INGENIERA SOCIAL: TÉCNICA DE ATAQUE PHISHING Y SU IMPACTO EN LAS EMPRESAS COLOMBIANAS

JENNY PAOLA GIRALDO MARTÍNEZ

IVÁN GUILLERMO DUARTE PACHECO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD DE INGENIERIA Y CIENCIAS BASICAS

ESPECIALIZACION EN SEGURIDAD INFORMATICA

SALAMINA, CALDAS ACACIAS, META

2018

INGENIERA SOCIAL: TÉCNICA DE ATAQUE PHISHING Y SU IMPACTO EN LAS EMPRESAS COLOMBIANAS

JENNY PAOLA GIRALDO MARTÍNEZ
IVÁN GUILLERMO DUARTE PACHECO

Monografía

Director proyecto:
JUAN JOSE CRUZ GARZON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE INGENIERIA Y CIENCIAS BASICAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SALAMINA, CALDAS - ACACIAS, META
2018

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Salamina, Caldas 23 noviembre de 2018

DEDICATORIA

Dedico este trabajo especialmente a Dios, quien es mi motor de vida y la fuente de inspiración para realizar las cosas, además es el quien me ha permitido escalar hasta donde estoy a pesar de los tropiezos y dificultades.

A mi madre Blanca Lucrecia Martinez Bolaños quien es una persona indispensable en mi vida, ya que es mi guía y siempre me demuestra su amor y apoyo incondicional.

A mi padre Francisco Javier Giraldo Muñoz y mi tia Alba Dariela Giraldo Muñoz quienes me apoyan en mis decisiones y me aconsejan para ir siempre por el buen camino, siempre quieren lo mejor para mí.

Jenny Paola Giraldo Martinez

Quiero dedicar este logro en mi vida a Dios y a mis padres Guillermo Edilson Duarte Hernández y Elba Pacheco Amézquita quienes siempre han estado ahí, apoyándome para salir adelante, ya que ellos han sabido como formarme y guiarme para ser la persona que soy hoy en día.

Y a las diferentes personas que estuvieron a lo largo de este proceso de formación y me tuvieron paciencia para sacar adelante este proyecto en mi vida

Iván Guillermo Duarte Pacheco

AGRADECIMIENTOS

Queremos agradecer a todos nuestros tutores, ya que todos con su conocimiento aportaron un granito de arena para la construcción de este documento que es de gran ayuda no solo para nosotros sino también para la sociedad.

Es importante nombrar y agradecer a nuestro director de proyecto de grado Juan Jose Cruz pues fue la persona que nos guio por el camino correcto para poder salir adelante con nuestro proyecto.

A la Universidad Nacional Abierta y a Distancia por ser participe en el logro de nuestro gran sueño ser especialistas en seguridad informática.

CONTENIDO

Pág

LISTA DE FIGURAS

INTRODUCCION

Es importante tener en cuenta que actualmente la informática crece a pasos agigantados y es allí donde se hace necesario saber y aprender cómo es la forma en que nos debemos proteger. José María Alonso, conocido como Chema Alonso promueve el uso correcto y responsable de estas tecnologías que hay actualmente y, también nos informa de que manera estamos siendo blanco fácil para los diferentes delincuentes en la parte de la seguridad de la información, es decir no estamos protegiendo nuestra información vital, como lo es el número de cedula, el nombre y apellido completo, nuestros correos electrónicos, las fotos que publicamos en las redes sociales, en donde nos encontramos ubicados, etc. Pero hay algo importante que debe incluir y es en la parte de la información que no se encuentra tan fácil en nuestros perfiles informáticos como, por ejemplo, lo es que es el Facebook y demás redes sociales que hay actualmente. Es la información que a diario compartimos con otras personas casi de una forma automática.

En los últimos años, se ha evidenciado que este problema inquietó a las autoridades y, que se están diseñando y desarrollando diferentes planes de contingencia, para que cada una de las empresas u organizaciones que realicen estas bases de datos relacionales o no relacionales se hagan responsables de la seguridad de dicha información para los diferentes usuarios, que sean privados más no públicos, desde luego teniendo en cuenta de los mismos usuarios si lo quieren publicar a todas las personas en sus redes sociales.

Además, las diferentes técnicas utilizadas actualmente por los delincuentes informáticos para poder dicha información de sus víctimas son innumerables y, por lo tanto, cada día desarrollan nuevas técnicas y combinan algunas técnicas clásicas para desarrollar diferentes tipos ataques informáticos. Para este caso las técnicas que nos competen en esta investigación son, la Ingeniería social y el Phishing. Ambas técnicas son vitales para llevar a cabo diferentes delitos informáticos., el cual podemos partir de la base que existe un mundo virtual similar al mundo real, pero en este no existen controles adecuados, ni normas, ni leyes como las que hay actualmente que regulan nuestra convivencia y por supuesto limitan el abuso al indefenso, es por eso que la mayoría del tiempo que nos encontramos en la red, estamos por nuestra propia cuenta, y es aquí en donde decidimos hasta donde llegar y protegernos de esta misma. Hoy en día solo recibimos información de los riesgos existentes que hay en cada momento que pasa en la sociedad global.

1. RESUMEN

Actualmente, el mundo de la tecnología se encuentra en constante cambio y actualización, ya que este avanza a pasos agigantados y todos en el mundo hacemos parte de él.

En este documento se podrá evidenciar de forma clara los conceptos básicos de la ingeniería social y el Phishing, las técnicas utilizadas por los delincuentes para atacar sus víctimas y una guía para tener en cuenta y que las empresas y no sean blanco fácil para los delincuentes, un factor importante a tener en cuenta es que no existen fórmulas mágicas para contrarrestar este tipo de delitos, ya que el eslabón más débil de la cadena es el usuario y este es uno de los más difíciles de educar.

El internet y las redes son las herramientas que posibilitan la interconexión de las empresas, lo que hace que estas mejoren su productividad y sus conexiones nacionales e internacionales, pero esto hace que también sean blanco de los ciberdelincuentes que se encuentran al asecho en las redes. Actualmente en centro cibernético policial de Colombia (CAI Virtual); lugar donde se realizan estudios acerca de los delitos informáticos, durante los últimos 4 años ha evidenciado un incremento significativo en las denuncias de las empresas sobre ataques informáticos, reporte que pone en alerta a los empresarios colombianos, puesto que su información es vital para el funcionamiento de estas. “En el año 2014, del total de incidentes atendidos, el 92% afectaban a los ciudadanos del común, para el año 2015 el 63% y en el 2016 el 57%, presentando una disminución del 35%. Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos”[1].

Un factor importante a tener en cuenta es no contar con políticas de seguridad claras, lo que desencadena malas prácticas en el uso de los sistemas informáticos y de la red informáticas, el cual es uno de los puntos más importantes para que el departamento de seguridad de la información tenga en cuenta a la hora de protegerla.

[1]Estadística Centro Cibernético Policial. Plataforma de atención incidentes, 2017. P.10-12.

De acuerdo a diferentes investigaciones del centro cibernético, la *ingeniería social*, es uno de los métodos más utilizados por los atacantes para poder engañar a los usuarios informáticos, para que puedan realizar alguna acción que normalmente puede producir consecuencias negativas, como la descarga de un software malicioso (malware) o también la divulgación de información personal de la víctima[2].

Un factor importante a tener en cuenta de acuerdo a un estudio realizado por BID, MINTIC y OEA[3], se observó que, de manera general, las organizaciones colombianas que contestaron que se sienten preparadas, de hecho, adoptan más medidas de seguridad que las demás organizaciones., como por ejemplo, las grandes empresas tienden a adoptar más medidas de seguridad que una microempresa, así como las entidades públicas nacionales tienen una preocupación más grande con la seguridad digital que las entidades de orden territorial.

Se espera que esta monografía sirva de soporte para darle claridad a las falencias en las empresas colombianas en la parte de los ataques de Phishing, utilizados en la ingeniería social, para obtener las diferentes vulnerabilidades que hay y cómo generar una solución adecuada de acuerdo a los protocolos de seguridad establecidos., en el que se identificará ciertas características de este tipo de ataque "Phishing", de cómo caer en la trampa de estos ciberdelicuentes, y de esta manera lograr una reevaluación en la parte de la seguridad informática en las diferentes empresas colombianas, en el que se debe tener en cuenta los diferentes casos sucedidos a nivel nacional. Además, también le puede suceder a una persona natural que lo puedan hackear, dependiendo del interés del atacante.

[2] Ingeniería social y seguridad informática. 2018.

[3] Impacto de los incidentes de seguridad en Colombia 2017, Policía Nacional

2. TITULO

INGENIERA SOCIAL: TÉCNICA DE ATAQUE PHISHING Y SU IMPACTO EN LAS EMPRESAS COLOMBIANAS

ÁREA DE CONOCIMIENTO: Seguridad Informática

LÍNEA DE INVESTIGACIÓN: Estudio monográfico de ingeniera social

3. PLANTEAMIENTO DEL PROBLEMA

3.1 ANTECEDENTES

El delito informático implica diferentes actividades criminales que en la mayoría de los países han tratado de incluir en figuras típicas que relacionan con el carácter tradicional, como, por ejemplo, los diferentes tipos de robos, como también los hurtos, los fraudes, los diferentes tipos de falsificaciones, los perjuicios, las estafas, y los sabotajes que hay actualmente, entre otros., pero, sin embargo, se debe destacarse que el uso de las técnicas informáticas han generado nuevas posibilidades del uso indebido de los computadores, como también de los teléfonos inteligentes y otras tecnologías, en el cual, ha generado una necesidad de regulación en la parte de la seguridad de la información y en la parte del derecho.

También se debe tener en cuenta que en el año 2016 ha habido un aumento notable en los ataques de phishing, según un nuevo reporte del Anti-Phishing Working Group (APWG); El informe muestra que en el primer trimestre del año 2016 hubo más ataques de phishing "que en cualquier otro momento de la historia". El nivel más alto en la actividad maliciosa fue entre octubre de 2015 y marzo de 2016, con incidentes que se incrementaron en un 250%, resaltó el estudio. “los ataques de phishing son cada vez más agresivos”.

El objetivo del engaño es de adquirir información confidencial del usuario como lo que son las contraseñas, las tarjetas de crédito o lo que son los datos financieros y bancarios, como también las estafas, entre otras. Además, el delito informático de phishing se puede producirse de varias formas, como, por ejemplo, un simple mensaje al teléfono móvil, una llamada telefónica, un sitio web que simula una entidad (sitio web falso), una ventana emergente, y la más usada y conocida por los internautas, lo que son la recepción de un correo electrónico hacia las víctimas por sus victimarios.

SMS (mensaje corto): la recepción de un mensaje donde se le solicita los datos personales, como el correo electrónico, el nombre y apellido completo, la fecha de nacimiento, el numero celular, etc.

Llamada telefónica: la persona puede recibir una llamada telefónica, en el que el emisor (el hacker de sombre negro o el ingeniero social) suplanta a una entidad privada o también una entidad pública para que la víctima le facilite los datos privados.

Página web o ventana emergente: es una de las clásicas y una de las más usadas, el cual se simula suplantando visualmente la imagen de una entidad oficial,

empresas, entre otras, generando una copia casi exacta de la entidad oficial. El objetivo principal es que el usuario facilite sus datos privados. Una de las que se utilizan es la imitación de páginas web en entidades bancarias.

En Colombia existe una legislación referente al delito informático de phishing, pero que desde luego se carece una actualización constante sobre este delito, y por supuesto de capacitar a los trabajadores de las empresas y entidades públicas y privadas sobre este delito que pone en riesgo la estabilidad de las empresas y organizaciones en Colombia.

3.2 FORMULACION DEL PROBLEMA

¿Cómo se puede identificar un ataque de phishing ocasionado por la ingeniería social y que contramedidas de seguridad informática se pueden aplicar para las empresas colombianas?

3.3 DESCRIPCION DEL PROBLEMA

En la actualidad el comercio electrónico es uno de los temas que más se hablan y se discuten en los diferentes tipos de empresas a nivel global y desde luego es uno de los temas más relevantes en el mercado empresarial, puesto que no solo les interesa a las empresas y organizaciones; ya que por medio de este llegan a cualquier lugar del mundo, sino que también se ahorran en gastos de personal, vigilancia, servicios públicos entre otros. Para las personas del común también es importante ya que por medio de este servicio que otorga estas empresas y organización pueden encontrar una variedad de productos sin salir de su hogar y a precios mucho más cómodos.

Por lo anterior, existe una gran variedad de información, en el que se da un nuevo inicio y creatividad para el manejo de varias herramientas informáticas y psicológicas; es allí donde los ciberdelincuentes aprovechan cualquier descuido no solo de las empresas sino también de las personas naturales. Y se valen de técnicas como la ingeniería social con sus métodos y el phishing para cometer estos tipos de delitos.

Es importante tener en cuenta la aplicación de políticas de seguridad y capacitación del personal, para mitigar este tipo de delitos, también es fundamental conocer cómo es que los delincuentes atacan y cuáles son sus principales blancos y objetivos.

Por medio de la ingeniería social los delincuentes realizan los ataques a las empresas, ya que el usuario es el punto más débil del eslabón, y no solo es la parte

más débil de la cadena de custodia, sino que también es mucho más fácil realizar un engaño social que hacer ataques a los sistemas de información y demás. Cabe anotar que el phishing es un tipo de ingeniería social, mediante este tipo de engaños es que atacan a las personas o a las empresas, generalmente por correo electrónico. Es Importante aclarar que debemos estar siempre alertas y conocer acerca de este tipo de temas, ya que por desconocimiento también podemos caer en el anzuelo de los ciberdelincuentes que siempre se encuentran al asecho.

4. JUSTIFICACION

Mediante este documento guía se pretende contribuir al conocimiento de los incidentes con los que han sido afectadas las diferentes empresas colombianas, y sus posibles defensas ante estas situaciones. Informarnos acerca de la legislación existente en el país, para identificar las formas en que las empresas se pueden apoyar y así reducir el impacto de delito. Además, con la información recolectada se puede tener una visión completa de los ataques que sufren las empresas tanto el sector público como el privado.

Es necesario que los usuarios como lo son los particulares como también el de muchas organizaciones y empresas entiendan o generen conciencia de cuál es su papel en la parte de la seguridad informática y, como pueden fomentar y desde luego contribuir a prácticas seguras que nos lleven a un muy buen nivel de protección frente a los diferentes ataques que usan este método. Ya que pueden implementar una variedad de controles por medio de software y hardware, pero no obstante si el usuario evidencia practicas inseguras pone en jaque cualquier organización u empresa.

Un factor importante a tener en cuenta y que este estudio lo puede mostrar, es que tan preparados se encuentran las empresas colombianas para hacer frente a este tipo de incidentes informáticos, y que tipo de protección es necesaria para contrarrestarlos, puesto que mediante este tipo de información podremos contribuir a realizar diagnósticos. “Otro punto importante y lo que dificulta un poco la estadística que las empresas no reconocen ser víctimas por miedo a perder clientes”[4].

[4] Informe de amenazas del cibercrimen en Colombia 2016 – 2017 policía nacional

Para que las empresas tengan claridad en los procesos de prevención de incidentes, se recolectaran una serie de herramientas de seguridad informática, en las cuales se podrán ayudar a contrarrestar los ataques en las empresas mediante diferentes herramientas de hardware y software libre y licenciados existes.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Realizar un estudio monográfico sobre la ingeniería social y las técnicas de phishing en las empresas colombianas.

5.2 OBJETIVOS ESPECIFICOS

1. Identificar y analizar los conceptos básicos de ingeniería social y el phishing.
2. Realizar un estudio acerca de las principales técnicas de ataque phishing en las empresas colombianas.
3. Identificar las herramientas y los procedimientos a seguir cuando ocurre un ataque de phishing
4. Elaborar un documento guía que sirva de referente informativo para la identificación y solución de los ataques mediante phishing e ingeniería social en las empresas colombianas

6. MARCO REFERENCIAL

6.2 MARCO TEORICO

"La seguridad de la información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a las organizaciones asegurar la confidencialidad, integridad y disponibilidad de su sistema información"[5].

Mientras tanto que "la seguridad informática consiste en la implementación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad y la fiabilidad"[6].

6.2.1 **Antecedentes.**

En la parte del desarrollo de la seguridad de la información, "ocurrió un momento extraordinario, el cual, el primer ataque informático de la historia, sucedió el 13 de enero de 1989., en el que una revista especializada regalaba disquetes promocionales, los cuales resultaron infectados por un virus informático, el cual afectó a decenas de empresas y a personas particulares" [7]. Al mismo tiempo, surge el virus Darkavenger, en el cual, "causa un daño lento en el sistema operativo y, en ese mismo año, IBM comercializa el primer programa antivirus"[8], en el mercado, lo que generó una perspectiva con un

[5] MIFSUD, Elvira. "Introducción a la seguridad informática" [en línea]. [Madrid, España]: Observatorio Tecnológico, marzo 2012 [citado en 20 noviembre de 2017]. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridadinformatica?start=1.

[6] Ibid., p. 2.

[7] RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. "Ingeniería Social, una amenaza informática". [en línea], septiembre 2009 [citado en 25 abril de 2017]. Disponible en Internet: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica>

[8] FICARRA, Francisco. "Los virus informáticos: Entre el negocio y el temor". Revista Latinoamericana de Comunicación CHASQUI [en línea], junio 2002 [citado en 25 abril de 2017]. Disponible en Internet: . ISSN 1390- 1079.

panorama que prometía generar grandes ingresos económicos en la parte de la protección de la información.

