CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS).

Monsalve, Jaime.
jaime_monsalve03@hotmail.com.
Universidad Piloto de Colombia.

***Resumen*—**El objetivo del presente artículo es presentar la actualidad de las amenazas y ciberataques al que se expone el recurso humano en la red de cualquier empresa en Colombia. Se tratarán las amenazas más reconocidas y como estas se pueden aprovechar hoy en día del recurso humano, el cual es el eslabón más débil de cualquier empresa ya sea grande, mediana o pequeña y de su respectiva información. También este articulo informa sobre como los continuos avances tecnológicos traen nuevos riesgos de seguridad y por lo tanto el recurso humano no tiene el entrenamiento justo y necesario para identificar estos tipos de ataques y sus consecuencias al ser perpetuado en las redes de estas empresas. Se plasmará también el cómo evitar estos ataques cibernéticos brindando una concienciación para prevenir los mismos. Generando una cultura de ciberseguridad para la protección de datos y el cuidado de la imagen de cualquier empresa.

***Abstract*—**The objective of this article is to present the current threats and cyber-attacks that expose human resources in the network of any company in Colombia. It will be the most recognized threats and how they can be used today by the human resource, which is the weakest link in any company, whether large, medium or small, and their respective information. This article also informs about how the continuous technological advances bring new security risks and therefore the human resource does not have the right and necessary training to identify these types of attacks and their consequences when perpetuated in the networks of these companies. It will also reflect how to avoid these cyber-attacks by providing an awareness to prevent them. Generating a culture of cybersecurity for the protection of data and the care of the image of any company.

***Índice de Términos*—**Ciberataques, ciberseguridad, malware, phishing.

I. Introducción

En la actualidad existe una guerra denominada guerra cibernética la cual se enfoca y está dirigida a los sistemas informáticos donde la información juega un rol importante y se puede tomar como el activo más importante para cualquier entidad; una vez esta sea robada o se vulnere se puede decir que los pilares de la seguridad informática como la confidencialidad, integridad y disponibilidad de esta fue alterada. El mundo hoy en día se enfrenta a constantes ciberataques los cuales no son visibles en su acción, pero sus consecuencias son catastróficas. Con el avance de la tecnología, lo cual es con pasos agigantados, la manera de pensar y actuar ha cambiado significativamente permitiendo así la manipulación correcta o incorrecta del tráfico de datos o de la información. La tecnología y la información hacen que día a día el mundo esté conectado y se pueda compartir información sensible tal como información bancaria, historial clínico, datos personales etc. El valor comercial de la información no tiene precedente para los ciberdelincuentes (personas con conocimiento suficiente para vulnerar cualquier sistema de información) y es vendida en un mercado por un valor infravalorado a personas con pretensiones de extorsionar o perpetuar ciberataques con fines lucrativos.

Así que este artículo describe las principales amenazas y ciberataques a los que la población está expuesta sin importar la labor, también sobre los efectos que pueden generar si no se mantiene cuidado sobre estos y cómo se pueden seguir algunas recomendaciones para no caer frente a los ciberdelincuentes que acechan en todo momento de los 365 del año y en cualquier lugar del planeta.

II. Ciberseguridad

En el transcurso de la historia de la ciberseguridad, el factor humano siempre ha estado ligado de una manera u otra con la evolución de esta. Desde la antigüedad el hombre ha enfrentado un mundo de supervivencia lo cual lo ha obligado a crear estrategias que le permitan continuar con su ciclo de vida. Como efecto de estas adversidades se procedió a generar herramientas de protección ante los peligros que le acechaban; en primera instancia peligros tales como: fuego, inundaciones, ataques de otras tribus, ataques de animales etc. Ante la necesidad se crearon herramientas o armas para protegerse desarrolladas con materia prima natural tales como: maderas, plantas, piedras etc. De forma natural el hombre estaba desarrollando la primera seguridad: la física.

La preocupación que conlleva a preservar la vida se convirtió en una necesidad obligatoria para salvaguardar la especie y evitar su extinción. Es desde entonces que el ser humano se ha

enfrentado a toda clase de amenazas durante su largo camino en busca de la seguridad. Hoy en día, el objetivo de la seguridad ha evolucionado, dejando atrás el único objetivo de preservar la especie humana, mostrando otros tipos de seguridad, tales como: seguridad física, seguridad económica, seguridad laboral, seguridad social etc. La ciberseguridad hoy en día juega un papel muy importante con lo que es el riesgo, amenaza y vulnerabilidad, estos términos se pueden considerar como una ecuación que tiene relación entre sí, donde la vulnerabilidad es toda aquella debilidad de un sistema informático y una amenaza puede explotar fácil o difícilmente, es decir, la amenaza toma ventaja de esta vulnerabilidad y lo materializa en un riesgo cibernético.

Es por eso que la ciberseguridad es el grupo de servicios, mecanismos y políticas que aseguran que la forma operativa de un sistema puede ser segura. La ciberseguridad se encarga de asegurar datos, información, transacciones, procesos, productividad, software y reputación al momento de navegar en el ciberespacio. Su principal objetivo global es proteger de todo tipo de ciberataques, accesos no autorizados y de robos en todos los dispositivos que en si posean información. A continuación se da a conocer cada una de las etapas del proceso de la ciberseguridad y cuál es su importancia.

Prevención: En esta fase, es importante que los usuarios o empresas estén informados de la evolución de las amenazas, de las posibles estafas y de qué soluciones existen contra ellas. Se recomienda que las personas tengan conocimientos básicos sobre ciberseguridad para que puedan utilizar de manera prudente, eficaz y eficiente, todos los medios a nuestro alcance. Por otro lado, es necesario conocer el funcionamiento de las herramientas o productos de seguridad, sus características y su forma de actuar para sacarle el mayor provecho y conseguir la protección más efectiva.

