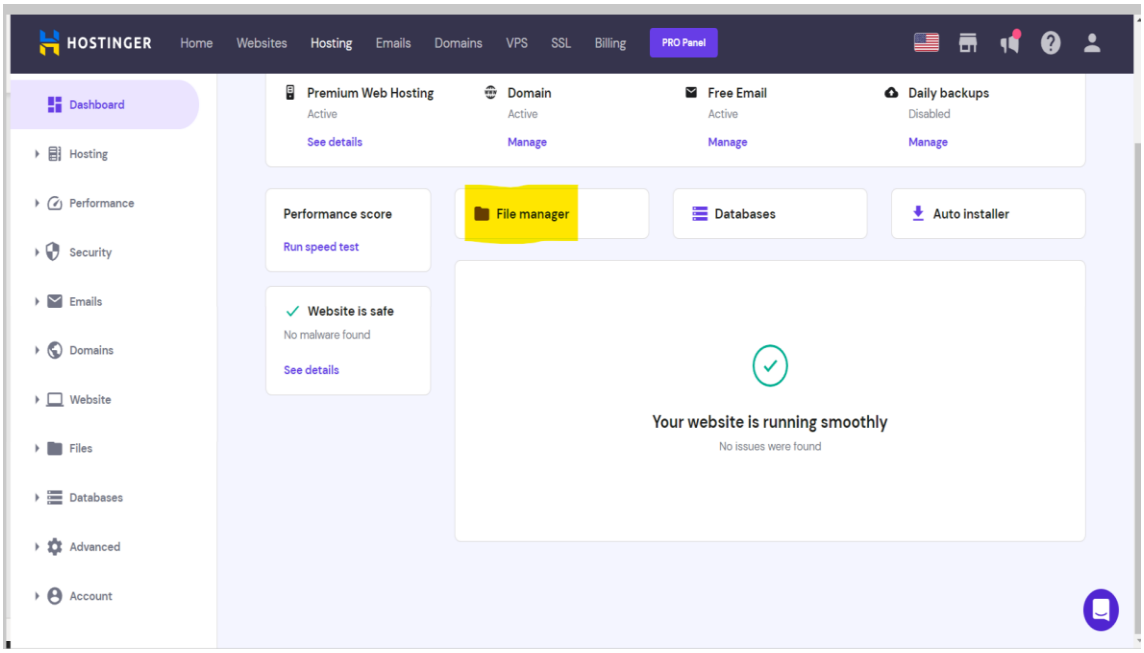

Figura 17 *Subir la Página Web al Hosting*

Nota. Hay que dirigirse a file manager

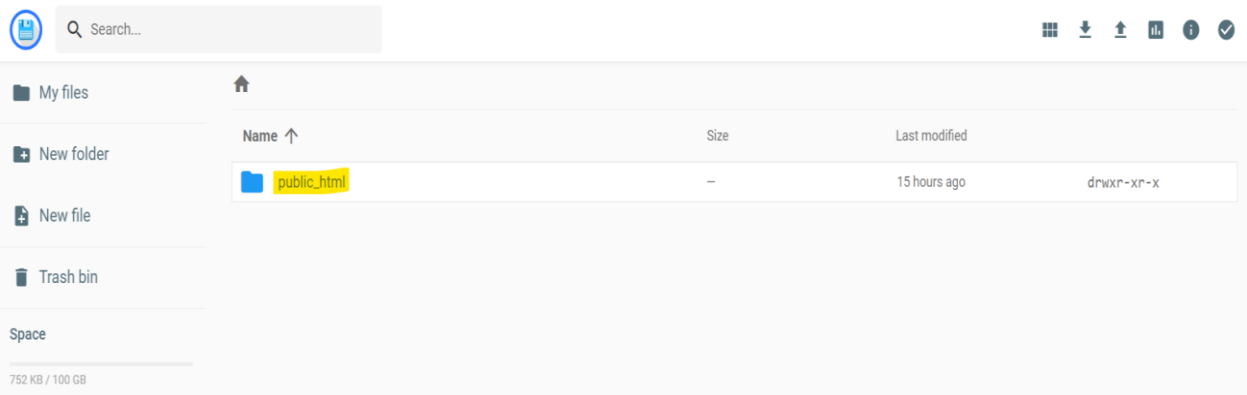

Figura 18 *Ingreso a la carpeta public*

Nota. Una vez dentro se puede subir la carpeta donde se tiene la página web diseñada. Es importante que se ponga dentro de la carpeta public ya que de esta forma la página se publicará.