Actualmente se ha desarrollado diferentes estudios e investigaciones, que reflejan el esfuerzo de identificar, observar, organizar y analizar los avances tecnológicos, como también en la búsqueda de nuevas formas de salir del círculo vicioso de la sociedad, y el de estar día a día sobre la seguridad informática, como son los proyectos de grado, que están relacionados con el tema expuesto. Por lo tanto, existen guías para el desarrollo de los trabajos dentro de las entidades educativas (universidades), en el que existen personas encargadas del área de sistemas que se encargan de revisar todo lo relacionado con la parte de la seguridad a partir de sus propias políticas y protocolos, como se basa en el presente trabajo, con el objetivo de concientizar y de llevar a cabo todo lo implementado, actualizado y por supuesto socializado para la parte de la comunidad académica.

La ingeniería social es una forma no convencional de obtener información deseada, de una manera rápida, sutil y segura de parte de la víctima, en el cual se basa en una variedad de engaños y de manipulación hacia los usuarios para poder obtener esa información confidencial de las empresas u organizaciones, como también del mismo individuo. Por lo tanto, hay ido evolucionando drásticamente, el cual ha sido una de las herramientas fundamentales para los delincuentes informáticos, ya que aprovechan de las vulnerabilidades encontradas de las víctimas.

Existen una variedad de formas de hacer un ataque de ingeniería social, como, por ejemplo, un atacante puede realizar una llama desde un punto, el cual llama a la víctima, el cual ya tiene un estudio previo sobre esa persona, el atacante imita la voz o se hace pasar por un funcionario de alguna empresa y obtiene la información deseada por la víctima que luego le permite obtener los accesos no autorizados de un usuario con altos privilegios y acceder a la red o a la base de datos de la entidad. Otra forma existente que hay, es por medio de la internet, el cual se puede crear avisos instantáneos ofreciendo oportunidad de ganancias, en el que se invita al usuario a registrarse, o también al que solo le den clic a un enlace que será re direccionado a una página falsa o el de enviar por medio del correo electrónico sobre la entidad bancaria del usuario, que es idéntica al sitio web oficial de esa entidad bancaria, informándole que debe actualizar sus datos personales, que hay una falla en esa entidad y que se ha presentado una vulnerabilidad en su contraseña, y es ahí donde las personas caen de una manera u otra, desde luego se debe añadir más información para corroborar ese aviso y que se vea algo legítimo, pero desde luego muchos usuarios utilizan casi las mismas contraseñas en otras redes, colocando la fecha de nacimiento de sus seres queridos, una canción que les guste, comida, lectura, nombres, etc., y es en esa parte en donde los delincuentes informáticos aprovechan de esas vulnerabilidades, y que desde

luego adjuntan algún tipo de archivo, en donde se puede ejecutar un malware, un keylogger, etc., y así obtienen las contraseñas, números de las cuentas bancarias, y que estos programas se ejecutan en un segundo plano.

Otro método que existe, es por medio de la basura de las víctimas, el cual consiste en encontrar información entre las canecas de basura en la oficina o en la casa, en el que se puede encontrar números de cuentas, números telefónicos, cartas, manuales de las políticas de la empresa u organización, planos de instalación, planos de la infraestructura, manuales de sistemas, fotos, CDs, DVDs, agendas personales, USB, microSD, memorias, etc. Ya que toda esta "basura" puede ser de una gran fuente de información para el atacante, ya que, si se encontrarse una agenda telefónica o de lo que hace, puede encontrar números telefónicos de los amigos, compañeros, familiares, trabajadores, jefes, "de las posibles víctimas que pueden ayudar a facilitar en dar más información". Además, también se puede encontrar organigramas, el cual permite revelar quienes están en cargos importantes dentro de la empresa. En la parte de los manuales de políticas, se puede encontrar la seguridad de la empresa, como también en los calendarios, los cuales hay personas que anotan que fechan se van a encontrar con aquellas personas, reuniones, entregas de trabajo, etc.

Existe otro método, y es uno de los más avanzados y complejos, el cual es la ingeniería social inversa, el cual permite en que el atacante realiza una suplantación de una persona que se encuentra en una posición de alto rango dentro de la empresa u organización, en el que el atacante tiene como característica principal la autoridad con la que trata a los trabajadores de dicha empresa, con el objetivo de que las demás personas "sus víctimas" les entregue los informes exigidos al atacante, sin realizarle ninguna pregunta, es decir copiar las características de esa persona.

Las personas que utilicen la ingeniería social, deben utilizar métodos básicos de persuasión, como, por ejemplo, la suplantación, también el de utilizar un poco la psicología, y de identificar las características de las víctimas y sus vulnerabilidades, para poder realizar sus acciones y cumplir sus objetivos. Pero desde luego, se debe tener en cuenta de los hackers (para este caso los ciber-delincuentes) no buscan el de obtener toda l información en un solo ataque, para que no sean descubiertos, pero que desde luego puedan conseguir toda esa información en varios ataques en diferentes ocasiones y momentos.

Otra de las características de la ingeniería social, es que se suelen enfocarse en la parte de los recursos humanos de las empresas, el cual existen diferentes tipos de personas. Una parte curiosa, es que la mayoría de los trabajadores pretenden siempre quedar bien y por esta razón, ellos brindan información sensible sin ninguna restricción a quien lo solicite, desde luego se debe realizar las preguntas correctas, en el momento correcto. Además, hay personas que tienen poco

conocimiento en el área de la informática o que también ignoran la existencia de los diferentes tipos de amenazas informáticos. En las empresas como también en las organizaciones tiene fallas al no implementar, controles básicos de seguridad informática que apoyen los diferentes procesos de protección de la información, con el objetivo de proteger y que algunas de estas empresas no lo realizan es porque dicen que son muy costosas.

En la parte de como disminuir estos ataques, es por medio de la educación, en que las personas que hagan parte de una empresa u organización, desde la persona que haga la limpieza, la secretaria, secretario, los encargados de la parte administrativa, los de los altos mandos, entre otros, deben estar actualizados sobre la seguridad informática, en el cual en la parte de la formación en las diversas técnicas de seguridad informática se debe iniciar en el personal encargado del sector TI (Tecnología de la Información) de la empresa, ya que son los responsables de transmitir los conocimientos adquiridos al resto de los trabajadores por medio de capacitaciones como parte de sus planes de acción y, con eso el de poder reducir un poco las amenazas que se encuentra día a día en las empresas y más en la parte de la ingeniería social se refiere.

Además, cualquier tipo de ataque informático cuenta con una metodología básica, que permite cumplir con los objetivos establecidos y corroborar cada uno de los movimientos necesarios, desde luego se debe tener en cuenta de la pretensión del atacante y de las barreras de seguridad con que cuenta el objetivo que se ha establecido. A continuación, en la ingeniería social existen varios métodos, en el que se debe tener en cuenta que hay varios pasos, que son:

- Paso 1. Identificar a la víctima: es aquí en donde el hacker plantea el objetivo y también estima las probabilidades de éxito que puede tener ese ataque., por lo tanto, el ataque puede estar dirigido a una persona o una empresa u organización. Esta es la actividad inicial antes de ejecutar el ataque de ingeniería social.
- Paso 2. Reconocimiento: una vez establecido el objetivo, el hacker inicia la búsqueda de datos sobre la víctima, en el que pueden servir para su ataque, además, se debe recordar en los párrafos anteriores de que ellos buscan información en la basura de su víctima, en la cesta de basura de su oficina o casa y, de tratar de desarrollar confianza o de realizar phishing.
- Paso 3. Crear el escenario: en este paso, es donde se realiza la configuración del escenario del ataque, ya que también depende del ingenio del hacker, de sus habilidades, ya que depende de la seguridad que existe en el que cuenta con la víctima, como también en las instalaciones físicas y sistemáticas que existen en una empresa, el cual el atacante ya haya analizado con anterioridad y de

realizar los puntos favorables y los contras que existen en este, y cumplir con sus objetivos.

- Paso 4. Realizar el ataque: el hacker pone en práctica técnicas como lo que es la ingeniería social inversa, entre otros tipos de ataques, como también el uso de diferentes softwares, como los son sniffers y los keyloggers, también realiza el escaneo de puertos y el de identificar y analizar los mapeos de redes, el phishing y, también el de ganarse la confianza de la víctima para cumplir con sus objetivos establecidos.
- Paso 5. Obtener la información: en este paso, es donde se realiza el control de la situación, como también de la red y del ordenador, el hacker con sus habilidades de ingeniería social procede a captar la información que necesita, ya sea por medio de un ordenador, de una memoria USB, de un teléfono inteligente, una cámara digital o también con herramientas informáticas, como lo es un malware, el cual permite enviar constantemente los datos a una dirección de correo electrónico o a una dirección IP.
- Paso 6. Salir del proceso de ataque: una vez cumplido con los objetivos establecidos del ataque por parte del hacker (que en la mayoría son los hackers de sombrero negro y grises o crackers) este abandona el lugar o la situación sin levantar sospecha, pero desde luego se debe quemar toda la evidencia, como, por ejemplo, las memorias RAM, disco duro, la placa madre o Board, entre otros elementos de hardware, el cual puede dejar evidencia del ataque.

El Phishing.

"El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima" [9].

¿Cómo funciona el Phishing?

Uno de los mecanismos más habituales de un phishing, es la generación de un correo electrónico falso, el cual permite simular que procede de una empresa u organización, con el objetivo de engañar a los usuarios. Dicho mensaje contendrá enlaces que pueden apuntar a una o a varias páginas webs que replican en todo o en parte del aspecto y de la funcionalidad de la empresa u organización, de la que se espera que el receptor mantenga una relación comercial. "Si el receptor del mensaje de correo efectivamente tiene esa relación con la empresa y confía en que

[9] Reyes Moya Raúl. (2013). Delitos Informaticos – Estudio concreto sobre Fraudes y Phising. [En Línea]: http://ns2.elhacker.net/phishing.pdf

el mensaje procede realmente de esta fuente, puede acabar introduciendo información sensible en un formulario falso ubicado en uno de esos sitios web"[10].

Tipos de ataques relacionados con

- Deceptive Phishing: este tipo de ataque es el más común, el cual consiste en el envio de un correo electrónico engañoso en lo que realiza es una suplantación de una empresa que ha seleccionado el atacante. El receptor pulsará en el enlace contenido en el mensaje, el cual es re direccionado a otra página, a un sitio web fraudulento.
- Malware-Based Phishing:en este tipo de ataque se refiere en la variante del delito que implica la ejecución de un software malicioso en la computadora. Ha veces algún tipo de malware se ejecuta de forma automática, otros necesitan alguna ejecución que debe realizar el usuario, en la mayoría de los malware se ejecutan en un segundo plano, para que el usuario no se dé cuenta de lo que está ocurriendo, también estos malware se pueden esconderse en una imagen, audio, documentos de texto, entre otros.
- Keyloggers y Screenloggers: estos son una variedad de malwares, en donde los keyloggers son programas que tiene la función de registrar las pulsaciones del teclado cuando la maquina en la que está instalada accede a un sitio web registrado o el de enviarlos a un correo electrónico especifico.
- Session Hijacking: "Describe el ataque que se produce una vez que el usuario ha accedido a alguna web registrada por el software. Estos programas suelen ir disfrazados como un componente del propio navegador"[11].
- Web Trojans: estos son algunos de los programas que aparecen en forma de ventanas emergentes sobre las pantallas de validación de páginas web legítimas. La víctima cree que está introduciendo los datos personales en un sitio web real, en lo que realmente está otorgando sus datos a un sitio web malicioso.
- System Reconfiguration Attacks: en este tipo de ataque se efectúa modificando los parámetros de configuración de la computadora de la víctima, como, por ejemplo, el de la modificación el nombre del dominio.
- Data Theft: en este tipo de ataque se trata de una variedad de códigos maliciosos que recaban a información confidencial de la víctima, que se encuentra almacenado en su computadora.
- DNS-Based Phishing ("Pharming"): en este tipo de delito se basa en la parte de la interferencia en el proceso de búsqueda de los dominios, es decir en modificar de forma fraudulenta la resolución del nombre de dominio, con el

[10] Reyes Moya Raúl. (2013). Delitos Informaticos – Estudio concreto sobre Fraudes y Phising. [En Línea]: http://ns2.elhacker.net/phishing.pdf

[11] Reyes Moya Raúl. (2013). Delitos Informaticos – Estudio concreto sobre Fraudes y Phising. [En Línea]: http://ns2.elhacker.net/phishing.pdf

objetivo de enviar al usuario, a la víctima a una dirección IP diferente, pero con las mismas características del sitio web.

- Hosts File Poisoning: para este caso es la transformación que se lleva a cabo por medio de un fichero de hosts que alberga en los servidores DNS.
- Content-Injection Phishing: "consiste en introducir contenido fraudulento dentro de un sitio web legítimo"[12].
- Man-In-The-Middle Phishing: para este caso el hacker realiza una intervención entre la computadora de la víctima y el servidor, con el objetivo de filtrar, leer y de modificar la información.
- Search Engine Phishing: "Los phishers crean buscadores para redireccionarte a los sitios fraudulentos"[13].

6.2 MARCO CONCEPTUAL

Definiciones del DRAE, 22 edición (2001):

Seguridad: "cualidad de seguro. (Mecanismo):- que asegura un buen funcionamiento, precaviendo que éste falle, se frustre o se violente."[14].

Información: "Comunicación o adquisición de conocimiento que permiten ampliar o precisar los que se poseen sobre una materia determinada. El conocimiento es lo que permite al soberano saber y al buen general intuir, esperar y anticiparse. (Sun Tse, siglo V a.C)"[15].

Protección: "Resguardar a una persona, animal o cosa de un perjuicio o peligro"[16].

Seguridad informática: es la rama de la ingeniería de sistemas, el cual se encarga de coordinar acciones para proteger la integridad y la privacidad de la información que son almacenadas en un sistema informático.

[12] Reyes Moya Raúl. (2013). Delitos Informaticos – Estudio concreto sobre Fraudes y Phising. [En Línea]: http://ns2.elhacker.net/phishing.pdf

[13] Reyes Moya Raúl. (2013). Delitos Informaticos – Estudio concreto sobre Fraudes y Phising. [En Línea]: http://ns2.elhacker.net/phishing.pdf

[14] Romero Alonso Luis (200). Seguridad informática – conceptos generales. disponible en: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

[15] Romero Alonso Luis (200). Seguridad informática – conceptos generales. disponible en: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

[16] Romero Alonso Luis (200). Seguridad informática – conceptos generales. disponible en: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

Propiedades de la seguridad informática: a continuación, se encontrará las principales propiedades de la seguridad informática:

a. Integridad: la información debe ser consistente, fiable y no propensa a alteraciones no deseadas. [17]
b. Disponibilidad: la información debe estar en el momento que el usuario requiera de ella. [18]
c. Autentificación: verificar la identidad del emisor y del receptor. [19]
d. Privacidad: la información debe ser vista solo por personas autorizadas a ello. [20]

Niveles de seguridad: actualmente se ha establecido diferentes niveles de seguridad, establecidos por la ISO en función al grado de importancia de la información que se requiere proteger. A continuación, se encontrará los siete niveles de seguridad, denominadas A1, B3, B2, B1, C2, C1, D. siendo el D de menor seguridad y A1 al de mayor, teniendo en cuenta que cada nivel incluye las exigencias de los niveles inferiores.

Nivel D: "Estos sistemas tienen exigencias de seguridad mínimos, no se les exige nada en particular para ser considerados de clase D"[21].

Nivel C1. "Para que un sistema sea considerado C1 tiene que permitir la separación entre datos y usuarios, debe permitirse a un usuario limitar el acceso a determinados datos, y los usuarios tienen que identificarse y validarse para ser admitidos en el sistema"[22].

Nivel C2. "Para que un sistema sea de tipo C2 los usuarios tienen que poder admitir o denegar el acceso a datos a usuarios en concreto, debe de llegar una auditoria de accesos, e intentos fallidos de acceso a objetos (archivos, etc.), y también especifica que los procesos no dejen residuos (datos dejados en registros, memoria o disco por un proceso al terminar su ejecución)"[23].

Nivel B1. "A un sistema de nivel B1 se le exige control de acceso obligatorio, cada objeto del sistema (usuario o dato) se le asigna una etiqueta, con un nivel de

[17] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf
[18] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf
[19] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf
[20] Seguridad informática
[21] Seguridad informática
[22] Seguridad informática
[23] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf

seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nominas, ventas, etc.)"[24].

Nivel B2. Un sistema de nivel B2 debe tener un modelo teórico de seguridad verificable, ha de existir un usuario con los privilegios necesarios para implementar las políticas de control, y este usuario tiene que ser distinto del administrador del sistema (encargado del funcionamiento general del sistema). Los canales de entrada y salida de datos tienen que estar restringidos, para evitar fugas de datos o la introducción de estos.

Nivel B3. "En el nivel B3 tiene que existir un argumento convincente de que el sistema es seguro, ha de poderse definir la protección para cada objeto (usuario o dato), objetos permitidos y cuáles no, y el nivel de acceso permitido a cada cual. Tiene que existir un 37 "monitor de referencia" que reciba las peticiones de acceso de cada usuario y las permita o las deniegue según las políticas de acceso que se hayan definido"[25].

Nivel A1. "Los sistemas de nivel A1 deben cumplir los mismos requerimientos que los de nivel B3, pero debe ser comprobado formalmente el modelo de seguridad definido en el nivel B1"[26].

¿Qué es un ataque informático?