También, es necesaria la protección física de las instalaciones para garantizar que nadie sin autorización pueda manipular los terminales, los accesos a la red o conectar dispositivos no autorizados.

Detección: En la detección, puede ocurrir que mientras se está produciendo el ataque o pasado un tiempo de su acción, la detección del malware que parte de un antivirus, comienza actuar protegiéndose de la amenaza. Si por el contrario, se da la segunda circunstancia, los problemas son mayores porque los hackers han podido actuar libremente durante un largo período de tiempo. Se estima que el período medio entre el momento en que se produce una brecha de seguridad y su detección es de 205 días, dato que se logrò obtener en el año 2014 de acuerdo a los estudios de ataques que se producieron a lo largo del año. Los dos aspectos más importantes a la hora de actuar en la detección de amenazas y ciberataques son la gestión de vulnerabilidades y la monitorización continua. Gracias a las herramientas de ciberseguridad existentes en la actualidad, los usuarios pueden detectar patrones de ataque de forma eficaz y hacerles un constante seguimiento.

Reacción o respuesta en la ciberseguridad: Si se produjo un ataque y los equipos o sistemas se han visto infectados, es importante actuar en varios campos. Por un lado, dar una respuesta técnica y sì finalmente se ha producido un robo de identidad o robo de datos, acudir a las fuerzas y cuerpos de seguridad del Estado e iniciar acciones legales para que los delitos que se hayan podido cometer no queden impunes. Para dar una respuesta técnica es primordial seguir cinco pasos con los que se podrá prevenir un robo de datos o acotar el impacto negativo del ataque: desconectar el equipo de internet, instalar un programa antivirus si no se tiene, realizar un análisis completo del sistema, modificar las contraseñas y hacer una limpieza manual. Es importante que toda organización tome medidas preventivas de su infraestructura computacional, al ser la información uno de sus activos empresariales principales, y porque será el obstáculo para ataques cibernéticos y cibercriminales.

Figura 1. Servicios de Ciberseguridad. Recuperado de: https://www.gmv.com/es/Sectores/Seguridad/

III. Ciberespacio

El ciberespacio constituye un escenario táctico, estratégico y operativo diferente de los espacios terrestre, marítimo, aéreo y exterior, que ha sido abarcado por lo diferentes expertos de ciberseguridad. El ciberespacio lo conforman todas las redes informáticas del mundo, todo lo que ellas conectan y controlan. No se trata solo de internet. Es importante dejar en claro la diferencia; Internet es una red abierta. Desde cualquier red de internet, podemos comunicarnos con cualquier ordenador que se encuentre conectado a una red diferente a la nuestra. El ciberespacio es la herramienta que nos permite transportar la información en la red, de manera segura y práctica, por ejemplo “la nube”. Algunas de esas redes privadas son muy semejantes a internet, pero, al menos teóricamente, se encuentran separadas de ella. Basado en lo anterior se puede decir que en el ciberespacio se realizan la mayoría de las actividades cibernéticas donde cualquier ser humano puede llevar acabo y que toda su información está expuesta allí para futuras transacciones u operaciones concurrentes. Internet sería entonces el canal de comunicación en el ciberespacio. Surge entonces la pregunta ¿Qué tan dependientes son las personas del ciberespacio hoy en día? La dependencia al ciberespacio ha sido orquestada a partir de la tecnificación de los Sistemas de Información y Comunicaciones (TIC), una vez la información se digitaliza, los niveles de vulnerabilidad en la red se hacen mayores, quedando a merced de quien tenga la capacidad de ingresar en

los sistemas internos y adquirir la información que desee. Como se sabe quien posee la información posee el poder.
Las personas pueden brindar su información en el momento en que realizan una transferencia bancaria a través de internet, o solicitar documentos importantes a través de la red, obviamente las empresas y toda entidad que maneje información digitalizada debería tener ciertos protocolos para la seguridad de la información de sus clientes y usuarios en general.

IV. Ingeniería Social

La ingeniería social es una técnica de fraude para la obtención de información confidencial, acceso o privilegios en sistemas de información, a través de la manipulación de usuarios legítimos. La ingeniería social se basa en el principio 'los usuarios son el eslabón más débil' y aprovechan la tendencia natural de la gente a confiar y a reaccionar de manera predecible ante ciertas situaciones - por ejemplo, proporcionando detalles financieros a un aparente funcionario de un banco o un supuesto compañero de trabajo. Así bien, los delincuentes se aprovechan del miedo, la compasión, la felicidad, la euforia y cualquier otra sensación o sentimiento que sea capaz de generar reacciones en las personas y termine por vulnerar su seguridad. Se maniobra psicológicamente a las personas para que estas mismas de manera inconsciente o inocente compartan información confidencial o hagan acciones inseguras para exponer cualquier organización o compañía al daño de imagen. La mayoría de las veces, los ataques se realizan por medio de correo electrónico o por teléfono para obtener información, realizar fraudes u obtener acceso ilegítimo a los equipos de las víctimas. Los ataques de ingeniería social comunes incluyen correos electrónicos de phishing, vishing (llamadas telefónicas de personas que se hacen pasar por una organización respetada) y baiting (del inglés "carnada", donde el atacante carga unidades de USB con malware y luego simplemente espera que el usuario las conecte a su máquina). Como es un tema más humano, las herramientas tecnológicas que implementan las compañías no pueden prevenir los ataques. Por eso, los atacantes recurren a este tipo de tácticas para vulnerar sistemas muy seguros y complejos. La ingeniería social también se extiende a las búsquedas de empresas y de amigos en LinkedIn y Facebook respectivamente o redes sociales en general, donde los criminales utilizan estas redes sociales para generar confianza y obtener datos. Con bastante frecuencia, el resultado final es la extorsión o el robo.

