INGENIERÍA SOCIAL: PHISHING Y BAITING

Cortés Hernández, Andrés Mauricio.
anmao94@hotmail.com
Universidad Piloto de Colombia

Resumen— En este artículo se encontrarán dos claros ejemplos, que darán a conocer la importancia de la ingeniería social y como esta se puede ver afectada en una empresa, debido al desconocimiento por parte de los funcionarios, ya que como consecuencia, la información puede verse afectada, robada, alterada, etc.

Se realizará énfasis en dos procesos de ingeniería social como son Phishing y Baiting. Cabe resaltar, que en estas dos técnicas que se probaron, se alcanzó a obtener información destacada y fundamental de los usuarios. Con la cual se pudo definir y distinguir cuáles son los puntos y las brechas de seguridad que se encuentran presentes en las compañías.

Abstract— In this article you will find two clear examples, which will make known the importance of social engineering and how it can be affected in a company, due to the ignorance by the company officials, since as a consequence, the information can be affected, stolen and altered.

Emphasis will be placed on two social engineering processes such as Phishing and Baiting. It should be noted that in these two techniques that were tested, it was possible to obtain outstanding and fundamental information from users. With which it was possible to define and distinguish which are the security points and breaches that are present in the companies.

Índice de Términos—Baiting, información, ingeniería social, phishing, seguridad informática.

I. INTRODUCCIÓN

Desafortunadamente, en la actualidad se está proliferando de manera exhausta constatando que la mayoría de los ataques de ciberdelincuentes usan técnicas de ingeniería social por eso es importante resaltar su importancia y verificar con detenimiento técnicas, que serán analizadas y permitirán dar respuesta a las faltas de seguridad y robo de información en una empresa.

Ahora bien, la ingeniería social se encuentra presente y forma parte esencial de muchos ámbitos de nuestra vida cotidiana; ya sea desde la infancia cuando se manipula a un adulto para obtener lo que se desea. No obstante, de la misma manera sucede en el campo laboral y en diversas ramas profesionales, se hace uso de técnicas con el fin de tener acceso por medio de la manipulación. De igual manera sucede con el uso de la información, una persona que sea mal intencionada puede valerse de diversas técnicas y dañar la confidencialidad que se le ha dado.

Teniendo en cuenta lo anteriormente expuesto, se deduce que se generan ataques y la acción de vender y tomar información privada a posibles competidores, es algo que sucede con frecuencia, y se generan dudas constantes, en la tarea de muchos funcionarios acerca de cuestionarse de los privilegios que se pueden dar a cada empleado, cómo se podría tal vez mejorar o garantizar la confidencialidad de los datos que se brindan día a día en los campos laborales y a su vez que grado de seguridad se tienen en las compañías y cómo mejorarlos con el pasar de los días.

La Ingeniería Social se sustenta en un sencillo principio: “el usuario es el eslabón más débil”. Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla [1].

A pesar de que existan medidas de seguridad, muchas veces estas no son suficientes para detener los ataques. Hay que tener en cuenta que, con los

datos robados, se puede revelar información relevante y confidencial. Por ejemplo, con el Phishing por medio de una estafa vía correo electrónico, se roban datos con fines maliciosos o se instala algún tipo de programa maligno en el equipo del funcionario, frente a eso es necesario tener consciencia acerca de los correos falsos que se puedan presentar en las compañías ya que los atacantes cibernéticos estudian a las empresas para poder enviar campañas que sean atractivas para los funcionarios.

De igual manera sucede con el baiting, se coloca a disposición información falsa, por medios físicos como dispositivos USB, CDs, por ejemplo, el uso de memorias con fines promocionales, los cuales llegan al funcionario de manera verídica para que las introduzcan en los computadores y así infectar las máquinas [2].

II. CONCEPTOS CLAVES

Dato. El diccionario de la Real Academia de la Lengua Española dice que "datos" son: "antecedentes necesarios para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho".

Los datos no son información más que en un sentido amplio de "información de partida" o "información inicial", pero los datos por si solos no permiten la adopción de la decisión más conveniente porque no aportan los conocimientos necesarios. Sólo una elaboración adecuada de los datos (un proceso de los datos) nos proporcionará el conocimiento adecuado [4].