Un ataque informático consiste en aprovechar algún tipo de debilidad o falla en el sistema (vulnerabilidad) en la parte del software, como también en el hardware e incluso, en las personas que forman parte de un ambiente informático (que puede incluir en las medianas, grandes empresas y organizaciones), con el objetivo de obtener un beneficio, y más en la parte económica, generando efectos negativos en la parte de la seguridad del sistema, que luego repercute de forma directa en los activos de la empresa u organización.

Tipos de Ataques Informáticos:

En esta parte, se debe identificar los distintos tipos de ataques informáticos, el cual se puede diferenciar en primer lugar entre los ataques activos, en el que producen cambios en la información de la víctima y en la situación de los recursos del sistema.

[24] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf

[25] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf

[26] Seguridad informática. disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf

Por otro lado, se encuentra los ataques pasivos, que se limitan a registrar el uso de los recursos y el de acceder a la información que se encuentra guardada en un ordenador, servidor, entre otras o transmitidas por el sistema.

A continuación, se encontrará los principales tipos de ataques contra redes y sistemas informáticos:

a. Actividades de reconocimiento de sistemas: en esta actividad se identifica porque están directamente relacionadas con los ataques informáticos, pero desde luego no provocan ningún daño al sistema, tiene como objetivo el de perseguir y obtener la información previa sobre las empresas y organizaciones (lo que son las redes y los sistemas informáticos), el cual realizan un escaneo de puertos para poder determinar qué servicios se encuentran activos o también el de un reconocimiento de versiones de sistemas operativos y sus aplicaciones.
b. Detección de vulnerabilidades en los sistemas: En este tipo de ataque se trata de detectar y documentar las posibles vulnerabilidades de un sistema informático, para este caso como ejemplo el Exploits.
c. Robo de información mediante la interpretación de mensajes: son otros tipos de ataques que trata de interceptar de los diferentes tipos de mensajes de correos electrónicos o también de los documentos que son enviados por medio de las redes de ordenadores como la internet, con el objetivo de vulnerar la confidencialidad del sistema informático y la privacidad hacia los usuarios.
d. Modificación del contenido y secuencia de los mensajes transmitidos: en este tipo de ataque, “los hackers tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático” [27], el cual los modifica de forma maliciosa, ejemplo, para poder generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque, es conocido como ataques de repetición.
e. Análisis de tráfico: en este tipo de ataque, tiene como objetivo el de observar los datos y los diferentes tipos de tráfico que son transmitidos a través de las redes informáticas, el cual utilizan herramientas informáticas como sniffers. Además, eavesdropping, es la interpretación del tráfico que se da en una red de forma pasiva, sin modificar su contenido.
f. Ataques de suplantación de la identidad:
    a. IP Spoofing (enmascaramiento de la dirección IP): permite que un atacante consigue modificar la parte de la cabecera de los paquetes que son enviados a un determinado sistema informático, para poder simular que lo que es enviado de un equipo distinto al verdadero equipo, es decir se realiza como una copia de su dirección.

[27] Álvaro Gómez Vieites (2014). Tipos de ataques e intrusos en las redes informáticas.

b. DNS Spoofing: este tipo de ataques, lo que realiza es de falsificar la DNS, pero desde luego en direccionar de forma errónea en los equipos afectados, debido a la traducción errónea de los nombres de dominio a las direcciones IP's, con el objetivo de facilitar el re direccionamiento de los usuarios de los sistemas afectados hacia el sitio web falso o también en la interpretación de sus mensajes de los correos electrónicos.
c. SMTP Spoofing: ahora, en este tipo de ataques, "permite el envío de mensajes con remitentes falsos, con el objetivo de engañar al destinatario o también el de causar un daño en la reputación del supuesto remitente, el cual es otra técnica frecuente de ataque basado en la suplantación de identidad de un usuario. Por lo tanto, se emplean muchos tipos de virus informáticos con diferentes técnicas de equipamiento para facilitar su propagación, al ofrecer información falsa sobre la posible infección en el sistema, es decir desvía la atención de los usuarios en otros objetivos, mientras se siga propagando estos tipos de virus informáticos"[28].
d. Capturas de cuentas de usuarios y contraseñas: además, es posible suplantar la identidad de los diferentes usuarios, por medio de las herramientas que permiten capturar las contraseñas, como los programas de software espía o también los dispositivos de hardware especializados que permiten realizar los registros de todas las pulsaciones en el teclado de una computadora, llamados keyloggers.

g. Modificación del tráfico y de las tablas de enrutamiento: "Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos"[29].

Amenazas: Causa potencial de un incidente no deseado, el cual puede provocar daños de diferentes tipos en un sistema o en una empresa u organización.

Antivirus: este es una de las categorías de software de seguridad, el cual protege una computadora de los diferentes tipos de virus que existen en el área de la informática, el cual se realiza en tiempo real y también mediante análisis al sistema, en el que pone en cuarentena y también elimina los virus que hay en el ordenador. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples.

[28] Álvaro Gómez Vieites (2014). Tipos de ataques e intrusos en las redes informáticas. P.25.
[29] Álvaro Gómez Vieites (2014). Tipos de ataques e intrusos en las redes informáticas. P. 26.

Contraseña: cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. “El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña”[30].

Exploits: “los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red”[31].

Firewall: “es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles”[32].

Hacker: son los mismos piratas informáticos. “Personas que se dedican a romper la seguridad de los sistemas de información. Existen en la actualidad, diferentes puntos de vista para el uso de esta palabra y otras relacionadas”[33].

¿Qué es la Ingeniería social?

Es una práctica es catalogada por muchos como el ataque informático más peligroso. Consiste en manipular psicológicamente a las personas para compartan información confidencial o tan solo obtener el mismo tipo de información de forma que el usuario no se entere de ello. Un factor importante a tener en cuenta es que es una estafa antigua, puesto que no se necesita tener conocimientos avanzados en informática para cometer este tipo de delitos.

Una frase muy escuchada para definir la ingeniería social es “toda cadena se rompe por el eslabón más débil" y este es el usuario del sistema o las personas del común, una empresa puede tener la seguridad tecnológica más avanzada y actualizada que exista en el mercado, pero si no ha creado conciencia en sus empleados o no tiene

[30] Op. cit., p. 8.
[31] Op. cit., p. 8.
[32] Op. cit., p. 9.
[33] BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia. Facultad de educación, 2015. 116 p.

unas políticas de seguridad claras y socializadas en la organización, este siempre será su punto débil. Y como lo expresamos anteriormente no se necesita ser técnico experto para el robo de la información. Se puede decir que es mucho más fácil para los ciberdelincuentes conseguir una contraseña que hackear un sistema informático, por esto el auge de la ingeniería social.

Esta información es compartida por la mayoría de usuarios siendo inconscientes de lo que están compartiendo. Es importante aclarar que la información no solo se encuentra en dispositivos tecnológicos también se puede acceder a esta desde bases de datos obtenidas en internet o compradas de forma virtual o física, otra fuente de información son los diferentes elementos de correo físico como cartas, facturas, documentos bancarios etc.

¿Qué es un Virus Informático?

Un virus informático es programa que se copia automáticamente (sin el conocimiento ni el permiso del usuario, de la víctima) ya sea por medios de almacenamiento, sin tener el conocimiento ni los permisos del usuario, de la víctima, ya sea por medios de almacenamiento o por internet, y tiene como objetivo de alterar el normal funcionamiento de la computadora, poniéndola como una maquina zombi, el de borrar los datos, crear puertas traseras, entre otras.

¿Qué es un Malware?

Malware es la abreviatura de “Malicius Software” (Software Malicioso), “con el objetivo de infiltrarse a las computadoras y servidores o en códigos de una computadora sin el consentimiento de su propietario y el de dañar el sistema o de causar un mal funcionamiento. Además, se propaga en las redes sociales, sitios webs fraudulentos, redes P2P (descarga con regalo), en dispositivos como en las USB, CDs, DVDs, teléfonos móviles, etc., también en sitios webs legítimos pero infectados, en los correos electrónicos, entre otras”[34].

¿Qué es un Ransomware?

Es un tipo de malware que actualmente se está propagando de forma rápida y muy activa por la internet. “La función de este malware es de impedir el acceso y

[34] Ministerio de educación [CO]. (2014). ¿Qué es un Malware?. P.45.

amenaza con destruir los documentos y otros activos de las víctimas si las víctimas no acceden a pagar el rescate que les exige"[35].

¿Qué es el Phishing?

El Phishing o también conocido como suplantación de identidad, es una clase de ingeniería social utilizada por los delincuentes informáticos para obtener información de las víctimas de manera fraudulenta. La herramienta que es utilizada preferentemente es el correo electrónico donde por medio de comunicaciones oficiales obtienen información sensible de los usuarios que ingenuamente responden a las preguntas planteadas, encuestas o formularios otorgando así sus datos personales de una forma muy sencilla. Es importante aclarar que estas herramientas son la base de cualquier delito informático puesto que de ellas se obtiene información materia prima para la ejecución de actividades ilícitas.

6.3 ESTADO ACTUAL

Actualmente, se ha ido mejorando en la parte de penalizar a las personas que cometan estos delitos informáticos en Colombia, ya que los organismos encargados de implementar las normas y las leyes legales en este país han observado que este tipo de delitos se ha ido incrementando constantemente. Pero en Colombia, en la parte de la seguridad de la información solo se vino a tratar de forma rigurosa hasta el año de 2009, con la creación de la ley 1273 de 2009 "por medio de la cual se modifica el código penal y se crea un nuevo bien jurídico denominado de la protección de la información y de los datos" [36].

Gracias al juez segundo de control de garantías el señor Alexander Díaz, experto en nuevas tecnologías del derecho y protección de datos., el cual él afirma que la ley de delitos informáticos de Colombia es una de las mejores a nivel continental según el congreso de la Fiadi (Federación Iberoamericana de Asociaciones de Derecho e informática). Por medio de esta ley, las empresas y las personas ya pueden contar con un instrumento para poder denunciar, cosa que no se podía

[35] Instituto Nacional de Ciberseguridad de España. (2017). PRESS START & INSERT BITCOIN – Ransomware: una guía de aproximación para el empresario.

[36] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4

anteriormente, ya que los mecanismos existentes no eran los apropiados para esa ocasión.

A continuación, se encontrará algunas normas en la legislación nacional de Colombia, que tratan sobre los delitos informáticos y sus penalizaciones, los cuales son:

Ley estatuaria 1226 de 2008: "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales" [37].

Ley 1341 de 2009: "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, también con esta ley se crea la Agencia Nacional de Espectro" [38].

Ley 527 de 1999: "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación." [39].

Ley Estatutaria 1581 de 2012: "por la cual se dictan disposiciones generales para la protección de datos personales" [40].

Las denuncias acerca de la ingeniería social y Phishing en Colombia, han ido aumentando, puesto que, aunque existe desinformación acerca del tema ya algunas son conscientes de este tipo de delitos y realizan las denuncias ante el cai Virtual. Muchas de las empresas utilizan sofisticadas herramientas de seguridad, pero desde luego el eslabón más débil en la cadena de la información es el ser humano., en el cual, las personas dejan ciertos puntos "vulnerables", como, el de dejar el ordenador encendido conectado a la red e irse a tomarse un tinto a una cafetería, es en esa parte en donde se identifica la vulnerabilidad de la víctima, en donde el ingeniero social ingresa, buscando una conectividad con esa persona, ganándose la confianza, una vez realizado ese objetivo, inicia otro paso, el cual es escudriñar

[37] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no. 47219. p. 1-12.

[38] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47426. p. 1-18.

[39] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999.

[40] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. no. 48587. p. 1-164

en la computadora de la víctima, una vez ingresado en la computadora, por medio de una USB, descarga un malware en el ordenador, infectando toda la red de la empresa o una parte para poder más adelante tomar el control de la red de la empresa.

También se puede observar las vulnerabilidades de las personas en los aeropuertos, como en el aeropuerto el dorado en Bogotá, en donde muchas personas utilizan el wifi gratuito que otorga el mismo aeropuerto o se conectan a redes wifi que no tienen contraseñas, sin saber del porque están hay esas redes y con qué objetivo tienen. También, se encuentra otra práctica de ingeniería social llamada "navegación por el hombro", el cual alguien se para detrás y le graba con su celular, simulando estar hablando, todo lo que teclea, buscando claves e información confidencial de la víctima.

A continuación, encontramos un caso de ingeniería social, el cual fue a la víctima Joaquín Rozo, trabajador de un prestigioso banco en Colombia, "quien un día accedió a prestarle el ordenador de la compañía a una de sus clientes frecuentes por unos minutos, para que ella pudiera descargar algunos archivos que eran requeridos por la misma entidad. Días después, la compañía confirmó haber sido víctima de robo de información., ya que la señora Rozo había instalado un programa malicioso que de acuerdo al reporte dado por la parte del departamento IT, sustrajo información de más de cuarenta y siete (47) mil trabajadores y ex trabajadores y, además de ciento y cincuenta (150) mil datos de clientes empresariales y naturales de los últimos años"[41].

"Patricia Gaviria, directora de Educación en ETEK International indica: "Los resultados de diversos estudios evidencian la importancia de tener en las compañías programas de Security Awareness, como una estrategia que apoya a las organizaciones en la tarea de concientizar a su equipo de trabajo sobre el cuidado, la navegación y la protección de la información que manejan a diario" [42].

De acuerdo a los informes de seguridad 2016 de Check Point, "uno de cada cinco (5) de los trabajadores es responsable de alguna brecha que afecta los datos corporativos y la descarga de malware en el servidor de una empresa en cada cuatro a cinco segundos, por lo que la concienciación del personal es una de las claves de seguridad para las empresa y organizaciones"[43].

En la parte de los ataques informáticos en Colombia en comparación con otros países demuestra de que las empresas aún no están lo suficientemente preparadas

[41] La ingeniería social al servicio del cibercriminal. (2017). Computerworld Colombia. [En línea]: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/
[42] La ingeniería social al servicio del cibercriminal. (2017). Computerworld Colombia. [En línea]: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/
[43] La ingeniería social al servicio del cibercriminal. (2017). Computerworld Colombia. [En línea]: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/

para poder enfrentar las amenazas informáticas que hay en la actualidad. De acuerdo a las cifras de los casos de ingeniería social a través del phishing "aumento de 2015 a 2016 en un 22,6% registrando más de 200 denuncias mensuales" [44]. "Por parte de la RSA señala que este tipo de ataques cibernéticos aumentan entre un 30% y un 40% cada año, por ende, equivale a un nuevo ataque de phishing cada 30 segundos" [45].

A continuación, existen otros casos de ingeniería social, ocurridos en empresas colombianas en los últimos años, que son:

- DIAN (17 de octubre de 2017): este caso ocurrió el martes 17 de octubre de 2017 en la dirección de impuestos y aduanas nacionales DIAN, en el que emitió un comunicado en donde se alertaba a la ciudadanía en general, sobre un nuevo ataque de ingeniería social por medio de correos electrónicos falsos, el cual son enviados a los correos de los usuarios (victimas) en nombre de la entidad tributaria, ya que estos correos electrónicos son enviados por medio de artimañas informáticos, haciendo creer a los usuarios que son oficiales esos correos, para que los ingenuos ciudadanos colombianos caigan en la trampa y así obtener los datos personales, y de esta manera poder robarles la información confidencial o de sus cuentas bancarias.
  Estas cuentas de correos electrónicos parecían oficiales, como, por ejemplo: acastillo@ediagro.com y minhacienda@dian.gov, con asunto, como: "Hasta la fecha no hemos recibido el pago de sus impuestos", "Notificación embargo DIAN" y "problemas con su situación fiscal", entre otros. Además, la autoridad tributaria DIAN, recordó en ese momento a los ciudadanos y a los contribuyentes que, es muy importante poder validar la información emitida por cualquier entidad ya sea pública o privada, y el de no descargar los archivos adjuntos que se envían en estos correos sospechosos para no ser afectados por esta conducta fraudulenta. En la siguiente figura 1., encontramos un mensaje enviado por correo de suplantación de la DIAN, tomada de un caso de una persona.

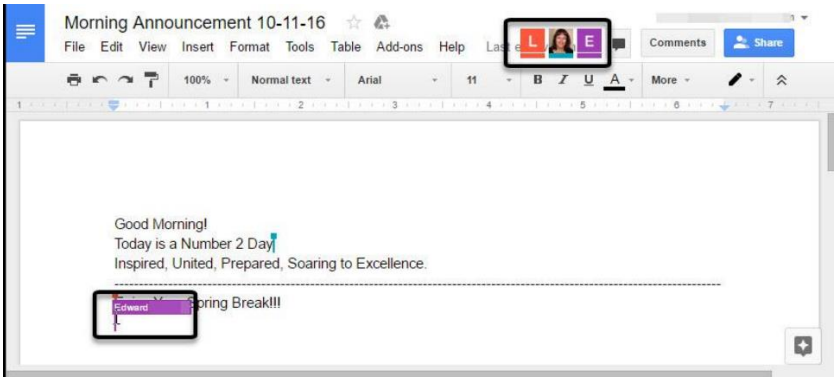
Figura 1., Mensaje enviado por Correo electrónico de suplantación de la DIAN 2017.