Figura 2. Proceso ingeniería social. Recuperado de: https://www.isecauditors.com/test-de-ingenieria-social

Internet y las redes sociales están creciendo exponencialmente cada día exponiendo información de los usuarios y las cuales estas herramientas no son conscientes de las posibles amenazas y riesgos que corren cuando realizan algún tipo de publicación, de información personal o de interés público. Los ciberdelincuentes aprovechan esas vulnerabilidades o publicaciones y manipulan a las personas que se convierten en víctimas, ya que, con base en la información recolectada en la red y engaños, pueden llegar a obtener información confidencial utilizándola luego en su contra para realizar algún tipo de cibercrimen. Los principales aspectos de la seguridad informática con relación a la ingeniería social son:

Es física y digital: La Ingeniería Social es una antigua estafa que se manifiesta en todos los ámbitos de la vida, por lo que sería un error pensar que se trata de algo nuevo o que solo se ve en el mundo online.
Su calidad es muy variable: La calidad de las estafas varía ampliamente. Por cada ingeniero social sofisticado que envía correos electrónicos de phishing iguales a los auténticos o que hace llamadas de vishing, habrá muchos otros que hablan mal el idioma, que tienen argumentos sin lógica e información confusa.
Es probable que no se percate del ataque: Lo más preocupante acerca de los ataques de este tipo es que no hay una advertencia inmediata, no hay ninguna señal clara de que se están atacando o de que tu equipo fue infectado. No aparece ninguna ventana emergente pidiendo bitcoins (como con CryptoLocker y otros tipos de ransomware), ni un anuncio de scareware que intenta convencerte para que descargues una aplicación o para que llames a un centro de servicio técnico.
Se enfoca principalmente en las empresas: La ingeniería social afecta a todos, pero los estafadores la utilizan cada vez más para atacar las grandes corporaciones y las PyME.

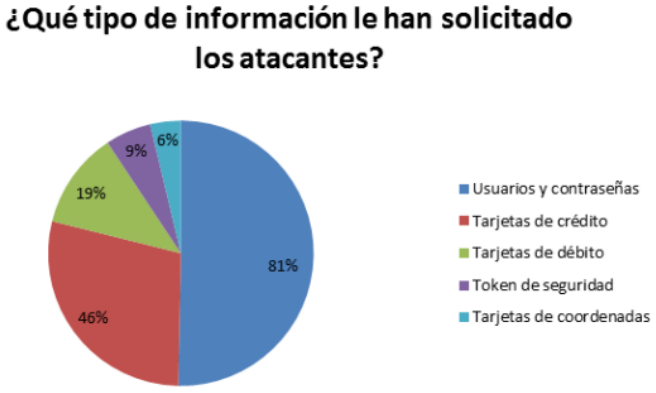

Figura 3. Información solicitada por atacantes. Recuperado de https://www.welivesecurity.com

V. Phishing

La función principal del ataque phishing consiste en el envío masivo de correos electrónicos a una empresa o entidad que, aparentando provenir de fuentes fiables (lo más común es fuentes falsas de entidades bancarias), intentan obtener datos

confidenciales del usuario o víctima, que posteriormente son utilizados para la realización de algún tipo de fraude como del beneficio propio o la venta de datos o información robada a la deep web. Para ello, suelen incluir un enlace que, al ser pulsado o hacer clic, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

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.

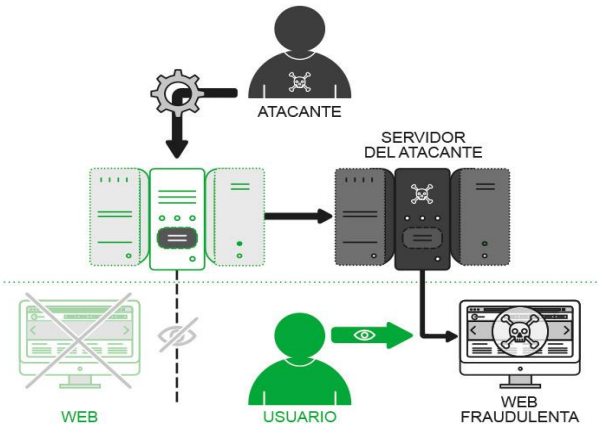

Figura 4. Simulación Phishing. Recuperado de https://es.godaddy.com/blog/que-es-el-phishing-y-que-tipos-existen/

VI. Qué tipo de información roba el phishing.

Datos personales o corporativos: los cuales se aprovechan de dirección de correo electrónico, números de documentos identificación y datos de localización y contacto.

Credenciales de acceso: Tales como redes sociales y cuentas de correo.

Información financiera: Números de tarjetas de crédito, números de cuentas bancarias e información de comercio electrónico.

VII. Tipos de phishing.

Spear Phishing: Una forma puntual de phishing cuyo objetivo es un grupo específico de individuos o una organización. Esta clase tiene como principal diferencia que está dirigido a personas o grupos reducidos. De esta manera las campañas son mucho más personificadas y con un porcentaje mayor de víctimas.

Raramente se ven casos que afecten entidades bancarias o redes sociales, debido a que no buscan la masividad sino todo lo contrario; en realidad, este tipo de métodos es utilizado en ataques como los APTs, apuntando a empleados de empresas con perfiles determinados. Esto significa que las víctimas podrían recibir correos personificados con nombre y apellido, incluso falsificando direcciones conocidas para generar una mayor empatía y confianza de un navegante incauto. Se debe tener en cuenta que si los ciberdelincuentes quisieran adentrarse en los sistemas buscarían el eslabón más débil dentro de la red. De este modo, no debemos esperar que el Gerente de Sistemas sea el blanco principal de este tipo de ataque, sino alguien con menos conocimientos técnicos de informática, como en muchos casos es alguien de áreas no relacionadas (por ejemplo, administración o recursos humanos). Esta metodología, en conjunto con Ingeniería Social y un estudio previo de las víctimas, da como resultado una sólida técnica con la que muy fácilmente se podría comprometer un sistema o red corporativa bajo el robo de credenciales. Por tal motivo, resulta fundamental una vez más la concientización y capacitación de los empleados en buenas prácticas de Seguridad de la Información.