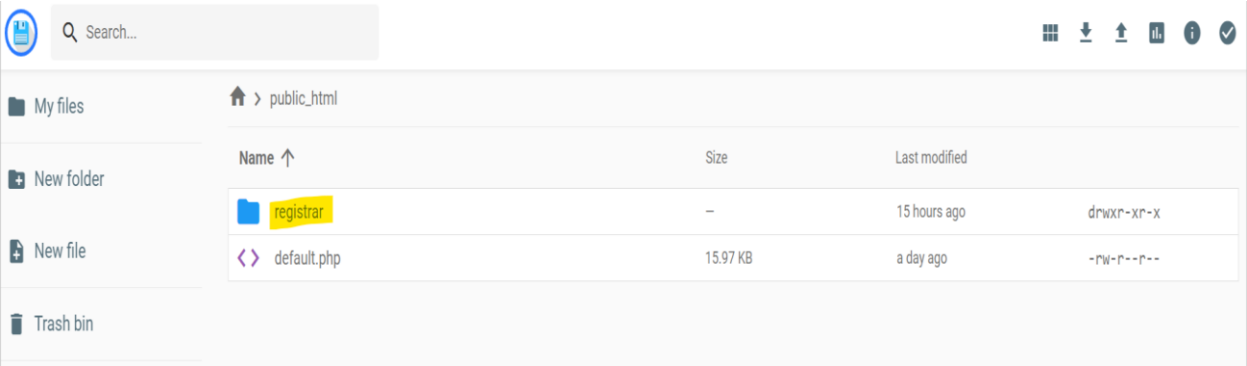

Figura 19 *Subir la carpeta con los archivos de la Página Web*

Nota. Una vez la carpeta se encuentras ubicada en el hosting. Se debe ingresar en cualquier navegador con el nombre del dominio/nombre de la carpeta/. Por ejemplo:

www.dominio.com/nombre_de_carpeta/

CAPÍTULO VII: ANÁLISIS DE RESULTADOS

7.1. Análisis de Resultados por género y edad

En el noveno reporte de estado de phishing realizado por proofpoint muestra que el 44% de las personas confían en un correo al ver un dominio conocido. Pero en el reporte se menciona que alrededor 30 millones de correos de phishing fueron en un contexto de Microsoft. Por otro lado, de los 75 millones de amenazas 1 de cada 10 fueron reportados por los usuarios, lo que demuestra una falta de conocimiento sobre cómo evitar y protegerse sobre el phishing. (Proofpoint, 2022)

A continuación, en la figura 20, se presenta figuras de resultados de la data recolectada dependiendo la edad y el género.