[44] La ingeniería social al servicio del cibercriminal. (2017). Computerworld Colombia. [En línea]: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/
[45] La ingeniería social al servicio del cibercriminal. (2017). Computerworld Colombia. [En línea]: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/

Fuente: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

Google Docs (5 de mayo de 2017): en ese tiempo, los usuarios que tenían correos electrónicos Gmail de google, realizaron un ataque de ingeniería social por medio de la técnica de Phishing, el cual esta técnica consiste en el de suplantar a un servicio o una persona. En este ataque, se enviaba un email de alguien, el cual decía de que habían sido añadidos a un documento de trabajo en conjunto, en este mensaje se le pide al usuario, a la víctima que haga clic en el enlace para visualizar el documento online, como se muestra en la siguiente figura 2., en donde aparecen las diferentes cuentas asociadas a ese trabajo colaborativo, y estas personas acceden a este enlace, y verifican que es un archivo falso, pero ya es demasiado tarde, ya que los atacantes han tenido tiempo para poder hacerse a la información confidencial que ellos necesitan.

Figura 2. Documento de Google Docs Falso



Fuente:
https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html

Además, google reconoció que este ataque ha sido superado en sus medidas de control y protección, y por lo tanto recomendó a sus usuarios que solo deben abrir los mensajes para colaborar en un documento de Google Docs si están plenamente seguros de que el remitente es el correcto.

7. CAPITULO I: CONCEPTOS BASICOS.

7.1 LA INGENIERIA SOCIAL.

7.1.1 ¿Qué es la Ingeniería social?

Actualmente la ingeniería social es conocido actualmente como el ataque informático más peligroso. Esta técnica se basa fundamentalmente en manipular psicológicamente a las personas, para que de esta manera entreguen información confidencial o poder obtener el mismo tipo de información de forma que el usuario no se dé cuenta de ello. Un factor importante a tener en cuenta es que es una estafa antigua, puesto que no se necesita tener conocimientos avanzados en informática para cometer este tipo de delitos.

Una frase muy escuchada para definir la ingeniería social es “toda cadena se rompe por el eslabón más débil" y este es el usuario del sistema o las personas del común, una empresa puede tener la seguridad tecnológica más avanzada y actualizada que exista en el mercado, pero si no ha creado conciencia en sus empleados o no tiene unas políticas de seguridad claras y socializadas en la organización, este siempre será su punto débil. Y como lo expresamos anteriormente no se necesita ser técnico experto para el robo de la información. Se puede decir que es mucho más fácil para los ciberdelincuentes conseguir una contraseña que hackear un sistema informático, por esto el auge de la ingeniería social.

Los delincuentes informáticos envían mensajes o links al azar para que de esta forma los usuarios la compartan siendo inconscientes de lo que están publicando. Un factor importante a tener en cuenta es que la información no solo se encuentra en dispositivos tecnológicos también podemos acceder a esta desde bases de datos obtenidas en internet o compradas de forma virtual o física, otra fuente de información son los diferentes elementos de correo físico como cartas, facturas, documentos bancarios etc.

Es fundamental tener en cuenta que la ingeniería social también tiene categorías de ataques a los usuarios; Ataques técnicos, al ego, de simpatía y de intimidación.

En el ámbito del cibercrimen, la ingeniera social es descrita como un método no técnico utilizado por los delincuentes cibernéticos para obtener información y de esta manera realizar fraudes u obtener acceso ilegal en los equipos de las víctimas.

La Ingeniería Social se basa en la interacción humana y está impulsada por personas que usan el engaño con el fin de violar los procedimientos de seguridad que normalmente deberían haber seguido.[46]

7.1.2 Categorías de ataques en la ingeniería social.

Cuando hablamos de ingeniería social inmediatamente pensamos en robo de información, pero también debemos tener en cuenta que existen diferentes categorías en las cuales podemos posicionar los diferentes ciberataques como son estos dos grupos:

7.1.2.1 Hunting.

Son los estos tipos de ataques son los que buscan obtener información específica del objetivo o las victimas con la menor exposición directa posible**.** O en pocas palabras con el menor contacto. Obtienen la información de sus víctimas y desaparecen. En la práctica hablamos de ataques de ingeniería social enfocados a obtener X dato (*normalmente credenciales de acceso a un servicio o cuenta, activación o desactivación de alguna configuración que puede complicar el objetivo final o como apoyo a un ataque mayor, dirigido y persistente*), de forma que el atacante se pone en contacto de alguna manera con la víctima, y la insta a realizar una acción cuyo desenlace es el pretendido inicialmente.

7.1.2.2 Farming.

Es lo contrario del Hunting. En el *farming* "el objetivo es mantener el engaño el mayor tiempo posible, para exprimir al máximo el conocimiento, recursos o posición

[46]5 cosas que debes saber de la ingeniería social, enero 2016, Eset Welaive security Disponible en: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/4

de la víctima. Para ello, se suele recurrir a granjas de identidades, que por lo general han sido robadas con anterioridad"[47].

7.1.3 Aspectos claves en la ingeniería social.

Según Kevin Mitnick[48], el éxito de los ataques de ingeniería social, se debe a cuatro principios básicos y comunes a todas las personas:

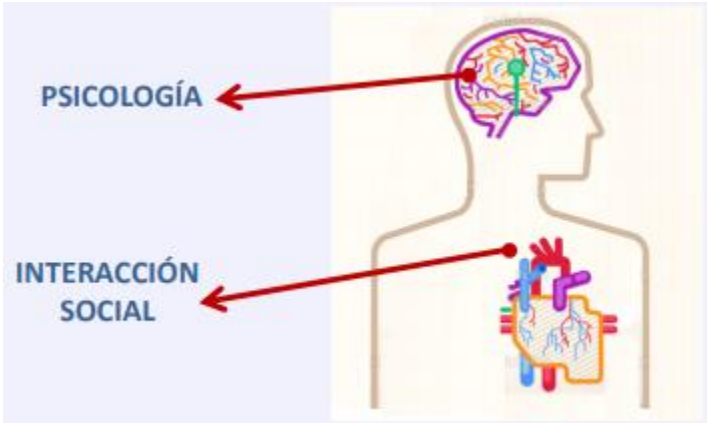
- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir "No".
- A todos nos gusta que nos alaben.

De acuerdo a lo anterior la ingeniería social tiene dos puntos clave en los que se basa el ciberdelincuente para realizar el ataque, ellos son la psicología (ya que por medio de halagos etc, pueden acceder a nosotros) y la interacción social ya que mediante las redes o la interacción con intrusos se logra el objetivo.

Figura 3. Puntos clave de ataque de la ingeniería Social

[47]Los 6 principios básicos de la ingeniería social, Pablo F Iglesias Disponible en: , https://www.pabloyglesias.com/mundohacker-ingenieria-social/

[48] Ingeniería social: Cuales son los tipos de ataque, Emiliano Piscitelli , 293 Revista USERS Disponible en: http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/



7.1.4 Tipos de ingeniería social

7.1.4.1 Catfishing.

Crean cuentas falsas, utilizando información de otros o inventándola. Haciéndose ver como la otra persona quiere.

7.1.4.2 Phishing.

Los criminales informáticos tiran correos anzuelos para ver que pescan, como es la traducción de su significado en español.

7.1.4.3 Spear Phishing.

Identifican un objetivo en particular y hacen investigación de sus perfiles, empiezan a enviarle correos con información de su interés, estos llevan código malicioso.

7.1.4.4 Baiting.

Dejar un dispositivo infectado con software malicioso para que la víctima lo encuentre y así poder atacar sus dispositivos posteriormente.

7.1.4.5 Dumpster Diving.

En algunas ocasiones las empresas envían a las papeleras documentación de la compañía a la basurera como manuales del sistema, organigramas, políticas entre otras. Por lo que los atacantes utilizan estos documentos para obtener información.

7.1.4.6 Piggybacking.

El atacante intenta entrar a un sitio donde no debería estar, pero con los permisos y las credenciales de alguien que verdaderamente si puede hacerlo.

7.1.4.7 Whalling.

Es un ataque de phishing dirigido a altos ejecutivos de la empresa, “caza de ballenas”.

7.1.4.8 Cartas Nigerianas.

Son mensajes falsos que llegan en donde lo invitan a consignar una cantidad mínima de dinero, para ganar una gran cantidad.

7.1.4.9 Ingeniería social a la inversa.

Es cuando el ingeniero social crea un problema y luego se involucra en el para solucionarlo.

7.1.4.10 **Shoulder Surfing**.

Espiar por encima del hombro a las personas.

7.1.4.11 **Quid pro quo**.

“Algo por algo” llama a números aleatorios de empresas manifestando que hay un problema técnico y para que de esta manera la victima de información y acceso a los SI. O ganar premios.

7.1.4.12 **Tailgaiting**.

Obtener acceso a un área restringida, mediante el engaño.

7.1.4.13 **Vishing.**

Consiste en hacer llamadas telefónicas encubiertas con encuestas para así sacar información a las personas.

7.1.5 Metodología de la ingeniería social

Existen tres fases, que son relevantes a la hora de realizar un ataque de ingeniería social, no es relevante el tipo ingeniería social que se está aplicando estas son:

7.1.5.1 Fase de acercamiento

Esta es la primera etapa, pues consiste en hacer el primer acercamiento a la víctima para de esta manera tratar de ganar su confianza. Normalmente, el ciberdelicuente se vale de técnicas de ingeniería social lo que permite al objetivo dominar la comunicación porque de esta manera detecta sus debilidades primarias para poder ser explotadas.

7.1.5.2 Fase de alerta

Posteriormente de la etapa de acercamiento se encuentra la fase de alerta, en donde se plantean diferentes opciones a la víctima y de esta manera medir y así observar su velocidad de respuesta bajo presión. En esta fase, el grado de interacción cambia y de repente se empieza a ser más activo: el atacante lanza propuestas sueltas; generalmente todas para afianzar la confianza inicialmente

establecida. Con esto se logrará que el objetivo revele más información de la que está dispuesta a entregar.

7.1.5.3 Fase de distracción

En esta fase; el atacante ya ha obtenido gran parte de la confianza que se necesita para conseguir que la víctima entregue los datos que desea obtener. “La victima ya se siente a gusto en la comunicación y baja sus defensas a niveles penetrables. En paralelo, el atacante domina prácticamente la comunicación; si bien no llega al punto de agobiar al objetivo para evitar que éste levante sus alarmas”[49].

7.2 EL PHISHING.

7.2.1 Historia del Phishing (Origen del término)

Este término utilizado frecuentemente como un tipo de ingeniería social, phishing proviene de la palabra inglesa "fishing" (pesca), lo que traduce en el español hacer que los usuarios "muerdan el anzuelo", y la persona que realiza el ataque se le denomina Phisher o delincuente.

La primera mención del término phishing se remonta a principios de enero de 1996. “(Se dio en el grupo de noticias de hackers alt.2600, aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 Magazine. El término phishing fue adoptado por quienes intentaban "pescar" cuentas de miembros de AOL. Utilizando algoritmos que generaban números de tarjetas de crédito aleatorios, estas cuentas podían durar semanas o meses antes de que una nueva fuera requerida. Posteriormente, AOL tomó medidas tardíamente en 1995 para prevenir esto, de modo que los crackers recurrieron al PHISHING para obtener cuentas legítimas en AOL)”[50].

[49] Conoce los riesgos y amenazas de la ingeniería social sobre tus activos y datos sensibles, Febrero 2018, Azury Mendoza Disponible en: http://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/

[50] Zabala, J. A. Responsabilidad Bancaria Frente al Delito de Phishing en Colombia. [En Línea] Colombia.

7.2.2 ¿Qué es el Phishing?

Phishing o suplantación de identidad es una técnica de ingeniería social, la cual es utilizada por ciberdelincuentes para obtener información de las víctimas de manera fraudulenta. En el phishing la herramienta por preferencia es el correo electrónico ya que de esta manera los ciberdelincuentes envían comunicaciones oficiales al azar y obtienen información sensible de los usuarios que ingenuamente responden encuestas o formularios otorgando de esta manera sus datos personales en bandeja de plata. Es importante aclarar que estas herramientas son la base de cualquier delito informático puesto que de ellas se obtiene información materia prima para la ejecución de actividades ilícitas.

7.2.3 Tipos de Phishing.

Este delito informático también cuenta con diferentes formas de operar, por esto es importante tener en cuenta como son:

7.2.3.1 Phishing de clonado o de redireccionamiento.

> Es un tipo de engaño de campaña, en donde se buscan aquellas víctimas para que estas estén interesadas en la publicidad engañosa e inserten los datos correspondientes en un formulario controlado por el atacante. Además, en este tipo de campañas engañosas, envían enlaces masivos por email, haciéndose pasar por alguien conocido o también en alguna marca que goce con el respeto de las víctimas, pidiéndole a esta que accedan lo antes posible, dándoles ciertas recompensas (en el que no se puede permitir que la víctima se tome su tiempo para pensar) para beneficiarse de una oferta, como puede ser, en un concurso, una rifa, descarga gratuita de contenido de pago., y el de obtener información importante, como también en un mensaje enviado o para solucionar un problema grave (tu cuenta bancaria ha sido bloqueada hasta que se demuestre ser el titular de la cuenta., otro ejemplo es, no has pagado la última factura y estás a un paso en estar en lista de morosos.

Disponible en: http://repository.ucatolica.edu.co/handle/10983/14943

7.2.3.2 Phishing de timo.

Este es otro tipo de ataque, que es considerado tradicional., en donde los vectores de ataque provienen del email, de las redes sociales y de los servicios de mensajería, pero, además, hay dos principales diferencias con el anterior ataque, el cual es:

No suelen ser tan masivos como el phishing de clonado: el cual su funcionamiento (más manual), no puede abarcar a tantísimo target, en el que parte de la fase inicial, de la toma de contacto.

Su objetivo no es robarnos credenciales, sino realizar algún tipo de timo más tradicional: para este caso, no habrá ninguna página web fraudulenta al final del ataque, en el que genera una especie de espiral de engaños, en el que se busca aprovechar nuestras debilidades que nos acabará obligando a seguir en contacto con el atacante.

Un ejemplo, para este caso, es cuando una persona extranjera o de otro departamento, se hace conocer por medio de las redes sociales, y le da inicio a la conversación, dándole un me gusta a una foto o un mensaje de texto, etc., y después de analizarlo varios días, te empieza a pedir dinero para viajar a tu país o departamento, y conocerlo personalmente, pasándose por esa persona que dice ser, sin decencia que casualmente te ha elegido a ti entre todo el resto de personas del mundo para dejarte el dinero o de pedirte tu dinero, siempre y cuando puedas hacer frente a las continuas retenciones de aduanas/cambios de divisas/impuestos, o el tráfico de fotos comprometidas que has compartido aparentemente con una persona de su edad o en el caso de niños y niñas que caen en trampas de estas.

7.2.3.3 Spear Phishing.

Este tipo de ataque se trata de un phishing dirigido a la consecución de un objetivo específico en una víctima especifica., en el que se realiza un estudio OSINT avanzado inicial, en el que permite conocer de antemano qué debilidades podría tener, para enfocar el ataque a que sea lo más creíble posible.

Si el objetivo es atacar a una empresa, lo habitual es de buscar a alguien del área administrativa y directivo de la empresa (usuario con acceso al sistema y que no suelen tener muchos conocimientos informáticos), y una vez que lo identifiquen y lo engañen, se ira accediendo y ascendiendo en la cadena hasta el equipo de IT, que suelen tener acceso a todo el material que se quiere obtener.

¿Los vectores de ataque? Para este caso también es por email o correo electrónico, pero también cada vez más redes sociales, en especial las profesionales como Linkedln, por lo tanto, es difícil defenderse en este tipo de ataque, ya que el delincuente va a tiro fijo y con la información publicada, puede saber mucho de nosotros como víctimas

7.2.3.4 Smishing o SMS phishing.

> Para este tipo de ataque, el correo electrónico o email sigue siendo el canal principal para las comunicaciones importantes, pero con la caída del SMS, y su paulatino uso para notificaciones importantes o segundos factores de autenticación, el mensaje de texto empieza a verse como una herramienta fiable para lanzar campañas de phishing.

"El smishing no es más que un phishing vía SMS, que habitualmente tiene como cometido que envíes un mensaje a un número de tarificación especial (concursos fail, mayormente), la suscripción a servicios premium (esto es, pagos recurrentes) o la multicanalidad con vista a una campaña de phishing avanzada (después de que el supuesto departamento de seguridad de Microsoft te contacte por mail para avisarte que te va a mandar ahora un SMS y debes confirmarles la clave, harás sencillamente todo lo que ellos te pidan)"[51].

7.2.3.5 Vishing o Voice Phishing.

> "Si el smishing es un tipo de phishing vía SMS, el vishing es lo mismo, pero vía centralita de telefónia (o VoIP). Y opera exactamente igual que el anterior. O bien por separado ("Oiga, le llamamos de su operadora, ¿puede confirmarnos que la clave de su router es 1234?"), o bien como apoyo para un ataque de spear phishing más efectivo".

Hoy en día, el phishing ha sido una de las principales amenazas que llegan a través del correo electrónico., aunque los cibercriminales cada día están buscando nuevas técnicas, por lo que buscan que dichos correos electrónicos tengan una mayor tasa de éxito. Se intenta buscar que la víctima los abra e interactúe con estos. Los correos electrónicos de phishing son fáciles de implementar. No requieren una gran preparación del atacante más que la elaboración de un correo que sea convincente

[51] Iglesias, F. Pablo. #Mundo Hacker: 5 tipologías de phishing que debería conocer. Consultor de Presencia Digital y Reputación Online.

ante los ojos de los objetivos. Sin embargo, son fáciles de detectar en la mayoría de ocasiones y no llegan a entrar en la bandeja de entrada. Además, los ciberdelincuentes están prefiriendo nuevas técnicas, en el que se introducen correos más sofisticados, es decir, más personalizados., en el que buscan la suplantación de identidad, pero con un mensaje que la víctima confié., como, por ejemplo, introduciendo un emisor de un nombre reconocible para la víctima.