Whaling: Apunta a niveles ejecutivos, empresariales o grandes peces. Los objetivos del "cyberwhaling" son en su mayoría ejecutivos, de preferencia los de más alto nivel, como CEOs, CFOs, y otros puestos que involucren tomas de decisión de alto nivel, gente responsable de manejar las finanzas y la información de las corporaciones. Las oportunidades de que caigan en un phishing de spam no son muchas, y en la mayoría de los casos caen con algo "especial".

Cloning: Este tipo de ataque utiliza la suplantación de identidad de un correo electrónico legítimo, y entregado previamente al buzón del usuario, de esa manera utilizarlos para crear un correo electrónico casi idéntico o clonado. El archivo adjunto o el enlace dentro del correo electrónico malicioso se reemplaza con una versión maliciosa y luego se envía desde una dirección de correo electrónico falsificada para que parezca que proviene del remitente original. Puede afirmar que se trata de un reenvío del original o una versión actualizada del original.

Phishing con geolocalización: Esta técnica es utilizada para permitir o denegar el acceso al sitio web falso de los usuarios de determinado país, por medio de la dirección IP o un servidor proxy. Cualquier acceso que se haga desde otra parte del mundo no autorizada, no podrá acceder a la página del phishing. El objetivo es hacer más eficaces estos ataques, teniendo más probabilidad de llegar a víctimas y países específicos, a fin de evitar ser reportados como sitios web maliciosos.

El flujo de actividad del phishing se puede mostrar de la siguiente manera:

- Falsificación de un ente de confianza.
- Envío de mensajes por algún medio de propagación.
- Un porcentaje de usuarios confían en el mensaje y hacen clic.
- Los usuarios acceden a un sitio web falso e ingresan sus datos personales.

Las consecuencias que puede llevar a cabo lo anteriormente descrito son:

Robo de cuentas bancarias, uso indebido de tarjetas bancarias o información bancario, estafas, venta de datos personales en

el mercado negro (Deep Web.), suplantación de identidad, envío masivo de publicidad.

El año anterior (2017) los ataques de phishing se perpetuaron cada vez más en la región, donde Colombia se vio afectada con un 12,6%.

Comparándolo con otros países de la región, Colombia ocupa el puesto 12, donde se ve reflejado una mejoría, lo cual no indica o quiere decir que se deba bajar la guardia frente a esta amenaza, antes esto ayuda a combatirla con más fuerza por medio de diferentes métodos de ciberseguridad como lo es la concienciación y el entrenamiento de esta misma.

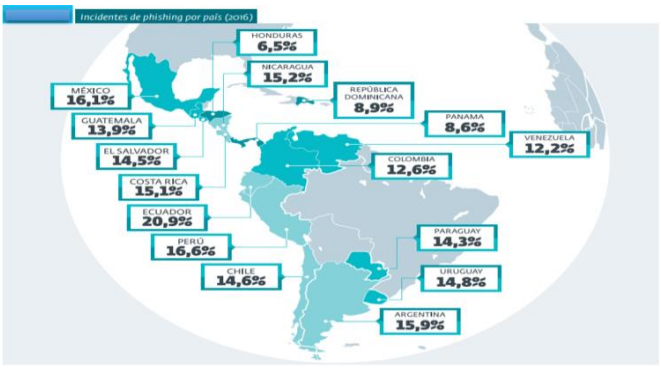

Figura 5. Incidentes de Phishing por país. Recuperado de https://www.eset.com/co/

Es evidente que este ataque cibernético cada vez más va aumentando y hay compañías que no ven esta amenaza como algo palpable o como algo que nunca les va a ocurrir. No toman medidas al respecto y la información que es crucial o confidencial para la empresa se está filtrando de manera sigilosa sin que los mecanismos de ciberseguridad (si los hay) los detecte. Cabe resaltar que lo mejor para este ataque de phishing es entrenar a los usuarios con campañas de concienciación y entrenamiento para incrementar el conocimiento de ciberseguridad en el recurso humano.

Un ataque phishing puede llegar a dañar la imagen de cualquier empresa ya que, si este ataque ha sido perpetuado, el robo de información puede generar perdidas económicas, es por eso por lo que a continuación en la siguiente grafica se presenta las ganancias de un atacante o pisher que puede llegar a alcanzar en el peor de los casos.

Figura 6. Efectividad de un ataque phishing. Recuperado de http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/3207-recomendaciones-para-evitar-el-phishing

Estudios realizados por la página web infospyware indica que en el peor de los casos un atacante puede llegar a ganar 10.000 USD de la siguiente manera:

- El adversario o pisher envía en un solo ataque 1’000.000 de correos maliciosos.
- De ese 1’000.000 de correos maliciosos, 5.000 correos fueron accionados o hicieron clic los usuarios.
- De esos 5.000 correos maliciosos, 1.000 usuarios ingresaron sus datos en el correo malicioso.
- Ya una vez el usuario ingreso sus datos, se tiene 10 USD por usuario comprometido.
- Por lo que se puede deducir claramente que, El atacante tiene 10.000 USD de ganancia por este ataque.

Solo se contempla el escenario que el atacante envía esta cantidad de correo por día, pero estudios indican que los atacantes no descansan y envían por hora más de 5’000.000 de correos.

Por lo anterior se puede deducir que las ganancias son exageradas y se debe aprender a disminuir estos ataques.