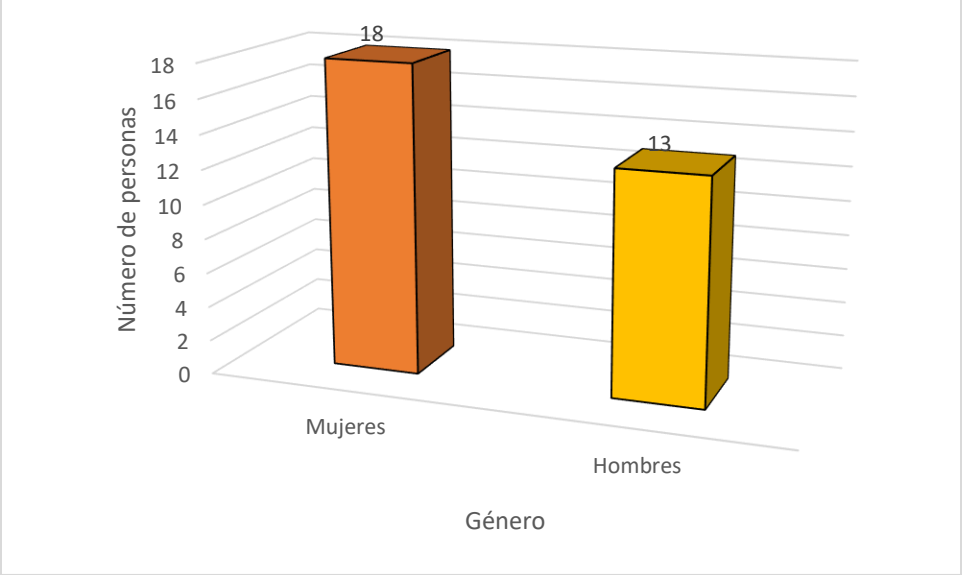

Figura 20 *Resultado de la Información por Género*

Se evidencia que entre las personas que ingresaron sus datos que fueron 31 personas en total, 18 fueron mujeres y 13 hombres. Por lo que se nota una tendencia que las mujeres en este ataque de phishing fueron las que más interesadas estuvieron por la publicidad.

A continuación, en la figura 21 se muestran los resultados obtenidos por edades

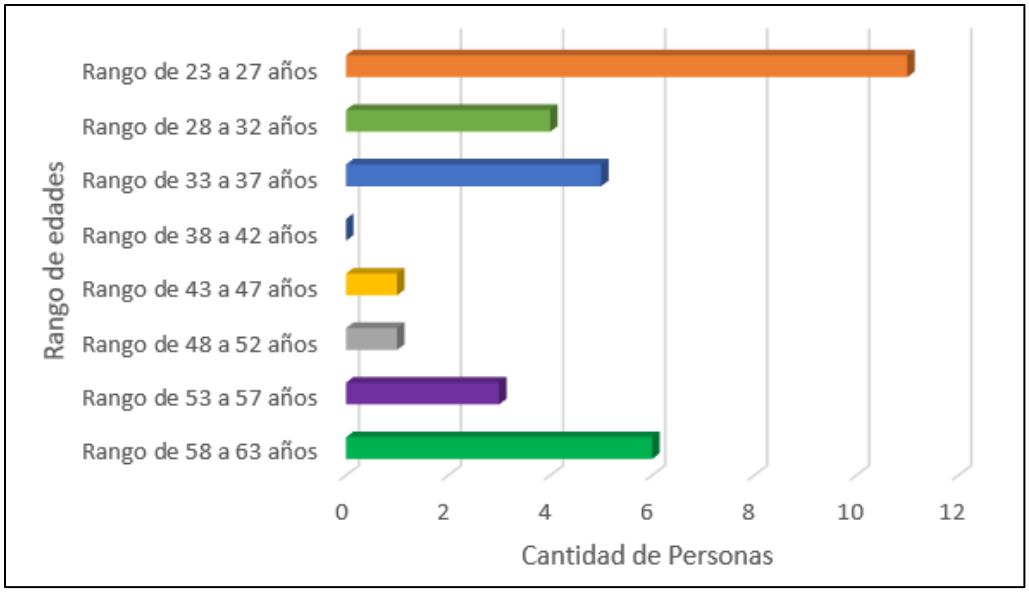

Figura 21 *Resultado de la Información por Edad*

El grafico anterior muestra que de las 31 personas que ingresaron sus datos predominan las personas que tienen una edad de entre 27 a 23 años. Hay que tener en cuenta que el tema para este ataque estaba dirigido para un público que necesita del uso de la tecnología. Es por esta razón que se predomina el grupo de edad de jóvenes de 27 a 23 años que probablemente tengan un trabajo y tengan gran conocimiento del uso de la tecnología. El siguiente grupo es de 63 a 58 años que puede que tengan cierto conocimiento de la tecnología pero que llenaron sus datos solo por el beneficio que la publicidad estaba ofertando sin tomar en cuenta que puede ser una estafa.