"Este método es más difícil de detectar con las soluciones de seguridad tradicionales porque, por lo general, no sigue un patrón. Esto sin duda dificulta la tarea para filtrar estos e-mails y hace que pueda llegar con mayor facilidad al destinatario. Además, utilizar la suplantación para entregar correos a la víctima, es la nueva forma de realizar ataques phishing. El objetivo final es el mismo de siempre: engañar al usuario para que transfiera dinero o divulgue información que podría conducir a un ataque más eficiente. Obtener las credenciales, en definitiva" [52].

En la parte del correo electrónico se incluyen un enlace de phishing, en el que se introducen un nombre en el que debe confiar la víctima, de que haya una mayor probabilidad de éxito. Por otra parte, existe otra táctica que generalmente se combina con la suplantación del nombre de visualización en usar una dirección con un nombre de usuario que sea confiable para la misma víctima.

En la actualidad hay nuevos ciberataques por email, en el que ahora existe un tipo de ataque de fraude del CEO, en el que básicamente se basa en que el atacante, suplanta la identidad del jefe de una empresa, y pide a un trabajador de la propia empresa, en el que normalmente es el que se encarga de la contabilidad, el cual se transfiere de una manera urgente a una determinada cantidad de dinero para cerrar un acuerdo.

"Según FireEye, el 90% de los ataques bloqueados durante el análisis fueron sin ningún tipo de malware, el 81% eran ataques de phishing, casi duplicándose en el último semestre" [53]. Además, los datos también indican que esta tendencia continuará aumentando, por lo tanto, los ataques de suplantación de identidad, el cual fueron el 19%, y sigue continuando estable, a ese valor.

Ahora, podemos detectar los diferentes tipos de ataques, en el cual FireEye ha publicado algunas tenencias destacadas de los diferentes tipos de ataques por email analizados., para este caso, los ataques con malware eran muy comunes tanto los lunes como los miércoles, sin embargo, los ataques de suplantación de

[52] Jiménez, Javier. Así están evolucionando los ataques de phishing para tener un mayor éxito.

[53] Jiménez, Javier. Así están evolucionando los ataques de phishing para tener un mayor éxito.

identidad se daban los viernes, ideal para hacer la “estafa del CEO”, ya que, si hicieran esto mismo cualquier otro día, es muy posible que el propio CEO estuviera en la empresa. [54]

7.2.4 Tipos de ataques relacionados con el Phishing.

7.2.4.1 Deceptive Phishing.

Este es una de las modalidades más comunes, en el cual, consiste en el envío de un correo electrónico engañoso, en el que se suplanta a una empresa, organización, entidad bancaria o gubermental. Ahora, en la parte del receptor pulsará en el enlace contenido en el mensaje, en el que desvía de manera inconsciente a un sitio fraudulento para la víctima en el ataque.

7.2.4.2 Malware-Based Phishing.

En este tipo de ataque se refiere a la variante del delito, en el que implica una o varias ejecuciones de uno o también de varios tipos de software malicioso en una computadora. En este caso el usuario deberá realizar alguna ejecución que permite la ejecución de este malware en el ordenador, como el de abrir un archivo, visitar un sitio web, descargar un archivo, ver un video, entre otras.

7.2.4.3 Keyloggers y Screenloggers.

Este es una variedad de particularidades de malware, en donde los keyloggers son programas que registran las pulsaciones del teclado cuando la computadora infectada acceda a una web registrada o también cuando tenga acceso a la red, en donde es enviada las capturas de teclado a un correo electrónico que se encuentra dentro del programa del keylogger, y los Screenloggers tienen la misma función, pero este tipo de programa lo que realiza es de capturar imágenes de la pantalla.

7.2.4.4 Session Hijacking: este tipo de ataque se da cuando se produce una vez que el usuario, la víctima ha accedido a algún sitio web registrado por el

[54] De luz, Sergio. (2018). Los ataques sin malware por correo electrónico aumentan en el último semestre.

software. Estos programas suelen ir ocultos como un componente propio o extensión de un navegador.

7.2.4.5 Web Trojans.

Estos son programas que aparecen en las ventanas emergentes de validación de páginas web legitimas., en el que el usuario cree que está introduciendo los datos personales a un sitio web legítimo, que puede ser de una entidad gubernamental, bancaria, empresa u organización.

7.2.4.6 System Reconfiguration Attacks.

Este tipo de ataque se efectúa modificando los parámetros de configuración de la computadora de la víctima, como, por ejemplo, a modificación del nombre de dominio.

7.2.4.7 Data Theft.

Este se trata de varios códigos maliciosos, en el que tiene como función el de recabar toda la información confidencial almacenada en esa computadora.

7.2.4.8 DNS-Based Phishing (“Pharming”).

Este tipo de delito se basa en la interferencia en la parte de los procesos de búsqueda de un nombre de dominio, esto quiere decir, que es de modificar de forma fraudulenta la resolución del nombre de dominio, en el que se enviaba al usuario a una dirección IP distinta.

7.2.4.9 Hosts File Poisoning.

Para este caso es la transformación de los ficheros de hosts que se encuentran en los servidores DNS.

7.2.4.10 Content-Injection Phishing.

Esta es una modalidad, en el que consiste en el de introducir contenido fraudulento dentro de un sitio web legítimo.

7.2.4.11 Man-in-the-Middle Phishing.

Para este caso, el ciberatacante se posiciona entre la computadora de la víctima y el servidor, en el que se filtra en este espacio, y que puede realizar modificaciones, el de leer la información.

7.2.4.12 Search Engine Phishing.

"Los Phishing crean buscadores para re direccionarte a los sitios fraudulentos"[55].

[55] Reyes Moya Raúl. (2013). Delitos informáticos. Estudio concreto sobre Fraudes y Phishing.

8. CAPITULO II: TECNICAS DE ATAQUES.

8.1 TECNICAS DE ATAQUE PHISHING.

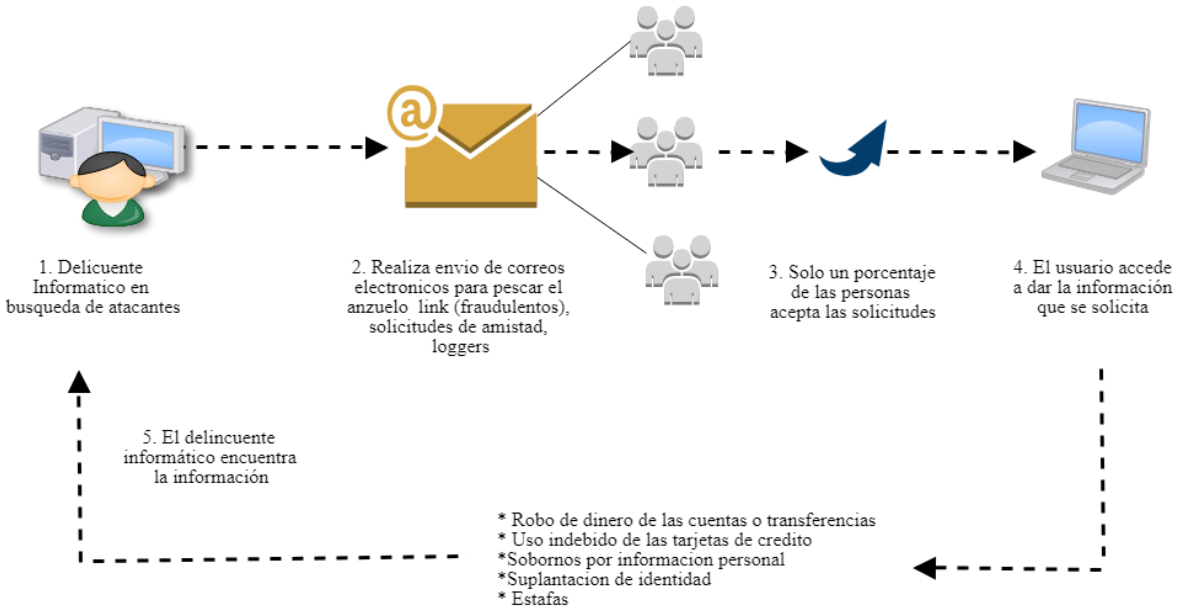
Un factor importante en las técnicas de phishing es que siempre tienen un objetivo final sin importar la modalidad que adopte el atacante y esta es engañar al usuario de dos formas una es para sacar dinero (transferencias) y la segunda es para que divulgue información confidencial lo que con lleva a un ataque posterior (obtener contraseñas).

¿Qué necesitan del usuario?: En la mayoría de los casos, necesitan que se realice una de dos acciones: clickar en un link o abrir un fichero adjunto. Cualquiera de estas acciones abrirá una puerta a la siguiente del ataque del hacker.

¿Cómo atacan?: Utilizan el factor humano, que es el eslabón más debil en la cadena de seguridad. El 95% de los incidentes relacionados con la seguridad, incluyen algún tipo de error humano.

Generalmente, como lo mencionamos anteriormente un ataque de Phishing comienza con un correo electrónico y sólo con que una de las víctimas ejecute la acción sugerida en el correo, los ciberdelincuentes tendrán la forma de actuar ante los objetivos y pasar a una segunda parte del ataque, que incluye entre otros ataques de denegación de servicio, bloqueo de sistemas, robo de información, e infecciones de malware.

Figura 4. Proceso de ataque Phishing



Autores: propio

Aunque existen diferentes tipos de phishing los cuales hablamos anteriormente, existe un modus operandi generalizado para este tipo de ataques como lo son:

La mayoría de las técnicas que utiliza el *phishing* utilizan la manipulación en el diseño del correo electrónico para lograr que el enlace o mensaje parezca legítimo de la empresa u organización gubernamental por la cual se hace pasar el ciberdelincuente.

Las URL ilegitimas o el uso de subdominios, son los trucos que generalmente utilizan los phishers para realizar sus ataques como podemos visualizar en el siguiente ejemplo http://www.nombredetubanco.com/ejemplo, en la cual el texto mostrado en la pantalla no corresponde con la dirección real a la cual conduce.

Otro ejemplo para encubrir enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares).

Otros intentos de *phishing* utilizan comandos en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legal sobre

la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método actualmente usado en las técnicas de *phishing* es que el phisher utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente grave, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Otro problema con las URL “es el relacionado con el manejo de Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios (por ejemplo *dominio.com* se ve similar a *dominio.com*, aunque en el segundo las letras "o" hayan sido reemplazadas por la correspondiente letra griega *ómicron*, "o"). Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones. A pesar de la publicidad que se ha dado acerca de este defecto, conocido como IDN spoofing o ataques homógrafos, ningún ataque conocido de phishing lo ha utilizado”[56].

Un aspecto claro a tener en cuenta es que las empresas toman medidas para contrarrestar los ataques de phishing una vez ya han ocurrido, actualmente las medianas y pequeñas empresas son las que más sufren a la hora de hablar de ciberataques ya que estas no tienen el presupuesto económico necesario para la protección, herramientas tanto de software como hardware y personal calificado para estos ataques.

De acuerdo al informe de seguridad cibernética para Empresas presentado por Cisco, que estudia los datos de 1,816 encuestados de Empresas en 26 países, ofrece un análisis del panorama que enfrentan las organizaciones más pequeñas en el tema de seguridad, y qué recomendaciones o acciones deben seguir estas organizaciones para atenderlo de una manera más efectiva.

Un dato relevante del informe es que el 53% de los encuestados experimentó un ataque. Esto a menudo tienen un impacto financiero duradero en una empresa, así como los gastos asociados para limpiar o eliminar los daños ocasionados. (Junior,

[56] The Homograph Attack, https://support.microsoft.com/es-es/help/834489/internet-explorer-does-not-support-user-names-and-passwords-in-web-sit

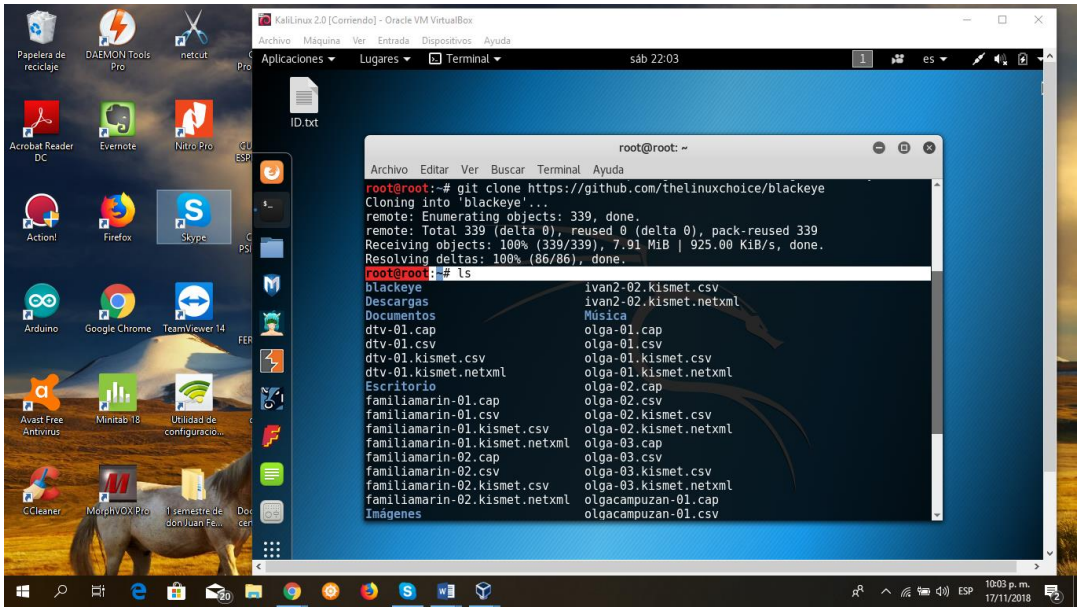
2018), otro de los datos arrojados por el informe es que los móviles son los más atacados, pero en controversia son los más difíciles de proteger.

Las empresas actualmente están considerando la adopción de servicios de almacenamiento en la nube, ya que esto ha tenido un aumento significativo en los últimos años.

9. CAPITULO III: IDENTIFICACIÓN DE LAS HERRAMIENTAS Y LOS PROCESOS EN UN ATAQUE PHISHING

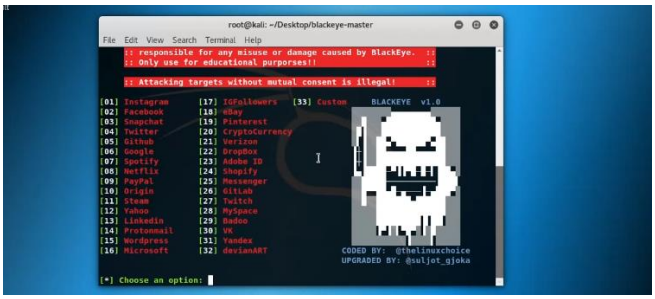
A continuación, se identificará la siguiente herramienta llamada Black Eye, el cual es una herramienta gratuita para hackear con phishing y es una de las más completas hasta ahora, el cual contiene 37 plantillas web+1 personalizables, con la función de recopilar información de IP y ubicación simplemente haciendo clic en el enlace. Además, admite las versiones móviles, y también admite plantillas de algunos sitios web que son un poco complicados de clonar, no obstante, no es compatible con algunas herramientas. **En las siguientes figuras 5 y 6, se encontrará la instalación del programa, como se verá a continuación:**

Figura 6. Descarga del Black eye



Fuente: autores.

Figura 6. Ejecutando Black eye



Fuente: autores.

Otra herramienta interesante es la Social Engineer Toolkit: esta herramienta está diseñada para realizar ataques avanzados contra las vulnerabilidades de una persona. Los métodos integrados en el kit de herramientas están diseñados para ser diferentes ataques que están dirigidos y enfocados contra una persona (víctima), una empresa u organización utilizada durante una prueba de penetración, en el que incluye phishing, recopilación de información, clonación de datos, entre otras.

Algunas de las herramientas SET más populares son los siguientes:

- Ataque Man in the Middle.
- Spear-Phisihing Attack Vector.
- Java Applet Attack Vector
- Metasploit Browser Exploit Method.
- Credencial Harvester Attack Method.
- Método de ataque Tabnabbing.
- Infectious Media Generator.

Browser Exploitation Framework (BeEF): ante todo, en los sitios web hay ciertas vulnerabilidades, como lo son: XSS, el cual es una de las vulnerabilidades más comunes en las diferentes aplicaciones web. BeEF (Framework de explotación del navegador) se utiliza para poder explotar una vulnerabilidad XSS y, además, se centra en los ataques del lado del cliente – usuario. Una vez realizado la explotación con esta herramienta en un sitio web, los usuarios de ese sitio web se convierten en víctimas y el navegador de las víctimas, el cual pueden ser controlados por el BeEF. Un hacker puede instalar complementos, mostrar ventanas emergentes, como también en el redirigir a cualquier URL. Además, también pueden hacer que las víctimas descarguen algún tipo de malware o cualquier programa malicioso.

HashCat: Hashcat puede crackear casi cualquier tipo de hash. Tiene dos variantes con dos algoritmos diferentes, uno es el craqueo de CPU, otro es el craqueo de GPU. Algoritmo de craqueo de GPU, OclHashCat es más rápido que el crackeo de la CPU tradicional porque la GPU tiene demasiados números de núcleos. OclHashcat utiliza multi-core para crackear miles de hash en menos de un

segundo. Esta poderosa herramienta para descifrar hash puede ser muy útil cuando la usas con una lista de palabras personalizada o un ataque de fuerza bruta[57].