VIII. Tipos de Ataques Comunes de Phishing.

- *Verificación de cuenta:* Este ataque aparenta venir o llegar al buzón de entrada de una compañía reconocida o con buen nombre (ejemplo: Netflix) y pregunta en su contenido ingresar a la cuenta y corregir un inconveniente con su cuenta. Este link apunta a una página web de una compañía legitima. En este caso no se debe dar clic en el correo malicioso, se recomienda ir directamente a la página y validar que la cuenta este en perfecto estado sin ningún inconveniente como lo describía el correo malicioso.
- *Compartir archivos en la nube:* Este tipo de phishing contiene un link que aparenta estar un archivo compartido en Google Docs, Drive de Gmail, One Drive de Outlook, Dropbox etc. Al darse clic en este link redirecciona a una de estas páginas de donde está el documento compartido y requiere un log in en esta misma. Como medida cautelar se recomienda no dar clic en este link. En lugar de eso ingresar a estos sitios y validar si realmente se encuentra este archivo compartido. Recordar que se debe verificar el emisor del correo.
- *Docusign:* Este tipo de ataque trata de persuadir el dominio de la página oficial de docusign. Donde el link conlleva a iniciar sesión y poder ver un documento. Dando este acceso a los atacantes pueden controlar el buzón de entrada de la víctima como sus contactos.
  Recomendación es no dar clic en el link e ir directamente a la página oficial de docusign (www.docusign.com).
- *Factura Falsa:* Presenta un documento falso como una factura sin pagar y reclama a su víctima que se vencerá la factura si esta no es pagada prontamente. Las victimas más comunes en una empresa de este tipo de Phishing es la parte administrativa y financiera.
- *Notificación de entregas Online:* Suele suplantar grandes empresas de entrega de correo tales como: FedEx, UPS etc. En el correo el atacante incluye una notificación de

entrega de un producto, pero esta notificación contiene un link o adjunto malicioso.

- *Estafa de impuestos:* El atacante con esta modalidad hace parecer provenir de una agencia de ingresos fiscales de gobierno un correo notificando que está atrasado en el pago de impuestos. En el mismo correo entrega un link donde se puede solucionar este problema para no incurrir en multas o acciones legales adicionales. Como recomendación es nunca compartir información personal ni financiera por medio de correo electrónico.

Para contrarrestar el phishing vía correo electrónico existen algunos consejos o recomendaciones importantes, los cuales son:

- No confiar en el nombre del sender o quien envía el correo electrónico.
- Tener cuidado con el lenguaje urgente o amenazante en la línea de asunto del correo.
- Comprobar si hay errores ortográficos en el correo; palabras mal escritas, saludos estándar y ausencia de contactos, dominios URL incorrectos, Estos puntos suelen ser habituales en phishing.
- Mirar, pero no hacer clic.
- No dar clic en adjuntos sospechosos enviados por contactos desconocidos.
- No brindar información personal.
- Validación de URL donde se redirige el correo malicioso.
- Tiene que tener coherencia tanto el link como la página web que se despliega.
- Ninguna entidad bancaria solicita información de cuentas, tarjetas de créditos, tarjetas débito etc.
- Si al buzón de entrada llega un correo sospechoso no darle reenviar a otras personas dentro de la empresa donde se labora, puede proliferarse el robo de información en otras personas.

Ante cualquier sospecha de correo electrónico no confiable lo más importante es contactarse con personal especializado en temas de ciberseguridad.

IX. METODOLOGÍA USADA POR UN ESPECIALISTA DE CIBERSEGURIDAD ANTE UN ATAQUE PHISHING.

Se puede entender como un especialista de seguridad informática como: aquella persona estudiada y actualizada ante el tema de ciberseguridad, donde sus conocimientos son plasmados para la prevención, análisis y remediación de ataques cibernéticos actuales. Adicionalmente, y enfocándose en el phishing se puede tener un análisis más profundo con un paso a paso donde se realice las validaciones que repercuten en este ataque malicioso.
El especialista realiza lo siguiente:

- *Análisis profundo del correo malicioso.*
  Se valida el emisor y receptor del correo. Sin importar si este es de una fuente de confianza. Se revisa el contenido de este, como el asunto descrito en el correo, archivos adjuntos y links sospechosos.
- *El especialista debe conocer la cabecera del correo.*
  Se selecciona y se copia para un análisis profundo de cada uno de los campos del encabezado.

Los campos más importantes de una cabecera de correo electrónico son:

- *From:* Contiene los datos del emisor en forma de correo electrónico.
- *To:* En este campo se introducen el receptor o los receptores.
- *CC:* Campo opcional donde se puede introducir la dirección o las direcciones que han de recibir una copia del mensaje.
- *Date:* Fecha y hora del mensaje.
- *Subject:* Este es el campo del asunto o el tema del mensaje.
- *Return Path:* Este campo suele estar al comienzo de este segundo bloque y proporciona las opciones para la devolución al servidor de correo, en caso de que la entrega no sea posible.
- *Received:* Deben existir como mínimo dos campos por encabezado, ya que para el envío de un correo son necesarios dos servidores, uno para el envío y otro para la recepción. En estos campos se encuentra la información relativa al camino que ha recorrido el correo hasta llegar al destino, incluida la fecha y las direcciones de los servidores que ha seguido.
- *Message-ID:* Identificación individual compuesta por un código de cifras, letras y un nombre de dominio.
- *Content Type:* Este campo contiene información sobre el tipo de texto y de fuente tipográfica del cuerpo del email.

Los resultados obtenidos después del análisis deben dar a conocer la veracidad o confiabilidad del emisor del correo.
Aunque el análisis se puede realizar manualmente por el especialista cabe resaltar que ya existen herramientas para el análisis de estas cabeceras de correos sospechosos como la herramienta de análisis Ip Tracker (https://www.iptrackeronline.com/email-header-analysis.php).
En este punto se debe seleccionar la opción “Submit Header for Analysis” para su posterior análisis y así poder analizar los resultados. Se puede validar resultados como la Ip de origen donde se envió el correo phishing.