7.2. Análisis de Resultados de contraseña

Acorde con el estudio realizado por NordPass en el cual analiza 3TB de datos de contraseña en el año 2022. Menciona que las contraseñas más utilizadas siguen siendo débiles debido a los hábitos que cada persona tiene. El estudio muestra que las personas normalmente usan temas sociales como películas, deportes o simplemente temas familiares. En cuanto al uso de caracteres especiales los resultados en estos estudios muestran que las personas no utilizan estos caracteres a

menos que sea obligatorio. (Nordpass, 2022). A continuación, en la tabla1 se observa los datos de las contraseñas clasificados por categorías

Categoría	Resultados
Uso de gestor de contraseña	1
Uso de nombres con números	17
Solo números	5
Con caracteres especiales	2
Con temas sociales	6
Total	31

Tabla 1*Contraseña por Categoría*

En cuanto a las contraseñas al ser estos datos sensibles solo se mencionará la tendencia de las personas al general una contraseña. Hay que mencionar que para el ataque no se puso ninguna restricción en cuanto a la contraseña ya que se quería analizar qué es lo que las personas ingresan.

En este caso se evidencia que varias de las personas utilizan nombres de personas junto con números consecutivos. También hay que resaltar que de todas las personas participantes uno ingreso una contraseña generada por un gestor de contraseñas que en la actualidad estos vienen integrados en los celulares. Pocas personas hacen uso de mayúsculas y minúsculas para sus contraseñas y solo 2 personas hacen uso de caracteres especiales

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- En conclusión, los ataques que utilizan ingeniería social muestran cómo los atacantes pueden aprovechar las vulnerabilidades de las personas y controlarlas para obtener información confidencial. El ataque controlado realizado identificó que las personas son más vulnerables al ofrecerles algo que sea atractivo, que como se mencionó anteriormente esto hace referencia el tipo de ingeniería social llamado Quid Pro quo. De las personas que ingresaron sus datos el género que predominó fue el de las mujeres.
- Los resultados muestran que las personas entre 23 a 27 años en este ataque son el grupo que más personas ingresaron sus datos. A pesar de que es un grupo que conoce sobre tecnología el hecho de ofrecer algo para su beneficio y emplear un tema popular en la publicación los hace que se conviertan en víctimas. Por otro lado solo 6 personas del grupo de 60 a 65 años ingresaron sus datos. Esto indica que gracias a la fase de investigación es que se pudo identificar a quien se debe aplicar el ataque con el tema seleccionado y obtener información del público que se desee.
- La campaña de concientización en el presente proyecto fue exitosa ya que cada usuario que ingresó sus datos recibió una pequeña capacitación sobre la ingeniería social y sus posibles riesgos. La concientización sobre la ingeniería social es de suma importancia en un ámbito personal y empresarial. En una organización se debe aplicar campañas de ingeniería social para identificar quienes son los colaboradores más vulnerables. Con

una buena capacitación de como identificar y evitar este tipo de ataques se reduce el riesgo.

- Los factores identificados que hacen a las personas más vulnerables en este ataque controlado son: ofrecer a la víctima algo atractivo o algo que necesita, la falta de conocimiento sobre el tema de ingeniería social es un factor que hace que las personas se conviertan en el eslabón más débil. Por último, según los datos obtenidos las contraseñas que usan las personas son muy simples y muy probablemente esta contraseña es usada para distintas cuentas. Esto al ser aprovechado por un atacante puede robar información de las distintas cuentas de la víctima.

6.2. Recomendaciones

- Se recomienda, hacer un análisis más exhaustivo en cuanto a la campaña de ingeniería social de este ataque. Es decir, poder ver quien abrió el correo y quien hizo clic. Para esto se puede implementar un desarrollo más avanzado el cual muestre la información mencionada y se almacene en la base de datos para poder realizar un análisis y descartar falsos positivos debido a herramientas antiphishing.
- Utilizar varias platillas de publicidad para no solo orientarse a un solo tipo de audiencia. Con estas se puede aplicar la técnica de spam(envió de varios correos) y observar si la victima ingresa sus datos. Se puede hacer uso de un dominio genérico para hacer el envío de los diferentes temas.
- Aplicar varios tipos de ingeniería social de los expuestos anteriormente y hacer un análisis de cuál de estos es el que más son víctimas las personas y poder genera una concientización.