BetterCap: es una de las herramientas más poderosas para poder realizar varios tipos de ataques Man-In-The-Middle., en el cual se puede manipular el trafico HTTP, HTTPS y TCP en tiempo real, como también el de buscar credenciales, entre otros. Se puede decir que esta herramienta BetterCap es la versión mejorada de la otra herramienta que es llamada Ettercap, el cual es otra herramienta muy popular para los ataques MIME. Además, la herramienta BetterCap tiene la capacidad de descifrar SSL/TLS, HSTS, HSTS precargados. También utiliza SSLstrip+ y el servidor DNS (dns2proxy) para poder implementar la derivación parcial de HSTS. Las conexiones SSL/TLS están terminadas., pero hay ciertas problemáticas, el cual la conexión descendente entre el cliente y el hacker no usa el cifrado SSL/TLS y permanece descifrada.

THC Hydra: Es una herramienta rápida y estable de derivación de inicio de sesión de red que utiliza un ataque de fuerza bruta o diccionario para probar varias combinaciones de contraseña e inicio de sesión en una página de inicio de sesión. Puede realizar ataques rápidos de diccionario contra más de 50 protocolos, incluidos telnet, FTP, HTTP, https, smb, varias bases de datos y mucho más[58].

Mapper de Red (Nmap): esta es otra herramienta, en el que simplemente escanea la red o un sistema, también permite escanear puertos abiertos, servicios en ejecución, NetBIOS, detección de OS, entre otros.

Aircrack-ng: Es una herramienta de descifrado de claves 802.11 WEP y WPA-PSK que puede recuperar claves cuando se han capturado suficientes paquetes de datos. Implementa ataques FMS estándar junto con algunas optimizaciones como ataques KoreK, así como los ataques PTW para hacer que sus ataques sean más potentes[59].

Se enfoca en diferentes áreas de seguridad WiFi:

---

[57] Rodriguez Pablo. (2018). Las diez (10) mejores herramientas de Kali Linux para Hackers éticos.

[58] Rodriguez Pablo. (2018). Las diez (10) mejores herramientas de Kali Linux para Hackers éticos.

[59] Rodriguez Pablo. (2018). Las diez (10) mejores herramientas de Kali Linux para Hackers éticos.

- Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por parte de herramientas de terceros.
- Ataque: ataques de repetición, autenticación, puntos de acceso falsos y otros a través de la inyección de paquetes.
- Pruebas: Comprobación de tarjetas WiFi y capacidades del controlador (captura e inyección).
- Cracking: WEP y WPA PSK (WPA 1 y 2).

Wireshark: este es otra herramienta, el cual es un analizador de red muy importante para los hackers. También es utilizado en la auditoría de seguridad de la red.

Esta herramienta utiliza filtros de visualización para el filtrado general de paquetes., el cual se puede examinar los detalles del tráfico en una variedad de niveles, en donde se identifica la información del nivel de conexión hasta el punto de los bits que componen un solo paquete. Por lo tanto, la captura de paquetes les puede proporcionar a un administrador de red, en informar los paquetes individuales, como en la parte de tiempo de transmisión, la fuente, el destino, el tipo de protocolos y también en los datos de los encabezados.

Metasploit Framework: este es una de las ultimas herramientas, el cual es para desarrollar y ejecutar código de explotación contra una maquina remota de destino. A continuación, se mostrará los pasos básicos para poder explotar un sistema que utiliza el framework, el cual incluyen:

- Elegir y el de configurar un exploit.
- Verificar si el sistema de destino deseado es susceptible al exploit elegido.
- También el de elegir y el de configurar un playload (código que se ejecutará en el sistema de destino al ingresar con éxito).
- También el de elegir la técnica de codificación para poder que el sistema de prevención de intrusiones (IPS) el cual ignora el payload codificado.
- Y por último el de ejecutar el Exploit.

A continuación, encontramos algunos pasos para evitar un ataque de phishing, los cuales son:

- Observar de forma detallada las URL en los enlaces de correo electrónico: para este primer paso, se debe revisar los correos electrónicos que son enviados de otras personas a la bandeja de entrada, el cual hay momentos que se adjuntan enlaces, pero antes de acceder, se debe pasar el cursor por encima, con el objetivo de ver la URL completa y el de poder saber si es

auténtico o no lo es. Además, se debe tener en cuenta que al ver un candado al inicio o el protocolo “HTPPS” no es garantía de autenticidad. Si uno como usuario no está seguro de esto, lo que se debe hacer es eliminar el enlace y el de acceder al sitio web capturando por completo el enlace en el navegador de preferencia.

- Typosquatting: este se refiere al uso de dominios parecidos al servicio legìtimo a los que dicen pertenecer, pero que a la vez tiene intensiones maliciosas. Ya que por lo general los hackers de sombrero negro, grises y algunos crackers, como también algunos ingenieros sociales utilizan la URL de una empresa importante, y solo le cambian una letra o un número, con el objetivo de engañar a la mayoría de los usuarios. Es recomendable revisar la ortografía de las URLs.

- Cuidado con las redes inalámbricas que se utilizan: se debe tener en cuenta este paso, ya que hay personas detrás de estas redes inalámbricas publicas sin contraseña, para que las personas (víctimas) se puedan conectar sin mayor esfuerzo, y así acceder a la información de las personas por medio de otras herramientas, el cual pueden acceder a cualquier tipo de aparatos electrónicos que se puedan conectar con las redes wifi. También el de no realizar transacciones, compras con las tarjetas débito y crédito en estas redes wifi públicas.

- Utilizar contraseñas seguras: en este paso, es recomendable para los usuarios el de crear, utilizar contraseñas complicadas, como, por ejemplo: mAriA1987@#&/87.

- No abrir emails que no se haya solicitado: antes de abrir un correo electrónico, se debe verificar si hay alguna alerta sobre algún ataque de phishing de la empresa u organización que lo envía. Si desconfías, solo debes llamar a la empresa y el de realizar las preguntas correspondientes.

- No hagas clic en los enlaces de los emails: Por lo general un ataque de phishing descarga varios tipos de malware a través de enlaces que se han adjuntado al correo electrónico del usuario, como también en los enlaces de mensajes de redes sociales, mensajes de whatsapp, etc.

- No descargar ficheros adjuntos: al igual que en los enlaces, se deberá tener mucha preocupación al descargar los ficheros adjuntos en las redes sociales, en los emails, y en el WhatsApp.

- Contar con un programa de formación antiphishing: este paso es en la parte donde se aplica a las medianas y grandes empresas, en donde se crea conciencia en los trabajadores sobre seguridad informática, en la parte de ingeniería social y sus consecuencias.

- Cambia su contraseña de inmediato: si en el caso de que caigas en un ataque de phishing no dudes en cambiar tu contraseña, si en tal caso de que te hackearon en tu cuenta de ahorros, debes comunicarte con tu entidad bancaria, para que realicen las acciones correspondientes.

10. CAPITULO IV: DOCUMENTO GUIA PARA PREVENIR LA INGENIERIA SOCIAL EL PHISHING EN LAS EMPRESAS COLOMBIANAS

Es importante tener en cuenta que para las técnicas de ataques phishing no existe una solución eficaz que logre eliminar por completo este tipo de amenaza, lo que se puede hacer es tomar medidas de seguridad que ayudan a mitigar el impacto de este ante las empresas.

Existen medidas de hardware, software y una de las que nos parece más importante es de implementar políticas de seguridad para este tipo de amenazas, además de realizar capacitaciones al personal y simulacros para evitar estos ataques.

A continuación, describiremos algunas formas en que podremos contrarrestar el phishing en las empresas colombianas.

10.1 Departamento de TI

Estas medidas son para los técnicos de las empresas, los cuales son los encargados del funcionamiento del departamento de tecnología de información.

1. Implementar herramientas de software para proteger las redes con antivirus, anti-phishing, antispyware, sistemas de protección total, antispam con funcionalidades de sandboxing (se crea un entorno seguro, no permite instalar software malicioso). Con estas herramientas se crean capas de seguridad, que evitan que esta amenaza llegue a nuestros trabajadores.

2. Implementar herramientas de hardware como lo son firewall UTM, routers y proxy, con una implementación de buenas políticas, con el objetivo de garantizar la detección de vínculos maliciosos.

3. Realizar simulacros con los trabajadores de la compañía, simulado un ataque ficticio de phishing y luego hacer retroalimentación en el simulacro realizado, teniendo en cuenta los puntos vulnerables y corroborar los demás puntos.

4. Contar con un “Hacker ético”: un hacker ético es un experto que tiene los mismos conocimientos que un hacker de sombrero negro o gris, pero los utiliza para probar la seguridad de nuestra red y observar el daño al que estamos expuestos, antes de que lo haga un hacker criminal. Y realizar pruebas de pentesting.

5. Implementar políticas de seguridad informática en toda la empresa, basadas en las siguientes recomendaciones.

    - Restringir el acceso remoto a la red
    - Utilizar únicamente el correo corporativo

6. Recomendaciones a los trabajadores en agregar a favoritos los sitios web de confianza que son utilizados a diario, como también de hacer seguimiento a las personas que se acaban de conocer en las redes sociales, como, también afuera de sus oficinas y dentro de estas mismas, de realizarles un seguimiento sin entrar a su privacidad. Pero, además, en esa investigación que se puede realizar a las personas y a los sitios web, se puede obtener información confidencial de con quien se va relacionar o a que sitio web va a ingresar y así con el objetivo de evitar fugas de información privada dentro y fuera de la empresa.
7. Realizar Backups, el cual se deben hacer copias de seguridad informática que se encuentran en los equipos de cómputo en una empresa u organización, el cual estos backups se deben realizarse de forma periódica por medio de dispositivos de almacenamiento externos, los cuales deben resguardarse en un lugar diferente al del original de los datos. Además, se pueden hacer de forma local o remota a través de infraestructura y de aplicaciones específicas ofrecidas para ellos.

8. Imagen del sistema: es recomendable realizar réplicas exactas de los discos duros de los equipos de cómputo de la empresa u organización ya configurado, a partir de instalaciones limpias pero que también se puedan usarse en equipos con datos ya incluidos, a fin de realizar las diferentes recuperaciones de forma más rápida y sencilla en un caso de daño en la computadora. Además, los sistemas operativos como Windows 7, Windows 8, 8.1 y Windows 10, incluyen herramientas para la elaboración de este tipo de respaldo.

9. Cifrado de particiones: realizar un cifrado de particiones para hacer ilegible la información contenida en estas, por medio de algunos algoritmos matemáticos simétricos, asimétricos o también híbridos, es recomendable hacerlo en todos los equipos portátiles y de escritorio de la empresa.

10. Autenticación: el departamento de informática debe crear usuarios y contraseñas seguras, no solo para el acceso a los sistemas operativos, si no, a las redes de datos, sistemas de información a la BIOS de cada computador de la empresa. Se debe tener en cuenta la longitud de las contraseñas estas deben ser alfanuméricas, caducidad (asignarles límites de tiempo) y la complejidad de las contraseñas de acceso atendiendo a las recomendaciones que para ello existen en normas o guías internacionales de seguridad de la información [60].

10.2 Usuarios

Es importante tener claro la concientización de los usuarios en el uso de las tecnologías de información, como responsables del departamento de informática y, aún más en la parte de realizar las diferentes campañas de capacitación y concientización acerca de todos los temas de actualidad de TI y de la seguridad informática.

1. Crear contraseñas complejas, ya que generalmente los usuarios utilizan el número de identificación, deben ser alfanuméricas y se deben cambiar periódicamente, como, por ejemplo: FernandA1995@#$@27.
    - Cambia las contraseñas cada tres o seis meses
    - Utilizar contraseñas diferentes para cada plataforma online que se utilice.
    - Evita contraseñas fáciles de adivinar (Esta página te puede ayudar a generar contraseñas de alta seguridad: https://lastpass.com).

[60] Plazas García Edna Roció. (2018). Ingeniería social en las empresas colombianas. Universidad nacional abierta y a distancia UNAD. Monografía. [En Línea]: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

2. Aprender a identificar los correos electrónicos de phishing, el cual existen algunas pautas a tener en cuenta para poder identificarlos.
    - Utilizan nombres y adoptan la imagen de empresas reales
    - Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa
    - Incluyen webs que visualmente son iguales a las de empresas reales
    - Como gancho utilizan regalos o la perdida de la propia cuenta existente
    - Existe una solicitud de información personal o de la empresa, tal como números de identificación, información financiera, claves usuarios entre otras., además, es importante tener en cuenta que las comunicaciones oficiales por lo general, no solicitan información personal del usuario en forma de un correo electrónico.
    - El mensaje es inesperado y no solicitado. Si en algún momento recibe un correo electrónico de una entidad o de una persona que rara vez trata, considera la posibilidad de esta sospechosa de correo electrónico.
3. Verificar la fuente de información de los correos entrantes.
    - La dirección del remitente no coincide con la firma en el mensaje en Sí.
    - Hay varios destinatarios y son direcciones aleatorias. Normalmente se envían mensajes corporativos directamente a los destinatarios individuales.
    - En el saludo del mensaje el nombre se encuentra extraído de la dirección de correo.
    - Pueden llegar mensajes en diferentes idiomas
    - El mensaje o los datos adjuntos piden que habilitar macros, ajustar la configuración de seguridad, o instalar aplicaciones.
    - El mensaje contiene errores**.** De tipo ortográfico, gramatical etc.
4. No hacer click a los enlaces que llegan al correo electrónico como adjunto.
    - Teclea directamente la dirección web en tu navegador o utiliza marcadores/favoritos si quieres ir más rápido.
    - Tener en cuenta las extensiones de dominio diferentes.
    - Verificar exhaustivamente la apariencia del sitio web, logotipos, errores ortográficos, entre otros
5. Introducir los datos confidenciales únicamente en las webs seguras.
    - Han de empezar por ‘https://’ y debe aparecer en tu navegador el icono de un pequeño candado cerrado.

6. No descargar archivos adjuntos pueden tener malware o programas para robarnos información.

7. Revisa periódicamente las cuentas del banco, ya que podemos ser blanco de un robo sin darnos cuenta.

8. Evitar publicar nuestros datos personales en sitios públicos, en foros, redes etc.

9. Infórmate constantemente acerca de los tipos de ataques actuales y el modus operandi de los delincuentes.

10. No confíes de los constantes anuncios de Google.

11. No compartir información con todo el mundo: no es recomendable compartir la información confidencial con cualquier persona que se les cruce en el camino, si se está trabajando en una empresa solo se debe compartir la información confidencial con los directivos o jefes de la empresa, a si se logra que la información esté más protegida y así la empresa sea menos vulnerable a los diferentes tipos de ataques informáticos.

12. No tener miedo de amenazas: las personas no debemos dejarnos intimidar por amenazas recibidas ya sea a través de redes sociales o personalmente. Muchos delincuentes informáticos utilizan ciertos elementos o información confidencial robada, para asustar a sus víctimas y llevarlas a hacer algo en contra de su voluntad, donde las personas terminan haciéndolo solo por temor. Si se siente atemorizado por alguna amenaza, pida ayuda a las autoridades policiales o cuéntele a alguna persona de confianza para que este le ayude[61].

[61] Plazas García Edna Roció. (2018). Ingeniería social en las empresas colombianas. Universidad nacional abierta y a distancia UNAD. Monografía. [En Línea]: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

11. RESULTADOS

Los resultados iniciales de esta monografía se obtuvieron por medio de la investigación dada, en el que se identifica la ingeniería social y los diferentes ataques de esta misma, de las herramientas que utilizan los ingenieros sociales, las metodologías que aplican, el engaño, y las vulnerabilidades que pueden presentar una persona, teniendo en cuenta que en la mayoría de estos ataques se realizan en empresas y organizaciones, para este caso es en Colombia, en el que cada día ha ido aumentado estos casos de ataques, y de la confianza de los mismos usuarios hacia los demás.

El objetivo de la ingeniería social por parte de los ciberdelicuentes, es de poder ganar el acceso no autorizados a las diferentes redes o también a la información de sus víctimas para cumplir con sus propios objetivos establecidos.