Otra herramienta de uso confiable para cualquier especialista de ciberseguridad es la herramienta de análisis es MX ToolBox (https://mxtoolbox.com/EmailHeaders.aspx). Para el uso debido de la herramienta se debe copiar la cabecera obtenida y pegarla en el campo “Paste Header” lego clic en “Analyze header”.
En este punto el especialista de ciberseguridad analiza los campos previamente mencionados, donde se evidencia que el correo analizado es estas herramientas es legítimo o malicioso. En el caso que sea malicioso se previene al usuario que reporta el correo, se documenta y se brinda recomendaciones.

Análisis Hipervínculo de correo sospechoso: Para el análisis del link adjunto en el correo sospechoso es necesario realizar lo siguiente:

- No accionar o hacer clic en el link sospechoso, ya que se puede descargar malware en el pc.
- Copiar el link. (Clic derecho copiar hipervínculo).

Existen hoy en día en Internet varios sitios para análisis de URL o de correos sospechosos, en este caso se utilizará la herramienta de análisis de Virus Total (https://www.virustotal.com/#/home/url), la cual presta el servicio en línea gratuito que analiza archivos y URLs que permiten la identificación de malware, detectado por motores antivirus y escáneres de sitios web. Si en alguna ocasión la URL ya fue analizada, el sistema le mostrara la última fecha en la que lo hizo, y da la opción para ver esos resultados o volver a validar para mostrar resultados más actuales. Si no ha sido analizada antes, le mostrara los resultados directamente. Los resultados que brinda esta página web pueden ser dos o que el link previamente almacenado no sea malicioso o la otra opción que sea malicioso. Si este link es malicioso, en la base de datos previamente configurada en Virus Total nos mostrara que empresas de seguridad lo muestran como malicioso. Al tener este reporte se puede deducir claramente que no es un email legitimo ni un link legítimo.

Análisis archivos adjuntos: Para el análisis de archivos adjuntos también se utiliza la herramienta de análisis online Virus Total (https://www.virustotal.com/#/home/upload). Se escoge la opción archivo y se procede a adjuntar el archivo a analizar. Con los resultados de análisis tanto de cabeceras como de hipervínculos y de correos adjuntos se procede a documentar los hallazgos y posteriormente a implementar las recomendaciones si existen o las hay. En un caso de Phishing siempre es recomendable y como buena práctica reportar el correo mal intencionado al proveedor de correo de seguridad, si no lo hay se recomienda bloquear el emisor del correo malicioso.
De esta manera no puede haber fuga de información y por lo tanto el impacto económico es mínimo y la imagen de cualquier empresa no es impactada negativamente.

X. Ataque DoS (Denegación de servicio).

Hoy en día es muy común ver que mientras se está haciendo una transacción "el sistema se caiga" y no permita acceder al usuario a realizar dicha transacción y también es muy común que una página web no esté disponible por cualquier motivo. Es por eso por lo que uno de los ciberataques activos de interrupción es la Denegación de Servicio (DoS) donde un atacante intenta agotar los recursos del activo de información que tiene como objetivo, impidiendo a los usuarios el acceso a la aplicación o servicio. Una variante de este tipo son los ataques Distribuidos de Denegación de Servicio (DDoS): un ataque DDoS tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Existen diversas formas de ataque DDoS: por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo.

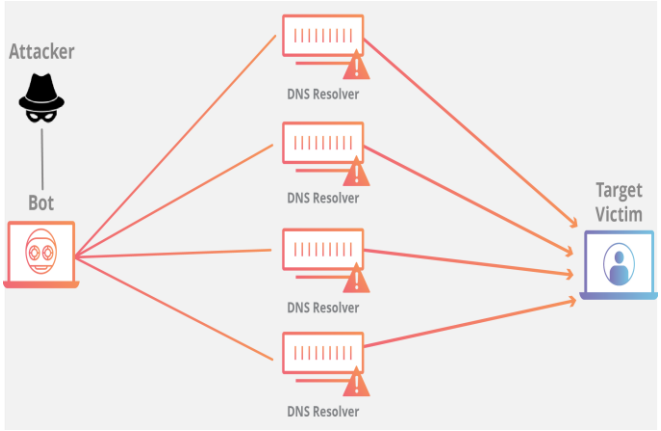

Figura 7. Arquitectura ataque de denegación de servicio. Recuperado de https://www.testdevelocidad.es/2018/03/02/ataque-ddos/

En este tipo de ataque se puede validar que el adversario o atacante compromete o complica un gran número de computadores conectados a la red mediante la explotación de vulnerabilidades de software de red, luego, el software de ataque es instalado en estos sistemas a través de canales seguros. Los equipos comprometidos en los que está instalado el software malicioso de ataque envían paquetes inútiles hacia una víctima al mismo tiempo. El volumen de tráfico malicioso generado por tales maquinas infectadas es tan alta que una víctima no puede gestionar y se paraliza al instante el servicio.

Los siguientes son los pasos más significativos para detectar un ataque de Dos y sus derivaciones:

- *Verificar el ataque.* No todas las interrupciones son causadas por un ataque DDoS. Configuraciones erróneas de DNS, problemas de routing, y error humano son causas comunes de interrupciones de red. Primero se debe descartar estos tipos de ataques no DDoS y distinguir un ataque de una interrupción común y corriente.
Descarte las interrupciones más comunes, entre más rápido pueda verificar que la interrupción en el servicio es un ataque DDos, más rápido podrá responder a él. Aun si la interrupción no fue causada por una configuración errónea u otro tipo de error humanos, puede haber otras explicaciones que semejen a un ataque DDoS. (como traceroute, ping, y dig) y descartar estas posibilidades. Descartar posibles problemas globales. Revisar los siguientes reportes del estado del Internet para determinar si el ataque es un problema global: Internet Health Report y Internet Trac Report.
- *Ponerse en contacto con los líderes de equipo.* Una vez que el ataque ha sido verificado, contacte los líderes de los equipos relevantes. Contactar al proveedor de servicios de banda ancha por medio de una llamada y confirmar con el proveedor que el ataque si está sucediendo; este proveedor puede brindarle información de cómo está pasando el ataque y

en algunas ocasiones ofrecerle asistencia. Una posible solución oportuna y rápida puede ser la de contactar al equipo de ciberseguridad o respuesta de incidentes de la empresa. Es de especial importancia recurrir al equipo antifraude tan pronto sea verificado el ataque. Lo ataques DDoS pueden ser usados como una pantalla para esconder una infiltración. Los registros que normalmente mostrarían una penetración pueden perderse durante un ataque DDoS. Por esta razón es que el registro independiente y de alta velocidad es tan importante.

- *Jerarquizar aplicaciones.* Una vez que el ataque ha sido confirmado y al enfrentarse a un ataque DDoS intenso con recursos limitados, cualquier organización debe de tomar decisiones de jerarquización. Los activos en línea de más alto valor normalmente generan también ganancias de alto valor. Estas aplicaciones son aquellas que se deben mantener online o con vida. Aplicaciones de menor valor, independientemente de su nivel de tráfico legítimo, deben ser deshabilitadas intencionalmente para que los recursos de procesamiento y de red pueden ser puestos al servicio de aplicaciones de mayor valor. Estas decisiones afectan el bolsillo de la empresa o su economía por lo tanto se deben tomar estas decisiones debidamente. En resumen, se debe decidir cuáles aplicaciones son de baja prioridad y pueden ser deshabilitadas durante un ataque. Esto puede incluir aplicaciones internas.
- *Proteger usuarios importantes y usuarios que trabajen remotamente.* Las direcciones IPs de los usuarios importantes de la compañía deben ser adicionadas a una lista blanca donde siempre debe tener accesos a las aplicaciones de la empresa. Estas IPs de los usuarios importante y remotos deben ser agregadas en diferentes puntos de la arquitectura de la red (Application Delivery Controller, Firewall etc.), y posiblemente hasta con el proveedor de servicios, para garantizar que el tráfico desde y hacia esas direcciones no sea interrumpido.
- *Limitar recursos* Si todos los pasos previos fallan al detener el ataque DDoS, puede verse forzado a simplemente limitar recursos para sobrevivir el ataque. Esta técnica rechaza tanto tráfico bueno como malo. De hecho, limitar la capacidad en muchos casos rechaza del 90 al 99 por ciento del tráfico deseable al mismo tiempo que permite que el agresor aumente los costos en su centro de datos. Para muchas organizaciones es mejor deshabilitar una aplicación que limitar su capacidad.

XI. Educación al recurso humano.

Usualmente en la mayoría de las compañías tienden a responsabilizar y remediar todos los problemas relacionados con la ciberseguridad a las áreas de tecnología y a los dispositivos de infraestructura diseñados para la protección de los sistemas e información. Pero dejan a un lado la parte de conciencia y educación a los colaboradores, desconociendo que el ser humano es el eslabón más débil de la cadena en este ámbito de seguridad.

De esta manera con el tiempo se han ido identificando estas necesidades de manera reactiva, ya luego de que han ocurrido los incidentes, fugas o robos de información, interrupción de los servicios, entre otros. Lo que ha conllevado a pérdidas no solo a nivel económico de varias organizaciones sino también generar mala reputación e involucrarlos hasta en problemas legales y regulatorios debido al desconocimiento de las leyes que ya vienen rigiendo estos ciberdelitos.

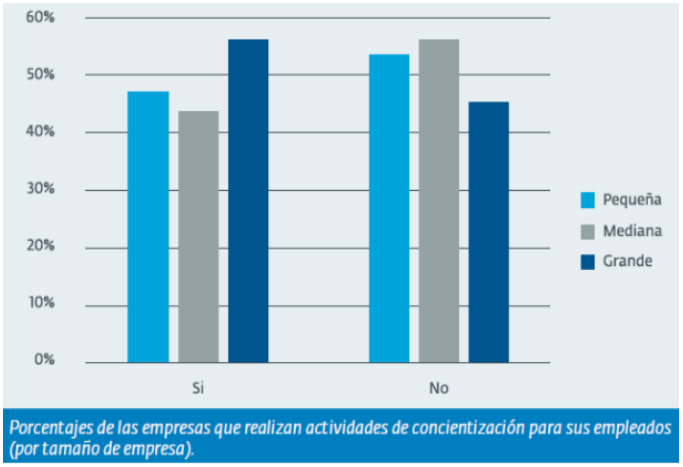

Figura 8. Resultados de empresas que brindan concienciación de ciberseguridad. Recuperado de http://blog.smartfense.com

Pero hasta que no ocurren estos desafortunados sucesos, las organizaciones no invierten en temas de educación y conciencia, lo que en muchos casos ya es demasiado tarde pero que al mismo tiempo con los constantes avances en las amenazas nunca sobrara realizar y mantener este tipo de planes de manera periódica y llevando un seguimiento de su comprensión y cumplimiento respecto a las políticas de seguridad y controles que puedan implementar según considere cada organización.

Así que, para tener una gestión más eficaz, este tipo de planes deben estar enfocados a determinadas áreas, personas, roles y funciones dentro de la organización. Manteniendo un aspecto de motivación fuerte, demostrando y dándole el valor que se merece a este tipo de sensibilizaciones.

Este tipo de actividades son de vital importancia para las organizaciones sin importar su finalidad, ya sean de tipo industrial, financiero, salud, entre otros. Según experiencias de compañías relacionadas y enfocadas a temas de tecnología y comunicaciones, estos planes son un plus y una parte primordial en la que deben participar todos los colaboradores cumpliendo y siguiendo de manera muy ética sus respectivas políticas.