BIBLIOGRAFÍA

¿Qué es la ingeniería social? (s.f.). Proofpoint: https://www.proofpoint.com/es/threat-reference/social-engineering

Baker, K. (13 de Febrero de 2023). *10 MOST COMMON TYPES OF CYBER ATTACKS*. Crowdstrike: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/#1.%20Malware

BIURRUN, A. (31 de Marzo de 2022). *Cómo saber si un enlace acortado es seguro antes de hacer clic en él*. La razón 25: https://www.larazon.es/tecnologia/20220331/yfwddfdt6valnkipotxoexdgdu.html#:~:text=Unshorten.it%20es%20un%20servicio,El%20funcionamiento%20es%20muy%20sencillo.

Bone, H. (5 de Mayo de 2023). *What is SPF (Sender Policy Framework)?* Proton blog: https://proton.me/blog/what-is-sender-policy-framework-spf#how-does-spfa-work

Conger, K., y Roose, K. (15 de Septiembre de 2022). *Uber Investigating Breach of Its Computer Systems*. The New York Times: https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

Easydmarc. (28 de Enero de 2022). *¿Cómo puede afectar la ingeniería social a una empresa a nivel organizacional?* Easydmarc: https://easydmarc.com/blog/es/como-puede-afectar-la-ingenieria-social-a-una-empresa-a-nivel-organizacional/#:~:text=Los%20efectos%20de%20la%20ingenier%C3%ADa,mala%20reputaci%C3%B3n%20para%20tu%20organizaci%C3%B3n.

Fortinet. (s.f.). *What is DMARC?* Fortinet: https://www.fortinet.com/resources/cyberglossary/dmarc#:~:text=DMARC%20verifies%20email%20senders%20by,domain%20to%20impersonate%20its%20employees.

Hadnagy, C. (2018). *Social Engineering The science of Human Hacking.* John Wiley & Sons, Inc.

How it works. (2021). VIRUSTOTAL: https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

Kali. (25 de Mayo de 2023). *ettercap-common*. Kali: https://www.google.com/search?q=traductor&oq=trad&aqs=chrome.0.69i59j69i57j69i65l2.1044j0j1&sourceid=chrome&ie=UTF-8&bshm=nce/1

Kaspersky. (s.f.). *What is Social Engineering?* Kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

KasRoudra. (Mayo de 2023). *KasRoudra/MaxPhisher*. Github: https://github.com/KasRoudra/MaxPhisher

Kennedy, D. (25 de Enero de 2022). *trustedsec/ social-engineer-toolkit*. Github: https://github.com/trustedsec/social-engineer-toolkit

Koyun, A., y Al Janabi, E. (2017). Social Engineering Attacks. *Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), 7533-7538.

Lubeck, L. (7 de Enero de 2021). *En 2020 se duplicaron las detecciones de ataques de ingeniería social*. Welivesecurity by ESSET: https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/

Maltego Technologies. (s.f.). *Increase the Speed and Precision of Complex SOC Investigations*. Maltego: https://www.maltego.com/reduce-your-cyber-security-risk-with-maltego/

Nordpass. (2022). *Top 200 most common passwords*. Nordpass: https://nordpass.com/most-common-passwords-list/

Pastor, J. (6 de Febrero de 2018). *Kevin Mitnick, genio o figura de uno de los hackers más famosos de la historia*. Xataka: https://www.xataka.com/seguridad/kevin-mitnick-genio-o-figura-de-uno-de-los-hackers-mas-famosos-de-la-historia

Proofpoint. (2022). *THREAT REPORT 2023 State of the Phish*. Proofpoint: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

ProofPoint. (s.f.). *What Is DKIM?* ProofPoint: https://www.proofpoint.com/us/threat-reference/dkim

Salahdine, F., y Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11*(4), 89.

Trellix. (2023). *What Is Security Information and Event Management (SIEM)?* Trellix: https://www.trellix.com/en-us/security-awareness/operations/what-is-siem.html