Información. En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno. De esta manera, si por ejemplo organizamos datos sobre un país, tales como: número de habitantes, densidad de población, nombre del presidente, etc. y escribimos por ejemplo, el capítulo de un libro, podemos decir que ese capítulo constituye información sobre ese país [4]. Dicha información es el conjunto de datos que al momento de ser organizados contiene un significado, esto transmitido al sentido de la Ingeniería social es muy importante ya que cualquier dato que se pueda extraer de alguien o algo se contempla como robo de información que es en lo que se enfoca las diferentes técnicas de dicha práctica.

Fig 1. Diagrama de flujo entre dato e información [4].

Informática. La informática es conjunto de conocimientos científicos y técnicas que estudia el tratamiento automático de información utilizando dispositivos electrónicos y sistemas computacionales. Incluye instrucciones en ciencias de la información, interacción persona-computador, análisis y diseño de sistemas de información, estructura de las telecomunicaciones, arquitectura y gestión de la información.

La informática ofrece formación sólida en programación, matemáticas y estadísticas, junto con el estudio de los aspectos de las ciencias éticas y sociales de los sistemas de información complejos. Las carreras en informática aprenden a analizar críticamente diversos enfoques de tratamiento de la información y desarrollar habilidades para diseñar, implementar y evaluar las herramientas de tecnología de la información [5].

Seguridad informática. La seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie

de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet [7].

Fig 2. Principios seguridad informatica [7].

Ingeniería social. El principio fundamental de la ingeniería social en el campo de Internet es lograr la colaboración de los usuarios legítimos de los sistemas para que activen mecanismos de hackeo, o bien envolverlos rápidamente en alguna estafa irremediable.

El engaño puede operar a través de un sólo medio (un correo electrónico, por ejemplo) con una breve historia para que el usuario entregue información sensible o haga clic en un enlace que activa códigos maliciosos. Pero también puede ser ejecutado a través de una secuencia de historias y acciones que incluyen el uso de plataformas múltiples: WhatsApp, mensajes SMS, redes sociales, pagos electrónicos, tarjetas prepago o depósitos bancarios, que conforme se enlazan, van haciendo más vulnerable a la víctima [6].

Phishing. El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

El escenario de Phishing generalmente está asociado con la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. El engaño suele llevarse a cabo a través de correo electrónico y, a menudo estos correos contienen enlaces a un sitio web falso con una apariencia casi idéntica a un sitio legítimo. Una vez en el sitio falso, los usuarios incautos son engañados para que ingresen sus datos confidenciales, lo que les proporciona a los delincuentes un amplio margen para realizar estafas y fraudes con la información obtenida.

La principal manera de llevar adelante el engaño es a través del envío de spam (correo no deseado) e invitando al usuario a acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios. A menudo, estos correos llegan a la bandeja de entrada disfrazados como procedentes de departamentos de recursos humanos o tecnología o de áreas comerciales relacionadas a transacciones financieras [9].

Baiting. Consiste en dejar dispositivos de almacenamiento extraíble (CD, DVD, USB) infectados con algún software infectado en algún lugar a la vista (por ejemplo, baños públicos, ascensores, aceras, etc.), esperando a que alguien los recoja y conecte a su dispositivo. Al hacerlo, aquél afortunado que encontró un USB misterioso el cual el software malicioso se instalara y permitirá que el hacker obtenga los datos personales del usuario [10].

Hacker. Persona apasionada por la seguridad de la información con avanzados conocimientos en el área de la informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes en plenitud tiene la capacidad de dominar en un buen porcentaje varios aspectos como: lenguajes de programación,

manipulación de hardware y software, telecomunicaciones; estas habilidades las utiliza con un buen fin, apoyando a empresas en el área de seguridad informática y de la información para solventar las brechas de seguridad y apoyar al área del SOC (Security Operation Center) [11].

Cracker. Es considerado un vandálico virtual. Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión [12]. Es por ello por lo que debemos tener diferentes capas de seguridad en nuestra compañía como en nuestros ordenadores personales con el fin de ser precavidos con el manejo de la información.