Los aliados estratégicos, proveedores y demás que estén relacionados con la organización. Al igual implementar un sólido sistema de gestión de Seguridad de la información lo convierte en un gran salto para contrarrestar estas amenazas, aprendiendo de los incidentes generados y realizando acciones de mejora sobre los controles que involucran más a los colaboradores. En un día laboral, todas las personas manejan y están en contacto con información de diferente índole. Así que deben estar atentas y activas a proteger la confidencialidad de esta (documentos, datos, dispositivos, etc.) ya sea de carácter interna o externa.

Para esto se recomienda lo siguiente:

- Guarde los documentos, discos, medios magnéticos, etc. que contengan información sensible en cajones bajo llave.
- Asegure físicamente los equipos portátiles con cables de seguridad (Guayas) para evitar robos.
- Bloquee la pantalla al alejarse o retirarse de su computadora (Windows + L).
- No deje a la vista o publique documentos con datos sensitivos, por ejemplo: nombres de usuarios y contraseñas, contratos, números de cuenta, datos de empleados, listas de clientes, etc.
- Use contraseñas sólidas y no las reutilice. Válido: "34bGUI7&89@))". No válido: "12345 o Eddy1".

- Mantenga la confidencialidad de las credenciales de acceso y no las comparta con nadie. ¡Recuerde que son como su cepillo de dientes!

- Realice copias de seguridad periódicas de la información y almacénelas en sitios seguros.

- Busque sobre la URL la letra S de HttpS al navegar por Internet, estas páginas dan confianza y mucho más si están solicitando datos personales u otra información relevante.

XII. Conclusiones.

Los ataques de phishing hoy en día están evolucionando y cada día son más creíbles, en donde su impacto, mayormente negativo, abarca más usuarios en cualquier compañía. Es por eso por lo que es necesario implementar reuniones y entrenamientos de concienciación de ciberseguridad frente al tema de phishing plasmando en estas demostraciones de como un ciberdelincuente puede efectuar un ataque phishing de manera fácil y eficaz, también la manera de identificar y prevenir este ciberataque.

Todos los usuarios del correo electrónico corremos el riesgo de ser víctimas de estos intentos de ataques. Cualquier dirección pública en Internet será más susceptible de ser víctima de un ataque debido a los spiders que rastrean la red en busca de direcciones válidas de correo electrónico. Éste es el motivo de que exista este tipo de malware. Es realmente barato el realizar un ataque de este tipo y los beneficios obtenidos son cuantiosos con tan sólo un pequeñísimo porcentaje de éxito.

La mejor manera de protegerse del phishing es entender la manera de actuar de los proveedores de servicios financieros y otras entidades susceptibles de recibir este tipo de ataques. Mantenerse informados con las nuevas tendencias y tipos de ataques de phishing podría ayudar a prevenirles.

También es recomendado limpiar constantemente el buzón de entrada y así poder caer en este ataque de phishing. Para estos se recomienda los siguientes pasos:

- Eliminar los correos no deseados.
- Usar el filtro de correo. Bloqueando los emisores de correo no deseados.
- Si su organización lo permite, tener asignado una cuenta de correo “Menos fácil de adivinar”. Si su correo es personal, proceder a crear una cuenta como la descrita anteriormente.
- No inscribir su cuenta de correo en sitios web o en perfiles de redes sociales.
- Tener un correo electrónico simplemente para usos públicos, es decir si necesita publicar en un foro o unirse a un grupo.
- Usar un antivirus confiable.
- Des escribirse de lista de correos.
- Nunca dar respuesta a un correo sospechoso, puede que el atacante este simulando ser la otra parte “confiable”.

XIII. Referencias.

[1] Internet – Conceptos de seguridad – Online. Disponible en http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

[2] Internet – Conceptos de seguridad – Online. Disponible en http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

[3] Internet – Conceptos de seguridad – Online. Disponible en http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

[4] Internet – Definición de ciberseguridad y riesgo – Online. Disponible en https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

[5] Internet – ¿Qué es ciberguerra? – Online. Disponible en http://www.pensamientopenal.com.ar/system/files/2016/02/doctrina42952.pdf.

[6] Internet – Que es Malware - Online. Disponible en https://iiemd.com/malware/que-es-malware.

[7] Internet - Ciberseguridad: la importancia de la protección de la información en el mundo actual. Disponible en https://reportedigital.com/seguridad/ciberseguridad/.

[8] Internet - La ingeniería social: el usuario continúa siendo el eslabón más débil – Online. Disponible en https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html.

[9] Internet – 5 cosas que debes saber sobre ingeniería social – Online. Disponible en https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/.

[10] Internet – 5 tipos de phishing en los que no debes caer – Online. Disponible en https://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/.

[11] Internet – ¿Qué es “whaling” y ¿cuál es la diferencia con el phishing? – Online. Disponible en https://latam.kaspersky.com/blog/whaling/8057/.

[12] Internet – Soluciones de Seguridad Eset – Online. Disponible en https://www.eset.com/co/

[13] Internet - Auditool – Online. Disponible en https://www.auditool.org

[14] Internet – Soluciones de Seguridad Panda – Online. Disponible en https://www.pandasecurity.com

[15] Internet – Cisco Systems – Online. Disponible en https://www.cisco.com

[16] Internet – Data Centers – Online. Disponible en http://searchdatacenter.techtarget.com

Autor.
Jaime Yesid Monsalve Mendez, nacido en Bogotá, Colombia en 1991, es graduado de Ingeniería de Sistemas de la Universidad Piloto de Colombia, cuenta con certificaciones en seguridad informática tales como: checkpoint, McAfee, zscaler, y se desempeña como analista de ciberseguridad en una multinacional de origen británico donde protege la información de dicha empresa.