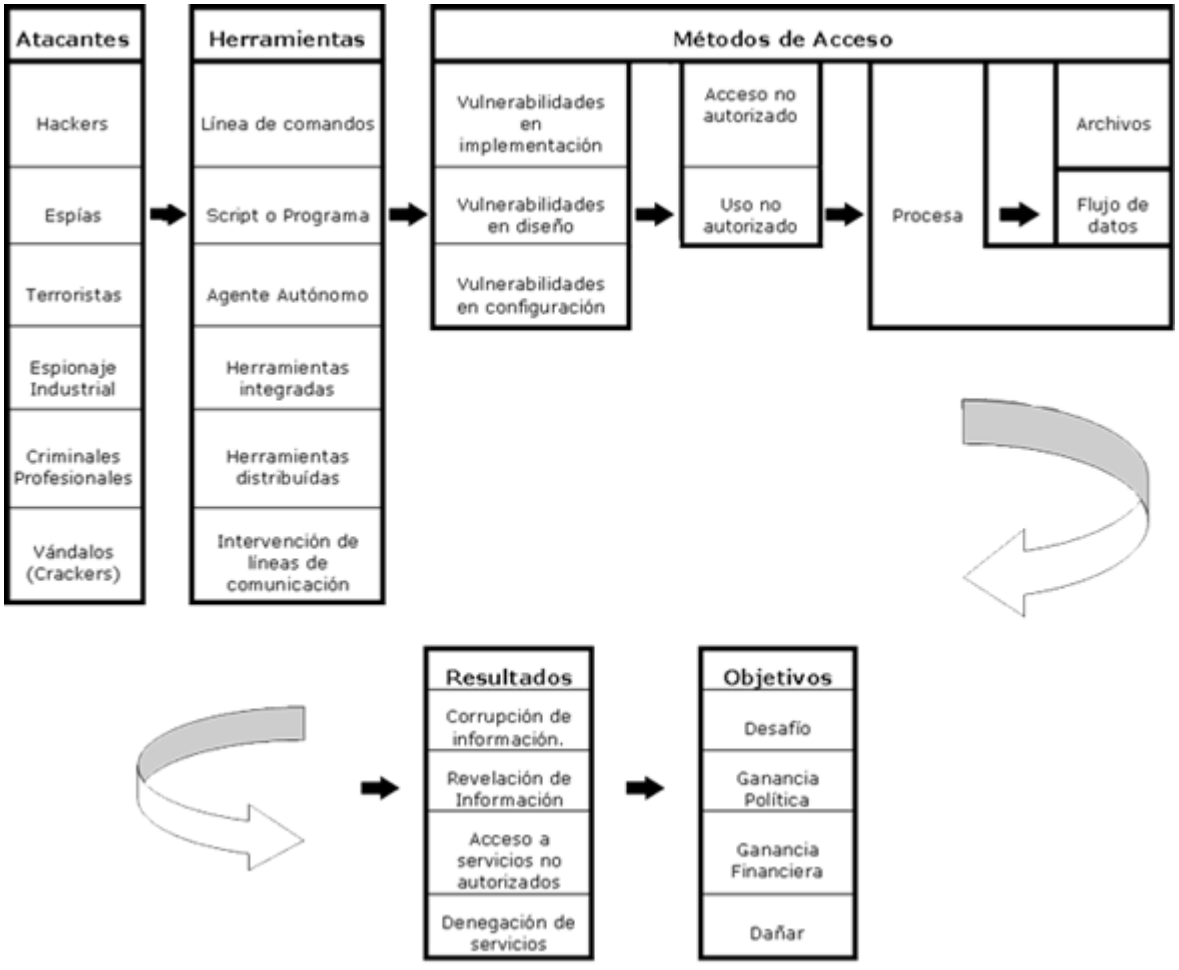
Además, existen también algunos objetivos específicos de los ataques de ingeniería social llevados a cabo en las diferentes empresas colombianas, que son:

- Las personas que utilizan las diferentes técnicas de ingeniería social, lo realizan para su propio bienestar, desde la parte económica, y así realizar varias investigaciones y desde luego en la creación de malware, ya que, para poder implementar los diferentes tipos de ataques cibernéticos a gran escala, es de una gran inversión económica como también de tiempo, para poder cumplir con los objetivos y sus metas.
- Además, también se puede hacer el robo de identidad de un individuo, en el cual se puede hackear algún perfil de las redes sociales y otras aplicaciones de comunicación, y así poder visualizar los archivos compartidos, con quien habla, como es su relación virtual con los demás, datos, etc., y así capturar esa información, de secuestrar y chantajear a la víctima pidiéndoles dinero, entre otras, para no revelar la información encontrada.
- Otro objetivo específico, es que los delincuentes realizan ataques de ingeniería social, para poder realizar las diferentes compras en internet, en el cual, capturan información de las tarjetas de crédito y débito a sus víctimas.

La ingeniería social es utilizada por los diferentes genios de la informática, algunos hackers, crackers, y personas del común, el cual buscan ser reconocidos, el de dejar una huella en el sistema, en las personas “víctimas”, algunos de estos lo realizan solo por jugar, otros por intereses propios.

Además, algunos ciberdelicuentes, utilizan la ingenieria social con otros métodos de hackeo, para poder acceder a las tarjetas de crédito y de débito, utilizando software y hardware para clonarlas, pero desde luego deben de ganarse la confianza de su víctima, como también, en el de intervenir sitios de comercio electrónico o de identidades bancarias para poder desviar las transacciones, como también el de secuestrar la información de estas entidades, compañías o particulares para poder exigir un pago a cambio de su devolución de los datos. Otros atacantes realizan estos mismos ataques con su don de convencimiento, y, además, persuaden a los demás, de sus doctrinas políticas, religiosa, psicológica, etc., para poder acceder a sus víctimas y el de convencerlas en realizar cualquier cosa que quiera su victimario.

A continuación, en la siguiente figura, se mostrará un esquema general de un ataque informático:



Fuente: https://www.segu-info.com.ar/ataques/ataques.htm

Además, se debe tener en cuenta de quienes son los más vulnerables a la ingeniería social, el cual puede ser cualquier empresa, sin importar su estructura, si es una empresa pequeña, mediana o grande, si es pública o privada, ya que todo tiene su vulnerabilidad, aunque no lo podemos notar a simple vista, pero al realizar un estudio minucioso, podemos encontrar esas vulnerabilidades. Si un trabajador de manera inconsciente proporciona información confidencial de la empresa o de el mismo por medio de un correo electrónico, de una llamada telefónica, de un sitio web, o el de responder alguna pregunta que es sospechosa, pero para el no, es donde encontramos esos puntos vulnerables. También se debe tener en cuenta de que algunas empresas grandes tienen mejores infraestructuras de tecnología e inyectan grandes cantidades de dinero para mejorar su seguridad para prevenir los diferentes ataques informáticos, y que desde luego tienen infraestructuras de redes complejas, y utilizan políticas de seguridad y algunos procedimientos a cumplir para poder resguardar la información en estas empresas, por lo tanto, son más difíciles de administrar y un ataque se puede realizar a las diferentes personas que estén integrado a la empresa e ir sacando pequeñas cantidades de información., como, por ejemplo: en empresas telefónicas, en hospitales, en instituciones militares, entidades financieras, medios de comunicación, entidades gubernamentales, entre otros. Por el contrario, el de realizar un ataque de ingeniería social en una empresa pequeña o mediana es un poco más difícil, pero no imposible, ya que normalmente los trabajadores se socializan más entre ellos, y el de identificar ciertas características entre ellos.

12. CONCLUSIONES

Al realizar el estudio teórico de la monografía acerca de los diferentes tipos de ataques de ingeniería social que se han dado en los últimos años en las diferentes empresas colombianas, se pudo observar y visibilizar que existen muchas falencias en las diferentes empresas que hay en Colombia frente al tema de la seguridad informática y de la información, el cual suelen escatimar en los diferentes gastos y la ausencia de ciertas actualizaciones en la parte de la seguridad de las empresas. De esta forma se logra establecer que el personal de una empresa colombiana es uno de los eslabones más débiles que hay a la hora de ejecutar un ataque de ingeniería social, por medio de algunas técnicas y metodologías, en el cual se puede realizar la suplantación de identidad por medio de llamadas telefónicas, como también espionaje, espionaje por encima del hombro, y observar las rutinas de las personas, sus gustos, entre otras.

Por medio de este documento se dio a conocer las diferentes técnicas de ataque phishing que existen actualmente y de cómo realizar un ataque con ingeniería social, identificando quienes son los más vulnerables a estos tipos de ataques, como también quienes son los que ejecutan los diferentes métodos de ingeniería social, para poder lograr identificar las diferentes vulnerabilidades en una empresa, específicamente en las empresas colombianas, como también en identificar y describir cuales son los objetivos de los ingenieros sociales, sus métodos, y de cómo ganarse la confianza de sus víctimas, ya que no solo mediante el correo electrónico podemos suministrar información valiosa de las empresas, si no directamente con las víctimas. La ingeniería social tiene como objetivo el de obtener la información de terceros, sin que las víctimas se den cuenta, de una forma no convencional para poder obtener la información deseada de una manera más eficaz y algo complicado, pero más seguro. Ya que estos ataques suelen realizarlos algunos grupos de hackers de sombrero negro, espías, ciberdelicuente, entre otros, en el que tienen varias personas con diferentes conocimientos y cualidades en el área de la seguridad informática.

En Colombia, la mayoría de las empresas que han sufrido estos tipos de ataques (ingeniería social) en los últimos años, son aquellas en las que pertenecen a las

entidades bancarias, el cual tienen muchos seguidores por la parte del manejo de recursos económicos que se dan en estas mismas entidades. Además, los ciberdelicuentes utilizan el método de phishing para el robo de información confidencial de estas empresas, el cual este método consiste en enviar correo electrónicos falsos a las diferentes cuentas de las posibles víctimas, en el que se les solicita a los usuarios en registrarse en esa página por un cambio en la base de datos de la entidad o que su clave debe ser cambiada, ya que lleva mucho tiempo el de no cambiarla, entre otras, para poder obtener los datos que ellos quieren.

Por medio de la guía que se especificó en esta monografía, existen diferentes alternativas que deben tener en cuenta los profesionales en TI y los usuarios para tratar de contrarrestar este tipo de ataques, puesto que De acuerdo a las cifras publicadas por el CaiVirtual se ha visto un alto incremento en el robo de información por medio de la técnica de ataque phishing, el cual se pudo corroborar que casi el 80% de la protección de la información está en la capacitación de los usuarios, de los administradores y gerentes en el área de la informática, ya que como nos dimos cuenta a lo largo de esta monografía son el eslabón más débil. Además de que en las empresas colombianas deben de implementar un CCTV propio y que adicionalmente de contar con el CCTV de una empresa de vigilancia, ya que debe estar monitorizado todos los puntos de una empresa.

13. RECOMENDACIONES.

Acatar los 22 pasos sugeridos para tener frente a los ataques de phishing en las empresas, aunque no garantiza que estemos 100% cubiertos ante estos ataques.

Mantener todo el personal de la empresa informado acerca de los diferentes ataques, ya que cada día se presentan en diferentes formas de atacar, pero siempre en base a lo mismo robo de información

Establecer un programa de capacitación en cuanto al tema de seguridad informática, para todos los trabajadores en las diferentes empresas colombianas, con el objetivo de consolidar una cultura de protección de la información dentro de estas mismas empresas. Además, estas capacitaciones deben hacerse periódicamente, y por lo tanto los ingenieros del departamento de TIC son los responsables de realizar estos programas de capacitación, como también el de estar actualizados en toda el área de la seguridad informática y de la información, como también el de estar avalados por los directivos de estas empresas colombianas.

Además, se deben establecer controles de acceso rápido y seguro, como, por ejemplo, la identificación biométrica, la identificación electrónica por medio de los códigos de barras de los carnets. Si en el caso de que algunas empresas no tengan los recursos necesarios para establecer estos controles, se deben realizar controles con los guardas de seguridad, que llenen una planilla, y desde luego tener unos datos de los trabajadores de estas empresas, para poder confirmar los datos.

Es importante para las empresas colombianas contar con un departamento de seguridad de la información, puesto que de acuerdo con las estadísticas actualmente son un blanco fácil para los ciberdelicuentes.

Además, se busca la forma de cómo evitar que las diferentes redes inalámbricas de las diferentes empresas colombianas se saturen y se vuelvan focos de inseguridad, el cual pueden poner en riesgo tanto en la parte de los usuarios, como también a la información y los activos tecnológicos de las empresas y organizaciones. Para este caso, es recomendable realizar un proyecto que actualice los dispositivos inalámbricos (AP’s y los routers), y que, además, genere redes inalámbricas que cuenten con las medidas básicas.

Otra recomendación, es el de administrar de manera correcta todos los usuarios con privilegios correspondientes por medio del director de sistemas de las empresas colombianas.

También, se debe tener en cuenta de que se debe tener una estructura básica, pero a la vez vigilada en la parte de los puntos de red del cableado dentro de la empresa.

Es recomendable que en la parte del reciclaje de los documentos que ya no son utilizados en la parte de los procesos administrativos de las diferentes empresas, deben ser destruidos, para que otras personas no puedan ver la información de estos documentos dentro y fuera de la empresa.

Implementar un control eficiente, con el objetivo de evitar que los usuarios de la red de la empresa puedan compartir los recursos a través de esta misma. Y, por último, realizar copias de seguridad de manera periódica, como en los sistemas operativos y en las bases de datos., el cual se hace significativo que se concientice a los usuarios para que se limiten a tener en sus computadoras solo la información relacionada con sus actividades laborales, y evitar el almacenamiento de información personal en los equipos de cómputo de las empresas.

CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
ANTEPROYECTO												
Portada	X											
Resumen	X	X	X	X								
Introducción	X	X										
Marco teórico	X	X	X	X	X							
Desarrollo investigación	X	X	X	X	X	X	X	X	X	X	X	X
Conclusiones											X	X
Bibliografía				X	X	X	X	X	X	X	X	X
Selección y delimitación del tema	X	X										
Formulación del tema de investigación	X	X	X	X								
Planificación de las actividades	X	X	X									
Identificación de fuentes	X	X	X	X	X							
PROYECTO												
Plan de trabajo						X	X	X	X	X	X	X
Recopilación de información						X	X	X	X	X	X	X
Organización información recopilada										X	X	X
Resultados obtenidos											X	X
Redacción Informe												X

BIBLIOGRAFIA

ADT. Always there. Consejos para proteger la empresa frente a los hackers informáticos. {En Línea}. {13 de noviembre de 2018}. Disponible en: https://www.adt.co.cr/corporativo/centro-de-recursos-corporativo/seguridad-en-corporativos/consejos-para-proteger-la-empresa-frente-a-los-hackers-informaticos

Anonimato. INGENIERÍA SOCIAL: HACKING PSICOLÓGICO. República dominicana. {En Línea}. {26 de octubre de 2018} Disponible en: https://www.owasp.org/images/**2**/27/02_**INGENIERÍA_SOCIAL**.pdf

Anonimato. Capitulo II. Seguridad Informática. {En Línea}. {10 de noviembre de 2018}. Disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf

Anonimato. La ingeniería social: explotando a los humanos, Monografía**,** @nms_george,. {En Línea}. {26 de octubre de 2018}. Disponible en: http://premios.eset-la.com/universitario/pdf/scam_box.pdf

Bajo, J. B. Phishing y otros delitos informáticos: el uso ilícito de Internet. Lex nova: La revista, (53), 6-10. (oct. - nov. 2018); p. (6-10).

Borghello Cristian. El arma infalible: la Ingeniería Social, Technical & Educational Manager de ESET para Latinoamérica. {En línea}. {27 de octubre de 2018} Disponible en: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

El TecnólogoEM. (2018). Tres técnicas de Phishing a tener en cuenta. {En Línea}. {16 de noviembre de 2018}. Disponible en: https://eliezermolina.net/3-tecnicas-de-phishing-a-tener-en-cuenta/

Iglesias F. Pablo. (2015). 5 Tipologías de Phishing que deberías conocer. Consultor de Presencia Digital y Reputación Online. {En Línea}. {07 de noviembre de 2018}. Disponible en: https://www.pabloyglesias.com/5-tipologias-de-phishing/

Inma. (2016). Esendex. Protege a tu empresa de los ataques de Phishing. {En Línea}. {15 de noviembre de 2018}. https://www.esendex.es/blog/post/protege-a-tu-empresa-de-los-ataques-de-phishing/

Jiménez Javier (2018). Así están evolucionando los ataques de phishing para tener un mayor éxito. {En Línea}. {07 de noviembre de 2018} Disponible en: https://www.redeszone.net/2018/09/13/asi-evolucionando-ataques-phishing-exito/

Las Pymes como blanco para los ciberdelincuentes. En: El espectador. Bogotá: (09 diciembre de 2018), p.3c.

Levinec. Olprod. Microsoft. Windows IT Pro Center. Suplantación de identidad (Phishing). {En Línea}. {12 de noviembre de 2018} disponible en: https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/phishing

Llinares, F. M. La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. Revista electrónica de ciencia penal y criminología, (15), 12. (oct. – nov. 2018); p. (15-22).