III. METODOLOGÍA

A. Técnica de Phishing.

Para la ejecución de la técnica de phishing se realizan los siguientes pasos, el primero de ellos que puede ser el más crítico ya que se realiza un análisis de personal puede ser afectado por la prueba de phishing. Para ello se identifica a que población se realiza lanzar el ataque, después se planea en que momento es preciso para llevar a cabo de enviar los correos masivos en este análisis se establecer qué tipo de campaña se puede lanzar como señuelo y por último ejecutar el ataque y esperar que los funcionarios caigan en esta técnica de ingeniería social.

Para ello se estudió a la empresa la cual contemplan un evento semestralmente las cuales son campañas de liderazgo interno para que los funcionarios puedan aplicar a nuevas convocatorias internas y así poder escalar profesionalmente, teniendo en cuenta la información recolectada en las campañas anteriores se diseñó un evento muy similar el cual es un correo que llegara al funcionario el cual estará segmentado en tres partes:

1ro. Pop-up de rastreo, el cual es implantado en el correo malicioso enviado para saber si el funcionario abrió el correo en la bandeja de entrada.

2do. URL maliciosa, la cual al momento de que el funcionario le de click este lo redirigirá a una página web maliciosa en la cual la persona tendrá que llenar un formulario en el cual dejará la información personal y corporativa pensando que es aplicando a la campaña.

3ro. Código QR, el cual será el señuelo para instalar una aplicación maliciosa en el celular del funcionario ya que la primera reacción de las personas al ver un código QR es coger su dispositivo móvil y así revisar que contiene el código el cual lo redirige a una página web en donde se descargara la aplicación diseñada en la campaña para poder tomar los datos del funcionario.

Este correo malicioso es enviado desde una cuenta que sea legítima para que los controles de seguridad perimetrales y de correo electrónico no tomen medidas correctivas y bloqueen el paso del correo y así pueda llegar a la bandeja de cada uno de los funcionarios a los cuales fue enviado el correo y no se quede en el SPAM ya que lo que se necesita es que las personas miren el correo y llenen el formulario.

Fig 3. Visualizacion del correo malicioso enviado.

Una vez el funcionario haya dado click en la URL maliciosa está lo redirigirá a una página web maliciosa donde tendrá que llenar un formulario

para la postulación de Líderes 2019.

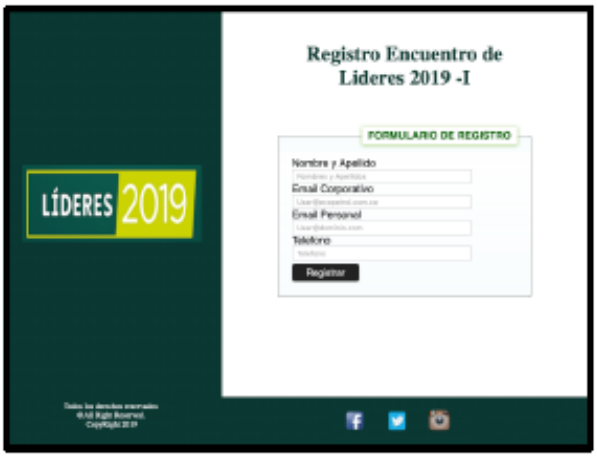

Fig 4. Formulario de inscripción.

Este formulario el cual tendrá que diligenciar el funcionario que desee postularse tendrá las siguientes casillas: Nombre / Apellido, Email corporativo, Email personal y Teléfono, cuando terminan de llenar las celdas tendrán que darle click en "Registrar" para que la información sea enviada un servidor externo donde se alojara en una base de datos con las personas que llenaron el registro.

Por otra parte, cuando el funcionario revise el correo y se da cuenta que hay un código QR adjunto, la primera reacción es sacar el celular y observar que información existe detrás del código, para ello al momento de escanear el código lo redirigirá a una página web donde descargada una aplicación maliciosa la cual será para llenar el formulario de la campaña "Líderes 2019".

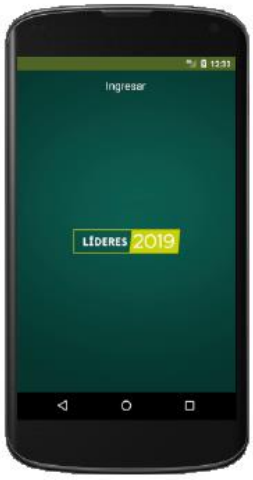

Fig 5. Apk maliciosa instalada en los dispositivos moviles.

Al momento de descargar la aplicación maliciosa el funcionario tendrá que diligenciar el mismo formulario que se ve en la URL del correo, sin embargo, la aplicación está diseñada de una manera muy similar con formas y colores del correo para que sea de mayor confianza para el funcionario y así llene el formulario con más aceptación.

B. Técnica de Baiting.

Para la ejecución de esta prueba se genera un archivo ejecutable malicioso el cual será guardado en dispositivos de almacenamiento externo o USB que serán distribuidos en diferentes puntos estratégicos como los baños, lugares de recepción, salas de conferencias y ascensores de la empresa para que los funcionarios cuando encuentren y conecten las memorias en sus equipos de trabajo, ejecutando el archivo malicioso.

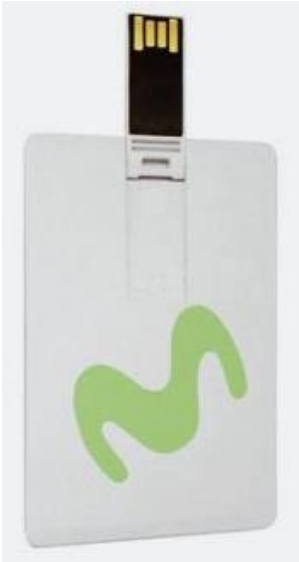

Fig 6. Diseño de la tarjeta USB maliciosa.

El diseño de la tarjeta USB es clave para que las personas la pongan en el pc ya que al tener el logo de algún proveedor de servicios de internet la hace confiable para el que el funcionario no sea reacio al momento de poner la memoria en el computador, una vez insertada la USB encontrará un archivo malicioso llamado Wifi gratis esto con el fin de que tenga similitud con el diseño de la tarjeta para que los funcionarios ejecuten el archivo.

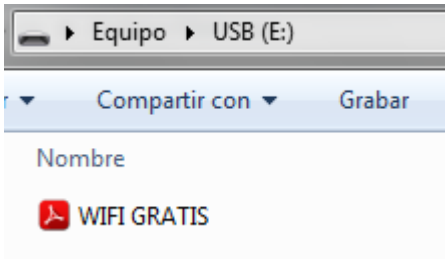

Fig 7. Archivo malicioso contenido en la tarjeta USB.

Una vez ejecutado el archivo malicioso "WIFI GRATIS" este contiene un archivo batch el cual capturará el nombre del usuario, la hora, la fecha y correrá el comando ipconfig /all en un símbolo de sistema de la sesión en la cual se corrió el ejecutable y esta información la guarda en un archivo en texto plano en la siguiente ruta C:\Users\Public, después este archivo con la información del funcionario lo envía al servidor 145.14.144.98 por el protocolo FTP, esta transferencia de información es debida a que una parte de la secuencia del archivo malicioso es abrir una ventana emergente pidiéndole autorización al funcionario a que le otorgue permisos de administrador para que él pueda enviar la información tomada.

IV. RESULTADOS

Se lanza la campaña de phishing llamada "Líderes 2019" por correo electrónico a la empresa de hidrocarburos la cual se envía a una población objetivo de 1175 personas.

- 892 correos electrónicos que visualizaron la imagen de la campaña, gracias al Pop-up de rastreo el cual envía un mensaje de que el correo fue abierto y leído al remitente.
- 352 visualizaciones del formulario del registro de la campaña ya que al ingresar a la URL adjunta en el correo se generará un log de la persona que ingresó a dicha página web.
- 76 personas diligenciaron el formulario entregando nombres, apellidos, emails corporativos, emails personales y teléfonos; esta información quedo guardada en el servidor externo.
- 57 personas descargaron la aplicación maliciosa diseñada para la campaña.
- 31 personas interactuaron con la aplicación maliciosa llenando el formulario y enviándolo al servidor externo.

Para la campaña del ataque de baiting se hizo un análisis de los lugares donde más transitaba los funcionarios en la empresa y en qué áreas los funcionarios no eran tan técnicos y pudieran ser vulnerables al ataque, los cuales fueron los baños, lugares cercanos a la recepción y los diferentes pisos de las áreas que no tuvieran personal no calificado técnicamente como contabilidad, diseño, recursos humanos, entre otros.

- 35 personas encontraron las tarjetas USB de las 40 que se esparcieron en la empresa.
- 7 personas entregaron las tarjetas USB al área de tecnología.
- 28 personas ingresaron la tarjeta USB a los equipos corporativos, corrieron el programa malicioso y enviaron la información al servidor.

V. RECOMENDACIONES

Las siguientes son algunas recomendaciones para las campañas de phishing, estas se pueden dictar en capacitaciones al personal que no tenga tantos conocimientos técnicos para crear concientización de los diferentes métodos que los atacantes pueden llegar a realizar para obtener la información personal.

- Evitar el SPAM ya que es el principal medio de distribución de cualquier mensaje que intente engañarlo.

- Tomar por regla general rechazar adjuntos y analizarlos aun cuando se esté esperando recibirlos.

- Nunca hacer clic en un enlace incluido en un mensaje de correo.

- Siempre intentar ingresar manualmente a cualquier sitio web. Esto se debe tener muy en cuenta cuando es el caso de entidades financieras, o en donde se nos pide información confidencial (como usuario, contraseña, tarjeta, PIN, etc.).

- Sepa que su entidad, empresa, organización, etc., sea cual sea, nunca le solicitará datos confidenciales por ningún medio, ni telefónicamente, ni por fax, ni por correo electrónico, ni a través de ningún otro medio existente. Es muy importante remarcar este punto y en caso de recibir un correo de este tipo, ignórelo y/o elimínelo.

- Otra forma de saber si realmente se está ingresando al sitio original, es que la dirección web de la página deberá comenzar con https y no http, como es la costumbre. La S final, nos da un alto nivel de confianza que estamos navegando por una página web segura.

- Es una buena costumbre verificar el certificado digital al que se accede haciendo doble clic sobre el candado de la barra de estado en parte inferior de su explorador (actualmente algunos navegadores también pueden mostrarlo en la barra de navegación superior).

- No responder solicitudes de información que lleguen por e-mail. Cuando las empresas reales necesitan contactarnos tienen otras formas de hacerlo, de las cuales jamás será parte el correo electrónico debido a sus problemas inherentes de seguridad.

- Si tiene dudas sobre la legitimidad de un correo, llame por teléfono a la compañía a un número que conozca de antemano, nunca llame a los números que vienen en los mensajes recibidos.

- El correo electrónico es muy fácil de interceptar y de que caiga en manos equivocadas, por lo que jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través de este medio.

- Resulta recomendable hacerse el hábito de examinar los cargos que se hacen a sus cuentas o tarjetas de crédito para detectar cualquier actividad inusual.

- Use antivirus y firewall. Estas aplicaciones no se hacen cargo directamente del problema, pero pueden detectar correos con troyanos o conexiones entrantes/salientes no autorizadas o sospechosas.

La siguiente campaña se generó para una empresa la cual fue víctima de Phishing; en esta campaña de concientización se pegaron carteles en diferentes sitios de la compañía como baños, ascensores y recepción, se crearon iCards para extenderlas por políticas de directorio activo y que se vieran en los computadores de todos los funcionarios y en las diferentes pantallas que se tienen en la compañía, el contenido de esta campaña fue la siguiente:

- NO acceda a sitios donde le pidan información personal.
- NO descargue archivos donde soliciten consultar su estado bancario.
- NO descargue archivos enviados por correo solicitando el pago de multas, moras, créditos bancarios, etc.
- NO entregue información personal cuando lo llamen sobre entidades bancarias, contraseñas, número de tarjetas de crédito, etc.
- SIEMPRE cuando se tenga alguna duda, sospecha, desconfianza, creencia, suposición o hipótesis sobre algún correo, página web, llamada, mensaje de texto SMS, archivos, pagos electrónicos o cuentas bancarias, por favor comunicarse con el área de tecnología e informar sobre el acontecimiento dado

para que personal experto realice las respectivas validaciones.

Esto con el hecho de que los funcionarios lean las frases y lo apliquen a su día a día laboral así evitando que las personas caigan en los ataques de ingeniería social.

VI. PLAN DE CONCIENCIACIÓN PARA EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN.

Según la NIST 800-50 la cual es la Creación de un programa de sensibilización y capacitación sobre seguridad de la tecnología de la información y con las tendencias para las buenas prácticas en un CDC (Cybersecurity Defenser Center) se generaron las siguientes actividades claves para concientizar a los funcionaros de cualquier empresa, enfocándose en estas tres acciones concientización, educación y entrenamiento.

A. *Concienciación.* El propósito es sensibilizar a las personas sobre los casos que existen de seguridad, la cantidad de robo de información que se realiza a nivel mundial y las diferentes técnicas que utilizan los crackers para poder quitar la información sensible de la persona.

1. Crear una campaña con una mascota publicitaria.
2. Definir un eslogan para la campaña. Un slogan bien estudiado, conceptualizado y construido es muchas veces un factor concluyente, que resume en pocas palabras lo que un producto, un servicio o una persona hará por las personas. Al ser de corta longitud (pocas palabras) y ser repetido constantemente en discursos o publicidad, el ser humano lo hace propio.
3. Elaboración de materiales diversos como pendones, posters, afiches, carteleras, protectores y fondos de pantalla, correos corporativos (con un logotipo representativo que indique la fuente), avisos en la intranet como imágenes, videos, presentaciones animadas o en la herramienta PowerPoint y documentos explicativos.
4. Creación y entrega de recordatorios como llaveros, tazas, lapiceros o tarjetas que dan una idea sobre construcción de claves seguras.
5. Elaborar juegos como monopolio o álbum de figuras con temas relacionados por supuesto con seguridad de la información.
6. Obras de teatro, stand up comedy o cuentacuentos (relacionados con temas de seguridad de la información).

B. *Educación*. La necesidad de que las personas tengan capacitación del personal interno en temas de seguridad mostrando campañas, boletines, ejercicios, lúdicas y casos de uso para que las personas tengan una mayor perspectiva sobre los riesgos que trae la ingeniería social.

1. Consejos, tests (mini auditorias).
2. Desarrollar trípticos.
3. Desarrollar trivias.
4. Concursos basados en pictogramas.
5. Uso de contraseñas seguras. La cantidad mínima de caracteres a usar es 8. Entre más larga una contraseña, menos probabilidad de ser vulnerada. Se deben combinar, letras, número, símbolos (#, $, %, &, etc.), signos de puntuación. Se debe cambiar con periodicidad de 30 días y usar una diferente por cada servicio en internet.
6. Encuestas evaluativas para verificar la retención de información sobre seguridad.
7. Precaución con el correo electrónico.
   - Realice un análisis antes de abrir algún correo.
   - Sospeche de los mensajes no esperados. Algunas veces vienen de

conocidos, por lo tanto, analice primero. Si de alguna forma Ud. sospecha, se aconseja llamar por teléfono al remitente para asegurarse.

- No use servicios de wifi gratuitos para acceder a sus cuentas bancarias, realizar pagos por internet, abrir correos, aplicaciones corporativas, ni escribir información sensible como la cédula, dirección de residencia o datos personales y bancarios en general, etc.
- Analizar los adjuntos en los correos, aunque provengan de fuente conocida. Cabe la posibilidad de que sean maliciosos. Ante cualquier sospecha, llame al remitente.

C. *Entrenamiento*. Se basa en la apropiación de habilidades y competencias de seguridad de la información con el objetivo de su aplicación en todas las actividades laborales y porque no personales.

1. Ataques dirigidos (simulados) para demostrar lo expuestos que están los empleados. Por ejemplo, enviarles un correo electrónico con archivo malicioso adjunto (con una advertencia y un consejo), dejar sueltos pendrives infectados (con una advertencia y un consejo).
2. Realizar capacitación sobre diferentes pruebas de vulnerabilidades a los funcionarios para saber en qué están mal y en que pueden mejorar.
3. Generar escenarios de pruebas para que las personas puedan ver que se les puede presentar en un ataque real.

VII. CONCLUSIONES

En las dos técnicas de ingeniería social se evidencia que el ataque fue exitoso y se valida que el ataque de phishing es el más vulnerable para una empresa debido a que el medio en el cual llega a los usuarios es el correo electrónico y la mayoría de las personas que están en una compañía revisan constantemente la bandeja de entrada y abren los correos cuando son sobre ofertas o postulaciones de nuevos cargos laborales.

Con la actividad de baiting las personas que no tienen experticia o malicia en el tema del robo de información pueden ingresar las memorias ya que pueden confundir con facilidad a las personas para que ingresen las unidades de almacenamiento externas y así robar información del usuario.

Para este tipo de escenarios de ingeniería social el único método para evitar estos ataques es socializar y concientizar a los usuarios de las compañías sobre ataques de ingeniería social y como a través de estos se puede filtrar información. Es necesario incluir cuáles son los mecanismos de protección y notificación ante la sospecha de estar siendo víctima de este tipo de ataques ya que puede realizarse de forma física o digital, se pueden utilizar diferentes técnicas para ejecutar estos ataques y se usan diferentes medios (correos electrónicos, páginas web, uso de medios de almacenamiento, redes sociales, llamadas, etc.), se enfocan en obtener información empresarial o personal.

El área de tecnología deberá comunicar a los funcionarios que cualquier acción sospechosa que se pueda enmarcar dentro de un ataque de ingeniería social el cual deberá comunicarse con dicha área de tecnología con el objetivo de hacer las validaciones correspondientes.

REFERENCIAS

[1] M. Mercè. (2002, Dic 26). “Ingeniería Social: Mentiras en la Red”. [En línea]. Disponible en http://ww2.grn.es/merce/2002/is.html

[2] C. Gutierrez. (2016, Ene 9). “5 cosas que debes saber sobre la Ingeniería Social”. [En línea]. Disponible en https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

[3] E. Castellanos. (2011, Jul 4). ”INGENIERÍA SOCIAL: CORROMPIENDO LA MENTE HUMANA”. [En línea]. Disponible en https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[4] Introducción a la Informática (2010). [En línea]. Disponible en https://datosuno.wordpress.com/unidad-1/introduccion/
[5] ¿Qué es Informática? (2009). [En línea]. Disponible en http://www.cavsi.com/preguntasrespuestas/que-es-informatica/
[6] El poder de la ingeniería social para realizar estafas en Internet (2017). [En línea]. Disponible en http://computerworldmexico.com.mx/poder-la-ingenieria-social-realizar-estafas-en-internet/
[7] Seguridad-Informatica-infografia-3 (2018). [En línea]. Disponible en http://acropoliscr.com/seguridad-informatica-infografia-3/
[8] ¿Qué es la seguridad informática y cómo puede ayudarme? (2019). [En línea]. Disponible en https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/
[9] Phishing (2005). [En línea]. Disponible en https://www.segu-info.com.ar/malware/phishing.htm
[10] M. Fernandez. (2019, May 6). "Ingeniería Social: ¿qué es el Baiting («cebar», o «poner carnada»)?". [En línea]. Disponible en https://blog.mailfence.com/es/que-es-baiting-ingenieria-social/
[11] DIFERENTES DELITOS INFORMÁTICOS (2014). [En línea]. Disponible en http://12357carlosaugusto.blogspot.com/2014/01/diferentes-delitos-informaticos.html
[12] ¿Qué es un Cracker? (2002). [En línea]. Disponible en https://tecnologia-informatica.com/que-es-un-cracker/

Autor

Mauricio Cortes. Ingeniero Electrónico de la Universidad Los Libertadores, año 2015, Ha sido analista en seguridad de la información realizando la atención de requerimientos e incidentes para diferentes proyectos, destacándose en el análisis de malware. También se ha desempeñado como especialista de seguridad de la información, siendo administrador de diferentes consolas de Antivirus. Estudiante de Especialización en Seguridad Informática en la Universidad Piloto de Colombia, año 2019.