Maestre Merino Manuel Carlos. Asociación Nacional de afectados del Phishing en España. {En línea}. {22 de octubre de 2018} España: Asociación Nacional de Afectaos. disponible en: http://www.asociacionafectadosinternet.es/phishing-bancario/

Microsoft. A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs *Microsoft Knowledgebase Database*. 28 de agosto de 2005

Norton Secured – power by Syamatec. Últimas tácticas de phishing y sus posibles consecuencias para las empresas, libro blanco. {En Línea}. {01 de noviembre de 2018}. Disponible en: http://docs.media.bitpipe.com/io_11x/io_117740/item_972566/phishing-tactics-es_W_newseal.pdf

Oxman Nicolás. Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming" noviembre 2013 Chile-Revista de Derecho (Valparaíso). {En Línea}.{23 de octubre de 2018} Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007

Pagnotta Sabrina. Las 5 historias de Ingeniería Social más ridículas del último tiempo. {En Línea}. {30 de octubre de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/

Panda – Mediacenter. (febrero, 2018).10 Consejos para evitar ataques de Phishing. {En Línea}. {14 de noviembre de 2018}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

PANDINI William. ¿Cómo protegerse de los ataques de Phishing? {En Línea}. {14 de noviembre de 2018}. Disponible en: https://ostec.blog/es/generico/protegerse-ataques-phishing

Prieto Álvarez, Víctor Manuel. Ramón Adrián Pan Concheiro. (2007). Virus Informáticos. Máster en Informática. {En Línea}. {11 de noviembre de 2018}. Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Rodríguez Pablo. (2018). Las 10 mejores herramientas de Kali Linux para Hackers éticos. {En Línea}. {12 de noviembre de 2018}. Disponible en: https://blog.ehcgroup.io/index.php/2018/04/05/las-10-mejores-herramientas-de-kali-linux-para-hackers-eticos/

Rodríguez Puentes, M. Responsabilidad Bancaria frente al Phishing (Doctoral dissertation, Universidad Nacional de Colombia-Sede Bogotá). {En Línea}. {03 de noviembre de 2018} Colombia. Disponible en: http://bdigital.unal.edu.co/53188/1/marcosrodriguezpuentes.2015.pdf

Salazar Aristizábal, N. A., & González Arango, M. Phishing: la automatización de la ingeniería social (Bachelor's thesis, Universidad EAFIT). {En Línea}. {02 de noviembre de 2018}. Disponible en: http://repository.eafit.edu.co/handle/10784/2443

Sergio de Luz. Los ataques sin Marware por correo electrónico aumentan en el último semestre. {En Línea}. {08 de noviembre de 2018} Disponible en: https://www.redeszone.net/2018/09/16/ataques-sin-malware-correo-electronico-aumentan-ultimo-semestre/

Sergio R Solis, Piggyback o el acceso por exceso de confianza. {En Línea}. {09 de noviembre de 2019}. Disponible en: https://www.video2brain.com/mx/tutorial/piggyback-o-el-acceso-por-exceso-de-confianza

Valencia Rodríguez, J. A. Análisis de un modelo para identificar alertas tempranas ante ataques de Phishing. Colombia. {En Línea}. {02 de noviembre de 2018}. Disponible en: https://repositorio.escuelaing.edu.co/handle/001/526

Verónica Becerra, Ingeniería Social, las técnicas con las que engañan a tu mente, {En Línea}. {10 de noviembre de 2018}. Disponible en: https://infosecuritymexicoblog.com/2017/05/08/ingenieria-social-las-tecnicas-con-las-que-enganan-a-tu-mente/

Yuly, P. P. IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA {03 de noviembre de 2018}.

Zabala, J. A. Responsabilidad Bancaria Frente al Delito de Phishing en Colombia.

[En Línea] Colombia. {En Línea}. {04 de noviembre de 2018}. Disponible en: http://repository.ucatolica.edu.co/handle/10983/14943

RESUMEN ANALITICO EDUCATIVO
RAE

Título del Proyecto	Ingeniera social: Técnicas de ataque phishing y su impacto en las empresas colombianas
Tipo de documento	Monografía Seguridad Informática
Nombres y Apellidos del Autor	Jenny Paola Giraldo Martínez e Iván Guillermo Duarte Pacheco
Año de la publicación	
Director	Juan José Cruz
Palabras Claves	Ingeniería social, phishing, malware, seguridad, protección, niveles de seguridad, ataque informático, IP Spoofing, DNS, SMTP, Amenaza, Antivirus, Contraseña, Exploit, Firewall, Hacker,
Descripción	

En este documento encontrara, información acerca de temas importantes actualmente en la ciberseguridad como lo es la ingeniería social y el phishing y la forma en que afectan a las empresas, podrán visualizar las estadísticas actuales, las cuales están muy elevadas en cuanto a este tipo de delitos.

Un factor muy importante y que las empresas deben tener en cuenta es que el usuario es el eslabón más débil de la cadena y que es allí donde debemos enfocar nuestra atención como profesionales en la seguridad de la información, puesto que la desinformación es una de las mayores causantes para caer en este tipo de delitos.

Se espera que esta monografía sirva de soporte para darle claridad a las falencias en las empresas colombianas en la parte de los ataques de Phishing, utilizados en la ingeniería social, para obtener las diferentes vulnerabilidades que hay y cómo generar una solución adecuada de acuerdo a los protocolos de seguridad establecidos., en el que se identificará ciertas características de este tipo de ataque “Phishing”, de cómo caer en la trampa de estos ciberdelicuentes, y de esta manera lograr una reevaluación en la parte de la seguridad informáticas en las empresas colombianas, teniendo en cuenta los diferentes casos sucedidos a nivel nacional. Además, también le puede suceder a una persona natural que lo puedan hackear, dependiendo del interés del atacante.

Fuentes

ADT. Always there. Consejos para proteger la empresa frente a los hackers informáticos. {En Línea}. {13 de noviembre de 2018}. Disponible en: https://www.adt.co.cr/corporativo/centro-de-recursos-corporativo/seguridad-en-corporativos/consejos-para-proteger-la-empresa-frente-a-los-hackers-informaticos

Anonimato. INGENIERÍA SOCIAL: HACKING PSICOLÓGICO. República dominicana. {En Línea}. {26 de octubre de 2018} Disponible en: https://www.owasp.org/images/**2**/27/02_**INGENIERÍA_SOCIAL**.pdf

Anonimato. Capitulo II. Seguridad Informática. {En Línea}. {10 de noviembre de 2018}. Disponible en: http://repositorio.utc.edu.ec/bitstream/27000/635/2/T-UTC-1089%282%29.pdf

Anonimato. La ingeniería social: explotando a los humanos, Monografía**,** @nms_george,. {En Línea}. {26 de octubre de 2018}. Disponible en: http://premios.eset-la.com/universitario/pdf/scam_box.pdf

Bajo, J. B. Phishing y otros delitos informáticos: el uso ilícito de Internet. Lex nova: La revista, (53), 6-10. (oct. - nov. 2018); p. (6-10).

Borghello Cristian. El arma infalible: la Ingeniería Social, Technical & Educational Manager de ESET para Latinoamérica. {En línea}. {27 de octubre de 2018} Disponible en: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

El TecnólogoEM. (2018). Tres técnicas de Phishing a tener en cuenta. {En Línea}. {16 de noviembre de 2018}. Disponible en: https://eliezermolina.net/3-tecnicas-de-phishing-a-tener-en-cuenta/

Iglesias F. Pablo. (2015). 5 Tipologías de Phishing que deberías conocer. Consultor de Presencia Digital y Reputación Online. {En Línea}. {07 de noviembre de 2018}. Disponible en: https://www.pabloyglesias.com/5-tipologias-de-phishing/

Inma. (2016). Esendex. Protege a tu empresa de los ataques de Phishing. {En Línea}. {15 de noviembre de 2018}. https://www.esendex.es/blog/post/protege-a-tu-empresa-de-los-ataques-de-phishing/

Jiménez Javier (2018). Así están evolucionando los ataques de phishing para tener un mayor éxito. {En Línea}. {07 de noviembre de 2018} Disponible en:

https://www.redeszone.net/2018/09/13/asi-evolucionando-ataques-phishing-exito/

Las Pymes como blanco para los ciberdelincuentes. En: El espectador. Bogotá: (09 diciembre de 2018), p.3c.

Levinec. Olprod. Microsoft. Windows IT Pro Center. Suplantación de identidad (Phishing). {En Línea}. {12 de noviembre de 2018} disponible en: https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/phishing

Llinares, F. M. La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. Revista electrónica de ciencia penal y criminología, (15), 12. (oct. – nov. 2018); p. (15-22).

Maestre Merino Manuel Carlos. Asociación Nacional de afectados del Phishing en España. {En línea}. {22 de octubre de 2018} España: Asociación Nacional de Afectaos. disponible en: http://www.asociacionafectadosinternet.es/phishing-bancario/

Microsoft. A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs *Microsoft Knowledgebase Database*. 28 de agosto de 2005

Norton Secured – power by Syamatec. Últimas tácticas de phishing y sus posibles consecuencias para las empresas, libro blanco. {En Línea}. {01 de noviembre de 2018}. Disponible en: http://docs.media.bitpipe.com/io_11x/io_117740/item_972566/phishing-tactics-es_W_newseal.pdf

Oxman Nicolás. Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming" noviembre 2013 Chile-Revista de Derecho (Valparaíso). {En Línea}.{23 de octubre de 2018} Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007

Pagnotta Sabrina. Las 5 historias de Ingeniería Social más ridículas del último tiempo. {En Línea}. {30 de octubre de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/

Panda – Mediacenter. (febrero, 2018).10 Consejos para evitar ataques de Phishing. {En Línea}. {14 de noviembre de 2018}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

PANDINI William. ¿Cómo protegerse de los ataques de Phishing? {En Línea}. {14 de noviembre de 2018}. Disponible en: https://ostec.blog/es/generico/protegerse-ataques-phishing

Prieto Álvarez, Víctor Manuel. Ramón Adrián Pan Concheiro. (2007). Virus Informáticos. Máster en Informática. {En Línea}. {11 de noviembre de 2018}. Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Rodríguez Pablo. (2018). Las 10 mejores herramientas de Kali Linux para Hackers éticos. {En Línea}. {12 de noviembre de 2018}. Disponible en: https://blog.ehcgroup.io/index.php/2018/04/05/las-10-mejores-herramientas-de-kali-linux-para-hackers-eticos/

Rodríguez Puentes, M. Responsabilidad Bancaria frente al Phishing (Doctoral dissertation, Universidad Nacional de Colombia-Sede Bogotá). {En Línea}. {03 de noviembre de 2018} Colombia. Disponible en: http://bdigital.unal.edu.co/53188/1/marcosrodriguezpuentes.2015.pdf

Salazar Aristizábal, N. A., & González Arango, M. Phishing: la automatización de la ingeniería social (Bachelor's thesis, Universidad EAFIT). {En Línea}. {02 de noviembre de 2018}. Disponible en: http://repository.eafit.edu.co/handle/10784/2443

Sergio de Luz. Los ataques sin Marware por correo electrónico aumentan en el último semestre. {En Línea}. {08 de noviembre de 2018} Disponible en: https://www.redeszone.net/2018/09/16/ataques-sin-malware-correo-electronico-aumentan-ultimo-semestre/

Sergio R Solis, Piggyback o el acceso por exceso de confianza. {En Línea}. {09 de noviembre de 2019}. Disponible en: https://www.video2brain.com/mx/tutorial/piggyback-o-el-acceso-por-exceso-de-confianza

Valencia Rodríguez, J. A. Análisis de un modelo para identificar alertas tempranas ante ataques de Phishing. Colombia. {En Línea}. {02 de noviembre de 2018}. Disponible en: https://repositorio.escuelaing.edu.co/handle/001/526

Verónica Becerra, Ingeniería Social, las técnicas con las que engañan a tu mente, {En Línea}. {10 de noviembre de 2018}. Disponible en: https://infosecuritymexicoblog.com/2017/05/08/ingenieria-social-las-tecnicas-con-las-que-enganan-a-tu-mente/

Yuly, P. P. IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA {03 de noviembre de 2018}.

Zabala, J. A. Responsabilidad Bancaria Frente al Delito de Phishing en Colombia. [En Línea] Colombia. {En Línea}. {04 de noviembre de 2018}. Disponible en: http://repository.ucatolica.edu.co/handle/10983/14943

Contenidos

El presente documento de trabajo de grado contiene cuatro capítulos dentro de los cuales se desarrolla la explicación de la ingeniería social y como documento final encontraremos una guía donde recopila como nos podemos prevenir de los ataques de phishing dentro de las empresas.

CAPITULO I: CONCEPTOS BASICOS: se explica en detalle que es la ingeniería social, el phishing y los tipos de estos delitos que existen actualmente para que de esta forma el lector se encuentre actualizado en cuanto a estos términos.

CAPITULO II: TECNICAS DE ATAQUE: encontrara las técnicas que utilizan los ciberdelincuentes para atacar sus víctimas.

CAPITULO III: IDENTIFICACIÓN DE LAS HERRAMIENTAS Y LOS PROCESOS EN UN ATAQUE PHISHING: como su nombre lo indica muestra algunas de las herramientas utilizadas por los delincuentes para atacar sus víctimas.

CAPITULO IV: DOCUMENTO GUIA PARA PREVENIR EL PHISHING EN LAS EMPRESAS COLOMBIANAS: en este capitulo se resumen algunas formas de prevenir el phishing en las empresas tanto para usuarios como para el departamento de TI.

Metodología

Para esta monografía como opción de grado, se relacionaron con el tema principal

de ingeniería social y las diferentes técnicas de ataques de phishing, en el que se identifica una variedad de conceptos en el ámbito de la seguridad informática, como: Ingeniería social, phishing, malware, seguridad, protección, niveles de seguridad, ataque informático, IP Spoofing, DNS, SMTP, Amenaza, Antivirus, Contraseña, Exploit, Firewall, Hacker. Gracias a este trabajo, se pudo enmarcar dentro de una metodología exploratoria, el cual consiste en indagar acerca de un fenómeno poco conocido, es decir que hay poca información, con el fin de explorar la situación. El objetivo principal de este tipo de investigación es de identificar los diferentes aspectos para poder definir mejor algún evento o formular investigaciones en otros niveles de estudio. Además, está dirigido a un enfoque cuantitativo y cualitativo, en el que se determinaron las siguientes fases para lograr ese objetivo de la monografía:

Fase 1: contextualización de la propuesta: el cual se desarrolló esta propuesta (monografía) como opción de grado de la especialización en seguridad informática el primer semestre del presente año (2018), el cual nosotros como integrantes de esta monografía fue desarrollada para identificar los diferentes factores que se presentan en Colombia en la parte de la ingeniería social y las diferentes técnicas de ataques de phishing y sus métodos.

Fase 2: Diseño de la monografía: primero que todo el desarrollo de esta monografía fue el de enfocarnos en los diferentes casos que se han presentado en las empresas y organizaciones en Colombia, de cómo podemos evidenciar un ataque de ingeniería social, como es el desarrollo de este tipo de ataque, el cual está relacionado en la parte de la psicología, de las vulnerabilidades de las víctimas, de manejar correctamente el tema con la víctima, entre otros.

Fase 3: explicación de la metodología de la ingeniería social: en esta fase es donde se explica la metodología que utilizan los ingenieros sociales, los cuales son: fase de acercamiento, fase de alerta y fase de distracción, pero desde luego se identifica los aspectos claves de la ingeniería social, los tipos de ingeniería social, y en la parte de phishing, como los tipos de phishing, tipos de ataques relacionados con el phishing, entre otros.

Fase 4: explicación de las técnicas de ataques: en esta fase es donde se identifica y se explica las técnicas de ataques de phishing.

Fase 5: identificación de las herramientas y sus procesos: en esta parte es donde realiza la identificación de las herramientas que se utilizan en la ingeniera social y el phishing. Y desde luego el desarrollo del documento guía para poder prevenir el phishing en las empresas colombianas.

Conclusiones

- Al realizar el estudio teórico acerca de los ataques de ingeniería social que se han dado en los últimos años en las diferentes empresas colombianas, se pudo observar y visibilizar que existen muchas falencias en las diferentes empresas que hay en Colombia frente al tema de la seguridad informática y de la información, el cual suelen escatimar en los diferentes gastos y la ausencia de ciertas actualizaciones en la parte de la seguridad en las empresas. De esta forma se logra establecer que el personal de una empresa colombiana es uno de los eslabones más débiles que hay a la hora de ejecutar un ataque de ingeniería social, por medio de algunas técnicas y metodologías, en el que se realiza como la suplantación de identidad por medio de llamadas telefónicas, también en la parte del espionaje, lo que es el espionaje por encima del hombro, el de observar las rutinas de las personas, sus gustos, entre otras.

- De acuerdo a las cifras publicadas por el CaiVirtual se ha visto un alto incremento en el robo de información mediante la técnica de ataque phishing, pudimos corroborar que casi el 80% de la protección de la información está en la capacitación de los usuarios, ya que como nos dimos cuenta a lo largo de esta monografía son el eslabón más débil.

- La ingeniería social tiene como objetivo el de obtener la información de terceros, sin que las víctimas se den cuenta, de una forma no convencional para poder obtener la información deseada de una manera más eficaz y algo complicado, pero más seguro. En estos ataques suelen de realizarlos algunos grupos de hackers de sombrero negro, espías, ciberdelicuente, entre otros.

- Por medio de este documento dimos a conocer las diferentes técnicas de ataque phishing que existen actualmente y de cómo realizar un ataque con ingeniería social, identificando quienes son los más vulnerables a estos tipos de ataques, como también quienes son los que ejecutan los diferentes métodos de ingeniería social para poder lograr identificar las diferentes vulnerabilidades en una empresa, específicamente en las empresas colombianas, como también en identificar y describir cuales son los objetivos de los ingenieros sociales, sus métodos, y de cómo ganarse la confianza de sus víctimas, ya que no solo mediante el correo electrónico podemos suministrar información valiosa de las empresas, si no directamente con las víctimas.

- En Colombia, la mayoría de las empresas que han sufrido estos tipos de ataques (ingeniería social) en los últimos años, son aquellas en las que pertenecen a las entidades bancarias, el cual tienen muchos seguidores por la parte del manejo de recursos económicos que se dan en estas mismas entidades. Además, los ciberdelicuente utilizan el método de phishing para el robo de información confidencial de estas empresas, el cual este método consiste en enviar correo electrónicos falsos a las diferentes cuentas de las posibles víctimas, en el que se les solicita a los usuarios en registrarse en esa página por un cambio en la base de datos de la entidad o que su clave debe ser cambiada, ya que lleva mucho tiempo el de no cambiarla, entre otras, para poder obtener los datos que ellos quieren.

- En las empresas colombianas deben de implementar un CCTV propio y que adicionalmente de contar con el CCTV de una empresa de vigilancia, ya que debe estar monitorizado todos los puntos de la empresa.

Nombre y apellidos de quien elaboró este RAE	Jenny Paola Giraldo Martínez e Iván Guillermo Duarte Pacheco
Fecha en que se elaboró este RAE	7 de diciembre de 2018

Revisado por: